Scholars' Mine

Doctoral Dissertations Student Theses and Dissertations

Spring 2020

System efficient ESD design concept for soft failures

Giorgi Maghlakelidze

Follow this and additional works at: https://scholarsmine.mst.edu/doctoral_dissertations

Part of the Computer Sciences Commons, and the Electromagnetics and Photonics Commons

Department: Electrical and Computer Engineering

Recommended Citation

Maghlakelidze, Giorgi, "System efficient ESD design concept for soft failures" (2020). *Doctoral Dissertations*. 3042.
https://scholarsmine.mst.edu/doctoral_dissertations/3042

This thesis is brought to you by Scholars' Mine, a service of the Missouri S&T Library and Learning Resources. This work is protected by U. S. Copyright Law. Unauthorized use including reproduction for redistribution requires the permission of the copyright holder. For more information, please contact scholarsmine@mst.edu.

SYSTEM EFFICIENT ESD DESIGN CONCEPT FOR SOFT FAILURES

by

GIORGI MAGHLAKELIDZE

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

2020

Approved by:

DongHyun Kim, Advisor
Harald Gossner
Daryl Beetner
Chulsoon Hwang
Victor Khilkevich

© 2020

Giorgi Maghlakelidze

All Rights Reserved

PUBLICATION DISSERTATION OPTION

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

Paper I, found on pages 3–30, IC Pin Modeling and Mitigation of ESD-induced Soft Failures, has been submitted to *IEEE Transactions on Electromagnetic Compatibility*.

Paper II, found on pages 31–54, Pin Specific ESD Soft Failure Characterization Using a Fully Automated Set-up, has been published in the proceedings of the *40th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD)*, September 2018.

Paper III, found on pages 55–70, Latch-up Detection During ESD Soft Failure Characterization Using an On-Die Power Sensor, has been published in *IEEE Letters on Electromagnetic Compatibility Practice and Applications*.

ABSTRACT

This research covers the topic of developing a systematic methodology of studying electrostatic discharge (ESD)-induced soft failures. ESD-induced soft failures (SF) are non-destructive disruptions of the functionality of an electronic system. The soft failure robustness of a USB3 Gen 1 interface is investigated, modeled, and improved. The injection is performed directly using transmission line pulser (TLP) with varying: pulse width, amplitude, polarity. Characterization provides data for failure thresholds and a SPICE circuit model that describes the transient voltage and current at the victim. Using the injected current, the likelihood of a SF is predicted. ESD protection by transient voltage suppressor (TVS) diodes is numerically simulated in several configurations. The results strongly suggest the viability of using well-established hard failure mitigation techniques for improving SF robustness, and the possibility of using numerical simulation for optimization purposes. A concept of soft failure system efficient ESD design (SF-SEED) is proposed and shown to be effective.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my Ph.D. degree advisor, Dr. DongHyun Kim, for guiding me through the degree program. My utmost gratitude to Dr. David Pommerenke for his continuous support, advice and guidance in my research work and the bulk of my degree. I would like to thank Dr. Harald Gossner for his guidance, insight, and patience in the last 3 years. These three individuals have been the source of inspiration, wisdom, learning, and formation of myself as a researcher and a professional. None of this would be possible without them.

I would like to thank the current and former faculty of EMC Laboratory: Dr. Daryl Beetner, Dr. Chulsoon Hwang, Dr. Victor Khilkevich, Dr. Jun Fan, and Dr. James Drewniak for giving me a chace to join this laboratoty and supporting me throughout the years. Many thanks to fellow students for long conversations and discussions late at night, for their friendship, encouragement, and trips to Donut King at 3AM. I consider it a privilege and a point of pride to have been a part of EMC Lab family and to have contributed to the community.

I am eternally grateful to my parents and brothers for their unwaivering support, for helping me receive the best education, and for cheering me up when the night was the darkest.

Lastly, thank you, Bonnie. You have been there for me every step of the way and I shall never forget it.

TABLE OF CONTENTS

SECTION

LIST OF ILLUSTRATIONS

PAPER I Page

PAPER II

PAPER III

LIST OF TABLES

PAPER I

PAPER II

PAPER III

1. INTRODUCTION

In paper I, a system-efficient ESD design methodology is developed for soft failures (SF) and applied to USB3 Gen 1 interface. The aim is to create a systematic approach of interface characterization, modeling and evaluating effectiveness of protection schemes. SF is studied extensively [1]-[10], but most of the studies are either purically empirical, or performed on extremely simplified devices (such as D flip-flop, etc.) in order to establish the root cause. Often, the root cause of a soft failure lies in noise and glitches on power rails as a result of direct or indirect ESD. In practice, the device under test (DUT) is very complex and it is either impractical or too expensive to study and model each interface at a high level of detail (i.e. individual registers and voltages) before being able to propose, test and release a design version robust to soft failures.

The process of system efficient ESD design (SEED) consists of two major parts. First, the desired interface is stressed with a transmission line pulser (TLP), its behavior observed and a measurement-based victim pin model is created. Then the pin model is combined with models of other parts that are relevant to ESD robustness: transmission lines, discrete components, interconnects, etc. Design changes are tested within the model in terms of stress at the victim pin, then compared to the damage thresholds. Common protection schemes include adding discrete components that are placed at different locations within the net under test. The damage thresholds of the victim are evaluated earlier experimentally or provided by device vendor. The process continues until the maximized robustness levels are achieved in simulation, then implemented in practice.

There are many discussions of SEED concept for soft failures [4] [6], but no implementation or validation could be presented. This work aims to demonstrate that such concept is viable and to validate it by testing and modeling a range of commonly used hard failure mitigation techniques.

Paper II shows the development of the systematic testing methodology of a complex DUT, which is the first step in the SEED process. Dependency of soft failure modes on pulse length and system state is established and 8 different failure modes are identified. An automated algorithm is developed and presented in detail.

Paper III shows a novel method for detecting of latch-ups in power domain by using on-die power sensors, without additional measuring instruments. Persistent power drain is one of the more pernicious threats to a mobile, battery-powered systems. This kind of failure is often not visually or audibly detectable, except in cases of obvious heating of the system. This means, it is likely to go undetected by the operator, until the battery is drained. The method of detection is shown to be effective and practical. One of the appeals is that these power sensors are often implemented as a part of CPU cooling and thermal control system, so little additional design effort is required.

First part of paper I is devoted to using results of papers II and III and proposing an empirical circuit model of the victim pin. The latter parts show the implementation of the SEED methodology as applied to the soft failure modes, correlation of the circuit model to the measurements, and comparison of commonly used ESD mitigation techniques. The results provide evidence for viability of the proposed methodology and for effectiveness of conventional ESD mitigation techniques against soft failures.

PAPER

I. IC PIN MODELING AND MITIGATION OF ESD-INDUCED SOFT FAILURES

Giorgi Maghlakelidze

Deparment of Eletrical and Computer Engineering, Missouri University of Science and Technology, Rolla, MO 65409

ABSTRACT

ESD-induced soft failures (SF) of a USB3 Gen1 device are investigated by direct TLP injection with varying pulse width, amplitude, and polarity. This allows to characterize the failure behavior of the interface and to create a SPICE model of the voltage and current waveform dependent failure thresholds. ESD protection by TVS diodes is numerically simulated in several configurations. The results show viability of using well-established hard failure mitigation techniques for improving SF robustness. A good agreement between numerical simulation for optimized board design and measurements are achieved. A novel concept of Soft Failure System Efficient ESD Design (SF-SEED) is proposed and demonstrated to be effective for making decisions for early product development, in board design and prototyping phase.

1. INTRODUCTION AND OVERVIEW

Electrostatic discharge-induced soft failures (SF) have been a subject of extensive investigations [1]-[10]. Many studies concentrate on empirically characterizing complex systems [1], some on studying simpler devices such as 16-bit microcontroller [2] units or simpler flip-flop structures and modeling them in detail with full-wave and circuit solvers [3] in order to understand the root cause of specific failures. Sophisticated characterization techniques are required in order to study each interface of a complex interface, such as USB3 SuperSpeed [4][6][7][8]. Often, the root cause of such a failure lies in noise and glitches on power rails as a result of direct or indirect ESD [3][4][5]. In most practical situations, however, the system is very complex and it is either impractical or too expensive to study and model each interface at a high level of detail (i.e. individual registers and voltages) before being able to propose, test and release a more robust solution.

System-efficient ESD Design (SEED) is a well-established concept in the industry [9][10]. It stands for the design optimization methodology that maximizes robustness of signal lines to ESD-induced hard failures (damage) by simulating the high current behavior of PCB components. Typically, a measurement-based victim pin model is created, then combined with other parts that affect ESD robustness: transmission lines, discrete components, interconnects, etc. Design changes are made in the model and evaluated in terms of stress at the victim pin, compared to the damage thresholds. Common protection schemes include adding discrete components (e.g. TVS diodes, CM chokes, etc.) that are placed at different locations within the interface under test. The damage thresholds of the victim are evaluated earlier experimentally or provided by device vendor. The process continues until the maximized robustness levels are achieved in simulation, then implemented in practice.

To date, there has been discussion of SEED concept for soft failures [4] [6], but no implementation or validation could be presented. This work aims to demonstrate that such concept is viable and to validate it by testing and modeling a range of commonly used hard failure mitigation techniques.

The methodology is applied to SuperSpeed lanes of a USB3 Gen 1 interface. A directional injection concept is developed for the high-speed interface and used to characterize the RX pins of the device under test. An automated test system is used to characterize the victim pin and classify the failure modes related to the interface. The characterization results are presented as soft failure likelihood as a function of injected stress levels, polarity, and rise time. This is an extension of a characterization methodology developed previously [7][8]. Eight failure modes across four severity levels are identified for the DUT. This information is then used to create a circuit model that outputs failure likelihood for the applied stress.

Section 2 of the paper contains DUT pin characterization setup, procedure, and the results. Section 3 describes pin modeling methodology and SF modeling methodology. Section 4 proposes a SEED-like simulation procedure for soft failures. Section 5 provides evidence for viability of the proposed procedure and discusses the results.

2. CHARACTERIZATION METHODOLOGY AND RESULTS

2.1. AUTOMATED SETUP DESCRIPTION

The goal of this setup is to characterize an I/O pin of an active device in terms of soft failure modes and thresholds under direct stress injection. This is achieved by running a series of automated stress tests, varying stress parameters and then statistically processing the resulting data.

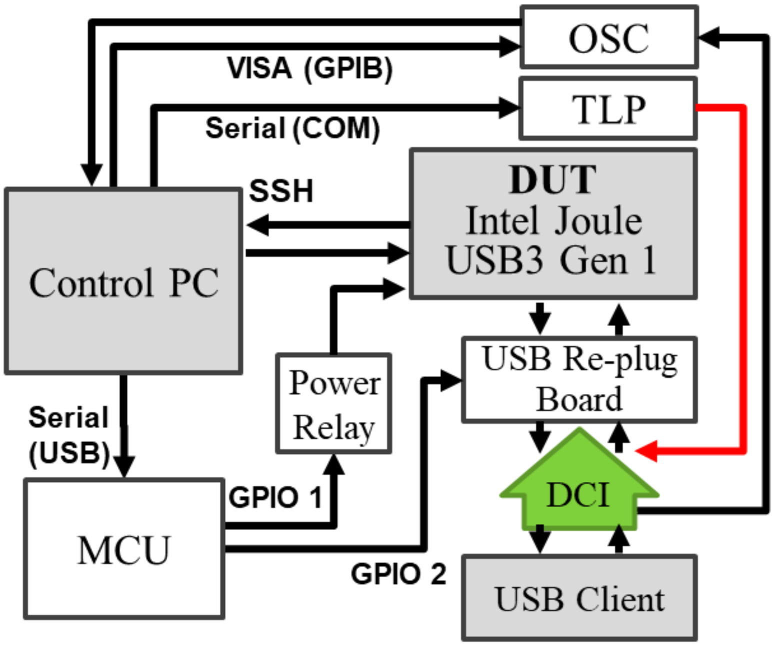

Figure 1. System diagram of the chracterization setup. The control PC interfaces with the TLP measurement system over GPIB and COM, controls a MCU via serial, and interfaces with DUT by SSH over LAN.

Most devices of the setup are controlled by a computer via several common interfaces (GPIB, COM, LAN, SSH). The system diagram is given in Figure 1. A standard TLP measurement system [16] is used to apply repeatable stress to the DUT pin and measure voltage and current transient waveforms.

A detailed description of the process algorithm and the system is given in [7]. For cohesion, a summary is provided below. The DUT is an Intel Joule system. It consists of two parts: a “compute module” (SoC, WiFi, eMMC) and an “expansion board” (interface fanout, PDN, ESD protection, filtering, etc.). The two boards plug in through a 100-pin HRS surface-mount SF40 interconnect.

The TLP pulses are injected into the active (i.e. “hot”) USB3 Gen1 interface SuperSpeed data lines of the DUT, without significant loading of the USB3 Gen 1 signal. This is achieved by using a low-capacitance TVS diode soldered at the point where TLP output connects to the data pin [11].

The injection point is located on the directional current injection (DCI) board. The structure allows to direct the bulk of the current into the host (DUT in this case), while protecting the other end – the client.

2.2. DIRECTIONAL CURRENT INJECTION BOARD

For purposes of soft failure characterization, it is important to achieve two things: 1) clarity of which side of the high-speed link fails, and 2) activity on the interface.

Normally, when a stress pulse is injected into a DUT, the current spreads in both directions from the entry point. Due to the complexity of a typical system, it is difficult to establish whether the host failed, or the client. Moreover, if the host is the DUT, different clients may introduce unwanted vendor-to-vendor variation. Thus, directional current injection structures are developed. The passive circuit [12] is effective and provides 60:1

directionality of the DUT current, but requires careful design and works for links with < 1 GHz bandwidth. For USB3 Gen 1 and higher or HDMI links or any other simplex high-speed data protocols, a new concept is proposed.

The concept as applied to USB3 Gen 1 Type A is illustrated in Figure 2. An isolation structure placed in series with the signal path. The directionality is facilitated by a flat-gain amplifier MMIC. Before and after the amplifier, resistive attenuators are placed. The system is designed so that total gain is ~0 dB in the relevant frequency range for the target technology. In case the channel loss is not sufficiently flat for high-speed links, an equalizer can be added to the structure. This complicates the design, but may be necessary for data rates above 5 GBPS.

In terms of the signal propagating along the differential pair, the structure is almost transparent. The stress injected at the output side of the isolation structure is split: most of the current propagates towards the victim pin, while a small part is absorbed by the attenuator and the amplifier output terminal.

Figure 3 contains the measurements performed on the test structure with a 100 ns TLP, in order to establish the effectiveness of the proposed concept. The results show that DUT is subjected to 90% of the total current from the TLP. 10% is absorbed by the isolation structure, while only several mA are seen at the protected (ADUT) side.

Typically, the soft failure tests are only performed up to a few amperes to avoid hard fails. The amplifier must be selected appropriately and stress pulse bounds should be well-controlled to avoid damage.

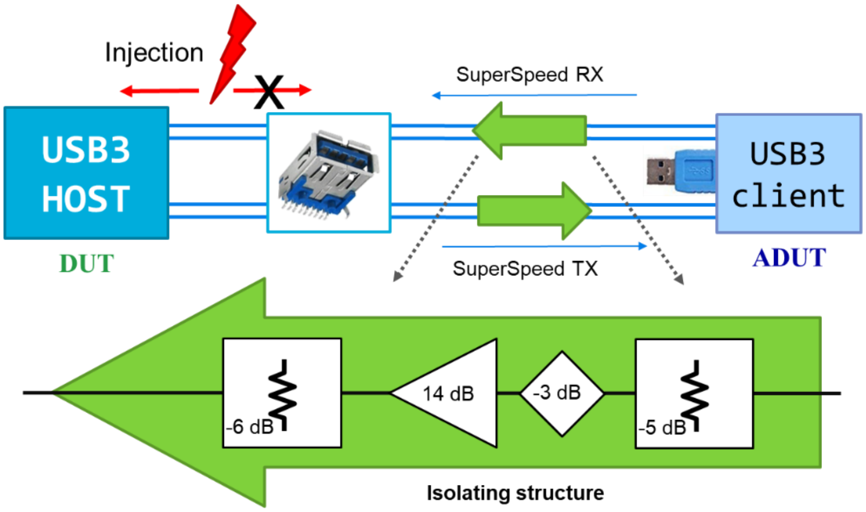

Figure 2. Isolation concept for directional current injection (DCI). The reverse direction of the structure absorbs the stress and prevents it from propagating towards the USB3 client.

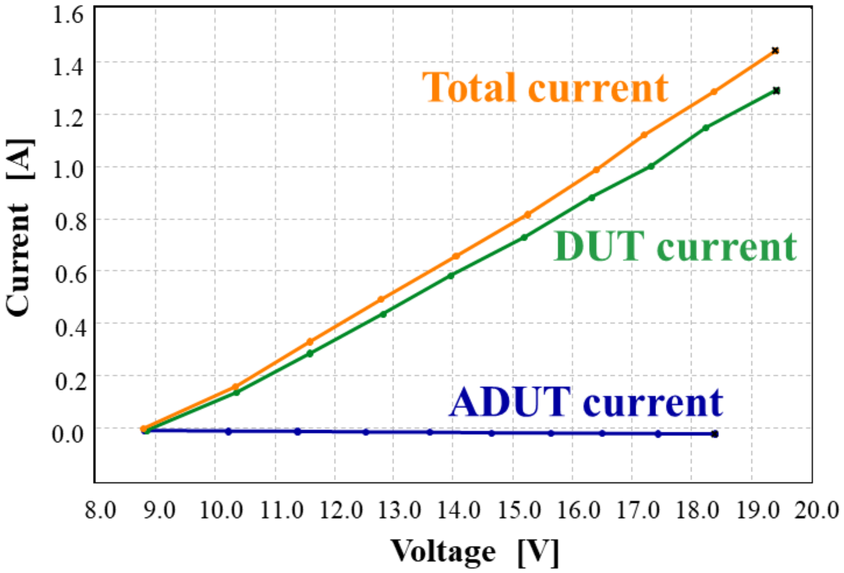

Figure 3. Current directionality when injecting at the DCI board. 90% of the current propagates towards the DUT. The protected side is isolated by the reverse direction of the amplifier, so milliamps of currents are detected at the ADUT side of the link path.

2.3. CHARACTERIZATION PROCESS AND OUTCOME

Typical characterization process starts by powering the system, calibrating TLP test system and establishing an active link. Then, a characterization loop proceeds to sweep injected stress levels and polarity. For each injection, the following major steps are taken:

1. Reset the DUT to nominal state;
2. Inject stress into the target pin;
3. Measure transient current and voltage waveforms;
4. Diagnose the SF mode based on the kernel logs;
5. Log the data and proceed to the next stress level;

More intricate details of the process are described in [7], [8].

After pulse length and polarity sweep concludes, the data is processed and grouped. The soft failures are grouped and categorized by two traits: visibility and whether any action is needed in order to resolve the error.

Table 1 contains the summary and examples of soft failures and categories observed in the process of USB3 host characterization.

The failure probability depending on the injection level is illustrated in Figure 4 for an USB3 SuperSpeed RX positive pin. The characterization results show that both for positive and negative stress injections, there is a sharp threshold after which failure rate is total of 100%, as shown by the dashed green curve. The victim is more prone to failure for negative polarity stress, as compared to positive. Failure modes for positive are split between three main ones: 1) USB3 client re-enumerates within the host operating system and continues functioning, failure cat. B; 2) USB3 client disappears from the host operating system, the failure is fixed by re-plugging the client, cat. C; and 3) latch-up at one of the power domains that presents as persistent power drain, requires total power cycle to fix, failure cat. D. The latch-up is detected by using an on-die power monitor [8].

Negative polarity pulses cause similar soft failures, but with higher severity. These include: 1) USB3 re-enumerations; 2) USB3 client disappears from the host, but requires a system software reboot to fix (bringing power down not required); 3) USB interface falls back to USB2 mode, requires software reboot; 4) USB3 client disappears from the host and requires at least a full power cycle in order to fix the soft failure. The latter failure mode is one of the more severe ones, as it requires bringing the power of the whole system down. In embedded systems that means taking out the battery, or flipping a hardware switch which is often either inconvenient or inaccessible in consumer electronics.

After device characterization and establishing SF modes and thresholds, this data is used to create a circuit model and optimize the design to improve device robustness to soft failure. The robustness improvement is quantified as increase in threshold values.

Table 1. Soft failure categories.

Cat.	**Visible**	**Action**	**Example for USB**
A	✗	✗	Bit errors; packets getting resent
B	✓	✗	Drop in data throughput; re-enumerated by the host
C	✓	✓	Stop of data transfer; re-plugging of the cable or power cycling required
D	✗	✓	Device re-enumerates, but latch-up is unnoticed and power cycling is required

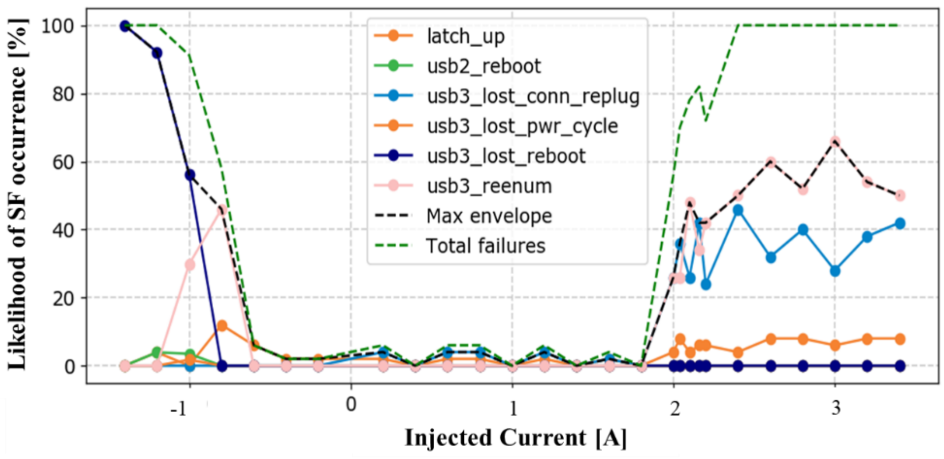

Figure 4. SF characterization results for SSRX_P pinfor 100 ns. The interface is more susceptible to negative stress, as indicated by the low 100% failure threshold, as compared to the positive half of the plot.

3. MODELING METHODOLOGY

3.1. VICTIM PIN QUASI-STATIC IV MODEL

The model of the victim pin is a standard 3-parameter diode to VDD and a diode to VSS that is based on measured quasi-static IV curve. The measurement consists of sweeping magnitude of 100 ns TLP pulse with trise=0.6 ns, then averaging 70-90% window of transient voltage and current waveforms. This model describes pin behavior for long stress pulses. Figure 5 shows good agreement between the model and the measurement above 0.3 A of the injected current. This is acceptable, because no failures occur at low levels of stress. When testing the DUT pin in order to create a diode model for soft failure analysis, one should limit the injection range to well below the levels of current and voltage that cause permanent damage (hard failure). A reasonably safe upper bound would be 70% of the hard fail threshold. Anything higher can either introduce damage immediately, or cause latent damage of the DUT due to the stress repetition for hundreds of times.

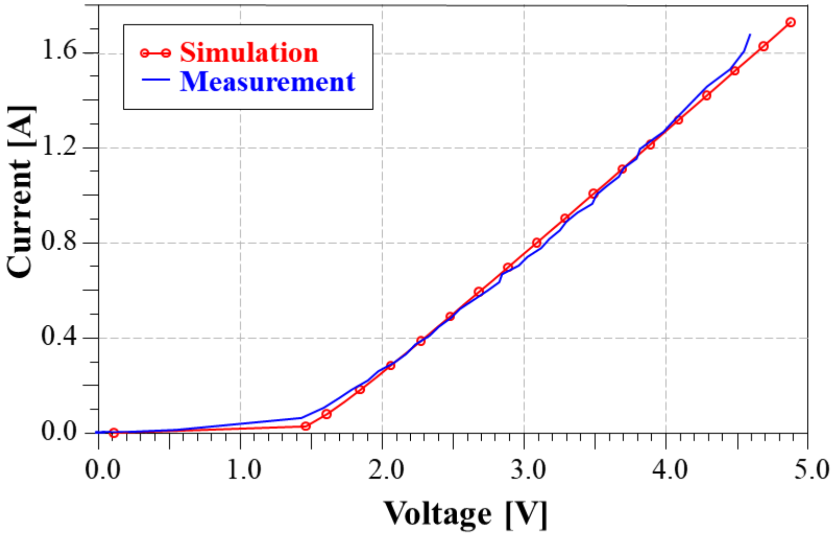

Figure 5. Model of the victim pin SSRX_P compared to the measured quasi-static IV curve. The characteristic remains the same whether the DUT is powered or not.

3.2. PIN SOFT FAILURE MODEL

The SF characterization determines the stress current threshold of different soft failures. To use this information in a SEED simulation two paths are possible. The SEED simulation can calculate and output the victim current, then in a post processing step it can be determined whether a soft failure occurs. A circuit-based alternative allows to obtain instant results, thereby removing the requirement of additional data post processing. For instant results during the SEED simulation, a circuit is designed that describes the victim’s reaction to the injected current.

The concept of soft failure model lies in essentially measuring the average current Iavg injected into the victim, then comparing it against the thresholds obtained in the process of pin characterization. Average current is obtained as follows:

$$I_{avg} = \frac{Q_{total}}{T_{TLP}} = \frac{1}{T_{TLP}} \int_{t0}^{t1} i_{victim}(t)dt \tag{1}$$

Figure 6 describes the SF pin symbol and the circuit that combines the I-V diode model and the SF model for the USB3 re-enumeration soft failure mode.

Part 1) of the SF detector has the Current Controlled Current Source as an ideal current probe. The two ideal diodes determine the stress current path for different stress polarities.

Part 2) of the circuit is a charge detector that measures total charge Qtotal injected into the victim pin.

Part 3) contains the circuit that detects whether the Iavg current threshold (specified by the pin symbol parameter) has been exceeded and the value probability of the SF. The DC voltage source outputs signal proportional to the failure likelihood as observed during the characterization process. The voltage-controlled switch isolates the output pin from the DC source.

The potential at the terminal of the charge detector's capacitor is used as control voltage Vctrl of the switch. Figure 7 illustrates how the potential tracks the integral of injected stress current. As the Vctrl reaches the threshold value, the switch shorts, thus bringing the output pin potential to the value of SF likelihood. The detector circuit and the SF output circuits are duplicated for each soft failure mode. All SF output pin fail levels are summed to provide the total probability that any failure would occur. P_{total} is output as voltage at a pin of the symbol.

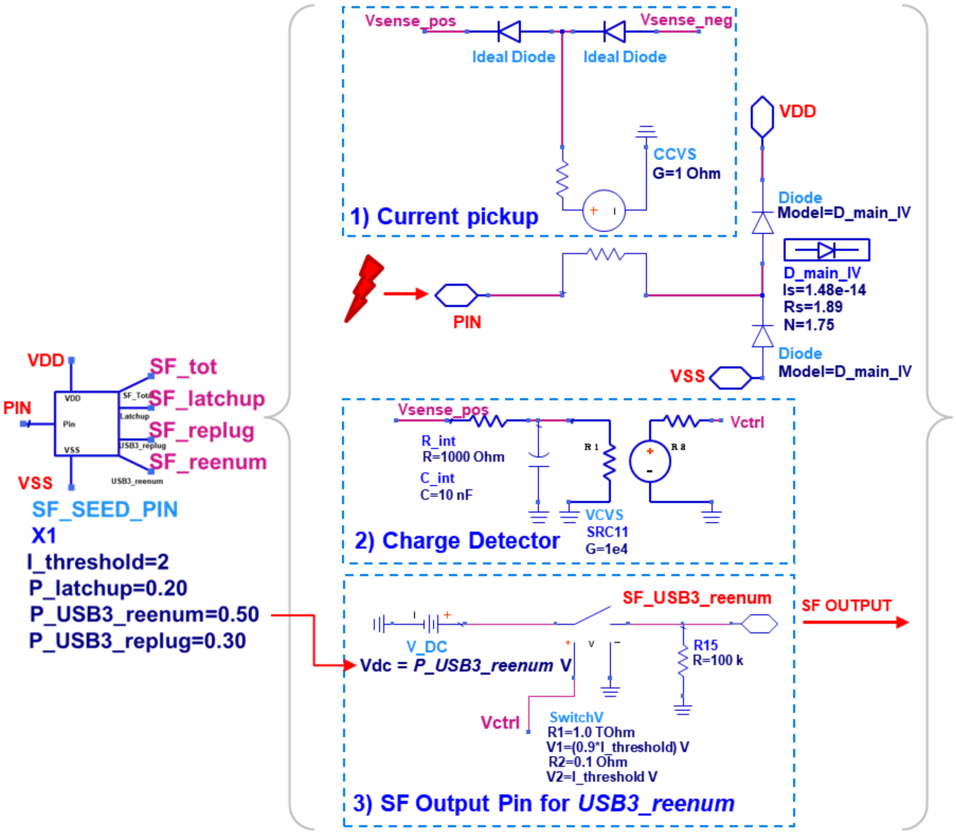

Figure 6. Circuit model of the SF detector and output.

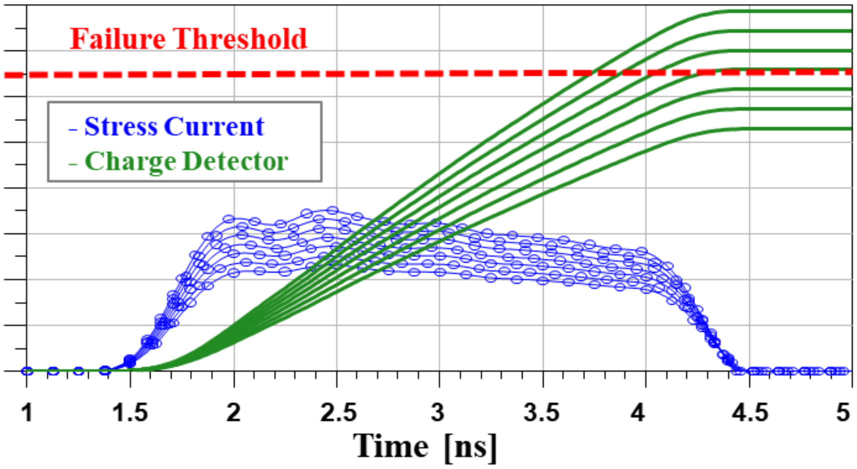

Figure 7. Charge detector of the SF Pin model output. The current is integrated and then the obtained charge is compared to the threshold value established during the measurement phase.

This SF model provides the failure probability directly during the simulation run and a post-processing is not required. This accelerated the process of design optimization as described in Section 4.

4. SOFT FAILURE SEED CONCEPT AND IMPLEMENTATION

System-Efficient ESD Design has been discussed [4] [6], but it has not yet been applied to soft failures. The methodology consists in essence of the following steps:

1. Pin characterization with TLP
2. Pin-specific modeling
3. Simulation of stress waveforms

First, the target interface is experimentally characterized on reference hardware, then a corresponding measurement-based physical and SF-pin models are developed. The viability of SEED methodology is explored in relation to soft failures of USB3 Gen 1 SSRX_P pin. Several mitigation schemes are tested experimentally to evaluate their effectiveness.

Figure 8 provides schematic overview of the interface model. TLP is modeled as pulse voltage source. The interconnect discontinuity and PCB traces are modeled based on TDR measurements. The victim pin is represented as a diode, as described in Section 3. Several external mitigation techniques are applied to the pin and the SF robustness is evaluated in terms of the SF threshold shift.

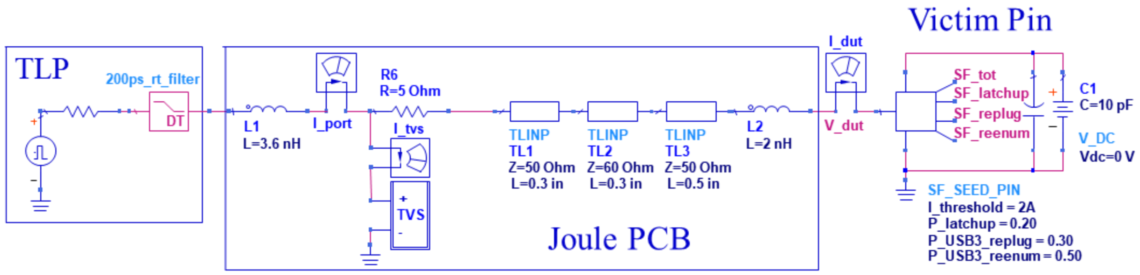

Figure 8. System model for the SSRX_P pin including several elements of the PCB, the USB connector and protection devices.

5. MITIGATION TECHNIQUES: RESISTORS AND TVS DIODES

Several external mitigation techniques are tested in this work, experimentally and within numerical models:

- An external current-limiting series resistor
- A current-diverting TVS diode to signal reference
- A combination of a series resistor and a TVS diode

Several values of series resistors are tested and compared, but standalone resistors are never used as a mitigation technique. Often, they are combined with a TVS diode placed between the protection diode and the victim. In terms of the stress, this means that there is a higher higher impedance towards the victim and the current is diverted to the TVS diode instead. In terms of voltage, it helps to raise the node potential at the diode terminal, which turns on the diode at lower current stress levels.

As a part of this investigation, several TVS diodes were first evaluated in terms of their quasi-static I-V characteristics. In the next step dynamic models were built to describe the turn on behavior. For this, a previously established modeling framework was used [13] [15]. The main idea is to divert the stress current away from the victim. The diode static characteristics are compared to the victim pin in Figure 9. Here, several I-V curves are compared against each other in terms of turn on voltage and dynamic resistance. The external diode that turns on at lower voltage than the victim's on-chip protection diodes (red curve) will provide stronger protection. In current situation, TVS1 turns on faster than the victim's on-chip protection and has much lower dynamic resistance. This is expected to improve the robustness of the pin. TVS2 turns on at a much higher voltage and therefore is not a viable protection option if used standalone. Two additional configurations are explored with TVS2 diode, where series resistors of R=5 Ω and R=10 Ω are placed between the victim and the diode. Experimental results and a qualitative model are presented in the following section.

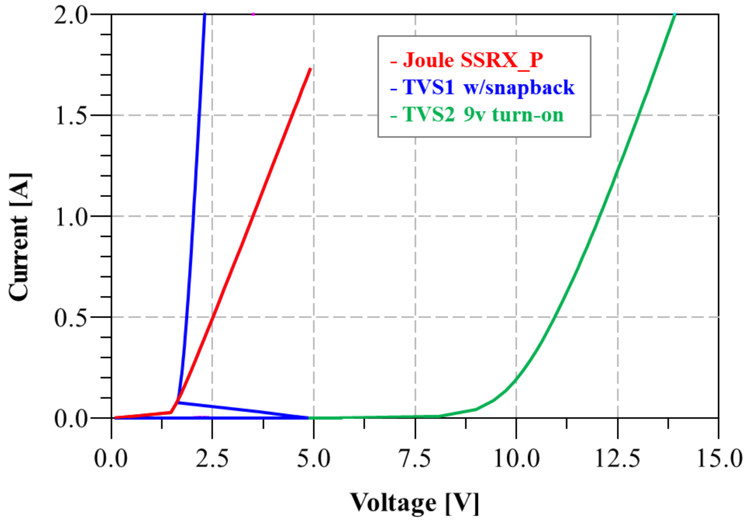

Figure 9. TVS diode IV curve compared to the victim pin SSRX_P.

6. RESULTS AND DISCUSSION

6.1. EXPERIMENTAL RESULTS

For each of the evaluated mitigation techniques, the DUT “expansion board” is modified, then tested for soft failure likelihood. The shift in the threshold is the criterium that quantifies an improvement of the interface pin robustness. “No protection” case is taken as a reference. All other configurations are tested with 100 ns and 2 ns TLP. The former is commonly used to represent a whole IEC discharge pulse directly into the pin. The short 1-2 ns pulses represent the stress coupled indirectly.

Figure 10 shows 100 ns TLP results and the improvement of SF robustness of USB3 interface SSRX_P pin. For the long pulses, adding a series resistor shows about +20 V improvement in SF threshold. Placing one TVS2 diode has no significant effect, while TVS1 diode improves the robustness by about +50 V. In order to achieve more effective results, TVS2 is combined with a series resistor (cases “TVS2 + 5 **Ω**” and “TVS2 + 10 **Ω**”). Both these cases show at least 150 V shift in SF threshold of Ptotal. There is a background rate of ~20% SF rate at lower stress levels. This can be explained if the DUT has multiple failure modes that manifest the same way, but have different root causes. Thus, only a part of the SF (~80%) have reduced, while ~20% have not been mitigated by the protection scheme.

Figure 11 is for 2 ns TLP and shows results for the protection schemes. Placing a series 5 **Ω** resistor gives only a marginal difference of +10-20 V. Placing one TVS2 diode improves the result for 2 ns pulses by +200 V. TVS2 + 5 **Ω** scheme also improves the robustness, but the levels are tested only till +160 V, to avoid interface damage. The best improvement is observed for TVS1 device, it snaps back at much lower voltage (Vt1 = 5 V) and has low dynamic resistance. No soft failures were observed for this case until 430 V stress pulse (~ 4 A). Higher cases were not tested to avoid damage to the interface.

It is shown that soft failures can be mitigated to some degree with the same devices typically used in hard failure prevention. The next step lies in creating a numerical circuit model that would allow design optimization procedure similar to well-established hard failure SEED.

Table 2. Summary of 100% soft failure thresholds in model vs measurement in terms of TLP charge voltage.

	100 ns TLP Threshold		**2 ns TLP Threshold**	
Configuration	**Model**	**Meas.**	**Model**	**Meas.**
No Protection	*90 V*	*90 V*	*230 V*	*230 V*
5Ω in series	+10 V	+20 V	+20 V	+10 V
TVS1 snapback	+320 V	+50 V	+420 V	>+160 V*
TVS2 9v turn-on	+0 V	+0 V	+160 V	>+160 V*
TVS2 + 5 Ω	+130 V	>+150 V*	+170 V	>+160 V*
TVS2 + 10 Ω	+500 V	>+150 V*	+800 V	>+160 V*

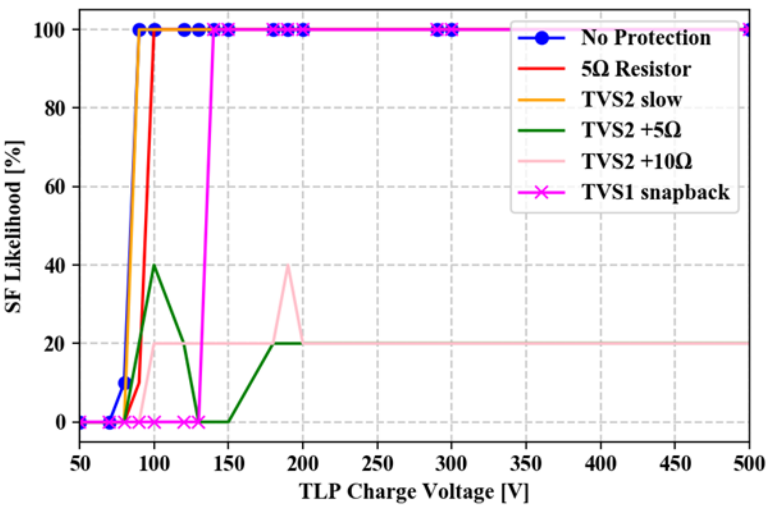

Figure 10. Measured overall SF threshold shift due to external protection placement, results for positive 100 ns TLP.

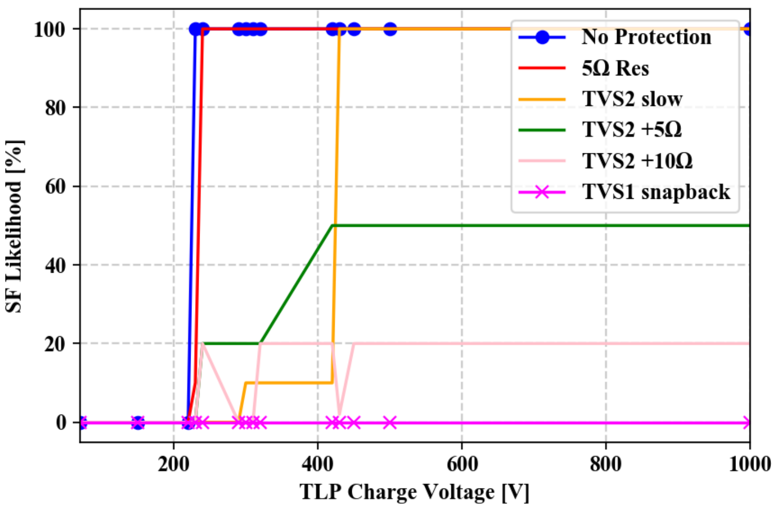

Figure 11. Measured overall SF threshold shift due to external protection placement, results for positive 2 ns TLP.

6.2. QUANTITATIVE CIRCUIT MODEL RESULTS

Simulations are performed for protection schemes tested in the experiment. The model includes the victim diode, SF pin model and the PCB. The outcomes are compared in Table 2, which shows that the proposed model generally predicts the change in SF threshold in cases of a standalone resistor or TVS2 diode for 100 ns pulses. In case of TVS1 snapback diode, the model overestimates the improvement, while for cases of TVS2 + 5 Ω and TVS2 + 10 Ω the observed threshold improvement was at least +150 V, but the tests were not pushed higher, for the risk of DUT damage. For 2 ns pulses the model also either predicts the change, or shows qualitative improvement.

The model provides results for two pulse lengths: 100 ns and 2 ns. The values of I_{avg} (100 ns) and I_{avg} (2 ns) were measured during the characterization and are used as the threshold value in the simulation. The model outputs change in threshold of overall failure likelihood P_{total}.

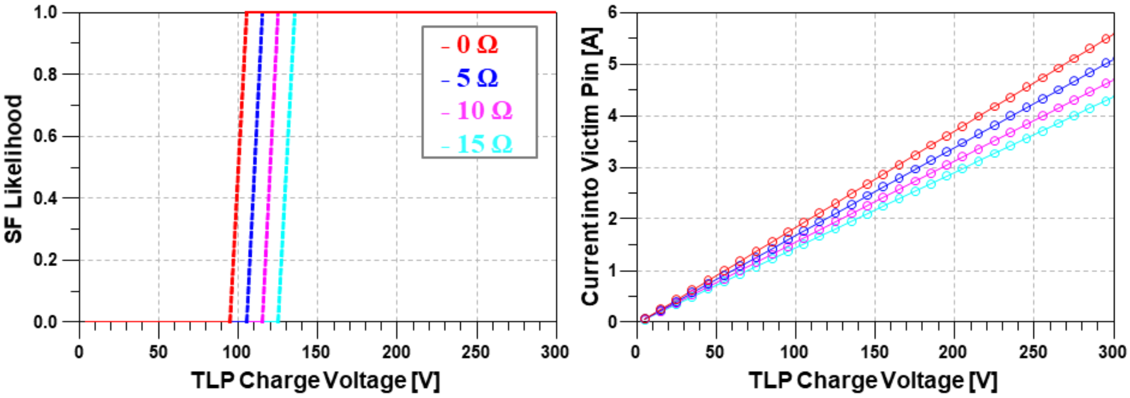

Figure 12. Left: shift in SF threshold as the series resistor limits current into the victim pin. Resistor value swept 0-15 Ω, simulation result. Right: current entering the victim pin, reduced as the resistance increases.

Adding a series resistor in order to limit the current flowing into the victim pin yields marginal improvements. Figure 12 shows the voltage output of P_total output terminal of the SF pin model (left) and the current flowing into the pin vs TLP charge voltage (right). This result closely correlates to the observations: SF threshold shift is proportional to the resistor value.

The case with TVS diodes varies from device to device and requires careful consideration of diode characteristics. The main purpose of the TVS devices is to clamp voltage on the pin and divert current. The outcome depends on both the diode choice and the victim characteristics.

In the case of TVS1, a diode with low trigger voltage Vt1, +320 V improvement is predicted by the model, as illustrated in Figure 13. The left side shows the shift in the SF threshold, the right side – current split between the victim DUT and the TVS diode. At ~50 V, it is observed that the snapback occurs and TVS1 goes into low-impedance mode, thus diverting vast majority of current away from the victim. This qualitatively matches the measurement, but overestimates the observed +50V shift in the measurement. This can be explained, in part, if some failure modes are caused by the peak stress current, instead of the average current.

TVS2 has higher turn-on voltage Vbr = 9 V, while the victim turns on @ Vbr = 1.5 V. This means that the diode will not have much effect on the current until much higher stress levels. Figure 14 (right) shows comparison between total current injected by TLP and victim pin current. The effect of the TVS2 diode, as expected, is small. Thus, the SF threshold is not affected by this device, as shown in Figure 14 (left) and confirmed by the measurement.

However, a possible way to improve the performance of a diode such as TVS2 is to combine it with 5Ω resistor series with the signal path. When combined – the victim and the resistor impedances combine into higher impedance path than TVS2. In this case, the diode turns on at lower stress levels and efficiently diverts the current away from the victim, improving robustness by at least +130 V.

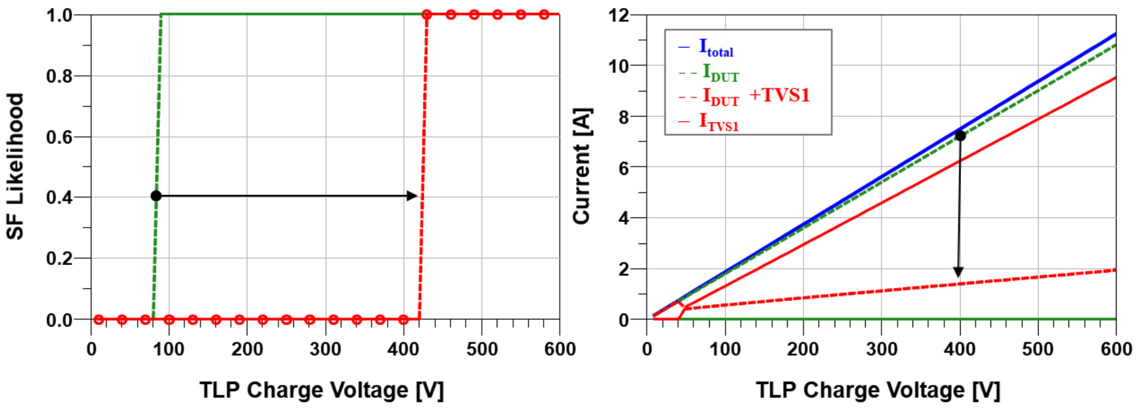

Figure 13. Simulation result using TVS1 as external protection. Left: the shift of SF threshold vs TLP voltage. Right: currents vs TLP voltage. The snapback is evident by the knee and sharp drop in the victim current.

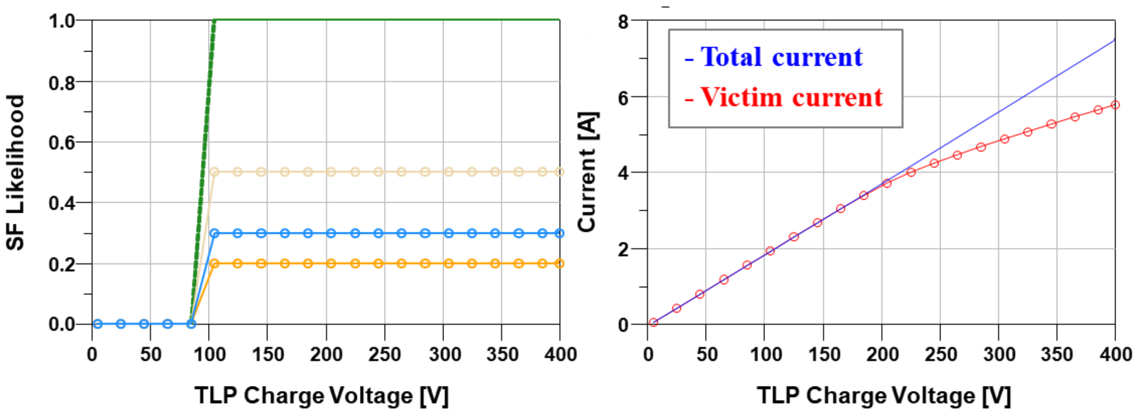

Figure 14. Simulation result using TVS2 as external protection. Left: no shift of SF threshold vs TLP voltage. Right: currents vs TLP voltage. This TVS diode turns on at higher voltage, thus no current is diverted away from the victim until much higher TLP levels.

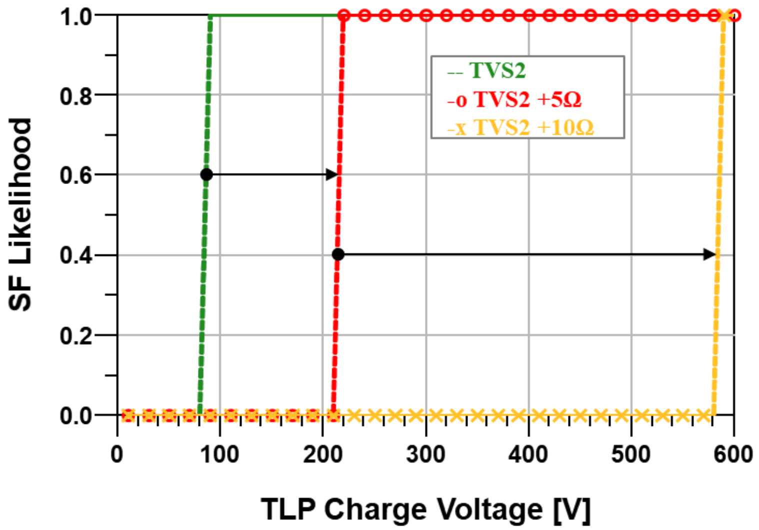

Figure 15. Simulation result using TVS2 and a resistor as external protection shows shifts of SF threshold vs TLP voltage.

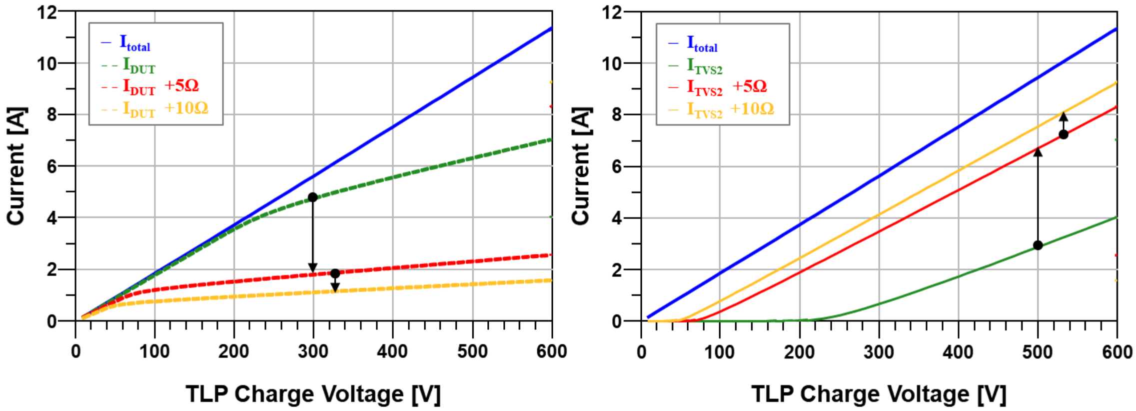

Figure 16. Simulation result using TVS2 and a resistor as external protection shows currents vs TLP voltage. With added resistance, the victim's impedance rises, thus, TVS2 turns on at lower TLP voltage and diverts current more effectively. Left: shows DUT current reduction because of adding the resistor; right: shows TVS current increase. The total injected current is given as a reference.

The shift in threshold is shown Figure 15 for R = 5 Ω and R =10 Ω values. The configuration of R = 10 Ω predicts +500 V improvement, however the result is confirmed only until +150V, to avoid damage to the DUT interface. The resulting DUT current reduction and TVS current increase are shown in the Figure 16. The impedance combination effect is illustrated in Figure 17. The intersections of the TVS2 diode with the other curves is where the diode becomes the dominant sink for the stress current.

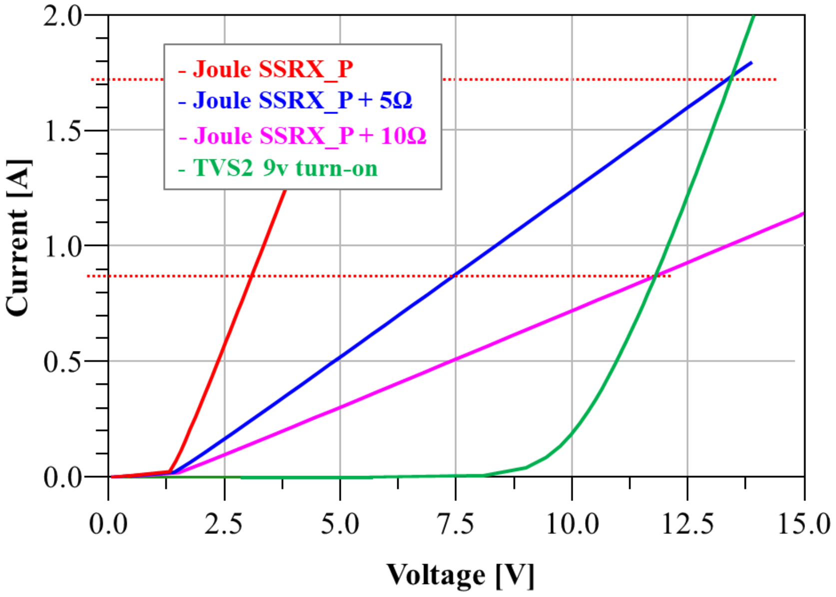

Figure 17. IV characteristic of combined victim and a series resistor. The intersection points with TVS2 chracteristic is where the diode becomes dominant and diverts the current away from the victim.

7. OUTLOOK

Based on this example that a soft fail SEED concept can be applied in a meaningful way to pre hardware design optimization, multiple directions of methodology enhancement are considered:

- A full system-level simulation can be performed for an IEC test to the system to extract the actual energy coupling into the victim pin indirectly.

- As the power delivery network can have a strong influence on certain soft failure types [3], the methodology can be expanded to account for the PDN.

- The method isn't limited to diodes and resistors. Common mode chokes (CMC) are also known to improve ESD robustness against hard fails, especially when used together with a TVS device [17]-[20]. SF SEED can help to investigate whether CMC can be used to improve SF robustness as well.

8. CONLCUSIONS

For the first time, it has been demonstrated that conventional ESD hard failure protection techniques can also be used to improve the system level ESD soft failure robustness for direct pin injection This is achieved by diverting most of the ESD-induced current away from the victim pin. This does not avoid bit-errors, but it prevents current injection into VSS, VDD or the substrate of the victim IC which can lead to errors that cannot be corrected by the protocol of the I/O. A well selected TVS clamps the voltage at the IC close to the signal levels, such that only a small amount of current will be forced by the ESD into the IC.

The reduction of the SF likelihood is investigated in a SEED-like simulation. This requires SEED models that include the soft failure behavior. 2 ns and 100 ns TLP are used to represent direct and indirect pulse injection.

The simulation of a large signal circuit model of the victim pin, comprising a virtual detector circuit and the SF threshold dependency, show a good match to the physical system. The proposed version of the system model is circuit-based; however, the same methodology can be applied in co-simulation with 3D full-wave solvers.

REFERENCES

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

[2] S. Yang et al, "Measurement techniques to predict the soft failure susceptibility of an IC without the aid of a complete software stack," IEEE EMCS 2016, pp.41-45

[3] M. Park et al., "Measurement and Analysis of Statistical IC Operation Errors in a Memory Module Due to System-Level ESD Noise," in IEEE Transactions on Electromagnetic Compatibility, vol. 61, no. 1, pp. 29-39, Feb. 2019.

[4] S. Koch, B. J. Orr, H. Gossner, H. A. Gieser and L. Maurer, "Identification of Soft Failure Mechanisms Triggered by ESD Stress on a Powered USB 3.0 Interface," in IEEE Transactions on Electromagnetic Compatibility, vol. 61, no. 1, pp. 20-28, Feb. 2019.

[5] Y. Xiu, N. Thomson and E. Rosenbaum, "Measurement and Simulation of On-Chip Supply Noise Induced by System-Level ESD," in IEEE Transactions on Device and Materials Reliability, vol. 19, no. 1, pp. 211-220, March 2019.

[6] B. J. Orr, S. Koch, H. Gossner and D. J. Pommerenke, "A Systematic Method to Characterize the Soft-Failure Susceptibility of the I/Os on an Integrated Circuit Due to Electrostatic Discharge," in IEEE Transactions on Electromagnetic Compatibility, Sep. 2019.

[7] G. Maghlakelidze, P. Wei, W. Huang, H. Gossner and D. Pommerenke, "Pin Specific ESD Soft Failure Characterization Using a Fully Automated Set-up," 2018 40th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Reno, NV, 2018, pp. 1-9.

[8] G. Maghlakelidze, H. Gossner and D. Pommerenke, "Latch-up Detection During ESD Soft Failure Characterization Using an On-Die Power Sensor", Electromagnetic Compatibility Practice and Applications, IEEE Letters on, 2019

[9] Industry Council on ESD Targets, White Paper 3: System Level ESD, Part II: “Implementation of Effective ESD Robust Designs”, September 2012

[10] Duvvury, C. and Gossner, H., “System level ESD co-design”, 1st ed. Wiley - IEEE, 2016

[11] T. Schwingshackl et al., "Powered system-level conductive TLP probing method for ESD/EMI hard fail and soft fail threshold evaluation," 2013 35th EOS/ESD Symposium, 2013, pp. 1-8.

[12] B. Orr, D. Johnsson, K. Domanski, H. Gossner and D. Pommerenke, "A passive coupling circuit for injecting TLP-like stress pulses into only one end of a driver/receiver system," 2015 37th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Reno, NV, 2015, pp. 1-8

[13] P. Wei, G. Maghlakelidze, A. Patnaik, H. Gossner and D. Pommerenke, "TVS Transient Behavior Characterization and SPICEBased Behavior Model," 2018 40th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Reno, NV, 2018, pp. 1-10.

[14] P. Wei, G. Maghlakelidze, J. Zhou, H. Gossner and D. Pommerenke, "An Application of System Level Efficient ESD Design for HighSpeed USB3.x Interface," 2018 40th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Reno, NV, 2018, pp. 1-10.

[15] L. Shen, S. Marathe, J. Meiguni, G. Luo, J. Zhou and D. Pommerenke, "TVS Devices Transient Behavior Modeling Framework and Application to SEED," 2019 41st Annual EOS/ESD Symposium (EOS/ESD), Riverside, CA, USA, 2019, pp. 1-10.

[16] TLP-1000 Series Transmission Line Pulse Generator. [Online]. Available: https://www.esdemc.com/products/system-level-esd-test/tlp-1000-series-transmission-line-pulse-generator/

[17] S. Bertonnaud, C. Duvvury and A. Jahanzeb, "IEC system level ESD challenges and effective protection strategy for USB2 interface," Electrical Overstress / Electrostatic Discharge Symposium Proceedings 2012, Tucson, AZ, 2012, pp.1-8.

[18] J. Werner, J. Schutt and G. Notermans, "Common mode filter for USB 3 interfaces," 2016 IEEE International Symposium on Electromagnetic Compatibility (EMC), Ottawa, ON, 2016, pp. 100-104.

[19] G. Notermans, H. Ritter, B. Laue and S. Seider, "Gun tests of a USB3 host controller board," 2016 38th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Garden Grove, CA, 2016, pp. 1-9.

[20] M. Ammer, S. Miropolskiy, A. Rupp, F. z. Nieden, M. Sauter and L. Maurer, "Characterizing and Modelling Common Mode Inductors at high Current Levels for System ESD Simulations," 2019 41st Annual EOS/ESD Symposium (EOS/ESD), Riverside, CA, USA, 2019, pp. 1-7.

[21] S. Marathe et al., "On secondary ESD event monitoring and full-wave modeling methodology," 2017 39th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Tucson, AZ, 2017, pp. 1-6.

[22] S. Marathe et al., "Software-Assisted Detection Methods for Secondary ESD Discharge During IEC 61000-4-2 Testing," in IEEE Transactions on Electromagnetic Compatibility, vol. 60, no. 4, pp. 1129-1136, Aug. 2018.

II. PIN SPECIFIC ESD SOFT FAILURE CHARACTERIZATION USING A FULLY AUTOMATED SET-UP

Giorgi Maghlakelidze

Deparment of Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla, MO 65409

ABSTRACT

A fully automated system is developed for the systematic characterization of soft failure robustness for a DUT. The methodology is founded on software-based detection methods and applied to a USB3 interface. The approach is extendable to other interfaces and measurement-based failure detection methods.

1. INTRODUCTION

In order to mitigate ESD-induced soft failures (SF) of a system, its robustness must first be evaluated. In light of the various parameters that influence the response of the system, it is best to use an automated characterization process. The outcome helps system-level and IC designers, and firmware developers.

The world of soft failures is diverse and has been studied in [1]-[8]. In this work, the device under test (DUT) is an Intel Joule 570x Internet of Things (IoT) platform. The USB3.0 interface was selected for characterization. USB3 related SFs were studied in [7]. Several disturbance methods were evaluated: system-level IEC, magnetic loop probe, conductive TLP injection, and directional injection. Soft failures were correlated to the stress parameters: the pulse rise time didn't seem to affect the failure threshold, while pulse width was found to be inverse proportional to it. The authors found no correlation between CPU stress and failure modes, but no other DUT load was explored. Furthermore, the root-cause analysis of more severe modes were performed and a strategy for SF-SEED was proposed. This work confirms some of the earlier findings and extends others. The main idea is to develop a software-based method for an automated and systematic pin-specific characterization, and to explore methods for such data processing that can extract useful information.

The automated system is able to provide quantitative information on the dependence of different failure thresholds on the injected pulse level, polarity, rise time, system load and state, pin-to-pin variation, etc. Eight failure types across four severity levels were identified for the given system and failure dependence on various system loads was established.

2. CHARACTERIZATION PROCESS

The TLP injection system by ESDEMC [9] was used to deliver repeatable pulses to the DUT. The TLP system combined with an oscilloscope allowed the injected currents and consequential voltages to be measured. The TLP was controlled through GPIB and COM interfaces to the "Control PC", as shown in Figure 1.

Additional in-house software on the "Control PC" handled:

- The detection and recognition of failure modes,
- Sweeping of injected stress levels and polarities,

- Controlling the DUT over secure shell (SSH) protocol through the network (either through cable - LAN, or WiFi - WLAN), and
- Controlling other peripheral hardware (MCU).

A microcontroller unit (MCU), controlled over a serial interface, was used to switch two power relays: one for power cycling the DUT, another for tripping the power of the USB3 client device plugged into the host DUT port (interface under test).

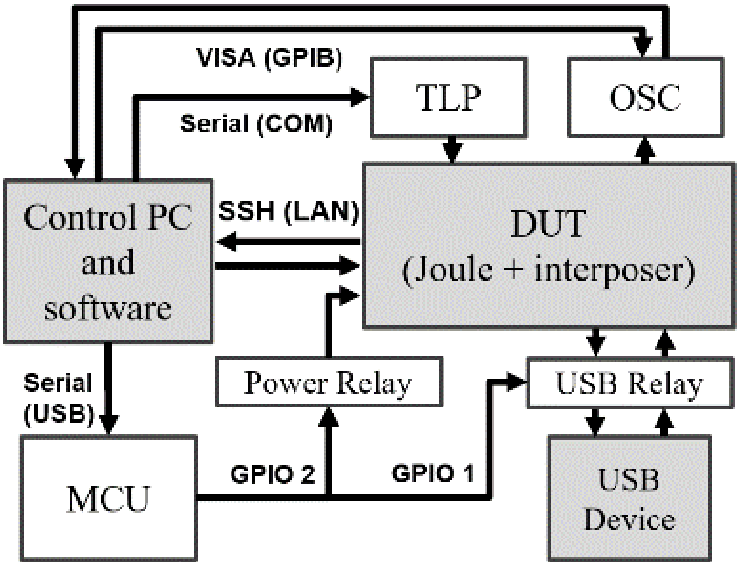

Figure 1. Overall system diagram.

2.1. SET-UP DESCRIPTION

2.1.1. Measurement Set-up. The Intel Joule system consists of two separate parts – an expansion board and a compute module, as shown in Figure 2. The compute module contains all the key ICs (CPU, RAM, eMMC, Bluetooth, WiFi, etc.), while the expansion board provides power and fan-out to various interfaces (HDMI, microSD, USB3, USB-C, GPIO) with respective ESD protection devices. The compute module plugs into the expansion board through a 100-pin HiRose (HRS) surface-mount SF40 interconnect. In order to isolate the effects of the IC itself, rather than the effect of external ESD protection, an interposer board was developed. It was placed between the expansion board and the compute module, allowing injection of TLP pulses into the running (i.e., “hot”) USB3 interface data lines of the DUT, without significant loading of the USB3 signals. This was achieved by using low-capacitance TVS diodes, an injection technique developed in [8]. The circuit is shown in Figure 3 and the board is shown in Figure 4.

In the current work, three pulse lengths were used in the robustness evaluation: 100 ns, 6 ns, and 2 ns. The injection and measurement setup for the 100 ns pulse is presented in Figure 5. Figure 6 shows the setup for the 6 ns and 2 ns injections.

The DUT and the peripheral hardware layout are depicted in Figure 7. The USB3 client device was a USB3.0 SanDisk memory stick. It is reasonable to expect that client-to-client variation will be minimal if TLP injection directionality is sufficiently high (i.e. the largest portion of the stress is injected towards the DUT, while the plugged in client experiences minimal stress).

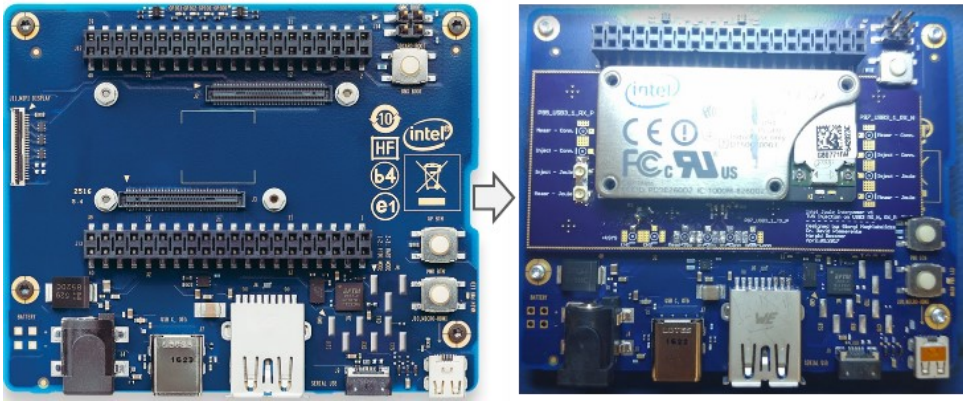

Figure 2. Left – expansion board with nothing pugged in; Right – compute module plugged into interposer, plugged into expansion board.

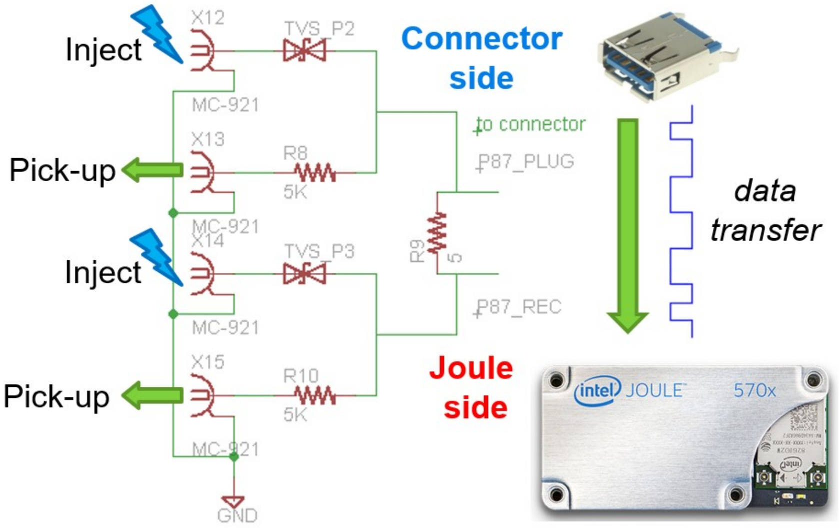

Figure 3. Injection and measurement circuit on the interposer board.

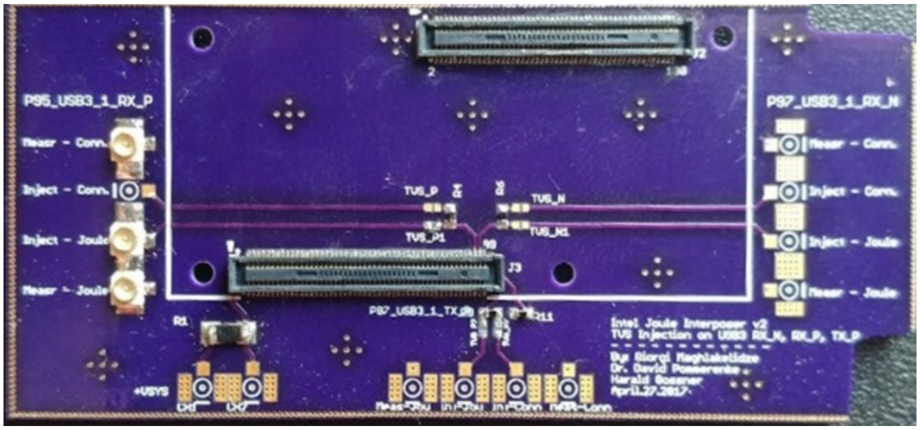

Figure 4. Populated interposer board photo, top view.

For the 100 ns injected pulse width, a current probe and deconvolution code was used to capture the injected current; for short pulses, a pick-off T combined with a delay line were used to separate the incident and reflected pulses (vf-TLP method).

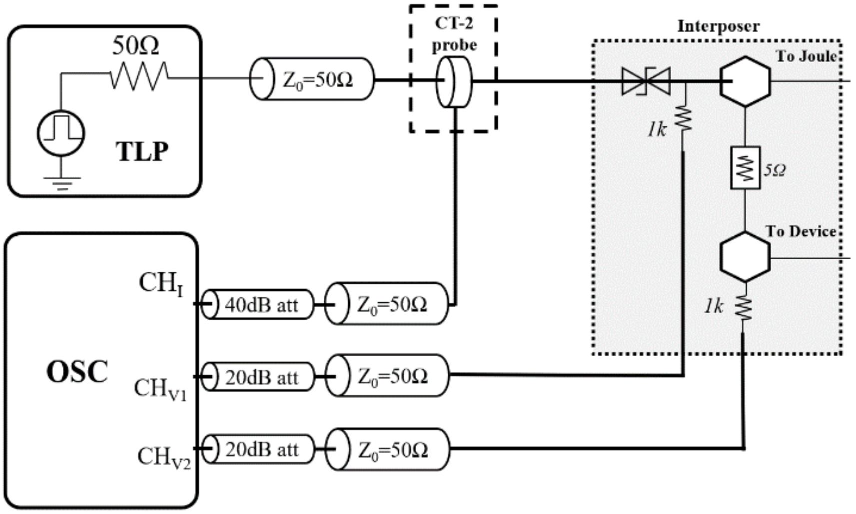

Figure 5. Injection and measurement setup diagram for 100 ns pulses (current deconvolution).

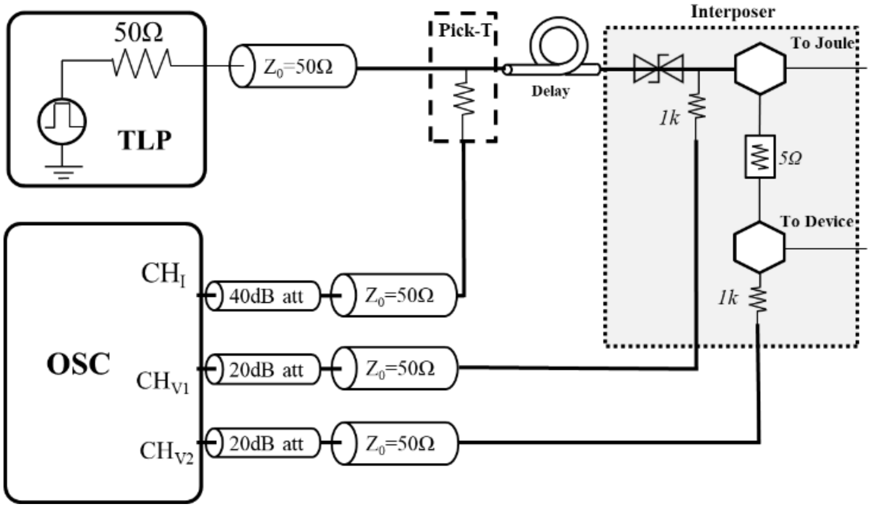

Figure 6. Injection and measurement setup diagram for 6 ns and 2 ns pulses (vf-TLP method).

2.1.2. Test Procedure for One Pulse. After calibrating the TLP injection and measurement system, the characterization procedure starts. For each injection level the following steps are taken:

1. Set the desired TLP voltage level;
2. Confirm that the DUT is in the “nominal” state (i.e. idle running and reporting);
3. Confirm that the interface under test is in the “nominal” state;
4. Inject a TLP pulse into the target pin;
5. Measure the waveforms and extract quasi-static voltage and current points;
6. Acquire kernel logs from the DUT;
7. Check if logs contain error messages;
8. Check if the interface under test is still in the “nominal” state;
9. If any abnormality is detected, classify and log the signature;
10. Detect soft failure mode;
11. Reset the interface to the nominal state (re-plug and check interface state);
12. If needed, reset the system to the nominal state;
13. Repeat for the next pulse level.

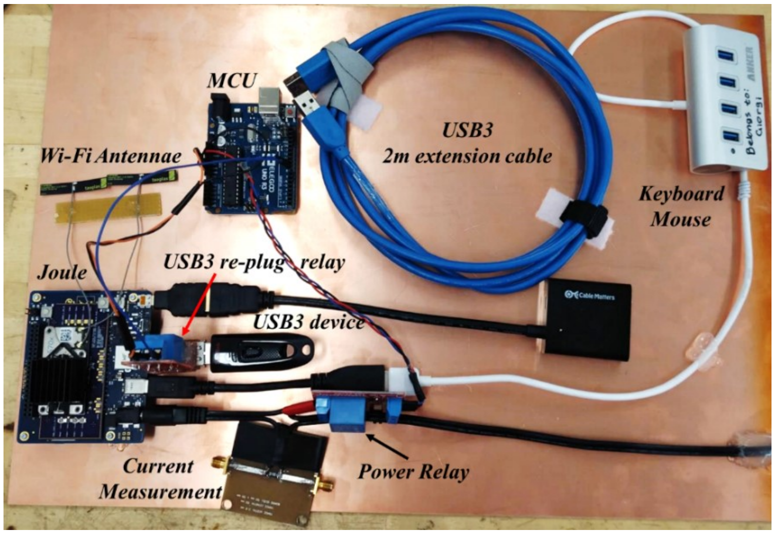

Figure 7. Photo of the DUT layout.

Each of the listed steps contains several sub-steps which complicate the process. The full algorithm is discussed in the subsequent sections.

2.2. AUTOMATION ALGORITHM

The algorithm flow is almost fully depicted in Figure 8. The whole automated characterization process is run mostly from the “Control PC” by two separate software programs, along with an additional software program running on the DUT. One is the TLP software, and another is an in-house Python script. Voltage level, polarity, number of pulses, and number of injections for each level are set in the TLP graphical user interface. The TLP GUI also controls each injection and measurement, calibration, and current deconvolution. Upon a successful TLP injection, the GUI reports measured data to the Python script via an interface ASCII file, and proceeds to wait until the next injection is initiated. A “successful TLP injection” means that the current and voltage waveforms were measured without oscilloscope clipping and triggering problems. If clipping occurs, the TLP has to fire again in order for the scope to retrigger. This may cause system upsets without a proper V-I measurement. However, this happens only when the system transitions to a new stress injection level. Since each pulse is repeated ~100 times, sufficient information is collected to measure enough points for a quasi-static IV curve.

Upon receiving the data from the TLP software, the Python script pulls the kernel logs from the DUT via the SSH interface. The DUT runs Ubuntu GNU/Linux operating system, so by running the *dmesg* command [15] and filtering for USB-related events with grep command, the algorithm can establish whether a USB-related SF has occurred.

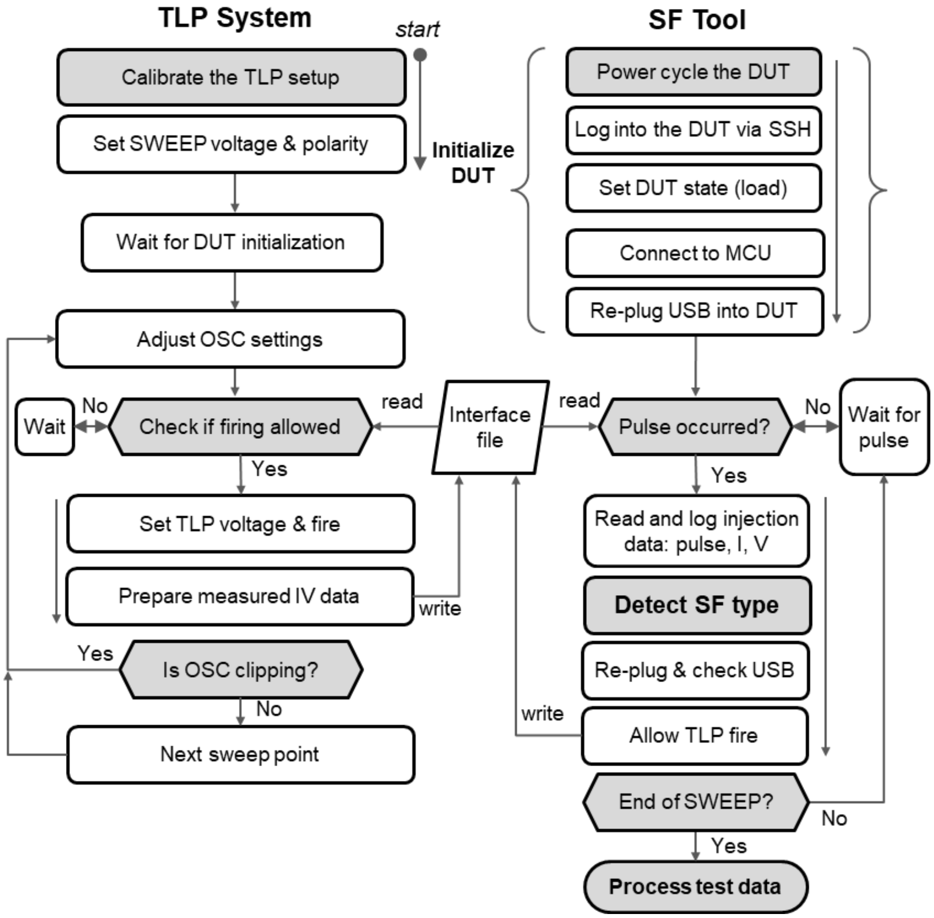

Figure 8. DUT SF characterization algorithm flow.

Some difficulty in the algorthm arises in three areas:

1. Bringing the DUT and the interface under test into the “nominal” state at every pulse;

2. Making sure that connections to the DUT and peripheral hardware are correctly opened and closed.

3. Differentiating between certain failure types based on the recovery method when the log message is unclear (e.g., failures that have similar signatures, but one requires a reboot, while the other – a power cycle).

These complications are caused by the SF and often manifest in the following ways:

- a disrupted connection to the DUT;
- causing a lost connection to the DUT due to a reboot;
- a need to reboot or power cycle the DUT to overcome the failure;
- a SF occurs, but no kernel message appears in the logs; the USB client device must be replugged to re-establish connection and re-evaluate the state of the DUT USB interface.

Obscurity of kernel messages can cause the algorithm to branch out and spend time “Detecting Soft Failure Type”, as depicted in Figure 9. The detection is rather simple: for each failure mode, there is a condition that needs to be satisfied. In the overall structure, there is a hierarchy of conditions that stack up from less severe to most severe. The left brach detects USB2 fallback-related failures, the right one detects USB3-related ones.

Because SF behavior varies somewhat randomly, each test is performed up to 100 times. The data points (TLP voltage, injected current, voltage, polarity, state of the system, SF type) from each test are recorded in a *.csv file and later processed by a Python script using Pandas (code library used for big data analysis) [13]. The multi-dimensional data analysis is aided by constructing pivot charts grouped by the desired characteristic (e.g., injected current, pulse width, rise time, etc.) and calculating how often an SF type has occurred for each variation.

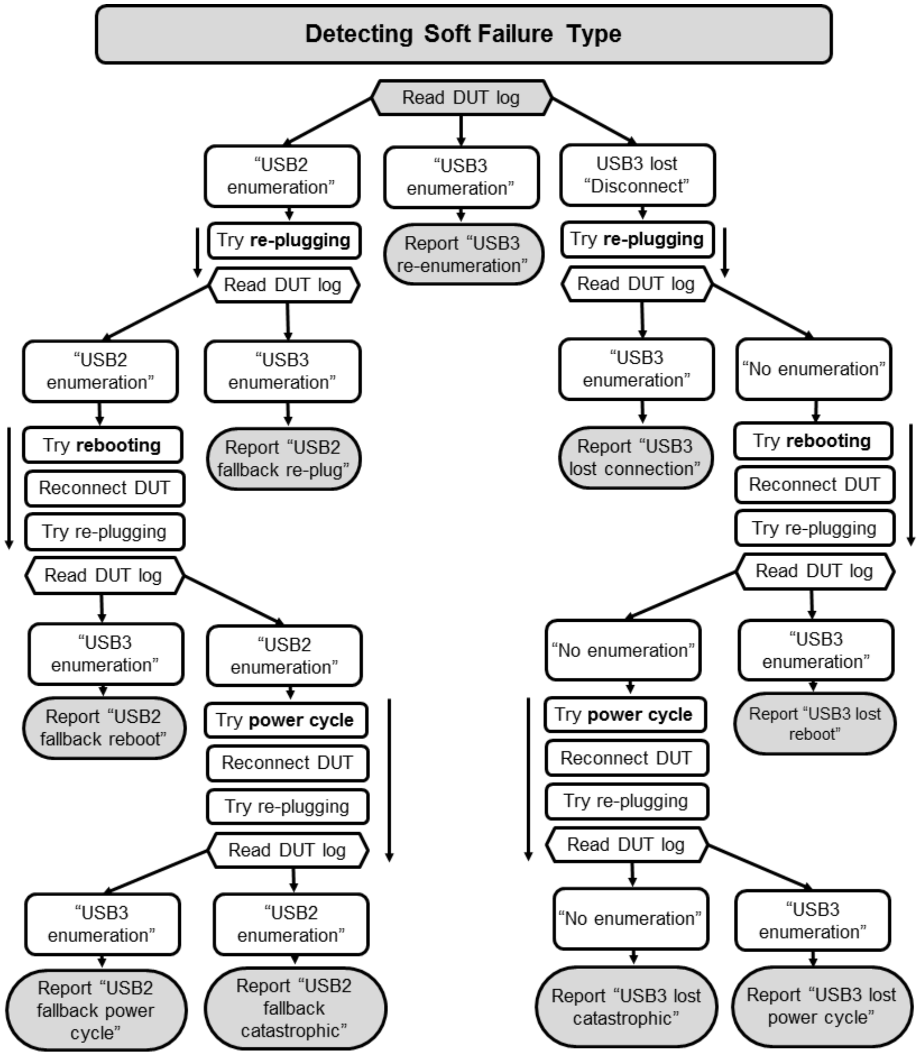

Figure 9. SF type detection algorithm.

3. RESULTS

3.1. ESD GUN TESTING

The Intel Joule development system was mounted inside an enclosure and a series of ESD gun tests were carried out. The purpose of the tests is to establish the range of soft failures when system-level stress is applied to different parts of the DUT: a) shield of

USB3 port, and b) DUT chassis. An ESD Gun, Noiseken ESS-2000 TC-815R, was used to inject impulses in the range between 1 kV and 9kV, in contact discharge mode. The DUT and the injection points are shown in Figure 10. Each injection was repeated 100 times, while the operator monitored and logged occurring soft failures. Discharging into the DUT chassis (point 1 in Figure 10) was relatively robust, causing the HDMI screen to flicker several times at higher discharge voltages, but having no reported USB failures. Screen flicker is a kind of SF within the system, but unrelated to the USB3 interface, so it is not discussed in detail.

The results of the ESD gun testing for system-level stress injected into the USB3 shield are shown in the Figure 11. Most of the soft failures are related to the HDMI screen (flickering, tinting with colors, screen turning off until HDMI cable replug). USB3 soft failures occur after 6kV, with a likelihood of <5% and varied severity: from re-enumeration of the device, to losing the connection and having to reboot the system. The logged failures correspond to the ones detected as a result of the automated characterization system, as discussed in detail in the subsequent sections.

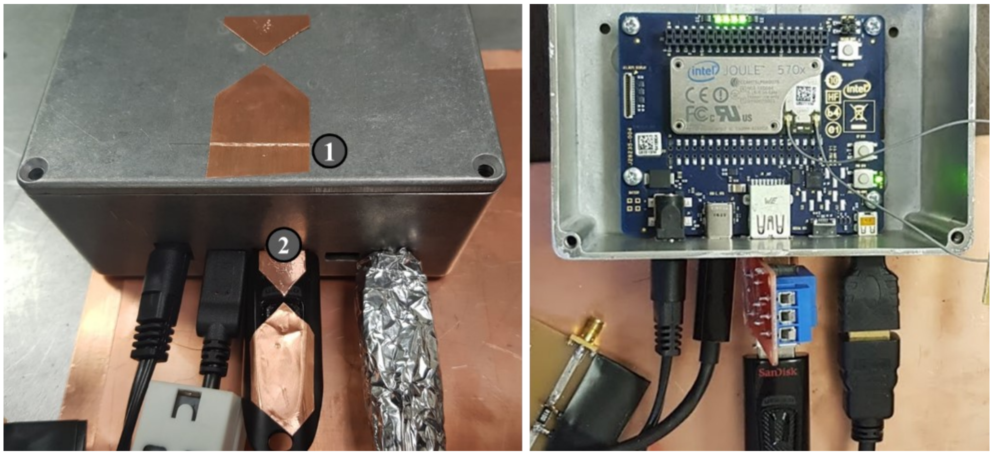

Figure 10. Left – injection points at the DUT chassis; Right – inside the chassis.

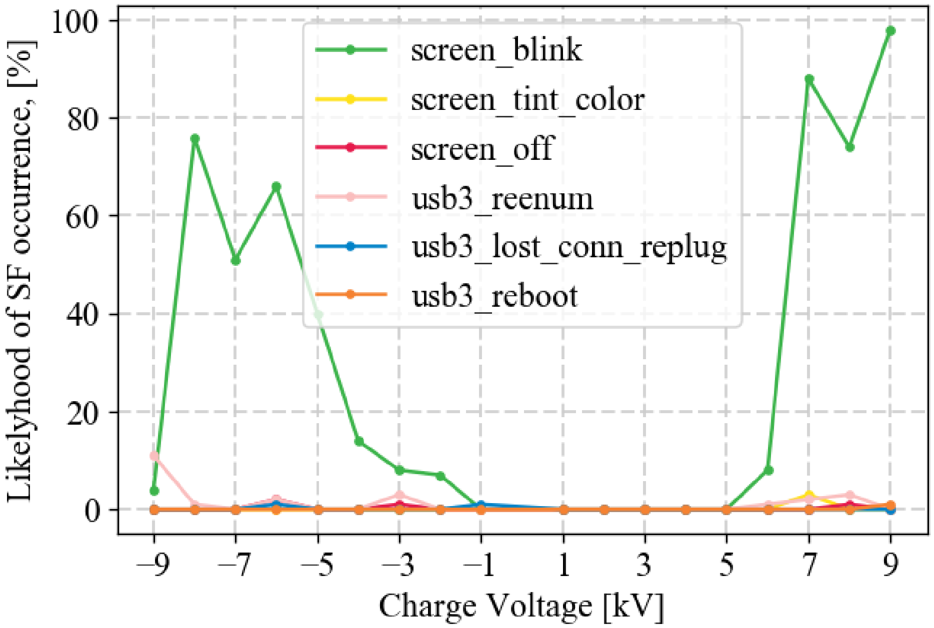

Figure 11. Results from ESD gun injection into the shield of USB3 interface of Joule expansion board.

3.2. SOFT FAILURE CLASSIFICATION

Observed soft failures can be categorized sufficiently well by Table 1 from [7], repeated here as Table 1. Category “A” is the least severe – the user does not notice the effect of failure and no intervention is required on their side. Category “B” is noticeable, but the system recovers without intervention (data transfer speed drops, the system reconnects to the client device, etc.). Category “C” is most severe and encompasses a varied family of failures, which may require as little as re-plugging the client device and as much as completely power cycling the DUT.

The failure modes observed for the DUT mostly fall in the most severe category C. The full list and corresponding descriptions are in Table 2.

Table 1. Categories of soft failures as per [7].

Cat.	Definition	Example for USB
A	Operator does not notice, no operator intervention	Bit errors; packets getting resent
B	Operator notices, no operator intervention	Drop in data throughput; connection re-established by the host
C	Operator notices, intervention required	Stop of data transfer; re-plugging of the cable or power cycling required

Table 2. Observed failure modes.

Mode	Observation	Cat.
1	Drop in the data rate; no operator action required	B
2.1	Client device re-enumerated in USB3 mode; functionality restored by the system	B
2.2	Client device re-enumerated in USB3 mode, a GUI pop-up message occurs functionality restored by the system, but user has to click the message	C
3	Client device falls back to USB2 mode; 3.1 functionality restored by re-plugging the device 3.2 functionality restored by rebooting the DUT 3.3 functionality restored by power cycling	C
4	Client device disappears; 4.1 Functionality restored by re-plugging the device 4.2 Functionality restored by rebooting the DUT 4.3 Functionality restored by power cycling	C
5	Wi-Fi functionality is lost; functionality restored by power cycling the DUT	C

The most common SF is “USB3 re-enumeration” (Mode 2), which means that the DUT has re-established the connection with the client device without user intervention; in this case, USB3 functionality is preserved and no further action is required. Sometimes this failure mode is accompanied by a GUI error message which requires user interaction, making this variation a Category C failure. The next failure mode variation is “fallback to USB2” (Mode 3). It occurs as a result of negative current injection and requires user intervention. The milder case requires a mere re-plugging of the client device; a more serious case requires system reboot or power cycling. These take much longer than a re-plug: 60-90 seconds to reboot vs 5 seconds to re-plug, which may be a major inconvenience to the operator. In case of positive high-current injections, a rare failure occurs that disables the USB interface and requires re-plugging, rebooting or power cycling (Mode 4). Occasionally, Wi-Fi functionality is lost (Mode 5), but no correlation between injection level and its occurrence has been established.

The worst case for modern hand-held and wearable devices is the soft failure that requires physically disconnecting the power. For portable devices that would mean taking out and re-placing the battery or flipping a physical switch. Neither of these are an option for different design and policy reasons (waterproofing, warranty, security, etc.). This makes the requirements for such failures to be more stringent than less severe failure modes.

3.3. VARIATION OF PULSE LENGTH

The results for the Sandisk USB client for 2, 6, and 100 ns pulse width stresses are shown in Figures 12-14 respectively. The pulse levels are swept from -70 V to

+170 V. The assymetry is explained by the high risk of hard failure if the negative stress is pushed to higher levels (at least for long-pulse case). The vertical axis is the likelihood of soft failure occurrence in percent; i.e., how often a particular SF has occurred out of all injected pulses for each particular pulse level and width. The horizontal axis is the TLP charge voltage. As expected, at lower injection levels, no failures occur. For all cases, there seems to be a threshold, beyond which SF probability jumps from 0% to a substantial amount (between 50% and 80%). For lower duration pulses, this threshold is higher due to lower amount of energy delivered into the system.

There seems to be little to no occurrence of serious soft failures for positive injections across the board. For positive current injections, only USB3 re-enumeration errors were observed. This is consistent across DUTs and other configurations. Only one case for the 100 ns injection had a somewhat severe fail – fallback to USB2, requiring the client to be re-plugged.

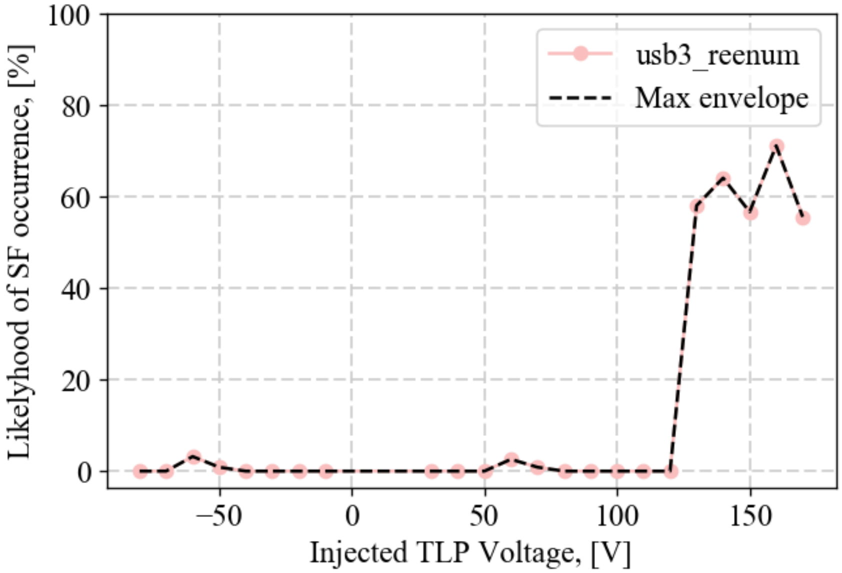

Figure 12. SF probability occurrence for 2 ns, against the TLP charge voltage.

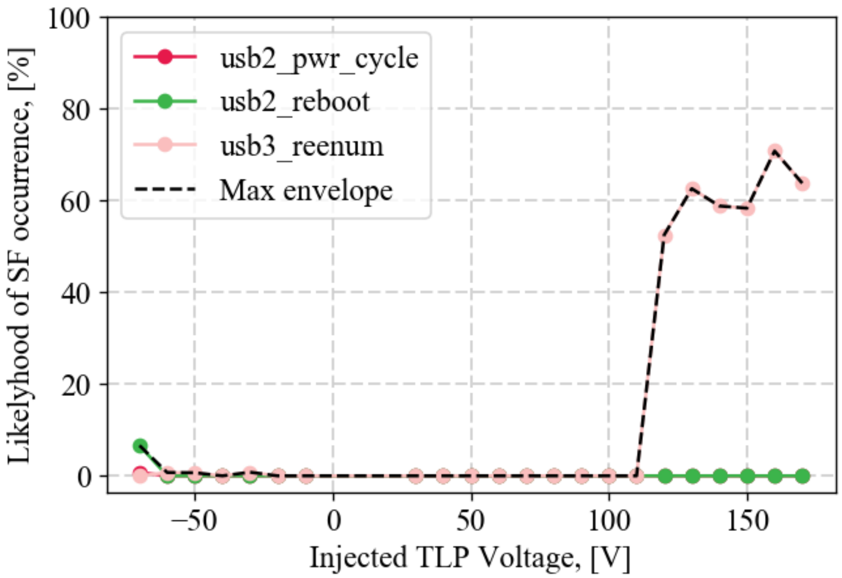

Figure 13. SF probability occurrence for 6 ns, against the TLP charge voltage.

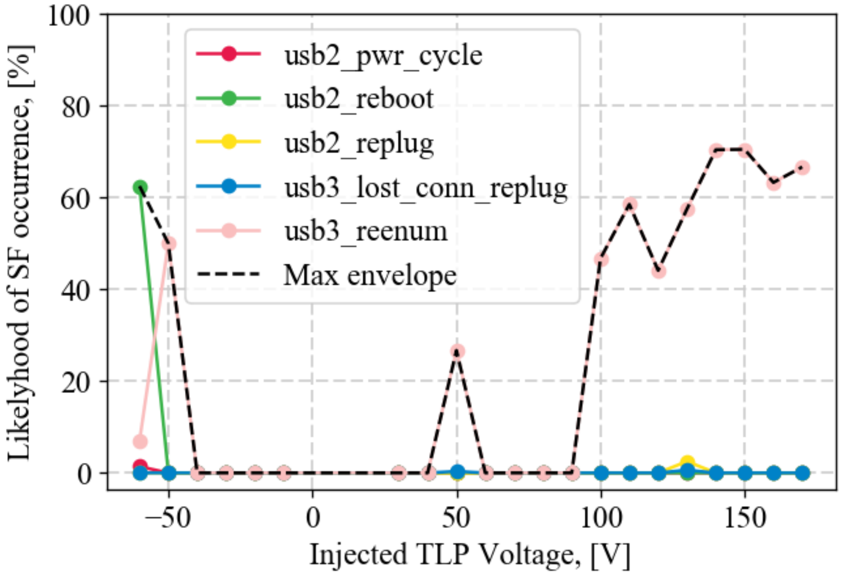

Figure 14. SF probability occurrence for 100 ns, against the TLP charge voltage.

Negative current injections have a lower threshold and a richer variety of severe failure modes. USB enumeration failure rates are very small for short pulses, but increase to 53% from 0% at -50V TLP injection for 100 ns disturbance. However, the most interesting observation is that enumeration errors fall in frequency (to <10%) as other failure modes become prevalent – such as USB2 fallback requiring a reboot (~60%) or USB2 fallback requiring a power cycle (<5%), or USB3 connection loss, requiring a replug (also <5%).

This may indicate that some other sub-system is failing more severely than the one which leads to the USB enumeration failure. These tests were completed within several days and consist of over 15,000 data points. The results seem consistent with [8], in so far as exhibiting the inversely proportional relationship between the pulse width and the failure threshold. In this case, the novel information is that negative current injections cause far more severe failures and that shorter pulses seem to cause less varied and less severe failures for the same injection levels. The rise time dependence is not explored, as there is firm evidence [7] that the correlation is weak.

3.4. VARIATION OF DUT SYSTEM STATE

One of the parameters of interest is soft failure occurrence under different system load conditions. There is prior evidence that the CPU load doesn’t have a significant influence on the likelihood of failure [7]. In this work, additional load conditions are explored by using a package stress-ng [14]. The package fully loads a 4-core CPU by using FFT function, reading and writing to RAM and eMMC. This load increases noise within the system, causing it to draw ~2x higher current and increasing overall system temperature. Hence, there is reasonable expectation that soft failures become more frequent, or more severe overall.

Ideally, one would repeat the full parametric sweep for each load condition. That increases characterization time many fold and is largely unnecessary, as baseline tests already show that no failures occur at lower injection levels. Therefore, in the interest of time conservation, only the threshold region for the positive injection sweep is selected for characterization under various load conditions. The results are shown in Figure 15.

The failure threshold stress current is the same for all cases and the occurrence levels vary between approximately 50% and 80%. Marginal variation from load to load is observed (within 10%). This confirms that the CPU load has only a weak influence on soft failure occurrence. RAM and eMMC loading shows similar results.

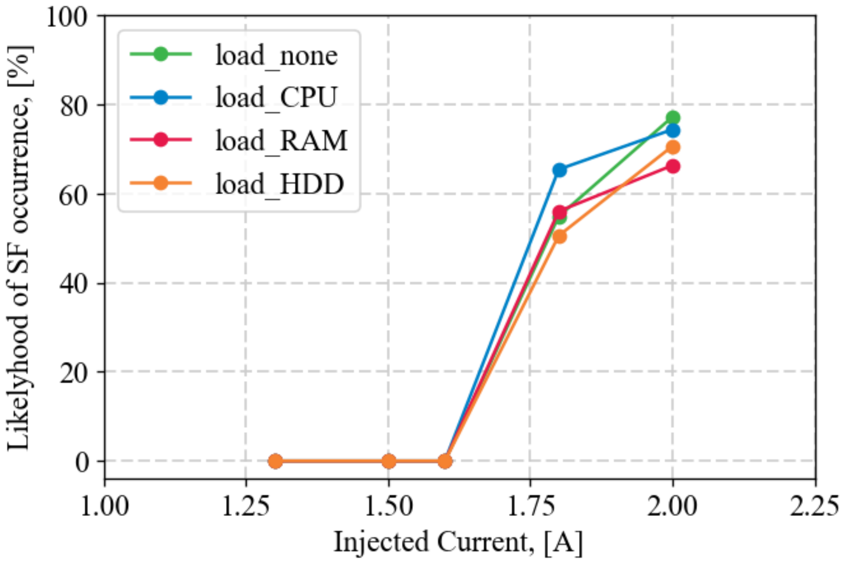

Figure 15. SF occurrence threshold due to positive injections under various system load states; 6 ns injected stress.

It must be noted that the DUT load condition sweep was not automated in this case, but automation is possible with reasonably small effort. For this, during the stage

"Set DUT State" in Figure 8, the operator defines several Linux command-line interface commands to be swept (one for each test condition) and one overarching loop is added that re-runs the algorithm for different load conditions.

4. DISCUSSION

The scope of this work is in automating the characterization flow and in expanding the knowledge about soft failure occurrence in complex systems. The root cause of specific soft failures is still being actively researched [3-6]. Specifically, with USB3 [7] [8] it has been found that more severe failures (fallback to USB2, etc.) occur due to power domain disturbances, while errors in data transmission are overwhelmingly consistent with lower-level pulses, where stress waveforms increase the signal peak-to-peak voltage.

One can draw practical conclusions from the obtained characterization data. From the expected ESD levels and the coupling paths, the designer can estimate the safe current waveforms and levels. These can be compared to the failure probability data from the IC characterization.

The system developer may establish a probability threshold for each failure mode and use the method for a "pass/fail" evaluation. Depending on the product purpose, 20% failure rate may be acceptable for SF not requiring operator intervention, while <1% may be acceptable for a SF that requires major actions like physical re-plugging or power cycling.

If soft failures are grouped, an envelope may be used to check the satisfaction of the passing criteria, e.g. “Max Envelope” on Figures 12-14.

A drawback of continuous, extensive TLP testing (especially with longer pulses) is the risk of “wearing out” the interface under test. This means introducing latent hardware failures by applying numerous pulses that under normal circumstances would not cause physical harm to the DUT.

Once the DUT is well characterized, the system designer can use that information to “get it right the first time” and/or reduce the number of product development iterations:

1. Make system design changes to mitigate some SF (system-, circuit-, and IC-level). This is especially beneficial in the early design stages of a product, when a designer is able to introduce additional protection, filtering, shielding, etc.

2. Make firmware or software improvements that would reduce severity or frequency of specific failure modes.

In cases that require inclusion of a measurement-based method (e.g. spike in current consumption of the interface) [4] [11] [12], at first it should be tested independently to establish the reliability and efficacy of the measurement method. Once the clear detection criteria are established, a function within “Detect SF Type” in Figure 9 can check if the criterion for detecting the SF has been satisfied.

In order to adapt this characterization method to a different interface, at first exploratory work must be done to establish the variety of soft failure modes. Then hardware and software efforts are carried out. In terms of hardware – auxiliary boards may need to be designed to facilitate re-plugging, power cycling the interface of interest, etc. In terms of software – a function set within “Detect SF Type” must be written. These functions inquire and establish whether the criteria for SF detection have been met. In addition, interface initialization functions may require change. The rest of the algorithm largely remains the same.

5. CONCLUSION

An automated system for SF robustness characterization was developed and applied to a USB3 interface of an existing development platform for a number of stress pulse lengths and system load conditions. Test results were processed and soft failure occurrence likelihood statistics were obtained for various levels of TLP injections, and both polarities. In the scope of this work, software-based detection methods were utilized, but the methodology is extendable to other interfaces and measurement-based failure detection methods as well.

The methodology has a wide application range, but is possibly most useful for high-reliability systems that could not tolerate soft failures. One of the directions for further research is a deeper investigation into SF occurrence depending on system states (CPU load, GPU load, etc.) and a wider range of disturbances. Characterization and data processing methods are well established and may be extended for further study.

ACKNOWLEDGEMENTS

The material is based upon work supported by the National Science Foundation, Grant IIP-1440110.

The authors would like to thank Nicholas Erickson of Missouri S&T EMC Laboratory for constructive criticism of the manuscript.

REFERENCES

[1] Industry Council on ESD Targets, White Paper 3: System Level ESD, Part II: “Implementation of Effective ESD Robust Designs”, September 2012

[2] Duvvury, C. and Gossner, H., “System level ESD co-design”, 1st ed. Wiley - IEEE, 2016

[3] N. A. Thomson et al, "Soft-Failures Induced by System-Level ESD," in IEEE Transactions on Device and Materials Reliability, vol. 17, no. 1, pp. 90-98

[4] S. Yang et al, "Measurement techniques to predict the soft failure susceptibility of an IC without the aid of a complete software stack," IEEE EMCS 2016, pp.41-45

[5] B. Orr et al, "A systematic method for determining soft-failure robustness of a subsystem," 2013 35th EOS/ESD Symposium, Las Vegas, NV, 2013, pp. 1-8.

[6] S. Vora, R. Jiang, S. Vasudevan and E. Rosenbaum, "Application level investigation of system-level ESD-induced soft failures," 2016 38th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Garden Grove, CA, 2016

[7] S. Koch et al “Identification of Soft Failure Mechanisms Triggered by ESD Stress on a Powered USB 3.0 Interface”, accepted by IEEE Transactions on EMC, 2018

[8] G. Notermans, H. M. Ritter, B. Laue and S. Seider, "Gun tests of a USB3 host controller board," 2016 38th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Garden Grove, CA, 2016

[9] ESDEMC Technology: https://www.esdemc.com/

[10] T. Schwingshackl et al., "Powered system-level conductive TLP probing method for ESD/EMI hard fail and soft fail threshold evaluation," 2013 35th EOS/ESD Symposium, 2013, pp. 1-8.

[11] J. Zhou, Y. Guo, S. Shinde, A. Patnaik, , O. H. Izadi, C. Zeng, , J. Shi, J. Maeshima, H. Shumiya, K. Araki, and D. Pommerenke, “Measurement Techniques to Identify Soft Failure Sensitivity to ESD” accepted by IEEE Transactions on EMC, 2018

[12] O. H. Izadi, A. Hosseinbeig, H. Shumiya, J. Maeshima, K. Araki, D. Pommerenke, “Systematic Analysis of ESD-Induced Soft-Failures As A Function of Operating Conditions”, 2018 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), Singapore, 2018

[13] Python Data Analysis Library pandas: https://pandas.pydata.org/

[14] Stress-testing package stress-ng for GNU/Linux: http://manpages.ubuntu.com/manpages/artful/man1/stress-ng.1.html

[15] Driver message command dmesg for GNU/Linux: http://man7.org/linux/man-pages/man1/dmesg.1.html

III. LATCH-UP DETECTION DURING ESD SOFT FAILURE CHARACTERIZATION USING AN ON-DIE POWER SENSOR

Giorgi Maghlakelidze

Deparment of Eletrical and Computer Engineering, Missouri University of Science and Technology, Rolla, MO 65409

ABSTRACT

ESD-induced latch up is detected with an on-die energy counter circuit. Raw values are accessed through a Linux operating system kernel call, then the power consumption is calculated. Persistent power consumption increase indicates the latch-up occurrence, thus avoiding the need of external equipment for its detection. The failure mode is not visually noticeable and requires full power cycling to fully recover.

Keywords: soft failure, electrostatic discharge, latch-up, USB3, kernel logs, Linux, on-die sensor, ESD, SEED.

1. INTRODUCTION

ESD-induced soft failures (SF) are temporary upsets in a functional system [1][2]. These upsets vary in severity between a minor inconvenience to more impactful problems like data loss, loss of functionality, or battery drain. Thus, in order to ensure system reliability, maximized soft failure robustness should be one of the goals during product development. The phenomenon is characterized on system [3] and pin-level [4] using various methods.

The current work extends previously developed software-based automated system to include latch-up detection via on-die sensors. This failure mode has been investigated in [2][5] and requires external equipment, such as a thermocouple or a thermal imaging camera. These methods rely on detecting heat dissipated by the latch-up current, which is an external manifestation of the phenomenon and takes time to manifest. In addition, this effect may not be detectable by heat if the DUT is equipped with an active cooling system (e.g. a fan). The proposed method solves the requirement of external equipment needed to detect a latch-up.

Soft failure robustness thresholds are investigated for USB3 Gen 1 interface of Intel Joule Internet of Things platform. Pulse-length and polarity dependence, pulse rise time, CPU loading effects, temperature, and other parameters are studied in [7][3]-[9]. The results are quantitative, statistics that show the probability of SF occurrence based on injected pulse characteristics. Twelve failure signatures are observed and categorized into 6 failure modes. A deep root-cause analysis is not performed, as the goal in the current work is to characterize a pin of a DUT as a "black box".

Table 1. Take-home messages.

1) Many ESD-induced soft failures can be detected within software (driver level, operating system level);
2) Some sub-systems (e.g. thermal & power control) can be co-opted for ESD characterization purposes
3) Latch-ups of can be detected by using on-die power consumption sensors during system operation;
4) Some latch-up failures cannot be resolved without full power cycle, which is a significant problem in embedded systems with a non-removable battery (e.g. smartphones)

2. CHARACTERIZATION PROCESS DESCRIPTION

Characterization setup consists of several active parts that are controlled by the Control PC. The setup is depicted as system diagram in Figure 1. The PC controls the HPPI Transmission Line Pulse (TLP) system [10] to inject 50ns pulses of various levels and polarity. Oscilloscope, 1 kΩ sense resistor and a current probe CT-2 facilitate voltage and current measurements at the stress injection point. The pulses are forced through an interposer designed to fit inside the DUT and provide access to USB3 nets – between the IC pin and the receptacle. The rest of the setup comprises an MCU that controls power relays for: a) system main 12 V supply – facilitates power cycling, and b) USB3 5V supply – to emulate re-plugging of the USB client device.

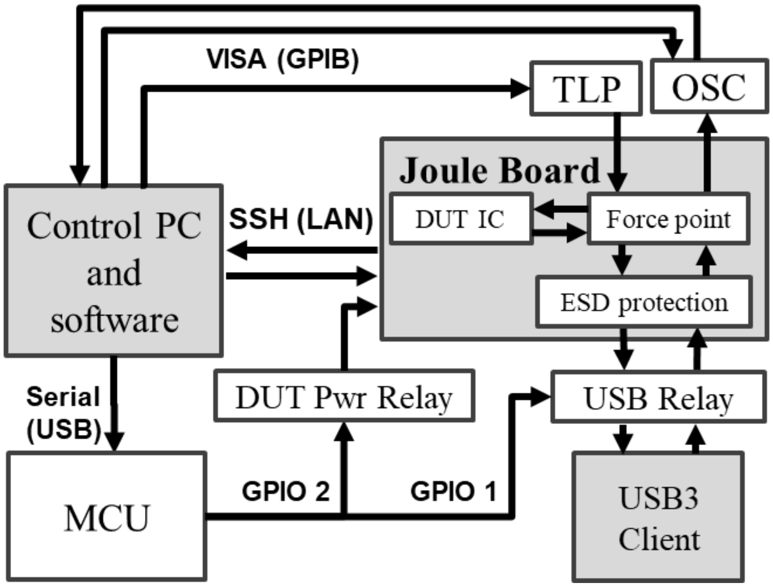

Figure 1. System diagram for the characterization setup.

The Control PC interfaces with the TLP and OSC through GPIB, communicates with MCU using COM and controls the DUT using SSH over WLAN. The latter can also be implemented through wired LAN (if the DUT has one available), or through using an USB-to-LAN adapter connected to an available USB port (independent of the USB3 controller under test). The PC runs custom software that controls the whole automated process that comprises: pulse parameter sweeping, measurement, SF detection and rectification, producing a report. A more detailed description of the systematic characterization methodology for one pin is given in [4].

2.1. STRESS INJECTION WITH INTERPOSER

Intel Joule IoT platform consists of two parts – an expansion board and a compute module, as illustrated in Figure 2. The latter contains ICs for the core functionality (CPU, RAM, GPIO, Wi-Fi, USB3, HDMI, eMMC, Bluetooth, etc.), while the expansion board provides power distribution network and fans out the interfaces (HDMI, microSD, USB3, USB-C, GPIO) and contains the external ESD protection devices. The part in the middle, the interposer, plugs in between the expansion board and the compute module. Using low-capacitance TVS diodes, TLP stress is injected directly into USB3 interface data nets [11].

Part of the stress propagates towards the DUT and causes SF, the other part - towards the USB3 client (“ADUT”), as shown in Figure 3. It is assumed that SF are caused only on the DUT side, as there are two mechanisms that limit the stress seen by ADUT:

1. Low-value series resistor that limits the current injected towards ADUT;
2. On-board ESD protection device placed at the USB3 receptacle by the Joule system designers.

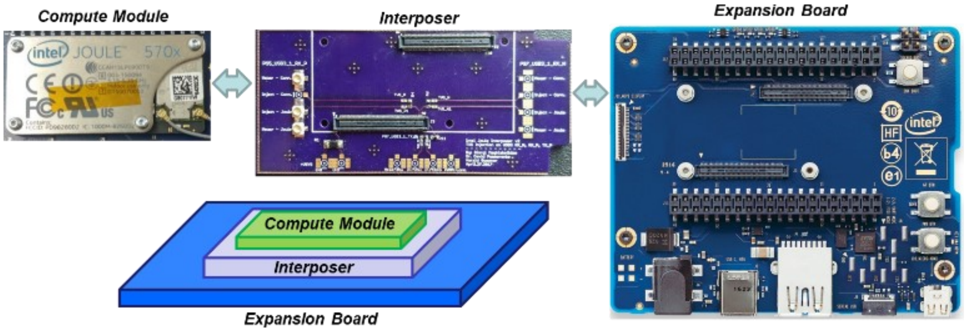

Figure 2. Joule System and the interposer board.

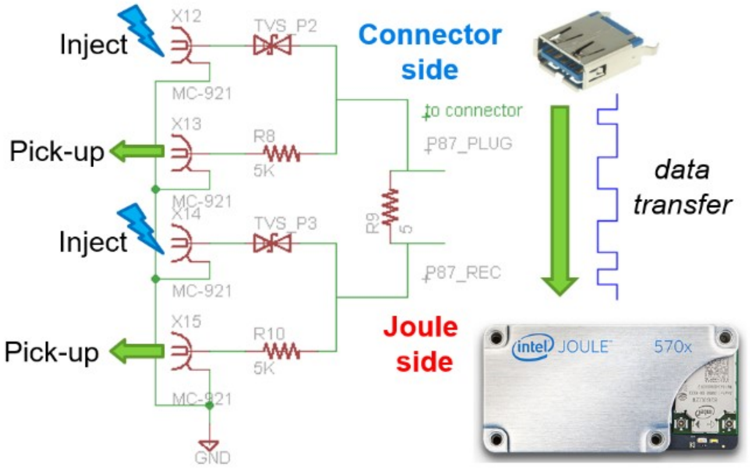

Figure 3. Force and measurement circuit, Joule interposer board.

2.2. AUTOMATION ALGORITHM

The characterization algorithm flow is depicted in Figure 4. It is based on [4] and has a new class of SF failure types implemented: latch-up.

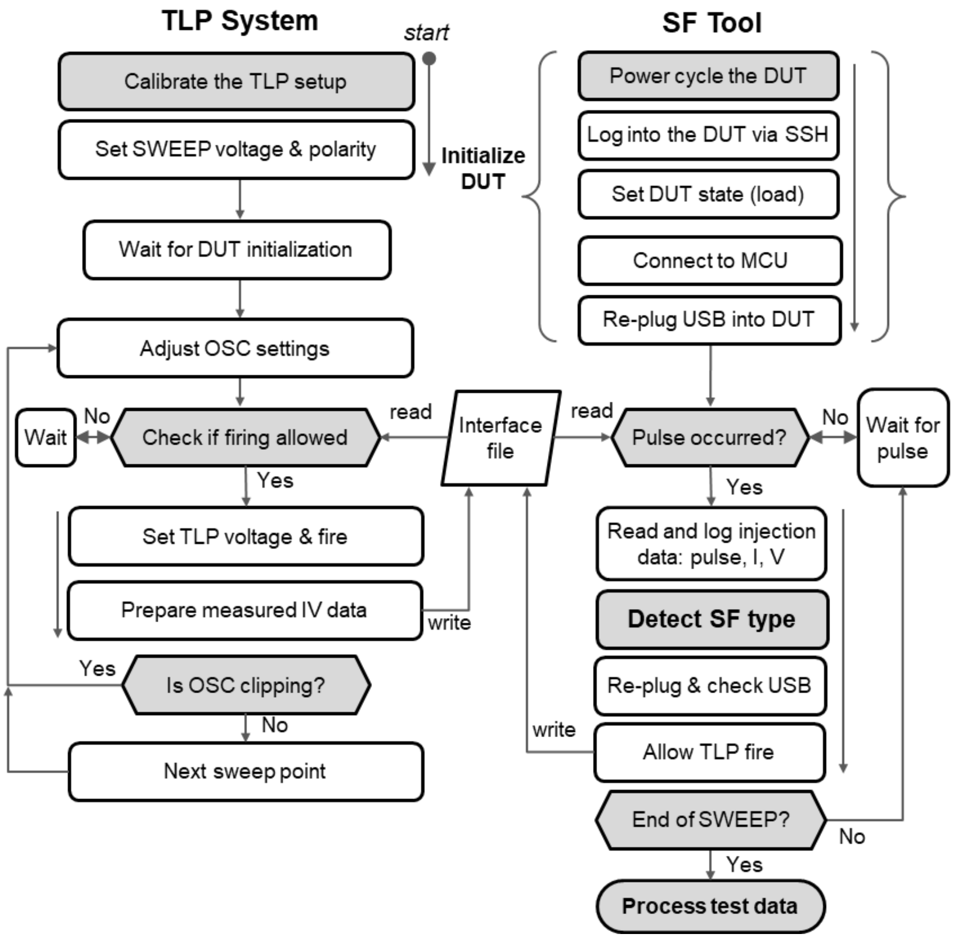

Figure 4. DUT SF characterization algorithm flow.

The "Control PC" software controls the TLP, its calibration, current deconvolution, checks the state of the DUT and the USB3 interface. If the USB3 interface and the DUT are in nominal condition, TLP firing is allowed. After a pulse is injected, information is gathered from the kernel logs by querying the DUT operating system, GNU/Linux, command dmesg [12]. Command grep filters out all the USB3-relevant results. If any failure signatures are detected, the state of the USB interface is reset. When needed, in order to achieve nominal state, the USB3 client is re-plugged, OS rebooted or DUT is power cycled.

Test information such as: TLP voltage, injected current, voltage, polarity, state of the system, SF type, are recorded in a *.csv file and processed using Pandas (function library for big data analysis) [13]. The multi-dimensional data is analyzed by making pivot charts, where data are grouped by the desired characteristic (e.g., injected current, pulse width, etc.) and calculating how often an SF type has occurred for each variation. Worst case failure rate is tracked over the whole parameter sweep, as well as a cumulative failure rate per 100 injections.

2.3. LATCH-UP DETECTION

In order to execute thermal control in the system, multiple on-die sensors are typically used in high-performance CPUs. In-built functionality of Joule CPU allows to measure energy for thermal management purposes. Run-time Average Power Limit (RAPL) automatically adjusts the processor power to maintain temperature targets. RAPL has “energy counter” that is accessed by the kernel and reports “energy spent by the processor in micro Joules” [14].

To measure time-average dissipated power, a first-order derivative approximation of energy is calculated:

$$P_{avg} = \frac{E(t_1)-E(t_2)}{t_2-t_1} \tag{1}$$

Energy spent at each moment in time can be found by accessing the counter register within the kernel. Within the Linux kernel, RAPL driver’s energy counter can be accessed every 1 second at:

/sys/class/powercap/intel-rapl/intel-rapl:0/energy_uj (2)

The specifics of the implementation and address will vary on other DUTs and the operating systems.

The latch-up presents itself as a sharp increase in power consumption, which persists over time, even if there is no load on the system. This is observed by monitoring the power profile over time and comparing the ongoing consumption to an idle one. An example of power profile over time during normal operation is presented in Figure 5.

When the system is idle and USB3 device plugged in, the consumption is about 0.5 W, while during file transfer it goes up to 1 W and can spike to 2 or 2.5 W for a short time. During maximum CPU or RAM operational stress test, power consumption peaks at just below 5 W and 2.7 W respectively, as illustrated in Figure 6.

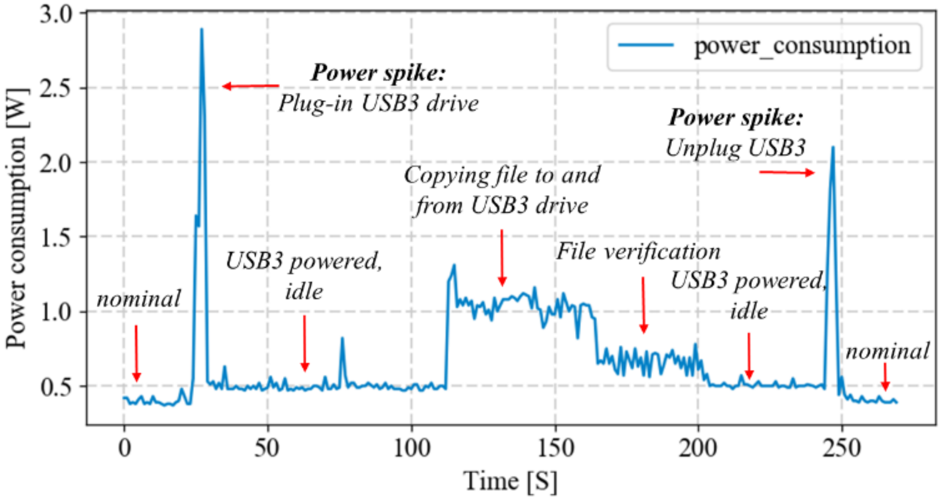

Figure 5. Power consumption profile for normal operating conditions.

Power profile shows constant drain after latch-up is triggered. Figure 7 shows baseline power consumption increase by 1 W because a latch-up was triggered somewhere in silicon of the power domain. Unplugging the USB3 device only reduces power consumption by 0.2 W, indicating that the soft failure occurred not on the USB client, but on the DUT – USB host. It is found that the soft failure cannot be resolved without full power cycle of the system.

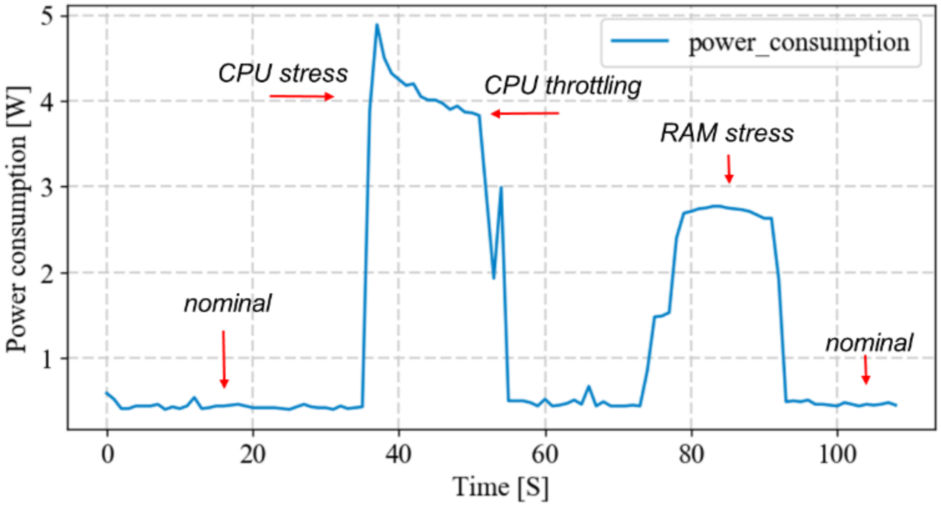

Figure 6. Power consumption profile for CPU stress and RAM stress test.

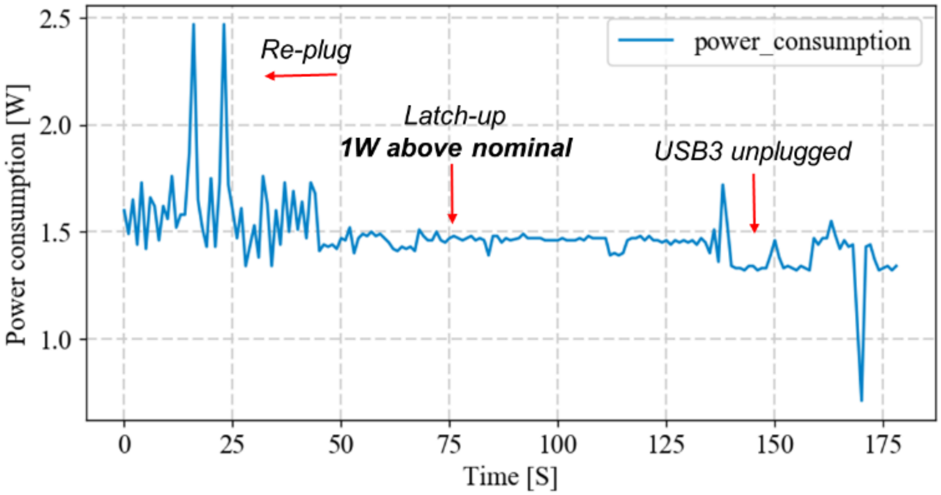

Figure 7. Power profile after latch-up occurs shows baseline power consumption increase by ~1 W.

3. RESULTS AND DISCUSSION

3.1. SOFT FAILURE CATEGORIZATION

The SF observed in the DUT are varied and can be differentiated into 6 failure modes, see Table 1. Mode 1 is relatively harmless from the failure perspective. Mode 2 is "USB3 re-enumeration" and is the most common. Here, the DUT re-initializes the client device without user intervention; i.e. USB3 is functional and no other intervention is required. Mode 3 is "fallback to USB2", which occurs most often when negative current is injected. It may require different levels of user involvement. The simplest case requires a re-plugging of the USB device. The more demanding SF require system reboot or power cycling and can take up to 90 seconds. Mode 4 happens rarely, at positive injections - the USB interface goes down and requires re-plugging, rebooting or power cycling (similar to Mode 3). Mode 5 is rare and it exhibits itself by loss of Wi-Fi functionality. Mode 6 can entail less severe SF being observed, but they are accompanied by a latch-up, which is not visually obvious to the system operator. USB interface is still functional, but significant power drain is persistent.

The observations have been categorized in [4], repeated here as Table 2 and improved to include the latch-up types of the SF. Category "A" is mostly harmless as the user does not notice the failure and no action is required. "B" is noticeable, but the system recovers by itself. "C" and "D" are most severe and include a wide family of failures. These require as little as re-plugging the client device, but could possibly require completely power cycling the DUT (physically disconnecting the power supply). This can be the worst for modern phones and wearable devices that have non-replaceable batteries and are sealed for waterproofing or other reasons.

Table 2. Failure modes observed on the DUT.

Mode	**Observation**	**Cat.**
1	Drop in the data rate; no operator action required	B
2.1	Client device re-enumerated in USB3 mode; functionality restored by the system	B
2.2	Client device re-enumerated in USB3 mode, a GUI pop-up message occurs functionality restored by the system, but user has to click the message	C
3	Client device falls back to USB2 mode; 3.1 functionality restored by re-plugging the device 3.2 functionality restored by rebooting the DUT 3.3 functionality restored by power cycling	C
4	Client device disappears; 4.1 Functionality restored by re-plugging the device 4.2 Functionality restored by rebooting the DUT 4.3 Functionality restored by power cycling	C
5	Wi-Fi functionality is lost; functionality restored by power cycling the DUT	C
6	Latch-up occurs; 6.1 Device re-enumerates in USB3 mode 6.2 Device disappears Latch-up resolved only by power cycling	D

“D” is the category for the latch-up type failures. They are unnoticed without special measurement equipment, so the user may be unaware of the additional power drain in their system. In case of battery-powered devices, this maybe of utmost importance, as any waste of energy significantly reduces system life and may degrade the battery itself.

Such complications would require the system design to have a higher degree of immunity to SF. This systematic characterization process is important to reliably test the system robustness.

Table 3. Soft failure categories.

Cat.	Noticeable	Interaction Needed	Example for USB
A	✗	✗	Bit errors; packets getting resent
B	✓	✗	Drop in data throughput; connection re-established by the host
C	✓	✓	Stop of data transfer; re-plugging of the cable or power cycling required
D	✗	✓	Device re-enumerates, but latch up is unnoticed

3.2. INTERPRETATION OF CHARACTERIZATION RESULTS

Two USB3 Gen 1 client devices were tested to establish client-to-client variation:

1. Sandisk Ultra 16GB
2. Transcend JetFlash 16GB

The results seem to be similar between the two DUTs. The test conditions were as close to identical as possible: only the memory sticks were swapped between tests. Figure 8 for a Transcend memory stick. On the horizontal axis is the TLP charge voltage. At lower injection levels, little to no failures occur. At 100V charge voltage SF rate is increasing, to reach 100% cumulative failure rate at 110V. This is a sharp threshold, which corresponds to ~2A injected current.

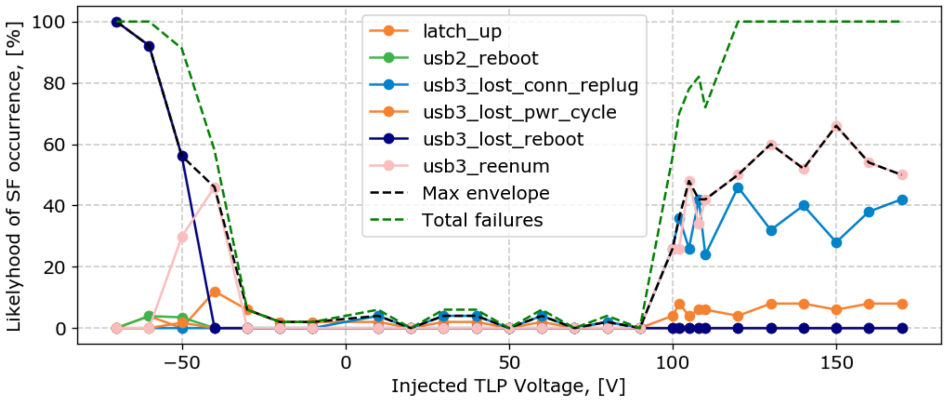

Figure 8. SF likelihood with Transcend JetFlash client for 50 ns TLP.

For positive stress current the following SF are common: a) USB3 re-enumeration, b) USB3 losing connection and requiring only a re-plug, and c) latch-up (consistently under 10% after 100 V). For negative injections, there is also a threshold for 100% failure rate, but it corresponds to about -1 A. The SF modes include USB3 enumeration, but are quickly dominated by USB3 losing connection and requiring a full power cycle (>90% failure rate). Negative stress seems to correlate to a richer variety and more serious SF modes: USB2 fall back, requiring restart and reboot, USB3 disappearing from the system, latch-up, etc. Further negative stress levels were not investigated, as there was a high chance of inducing hard failures (the DUT is far more susceptible to negative current, USB3 interface damaged at -2 A injection).

Similar results are observed for Sandisk Ultra, the characterization outcome is shown in Figure 9.

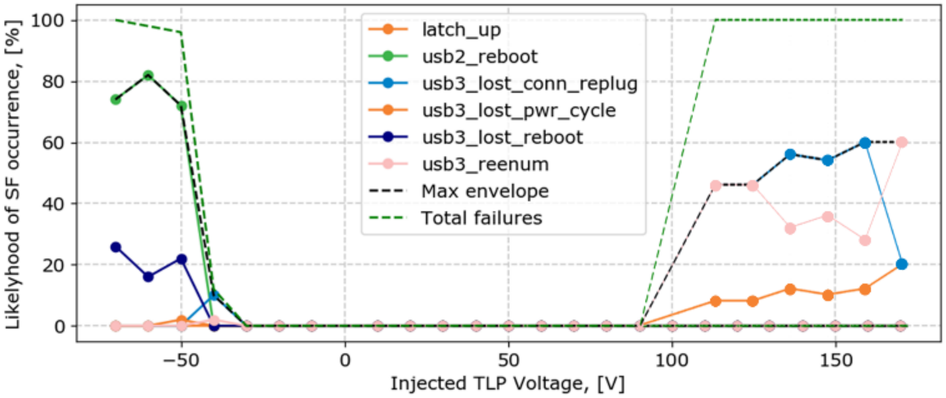

Figure 9. SF likelihood with Sandisk Ultra client for 50 ns TLP.

4. CONCLUSION

An automated characterization provides useful information to a system designer in terms of SF failure thresholds, despite the DUT being considered as a “black box”. Cumulative failure rate curve can be effectively used against a pass-fail threshold. Several less severe failures modes can be excluded from the analysis, because they are auto-resolved by the interface protocol. A designer may try different methods (software or hardware) to mitigate the soft failure, e.g. as diverting stress current away from the victim, then characterize the pin again. System robustness is considered “improved” if the failure thresholds shift to higher stress levels.

Addition of latch-up detection gives the possibility to detect 100% of failure rate without external equipment. This can be used not only during design and test phases, but after deployment of the product. One of the disadvantages of the proposed method is that the energy counter sensor must be implemented on the die and in software (drivers and operating system). Depending on the vendor and the specific product, the thermal and power management system may not have an energy counter. In this case, one could attempt to use a temperature sensor as a slower and less accurate alternative. The main advantage is that the functionality is included with the thermal control subsystem and no additional measurement equipment is required.

ACKNOWLEDGEMENTS

The material is based upon work supported by the National Science Foundation, Grant IIP-1440110.

REFERENCES

[1] Industry Council on ESD Targets, White Paper 3: System Level ESD, Part II: “Implementation of Effective ESD Robust Designs”, September 2012

[2] Duvvury, C. and Gossner, H., “System level ESD co-design”, 1st ed. Wiley - IEEE, 2016

[3] N. A. Thomson et al, "Soft-Failures Induced by System-Level ESD," in IEEE Transactions on Device and Materials Reliability, vol. 17, no. 1, pp. 90-98

[4] G. Maghlakelidze et al, "Pin Specific ESD Soft Failure Characterization Using a Fully Automated Set-up", 40th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Reno, NV, 2019

[5] S. Yang et al, "Measurement techniques to predict the soft failure susceptibility of an IC without the aid of a complete software stack," IEEE EMCS 2016, pp.41-45

[6] B. Orr et al, "A systematic method for determining soft-failure robustness of a subsystem," 2013 35th EOS/ESD Symposium, Las Vegas, NV, 2013, pp. 1-8.

[7] S. Vora, R. Jiang, S. Vasudevan and E. Rosenbaum, "Application level investigation of system-level ESD-induced soft failures," 2016 38th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Garden Grove, CA, 2016

[8] S. Koch et al “Identification of Soft Failure Mechanisms Triggered by ESD Stress on a Powered USB 3.0 Interface”, accepted by IEEE Transactions on EMC, 2018

[9] G. Notermans, H. M. Ritter, B. Laue and S. Seider, "Gun tests of a USB3 host controller board," 2016 38th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Garden Grove, CA, 2016

[10] HPPI TLP System: https://www.hppi.com/

[11] T. Schwingshackl et al., "Powered system-level conductive TLP probing method for ESD/EMI hard fail and soft fail threshold evaluation," 2013 35th EOS/ESD Symposium, 2013, pp. 1-8.

[12] Driver message command dmesg for GNU/Linux: http://man7.org/linux/man-pages/man1/dmesg.1.html

[13] Python Data Analysis Library pandas: https://pandas.pydata.org/

[14] Intel Joule Thermal Management Guide: https://software.intel.com/en-us/node/738005

SECTION

2. CONCLUSIONS AND RECOMMENDATIONS

In the first paper of this dissertation, it has been demonstrated for the first time, that conventional ESD hard failure protection techniques are effective against soft failures due to the direct pin injection. The improvement is achieved by diverting most of the ESD-induced current away from the victim. Simple bit-errors cannot be avoided, but this technique prevents current injection into VSS, VDD or the substrate of the victim IC which can lead to failures that cannot be corrected by the protocol of the I/O. A well-selected TVS diode clamps the voltage at the pin close to the signal. As a result, the current forced by the ESD into the IC is strongly reduced.

The reduction of the SF likelihood is investigated in a SEED-like simulation. This requires SEED models that include the soft failure behavior. 2 ns and 100 ns TLP are used to represent direct and indirect pulse injection. The simulation of a large signal circuit model of the victim pin, comprising a virtual detector circuit and the SF threshold dependency, show a good match to the physical system. The proposed version of the system model is circuit-based; however, the same methodology can be applied in co-simulation with 3D full-wave solvers.

The second paper provides a systematic approach for DUT characterization and data collection, which is used in the SF-SEED as basis of the empirical victim pin model. An automated setup and algorithm are presented and shown to be effective. Collected characterization data is organized into plots of SF likelihood vs. TLP charge voltage, then soft failure thresholds are extracted and used in the pin model. The results show that longer pulse lengths are associated with lower thresholds and more serious failure modes.

The third paper has shown that there is an effective way to use system thermal control sensors in order to detect latch-ups without external equipment. This is done throught an on-die energy counter that measured energy spent by the CPU at discrete time intervals. This technique contributes to the characterization methodology by helping to detect non-visible, but persistent failures that require operator intervention.

Combined, these publications show that soft failure SEED methodology is a viable way to characterize a system and strategize on improving soft failure robustness, quickly iterate on design changes and optimize for the highest ESD robustness. Additionally, it was shown for the first time, that several conventional hard failure ESD protection schemes can be very effective at mitigating soft failures.

BIBLIOGRAPHY

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

[2] S. Yang et al, "Measurement techniques to predict the soft failure susceptibility of an IC without the aid of a complete software stack," IEEE EMCS 2016, pp.41-45

[3] M. Park et al., "Measurement and Analysis of Statistical IC Operation Errors in a Memory Module Due to System-Level ESD Noise," in IEEE Transactions on Electromagnetic Compatibility, vol. 61, no. 1, pp. 29-39, Feb. 2019.

[4] S. Koch, B. J. Orr, H. Gossner, H. A. Gieser and L. Maurer, "Identification of Soft Failure Mechanisms Triggered by ESD Stress on a Powered USB 3.0 Interface," in IEEE Transactions on Electromagnetic Compatibility, vol. 61, no. 1, pp. 20-28, Feb. 2019.

[5] Y. Xiu, N. Thomson and E. Rosenbaum, "Measurement and Simulation of On-Chip Supply Noise Induced by System-Level ESD," in IEEE Transactions on Device and Materials Reliability, vol. 19, no. 1, pp. 211-220, March 2019.

[6] B. J. Orr, S. Koch, H. Gossner and D. J. Pommerenke, "A Systematic Method to Characterize the Soft-Failure Susceptibility of the I/Os on an Integrated Circuit Due to Electrostatic Discharge," in IEEE Transactions on Electromagnetic Compatibility, Sep. 2019.

[7] G. Maghlakelidze, P. Wei, W. Huang, H. Gossner and D. Pommerenke, "Pin Specific ESD Soft Failure Characterization Using a Fully Automated Set-up," 2018 40th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Reno, NV, 2018, pp. 1-9.

[8] G. Maghlakelidze, H. Gossner and D. Pommerenke, "Latch-up Detection During ESD Soft Failure Characterization Using an On-Die Power Sensor", Electromagnetic Compatibility Practice and Applications, IEEE Letters on, 2019

[9] Industry Council on ESD Targets, White Paper 3: System Level ESD, Part II: “Implementation of Effective ESD Robust Designs”, September 2012

[10] Duvvury, C. and Gossner, H., “System level ESD co-design”, 1st ed. Wiley - IEEE, 2016

[11] T. Schwingshackl et al., "Powered system-level conductive TLP probing method for ESD/EMI hard fail and soft fail threshold evaluation," 2013 35th EOS/ESD Symposium, 2013, pp. 1-8.

[12] B. Orr, D. Johnsson, K. Domanski, H. Gossner and D. Pommerenke, "A passive coupling circuit for injecting TLP-like stress pulses into only one end of a driver/receiver system," 2015 37th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Reno, NV, 2015, pp. 1-8

[13] P. Wei, G. Maghlakelidze, A. Patnaik, H. Gossner and D. Pommerenke, "TVS Transient Behavior Characterization and SPICEBased Behavior Model," 2018 40th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Reno, NV, 2018, pp. 1-10.

[14] P. Wei, G. Maghlakelidze, J. Zhou, H. Gossner and D. Pommerenke, "An Application of System Level Efficient ESD Design for HighSpeed USB3.x Interface," 2018 40th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Reno, NV, 2018, pp. 1-10.

[15] L. Shen, S. Marathe, J. Meiguni, G. Luo, J. Zhou and D. Pommerenke, "TVS Devices Transient Behavior Modeling Framework and Application to SEED," 2019 41st Annual EOS/ESD Symposium (EOS/ESD), Riverside, CA, USA, 2019, pp. 1-10.

[16] TLP-1000 Series Transmission Line Pulse Generator. [Online]. Available: https://www.esdemc.com/products/system-level-esd-test/tlp-1000-series-transmission-line-pulse-generator/

[17] S. Bertonnaud, C. Duvvury and A. Jahanzeb, "IEC system level ESD challenges and effective protection strategy for USB2 interface," Electrical Overstress / Electrostatic Discharge Symposium Proceedings 2012, Tucson, AZ, 2012, pp. 1-8.

[18] J. Werner, J. Schutt and G. Notermans, "Common mode filter for USB 3 interfaces," 2016 IEEE International Symposium on Electromagnetic Compatibility (EMC), Ottawa, ON, 2016, pp. 100-104.

[19] G. Notermans, H. Ritter, B. Laue and S. Seider, "Gun tests of a USB3 host controller board," 2016 38th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Garden Grove, CA, 2016, pp. 1-9.

[20] M. Ammer, S. Miropolskiy, A. Rupp, F. z. Nieden, M. Sauter and L. Maurer, "Characterizing and Modelling Common Mode Inductors at high Current Levels for System ESD Simulations," 2019 41st Annual EOS/ESD Symposium (EOS/ESD), Riverside, CA, USA, 2019, pp. 1-7.

[21] S. Marathe et al., "On secondary ESD event monitoring and full-wave modeling methodology," 2017 39th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Tucson, AZ, 2017, pp. 1-6.

[22] S. Marathe et al., "Software-Assisted Detection Methods for Secondary ESD Discharge During IEC 61000-4-2 Testing," in IEEE Transactions on Electromagnetic Compatibility, vol. 60, no. 4, pp. 1129-1136, Aug. 2018.

[23] B. Orr et al, "A systematic method for determining soft-failure robustness of a subsystem," 2013 35th EOS/ESD Symposium, Las Vegas, NV, 2013, pp. 1-8.

[24] S. Vora, R. Jiang, S. Vasudevan and E. Rosenbaum, "Application level investigation of system-level ESD-induced soft failures," 2016 38th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Garden Grove, CA, 2016

[25] J. Zhou, Y. Guo, S. Shinde, A. Patnaik, , O. H. Izadi, C. Zeng, , J. Shi, J. Maeshima, H. Shumiya, K. Araki, and D. Pommerenke, “Measurement Techniques to Identify Soft Failure Sensitivity to ESD” accepted by IEEE Transactions on EMC, 2018

[26] O. H. Izadi, A. Hosseinbeig, H. Shumiya, J. Maeshima, K. Araki, D. Pommerenke, “Systematic Analysis of ESD-Induced Soft-Failures As A Function of Operating Conditions”, 2018 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), Singapore, 2018

[27] Python Data Analysis Library pandas: https://pandas.pydata.org/

[28] Stress-testing package stress-ng for GNU/Linux: http://manpages.ubuntu.com/manpages/artful/man1/stress-ng.1.html

[29] Driver message command dmesg for GNU/Linux: http://man7.org/linux/man-pages/man1/dmesg.1.html

[30] HPPI TLP System: https://www.hppi.com/

[31] Intel Joule Thermal Management Guide: https://software.intel.com/en-us/node/738005

VITA

Giorgi Maghlakelidze received B.S. degree in Electrical and Electronics Engineering from Ivane Javakhishvili Tbilisi State University, Tbilisi, Georgia in 2013. As a result of his research at EMC Laboratory, he received his Ph.D. degree in Electrical Engineering from Missouri University of Science and Technology, Rolla, MO, USA in May 2020.

In 2011-2013 Giorgi worked on numerical methods in electromagnetics as junior scientist in EMCoS Ltd, Tbilisi, Georgia. The year of 2016 was spent working as Signal Integrity Engineering Intern at Cisco Systems, San Jose, CA, USA. The work included developing high-speed SerDes characterization methodology, designing and characterizing high-speed networking backplane channels, invesitaging PCB glass-weave-induced skew. In the fall of 2018, he had interned with ESD Development group at Intel Mobile Communications GmbH, Neubiberg, Germany. The work and research were regarding soft and hard failure testing and automation, characterization of high-speed interfaces.

Giorgi's wide field of interest included electrostatic discharge, ESD soft failure characterization, signal integrity and EMI design in high-speed digital systems, numerical methods, computational electromagnetics, measurement methods and automation.

Mr. Maghlakelidze was a winner of the first place in the 2014 EMC Hardware Design competition held by the IEEE EMC Society. One of his works was nominated for best student paper at 2017 IEEE EMC Symposium.