Hardware and Software Combined Detection of System-Level ESD-Induced Soft Failures

Sandeep Vora, Rui Jiang, Prajwal Mysore Vijayaraj, Keven Feng, Yang Xiu, Shobha Vasudevan and Elyse Rosenbaum

Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, 1308 W. Main St. Urbana, IL 61801

Abstract – A semi-custom microcontroller is subjected to IEC-61000-4-2 ESD. A scan chain and memory read-out programs enable identification of the hardware blocks that experience soft failures. Voltage monitors are used to correlate the occurrence of those failures with the magnitude of noise on power supplies.

I. Introduction

Large currents and electromagnetic fields are generated by system-level electrostatic discharges (ESD). The fields can generate noise on signal traces. And, if the ESD current enters a signal pin of an integrated circuit (IC), the IO signal may become corrupted or noise may be generated on the IC's supply nets [1][2]. If the IC is powered-on at that time, the resulting noise may cause the IC to malfunction and data to become corrupt [3][4]. The noise can be detected and characterized with ESD monitors [5][6] and its effects seen at the software level [4][7].

Soft failures in ICs with computational capabilities can be monitored through software by running program suites that test the full functionality of the IC; this approach works in all but the most severe of cases, i.e., those in which system reset or hang occurs. Precise detection of hardware soft failures at the logic-level may be achieved through modification of the register-transfer level (RTL). By combining hardware noise detectors with RTL detection and software detection, a clear picture of physical, location-based vulnerability along with severity of a failure from a user perspective can be obtained.

This work presents a semi-custom microcontroller for ESD soft failure analysis. It includes hardware ESD monitors that measure noise on power supply busses [5][8]. The RTL was customized to produce status bits that give information about the execution of a program, for example, reporting whether the program counter is incrementing or an out-of-bounds memory address is encountered. Finally, the design includes a scan chain so that the contents of specific registers may be read out after an ESD event, allowing one to identify exactly which registers were affected by the ESD.

II. Test Chip

A. Overview

The microcontroller test chip was fabricated in a 130-nm technology. The test chip's layout is shown in Figure 1. Power is supplied through two on-board LDOs. The power supply for the IO circuits is 3.3 V (V_{DDIO}) and the other circuitry is connected to a low voltage supply that ranges from 1.2 V to 1.5 V (V_{DD}).

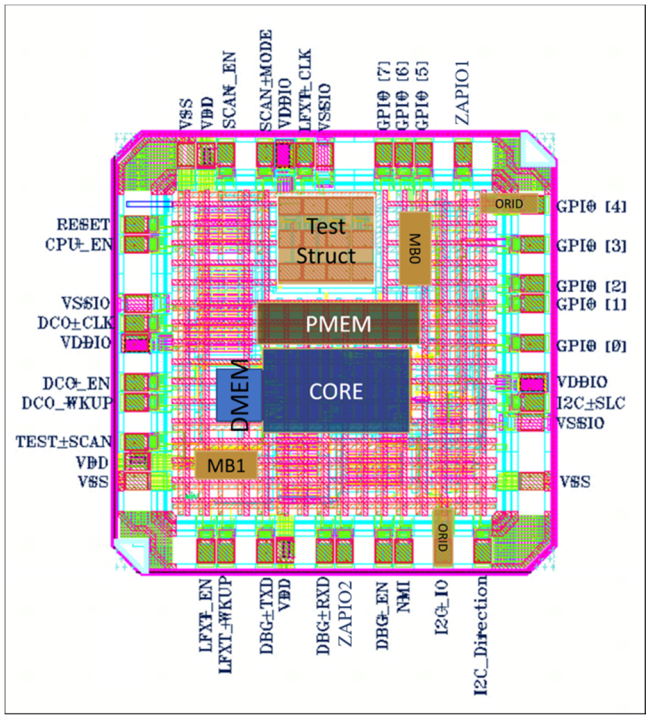

Figure 1: Chip layout view. MB0 and MB1 specify monitor bank 0 and 1, respectively.

There are three pad cells for each of V_{DDIO}, V_{SSIO}, V_{DD}, and V_{SS}, equally spaced along the edge of the chip. Each V_{DD} [V_{DDIO}] supply cell contains an active rail clamp with a single-stage trigger circuit; the trigger circuit was designed to respond to power-on ESD. The

ESD protection for each supply domain was designed to handle 8 kV HBM. The turn-on voltage of the single-stage rail clamp was reduced by adding a poly-resistor to the inverter, as shown in Figure 2. The RC trigger was designed for a 1 µs delay.

Each IO cell contains dual-diodes and secondary protection. Each input circuit contains a Schmitt trigger to enhance noise immunity. The Schmitt trigger circuits for the external clocks, DCO_CLK and LFXT_CLK, are sized to maintain the input duty cycle. The reset line is heavily filtered on board, with an additional 10 ns RC filter on-chip to minimize system resets from coupled noise. Two IO cells, labeled ZAPIO1 and ZAPIO2, are configured as "external pins" that are the ESD entry points.

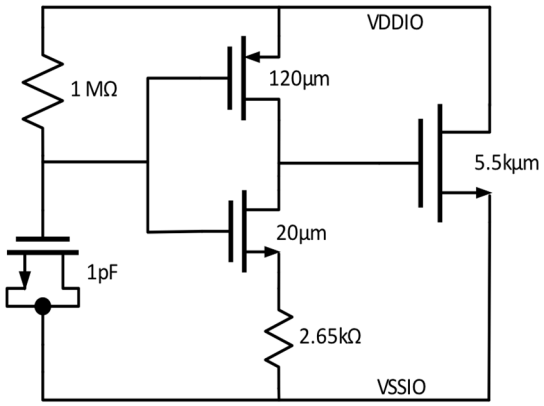

Figure 2 : Single-stage rail clamp with a switching threshold optimized for power-on ESD.

B. Microcontroller Core

The microcontroller core was synthesized using the RTL of the openMSP430 [9], an open source microcontroller which replicates many of the features of the commercial 16-bit MSP430 microcontroller. The circuit was synthesized for a main clock frequency of 100 MHz. A second clock at 32 kHz is used for GPIO communication. The synthesis was completed using ARM standard cells.

The microcontroller's CPU follows the Von Neumann model. It has a 27-instruction instruction set architecture (ISA) with an interconnected 3-state instruction pipeline for instruction decoding. The core incorporates sixteen 16-bit registers, four of which serve as the program counter, stack pointer, status register and constant generator. The remaining registers are general-purpose registers (GPRs).

On-chip memory consists solely of SRAM. The program memory (PMEM) stores program instructions and the data memory (DMEM) stores the results of the instructions. The PMEM cannot be modified by the program during its execution, effectively making it read-only. There are 4 kB of PMEM and 1 kB of DMEM.

C. Scan Chain

The core also features a scan chain, inserted during synthesis. This piece of hardware allows the user to serially shift a known set of values through the registers while simultaneously reading out the previously stored values. The chain is used to readout and reset registers between IEC discharges, which allows for the detection of ESD-induced bit flips. The scan chain can be read out even if the application crashes.

In normal operation, the scan chain is not enabled. In scan mode, the core is halted, and the set of registers used in normal operation are configured into one large shift register. This shift register is isolated from the core's logic circuitry while shifting in new data and reading out stored data. Approximately 1,500 bits are connected in the scan chain.

D. Noise Monitors

Two types of supply voltage monitors [5] are included on this test chip. The over-voltage (OV) monitor measures the peak positive excursion on a supply rail and the under-voltage (UV) monitor measures the peak negative excursion. Those monitors store the measured voltage for a time interval that exceeds the duration of an ESD event. The stored value is sampled by a 2-bit asynchronous ADC and saved in latches for later readout; a larger output code indicates a larger voltage excursion. A supply voltage monitor connected to the 3.3 V supply is denoted as HV and a monitor circuit for the 1.5 V supply is denoted as LV. Four supply voltage monitors—HVOV, HVUV, LVOV and LVUV — were placed in each of two monitor banks (MB0 and MB1), which were then put roughly on opposite sides of the chip (Figure 1). Standalone versions of the supply voltage monitors were placed on the chip for calibration purposes. The data are presented in Section IV.A.

Since the injected ESD current primarily returns to the circuit board via the IO's supply and ground pins, it is expected that HV monitors will have non-zero output readings following most ESD events. In contrast, the LV monitors will record supply noise only if the disturbance propagates from the 3.3 V supply domain to the 1.5 V supply domain through the anti-parallel diodes (APD) that link V_{SSIO} to V_{SS}, or if the ESD energy couples to the wire bonds of the V_{DD} or V_{SS} supply cells.

The monitor circuits' outputs can be read by the microcontroller core or the outputs can be sent directly to a GPIO pin for read-out.

E. RTL Monitors

The RTL of the openMSP430 core was modified to include six status bits:

1. Bit that alternates between 1 and 0 while the program counter (PC) is incrementing.
2. Bit that flips from 0 to 1 when the program finishes running.
3. Bit that flips from 0 to 1 if a PMEM address is out of bounds.
4. Bit that flips from 0 to 1 if a DMEM address is out of bounds.
5. Bit that flips from 0 to 1 if program runs longer than a programmed number of cycles.
6. Bit that flips from 0 to 1 when an error correcting code (ECC) module in the I^2C (a bus communication protocol) detects an error.

These status bits give insight into soft failures that would normally not be visible in an ordinary microcontroller or CPU. If the microcontroller core stops running a program following an ESD event, monitors 1 through 5 can help diagnose the cause. Monitor 1 is monitored before, during, and after the ESD event, while monitors 2 through 5 are read after each discharge to determine if the program ran correctly or stopped prematurely. However, due to the simplicity of the programs that are used in this study, it does not benefit from the extra debug capabilities

Similar to the voltage monitors, the RTL monitors can be read by the microcontroller's core as well as externally.

III. Test Board

The equipment under test (EUT) consists of a 4-layer FR4 circuit board, shown in Figure 3. The EUT was powered through a benchtop power supply. There are 3.3 V and (adjustable) 1.2-1.5 V power domains on the board, corresponding to those on the test chip. Sufficient decoupling capacitance (decap) is included on each of the power nets, and decaps of various sizes were placed around the chip following best practices. Probing of the on-board voltage rails showed only minor fluctuations during ESD, which are likely caused by the probe acting as an antenna.

Since the chip contains IOs intended for ESD testing, the board includes traces out to the edge. This is where the tip of the ESD gun is placed for a contact discharge to a signal line. For ease of testing, most control and data signals are routed through USB connectors (not using the USB protocol) to an external computer.

Both clocks are generated on board by crystal oscillators and are placed as close to the chip as possible to minimize noise coupled to the clock line. In scan mode, for synchronous data readout, the main clock needs to be a user-defined clock instead of the on-board crystal oscillator. A mechanical relay is used to switch between the user-defined clock and the crystal.

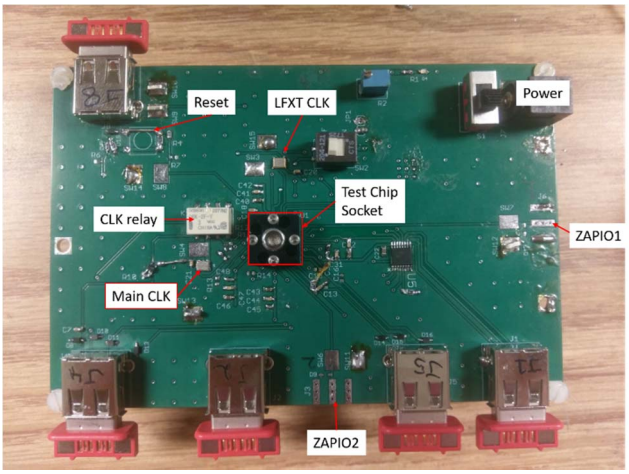

Figure 3: Board serving as the EUT.

IV. Measurement Results

A. Voltage Monitor Calibration

TLP testing of supply voltage monitor test circuits was performed to determine the range of supply voltage excursions that correspond to a particular output code. The current pulses have a 200 ps rise-time and a 2 ns pulse width. A bias-tee is used to inject the pulse onto the powered-up supply bus, and the supply bus voltage waveform is recorded.

In the full circuit, each voltage monitor's output is digitized by an ADC. The test structures do not include the ADC; instead, the output stage is a voltage follower that presents the same loading as the ADC. The voltage follower's transfer characteristic is known. Therefore, by measuring the voltage follower's output, we determine the amplitude of the voltage monitor's output signal for a given under- or over-voltage excursion on the supply. On the basis of those measurements, Table 1 and Table 2 are constructed to provide the mapping from a monitor circuit's output code to the peak amplitude of the supply noise. However, if the supply disturbance is of much shorter duration than the (vf)TLP pulse used in this experiment, then a larger disturbance is needed to achieve a given output than is indicated in the tables, due to the limited bandwidth of the voltage monitor.

Table 1: HV monitor calibration results. A supply voltage monitor's output code increases as a function of the magnitude of the supply voltage noise. The nominal value of V_{DD} is 3.3 V. V_{MIN} denotes the lowest value of V_{DD} (under-voltage) and V_{MAX} denotes the highest value of V_{DD} (over-voltage). Calibration is performed using 2 ns (vf)TLP.

HVUV	
V_{MIN} (V)	Output Code
$2.64 < V_{MIN} < 3.3$	00 (0)
$1.56 < V_{MIN} < 2.64$	01 (1)
$0.48 < V_{MIN} < 1.56$	10 (2)
$V_{MIN} < 0.48$	11 (3)
HVOV	
V_{MAX} (V)	Output Code
$3.3 < V_{MAX} < 3.57$	00 (0)
$3.57 < V_{MAX} < 4.51$	10 (1)
$4.51 < V_{MAX}$	11 (3)

Table 2: LV monitor calibration results. Nominal V_{DD} is 1.5 V. Calibration used 2 ns (vf)TLP.

LVUV	
V_{MIN} (V)	Output Code
$1.06 < V_{MIN} < 1.5$	00 (0)
$0.63 < V_{MIN} < 1.06$	01 (1)
$0.21 < V_{MIN} < 0.63$	10 (2)
$V_{MIN} < 0.21$	11 (3)
LVOV	
V_{MAX} (V)	Output Code
$1.5 < V_{MAX} < 2.06$	00 (0)
$2.06 < V_{MAX} < 2.15$	10 (1)
$2.15V_{MAX}$	11 (3)

B. ESD Test Results

ESD testing was performed using an IEC 61000-4-2 test bed with an IEC-compliant ESD gun. All tests were performed with the EUT powered-on.

1. Voltage Monitor Readings

The ESD gun was discharged into ZAPIO1 and ZAPIO2 at precharge voltages ranging from -4 kV to +4 kV. A minimum of 100 discharges to each ZAPIO for three different test chips and each precharge voltage were performed. After each discharge, the output of each monitor was read by the external computer. The scan registers were read out at the same time; those results are presented in the next section.

Table 3 and Table 4 list the mode — the value that occurs most often — of the noise readings from the supply voltage monitors at a given precharge voltage. The data shown in these tables were collected from the under-voltage and over-voltage monitors located in both monitor bank 0 and monitor bank 1.

Discharges to ZAPIO2 resulted in larger outputs from the HV supply noise monitors in MB1 than did discharges to ZAPIO1, while discharges to ZAPIO1 caused more noise to be seen by the HV monitors in MB0. These results are attributed to a proximity effect — ZAPIO1 is significantly closer to MB0 and ZAPIO2 is closer to MB1.

However, the LV monitors indicate that discharges to ZAPIO2 result in more noise on V_{DD} at both monitor banks. This can be attributed to ZAPIO2's proximity to a V_{DD} pin. As mentioned earlier, noise can be transmitted to the V_{DD} domain through the APD or by EM coupling. Magnetic coupling to a V_{DD} bond wire will induce voltage noise on the supply.

Overall, the supply voltage monitors report higher amplitude noise on the chip power supply for positive discharges. This polarity dependency is corroborated by the measurement data and circuit simulations in [5] and [10], both of which provide an analysis of the phenomenon.

Table 3: The response of voltage monitor circuits in MB0 and MB1 to ESD applied to ZAPIO1. The mode values are listed; 100 discharges for each precharge voltage were used to calculate that quantity. Vpre is the ESD gun precharge voltage. Monitor output codes range from 0 to 3, with larger values denoting a larger amplitude voltage disturbance.

	MB0				MB1			
Vpre [kV]	HVOV	HVUV	LVOV	LVUV	HVOV	HVUV	LVOV	LVUV
-4	3	2	1	1	1	2	0	1
-3	3	1	1	0	1	1	0	0
-2	3	0	0	0	1	0	0	0
-1.5	3	0	0	0	1	0	0	0
-1	1	0	0	0	1	0	0	0
-0.5	1	0	0	0	1	0	0	0
0.5	1	0	0	0	1	0	0	0
1	3	1	0	0	1	1	0	0
1.5	3	2	0	0	3	2	0	0
2	3	2	0	0	3	2	0	0
3	3	2	0	1	3	2	0	1
4	3	3	0	2	3	2	0	2

Table 4: Response of voltage monitor circuits in MB0 and MB1 to ESD applied to ZAPIO2. The mode values are listed.

	MB0				MB1			
Vpre [kV]	HVOV	HVUV	LVOV	LVUV	HVOV	HVUV	LVOV	LVUV
-4	1	2	1	1	3	2	0	1
-3	1	2	1	1	3	1	0	1
-2	1	1	1	0	3	0	0	0
-1.5	1	0	0	0	3	0	0	0
-1	1	0	0	0	1	0	0	0
-0.5	1	0	0	0	1	0	0	0
0.5	1	0	0	0	1	0	0	0
1	3	0	0	0	3	0	0	0
1.5	3	1	0	1	3	1	0	1
2	3	2	0	2	3	2	0	1
3	3	2	0	3	3	2	0	3
4	3	2	0	3	3	3	0	3

2. Noise on Clock and Reset Lines

As noted above, the registers in the scan chain were read out along with the voltage monitors. Three initial states for the scan chain registers were used:

1. Write all zeros into the scan chain.
2. Write all ones into the scan chain.
3. Write a pseudo-random, replicable, bit sequence into the scan chain.

This experiment is designed such that any observed bit flips in registers will not be the result of corrupted data having propagated from the peripheral inputs because those inputs cannot be received when the chip is in scan mode. The possible causes of bit flips are as follows. (1) On-chip supply noise, which exceeds the register's noise margin. (2) Glitches on clock that cause the shift register to advance. (3) Glitches on control signals (e.g., DGB_EN, NMI, SCAN_EN) that reset some of the registers. Glitches on clock and control signals may be caused by board-level coupling to their traces, or by noise on the chip-level IO supply, which moves the switching threshold of the input circuit [11].

Initial states 1 and 2 are intended to reveal whether the registers are more prone to flipping if initially set to 0 or 1. Additionally, tests performed with those initial

states reveal the number of bit flips that occur without obfuscation from clock shifts.

Initial state 3 is used to determine the number of ESD-induced clock shifts. Should any number of glitches occur on the clock line, more than 700 registers will have values differing from their expected values. By minimizing the count of differing values, the number of clock shifts and bit flips can be determined.

When the chip is operated in scan chain mode, the clock is vulnerable to more board-level noise coupling than under normal operating conditions. The clock to run the scan chain must come from an external source in order to synchronize the receiver and the transmitter. The board trace for the external clock is longer than that for on-board clock because the former terminates at a connector at the board edge. In contrast, the on-board clock generator was placed as close to the chip as possible (Figure 3), to minimize coupled noise. Additionally, a connection must be formed between the EUT and the controlling computer; the cable may couple additional noise where it is unshielded.

Recall, bit flips due to clock noise are easily detected after a pseudo-random bit sequence (initial state 3) has been stored in the scan chain. Figure 4 shows the probability of a discharge onto ZAPIO1 causing between 1 and 11 clock glitches at each precharge voltage. As expected, the number of clock glitches increases with the precharge voltage. In the worst cases, 10 clock glitches were observed for a given ESD. Next, discharges were applied to ZAPIO2; more clock glitches are seen in this experiment as indicated in Figure 5. This likely results from the closer proximity of ZAPIO2 to the external clock line.

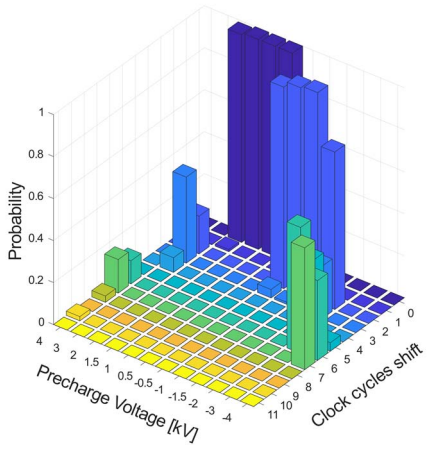

Figure 4: Probability of a discharge causing N clock shifts when board was set to use the external clock. Discharges performed to ZAPIO1 with the scan chain initialized with a PRBS pattern. Clock cycles shift refers to how many clock cycles were needed to shift the data to match the expected value.

Earlier, it was argued that the likelihood that ESD will cause clock glitches is lower under normal operating conditions in which the on-board clock is used. This assertion is confirmed by comparing Figure 6 with Figure 4 and Figure 5. The data in Figure 6 were obtained by removing the main crystal oscillator and tying the on-board clock pin low through a 10-kΩ resistor.

The reset signal is transmitted from an off-board source, making it also vulnerable to board-level noise coupling; however, large amounts of filtering help to mitigate glitches on RESET. Figure 7 presents the reset likelihood as a function of precharge voltage. The data are further separated by the number of clock glitches occurring after a reset. The number of clock glitches after a reset is determined by matching a shifted version of the scan chain's reset state to the post-ESD scan chain state. Resets are observed to occur only at high positive precharge voltages.

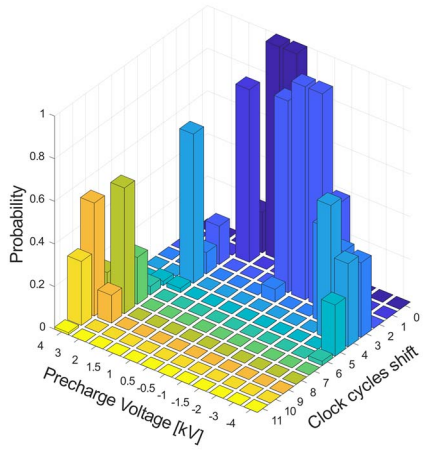

Figure 5: Probability of a discharge causing N clock shifts when board was set to use the external clock. Discharges performed to ZAPIO2 with the scan chain initialized with a pattern.

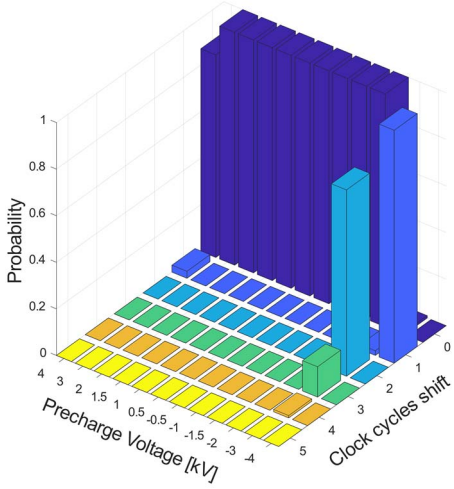

Figure 6: Probability of a discharge causing N clock shifts when board was set to use the internal clock. Discharges performed to ZAPIO1 with the scan chain initialized with a pattern.

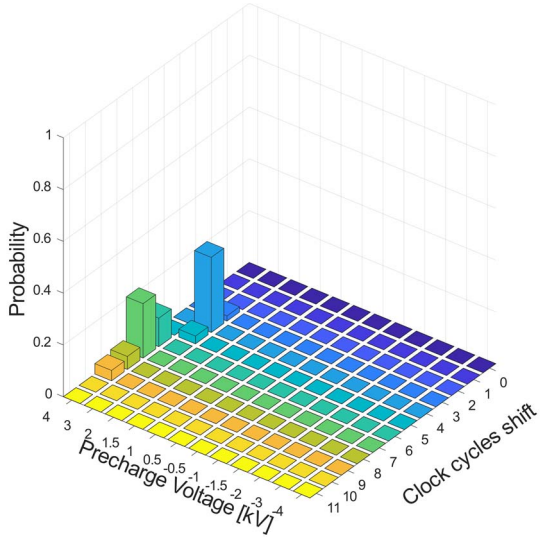

Figure 7: Probability of a discharge causing a reset *and* N clock shifts when board was set to use the external clock. Clock cycles shift refers to how many clock cycles were needed to shift the data to match the expected value. Same setup as for Fig. 4.

3. Bit Flips in Registers

By adjusting for clock glitches and excluding trials in which resets occurred, the number of bit flips for a given ESD event could be found. Figure 8 shows the number of trials in which a particular number of bit flips occurred. These are further organized by the precharge voltage at which the discharge occurred. It is observed that the number of bit flips is in the single digits for all precharge voltages other than +3 kV and +4 kV.

At +4 kV, the mode number of bit flips is approximately 200, which corresponds to a section of the scan chain being reset by glitches on control signals other than RESET (glitches on RESET would result in all the registers being reset). Similar section-wide register upsets were observed following +3 kV discharges, but with a reduced incidence. The large-scale upsets attributed to control signal glitches occur only for positive discharges. Since positive zaps have been shown to cause more on-chip noise, it is concluded that on-chip noise is the cause of those glitches. The registers that were upset are used in the following functional units in the CPU: DBG_UART, RTL monitor 1, interrupt request (IRQ), and the watchdog circuit.

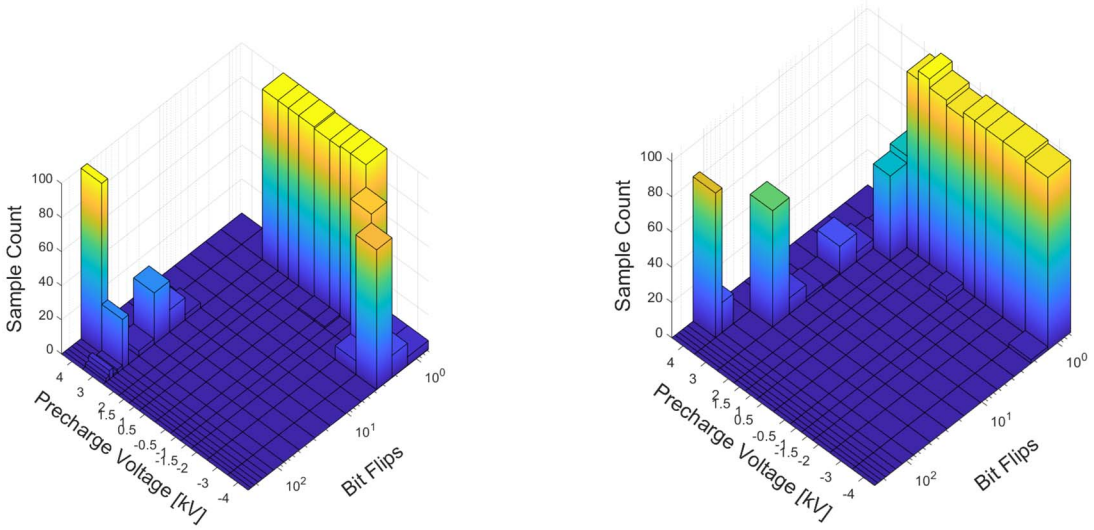

Figure 8: Number of trials at a given precharge voltage that resulted in a number of bit flips, after adjusting for clock glitches and removing trials where resets occurred, given an initial state of 0 for all registers in the scan chain. The number of bit flips were grouped in bins whose sizes increased logarithmically. The left-hand side shows bit flips caused by discharges to ZAPIO1. The right-hand side shows bit flips caused by discharges to ZAPIO2.

4. Operational Tests

In a second set of tests, simple programs were run during discharges into the ZAPIOs. These tests were designed to analyze the impact of ESD when logic, memory, and IOs are utilized. After each discharge, the contents of the SRAM, GPRs, and IOs were read via the UART debugger port by the external computer.

The debug unit often became unresponsive following discharges above 3 kV. The cause is diagnosed using the scan chain results presented in the last section. In the previous experiment, bit flips were frequently seen in the set of state registers for the debug unit. Those state registers determine what control signals the debugger uses to communicate with the external computer, and their corruption can disable communication with the debugger port. Since the debugging port is used to retrieve data during these tests, communication has to be re-established. The DBG_EN signal allows for resetting of this port while maintaining SRAM data integrity, a fact that the programs were written to take advantage of.

Three programs were developed to exercise different parts of the on-chip circuitry and provide insight about ESD-induced soft failures:

1. Program 1 sets every word of the DMEM to the value 0x1248. Afterwards, it infinitely loops to emulate a halted state during which a discharge is performed.
2. Program 2 sets all of the DMEM to the value 0x1248. Next, the program repeatedly iterates through the DMEM, reading out one word at a time into a temporary register and then writing it back to its original location in DMEM. The discharge occurs during the read/write operations.
3. Program 3 sets each GPR to a distinct known value. Each register is then used as a source and destination register for idempotent arithmetic operations. The discharge occurs during the arithmetic operations. Periodically, the contents of the registers are written into SRAM to preserve the data against a potential reset.

A minimum of 100 discharges were performed per test case and ZAPIO on each of four chips. To ensure that each program has finished initializing before an ESD, the test chip and external computer are synchronized.

a. Memory Tests

Programs 1 and 2 can reveal bit flips in DMEM. The occurrence of bit flips might differ significantly depending on which program is running. If that occurs, it can be concluded that the SRAM has a different susceptibility to ESD-induced data corruption when it is being accessed for read and write, relative to when it is not being accessed.

Each program was run in two test configurations. In the "1-trial reload configuration," the program is reloaded before the start of each experimental trial, thereby refreshing the PMEM. In the "10-trial reload configuration," the program is reloaded after every tenth trial. In the 10-trial reload test, if bit flips occur in PMEM, erroneous instructions potentially may be executed in subsequent trials. Recall that the PMEM of the test chip cannot be modified (written) during program execution; PMEM gets written to only when the program is loaded.

No bit flips in SRAM were observed when V_{DD} was 1.5 V for discharge levels up to ±5 kV at either ZAPIO. By comparing this finding to the results of the scan chain tests, one concludes that the SRAM is more immune to ESD-induced noise than are the registers. However, when V_{DD} was reduced to 1.2 V, bit flips were seen for +5 kV discharges to ZAPIO2. No bit flips in memory were observed following +5 kV discharges to ZAPIO1. This finding is consistent with the voltage monitor readings in Tables 3 and 4. The LVUV readings indicate that discharges at ZAPIO2 cause more supply droop than those at ZAPIO1.

Table 5: The table summarizes memory bit flip occurrences across three chips while program 1 was running in the 1-trial reload configuration. +5 kV discharges onto ZAPIO2 were performed with V_{DD} at 1.2 V. Incidence indicates the fraction of trials in which a particular number of bit flips occurs.

Total number of bit flips per trial	Incidence
1	0.12
2	0.07
3	0.31
4	0.01
5	0.01
6	0.33

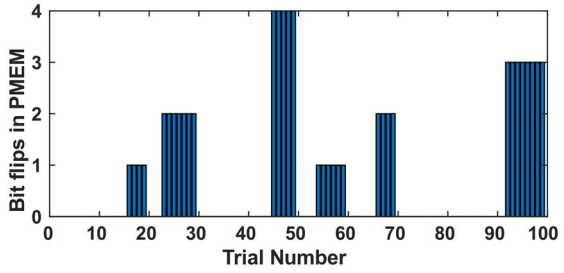

Figure 9: +5 kV discharges into ZAPIO2 with V_{DD} = 1.2V; program 1 was running in the 10-trial reload configuration. The bit flips in PMEM are retained until it is refreshed. The zaps were performed in increasing order of trial number.

Three chips were each subjected to 100 zaps at +5 kV while running program 1 in the 1-trial reload case.

Bit flips were identified by comparing the memory contents with a baseline (pre-ESD) readout of the complete memory space. Table 5 shows the incidence of bit flips in memory observed for an aggregate of the data. In one chip, there is a word in the DMEM that gets upset in each trial; more specifically, six SRAM cells in close proximity get upset. This results in a 33% rate for 6 bit flips, when aggregated across three chips, as shown in the table. Single bit flips occur in random locations at a rate of 0.6% and at consistent locations ("weak" cells) at a rate of 11.3%.

"Weak" cells that consistently get upset by ESD noise are attributed to process variations. For example, a mismatch between the transistors in a SRAM cell will reduce its noise margin, making the cell more vulnerable to supply variations.

Weak cells may have a preferred state, either 0 or 1, due to asymmetric noise margins. Recall that in the 10-trial reload configuration, the PMEM is restored to its original state only once every 10 trials. Once an SRAM cell gets disturbed due to noise, it may enter a preferred state after which the probability of it switching in the opposite direction is low. Therefore, it is expected that the number of PMEM bit flips observed per trial in the 1-trial reload configuration will be greater than that observed in the 10-trial reload. This conjecture is supported by the data shown in Figure 9; the erroneous bits are retained until the program memory is refreshed again.

The incidence of bit flips in DMEM did not vary significantly based on whether program 1 or program 2 was being executed. Despite program 2 being more complex, bit flips in PMEM did not, in most cases, interfere with its execution. In a small fraction of trials, bit flips in PMEM caused program 2 to write erroneous data into the DMEM due to the execution of incorrect instructions. This was established by looking at a temporal distribution of bit flips in both DMEM and PMEM. The large number of bit errors in DMEM were cleared after the PMEM was refreshed.

The SRAM cells are believed to be disturbed due to the undershoot in VDD with respect to VSS that occurs at high positive precharge levels. This may lead to a temporary loss of charge at the storage nodes of an SRAM cell. The cell may then flip its state after the power supply is restored depending on the asymmetry of the cross-coupled inverters.

b. ALU Tests

Program 3 is designed to investigate if ESD can corrupt arithmetic operations. ESD might affect the source or destination locations, or the ALU itself. +5 kV discharges were performed while program 3 was running. There were observable bit flips in the output of the ALU on three test chips denoted as A, B, and C. However, those bit flips were not a result of the GPRs or the ALU getting upset during operation. Instead, the PMEM was corrupted and all incorrect values in the registers could be traced back to the bit flips in PMEM.

Table 6: 5 kV discharges onto ZAPIO2 with V_{DD} = 1.2 V. The table lists the percentage of trials in which bit flips occurred in PMEM and the number of instructions that were corrupted in a given chip.

Test Chip	Percent of trials with flips in PMEM	Number of instructions with a bit flip in its MSB
A	100%	8
B	1%	1
C	100%	3

On test chips A and C, multiple instructions in PMEM are upset in every single trial. The addresses of those instructions are close to each other. In all cases, only the most significant bit of the instruction flipped. The bit flips for the most significant bits were observed to be bi-directional. The set of instructions that get upset on chip C are a subset of those that get upset on chip A. Test chip B did not demonstrate the same high frequency of bit flips in PMEM, but it also shared a bit flip with chips A and C. These results suggest that certain locations in the PMEM are most susceptible to ESD, perhaps being close to a noise source. The results are summarized in Table 6.

c. IO Glitches

While executing the above described programs, the contents of the GPIO registers were read out. For discharges above +3 kV, the bits stored in the GPIO receive and transmit registers are corrupted in every trial. This provides an indication of the stress level at which non-zap pins experience logic-level glitches due to coupled noise.

V. Conclusions

This work presents a custom test chip with a microcontroller core. Using both hardware voltage monitors and tailored programs, the mechanisms for soft failures caused by ESD are explored.

Clock glitches have an increasingly high likelihood of occurring as the ESD level increases, reaching near 100% occurrence at -4 kV in this work (Figure 6). This observation is of two-fold significance. First, although on-chip filters can effectively remove glitches from off-chip inputs (e.g., for the global reset signal), the clock is a high frequency input that would be adversely affected by low-pass filtering. Second, clock is a global signal that critically affects the operation of an entire chip. Without significant on-chip filtering, any peripheral input signal has a high probability of

experiencing glitches that lead to soft failures, as indicated by the data of Figures 7 and 8 and corroborating the findings in [11] [12].

Even if input glitches are rejected, however, bit flips in SRAM and registers may still occur. Spontaneous bit flips in registers, i.e., those that cannot be clearly attributed to spurious control signals, were observed to occur at a rate of at least 20% for zaps at ±4kV.

The SRAM proved to be more robust against soft failure than the registers. A small incidence of bit flips in registers was detected even at stress levels below ±3 kV, while it required discharges of +5 kV and a supply voltage reduction to 1.2 V for any SRAM bit flips to become manifest. This indicates that ICs have an increased susceptibility to ESD-induced soft failures as the supply voltage is decreased. At the highest stress level, most of the test chips had certain memory cells that upset consistently. These are termed "weak cells" and are believed to be memory cells that have a reduced noise margin due to process variations. The fraction of cells in the memory array that are "weak" is estimated to be about 0.025% in this study.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. 1526106. The authors would like to thank Mr. O. Girard for design of the open source core and useful discussions. We also thank Dr. Karan Bhatia of Texas Instruments for discussions about microcontroller design.

References

[1] R. Mertens, N. Thomson, Y. Xiu and E. Rosenbaum, "Analysis of active-clamp response to power-on ESD: power supply integrity and performance tradeoffs," *IEEE Trans. Device Mater. Rel.*, vol. 15, no. 3, pp. 263-271, 2015.

[2] Y. Xiu, N. Thomson, R. Mertens, C. Reiman and E. Rosenbaum, "Chip-level ESD-induced noise on internally and externally regulated power supplies," *EOS/ESD Symposium Proc.*, 2017.

[3] JEDEC, "System level ESD part 1: common misconceptions and recommended basic approaches," JEP-161, 2011.

[4] S. Vora, R. Jiang, S. Vasudevan and E. Rosenbaum, "Application level investigation of system-level ESD-induced soft failures," *EOS/ESD Symposium Proc.*, 2016.

[5] N. Thomson, C. Reiman, Y. Xiu and E. Rosenbaum, "On-chip monitors of supply noise generated by system-level ESD," *EOS/ESD Symposium Proc.*, 2017.

[6] A. Patnaik et al., "An on-chip detector of transient stress events," *IEEE Trans. Device Mater. Rel.*, vol. 60, no. 4, pp. 1053-1060, 2018.

[7] P. Maheshwari, T. Li, J. S. Lee, B. S. Seol, S. Sedigh and D. Pommerenke, "Software-based analysis of the effects of electrostatic discharge on embedded systems," *IEEE Annual Computer Software and Applications Conference Proc.*, pp. 436-441 2011.

[8] R. Mertens, "Understanding, modeling, and mitigating system-level ESD in integrated circuits," PhD Thesis, University of Illinois at Urbana-Champaign, 2015.

[9] O. Girard, https://opencores.org/project, openmsp430, 2009.

[10] Y. Xiu, "Failures caused by supply fluctuations during system-level ESD," PhD Thesis, University of Illinois at Urbana-Champaign, 2018.

[11] N. Thomson et al., "Custom test chip for system-level ESD investigations," *EOS/ESD Symposium Proc.*, 2014.

[12] N. A. Thomson, Y. Xiu and E. Rosenbaum, "Soft-failures induced by system-level ESD," *IEEE Trans. Device Mater. Rel.*, vol. 17, no. 1, pp. 90-98, 2017.