Analysis of Proton-induced Single Event Effect in the On-Chip Memory of Embedded Processor

Analysis of Proton-induced Single Event Effect in the On-Chip Memory of Embedded Processor

Corrado De Sio, Sarah Azimi, Luca Sterpone
Dipartimento di Automatica e Informatica (DAUIN)
Politecnico di Torino
Turin, Italy
{corrado.desio, sarah.azimi, luca.sterpone}@polito.it

David Merodio Codinachs
European Space Agency (ESA)
European Space Research and Technology Centre
Noordwijk, The Netherlands
david.merodio.codinachs@esa.int

***Abstract*— Embedded processors had been established as common components in modern systems. Usually, they are provided with different types and hierarchical levels of memory, some of them integrated into the same chip (on-chip memory). Due to the high density of transistors, memories are known to be particularly sensitive to soft errors. Soft errors afflicting memories can manifest in various forms besides traditional single-bit value corruption. In this paper, a comprehensive description of radiation-induced effects detected in the SRAM on-chip memory of an ARM Cortex-A9 MPCore during a proton-beam test is performed. The experimental setup, data acquisition methodology, and observed effects are reported in detail including a cross-section for different energies. Fault models for system-level reliability evaluation are proposed, complete with their distribution. Finally, the proposed fault models are used in fault injection campaigns on a software benchmark suite and results are discussed.**

***Keywords*—Burst Events, Fault Model, On-Chip SRAM, Proton Test, Radiation Effects, Reliability, SEE, SEU, SoC, Zynq.**

I. INTRODUCTION

In recent years, embedded processors have been characterized by enormous success, thanks to the emergence and establishment of ubiquitous computing. This success soon extended even to fields where safety is a concern. Automotive, space exploration, healthcare, and avionics are only a part of the industries that can take advantage of the technological advancements of embedded processors and more in general of system-on-chips (SoCs) and Commercial-Off-The-Shelf (COTS) components. In particular, systems-on-chips are integrated circuits where different components are embedded in the same chip. The advantages provided by such solutions are various, such as smaller size and higher performance especially thanks to the strong coupling between components, supported by on-chip communication. However, the adoption of these devices in mission-critical applications is still subject to their reliability, which must be evaluated in detail. Indeed, the continuous increase in miniaturization, frequency, and integration made them increasingly susceptible to soft errors.

Soft errors are events caused by factors external to the device that does not damage permanently the device but introduce a transitory error. They can be induced by various effects, such as noise and radioactive particles and they have been exacerbated by the increase of transistor density and lowage of voltage working values. Radiation-induced soft errors are caused by the interaction between radioactive particles and the electronic circuit silicon. The energy released in the electronic by the physic interaction may lead to various transitory effects such as Single Event Upset (SEU), Single Event Multiple Upset (SEMU), or Single Event Functional Interruption (SEFI) producing system misbehavior and data corruption [1]. Additionally, the scaling down of transistor size made radiation effects a concern even at ground level, stimulating interest in them also for industries other than avionics and space missions such as automotive and healthcare. Memory is one of the main components of modern SoCs but it is also very susceptible to these events due to their high transistor density. Given the integrated nature of SoCs and COTS, the analyses of their components, such as memories, need to consider the role that a component play in the system and how they are interfaced, connected, and used by other modules in order to enable a more comprehensive evaluation of how the faults affecting a single component contributes to the overall reliability of the whole system.

Usually, the evaluation of the radiation sensitivity of a memory component is based on electrical and physical simulations and radiation testing. However, the availability of COTS systems allows extending the reliability evaluation to a higher level, evaluating directly the error that propagates from memory to the system level (e.g., to the processor system). The detection of patterns of errors and thus the definition of fault models related to the specific system architecture and system-level allows for a more comprehensive analysis and mitigation approach. In particular, On-Chip SRAM (OCM) is an important integrated component of embedded processors and systems-on-chip. Indeed, radiation-induced effects can corrupt either data or code stored in memory leading to errors, exceptions, and failures. Many works have evaluated the sensitivity of SRAM memories to radiation effects. However, rarer is the analysis dedicated to evaluating faults affecting the on-chip memory of embedded processors considering the effect on the whole system, especially on the processor side. Additionally, the vast majority of works have focused only on SEUs and to a lesser extent on the SEMUs. More complex faults (e.g., memory resets, writing errors, memory locations stuck-ats) are rarely considered or evaluated.

A. Main Contributions

This work proposes two contributions. The first is the comprehensive analysis of the events observed on the on-chip SRAM memory of an ARM Cortex-A9 embedded processor during a proton test. In particular, the evaluation methodology is detailly reported and resulting events are categorized, analyzed, and discussed. Secondly, a set of fault models deriving directly from the radiation experiment are proposed. The proposed fault models describe and categorize radiation-induced errors as observed on the processor side during the proton beam test. They provide a valuable characterization of the events affecting the on-chip memory as they manifest from the processor side to enable realistic fault emulation, fault injection, and simulation analyses

useful for preliminary reliability evaluation or when a radiation test is not a viable solution. The proposed fault model suite is adopted in fault injection campaigns evaluating their effect on a group of four software applications running on a system-on-chip device.

To the best of our knowledge, while significant numbers of works are dedicated to the analysis of memories used by embedded processors, no work focuses on an analysis of the SEE effects in the integrated on-chip SRAM of embedded processors taking into account the fault models observed by applications running on the system rather than on SEUs and bit event cross-section only.

The paper is organized as follows: Section II reports previous works dedicated to the radiation sensitivity of embedded processors and system-on-chips. Section III describes the radiation test experiment and the obtained results. Section IV illustrates the proposed fault models. Section V exposes a comparison between fault injection campaigns using proposed fault models and the SEU fault model. Finally, Section VI contains conclusions and discussions on further works.

II. Related Works

Several works investigated the characterization and reliability against ionizing radiation of SRAM memories, as well as hard and soft microprocessors, including system-on-chip solutions. However, most works are dedicated to the system-on-chips as a whole without considering the specific contribution of the on-chip integrated SRAM component. Additionally, most of the efforts in the analysis of Zynq SoC memories focus only on the configuration memory of the device, associated with the programmable hardware part, without considering the processor system and its memory. About the characterization of SRAM memories, the authors in [2] and [3] provided a detailed characterization of SRAM memories considering the potential for being used as flux and particle detectors in the monitoring system of LHC of CERN. The work presented in [4] is dedicated to evaluating an SRAM COTS device irradiated with low-energy protons and neutrons. In [5], the authors provide a characterization of four memory devices implemented in different technologies in the range between 0.13 and 0.25 micrometers.

For what concerns microprocessors, reliability analysis is traditionally based on fault injection campaigns, radiation testing, or emulation. A RISC-V soft microprocessor has been evaluated by the authors at [6] against SEU affecting the two SRAM memories (i.e., configuration memory and BRAMs) of the hardware platform using fault injection. In [7], the impact of neutron-induced faults affecting an external DRAM used by an embedded processor running a convolutional neural network application is evaluated. The occurrence of single event upset, stuck-at errors, and block errors is reported. In [8], fault injection campaigns at the software level have been performed on the different software application, based on fault models including various SEE involving memory control circuitry too. The authors of [9] provide the results from neutron testing of a set of ARM processors and microcontrollers, including Zynq. It is asserted that Zynq reported an SEU cross-section comparable to traditional SRAM analysis. SEFI events leading to multiple SEUs in memory have been detected and recoverable only through a power cycle. A hybrid approach based on software fault injection for modeling SEUs affecting SRAM memories storing neural networks weights and SEU emulation for modeling hardware faults in neural-networks-dedicated hardware processors have been introduced in [10], and finally extended and completed in [11].

Only a few works have considered OCM. Authors of [12] performed an analysis of ARM Cortex A9 under proton irradiation. The characterization focuses on SELs, SEFIs, and SEUs, in the processor unit through software output analysis. However, no information is provided on the evaluation or cross-section of SRAM memories. In [13], the authors discuss experimental data on the heavy-ion irradiation of a COTS low-cost microcontroller, including an SRAM dynamic analysis, but reported events are limited to SEUs cross-section. Works presented in [14] and [15] analyze the memories composing the Zynq SoC, such as BRAMs, configuration memory, and OCM, against heavy-ions the former, and heavy-ions and protons the latter. A tentative of relating OCM errors with other components in SoC is presented in [16].

III. Proton Test Analysis

A proton test analysis has been performed at the Paul Scherrer Institute (PSI) Proton Facility. The experiment has been conducted by irradiating a Zynq-7020 system-on-chip with energies in the range of 16 and 200 MeV. Figure 1 shows the device in the irradiation room. The content of the on-chip SRAM memory has been continuously monitored through a software routine running on an ARM Cortex A9.

A. Test Platform and Testing Software

The hardware platform under test is a commercial PYNQ-Z2 board embedding a Zynq-7020 system-on-chip. The processor system of the Zynq-7020 consist of an ARM Cortex-A9 MPCore. A 256 KB SRAM memory is integrated into the same chip and connected with the processor through the Snoop Control Unit (SCU). The programmable hardware available on the Zynq-7020 has not been used during this test, but it has been monitored through a readback procedure. The on-board DDR memory (not directly irradiated) has been chosen for storing the test program in order to minimize the source of errors external to the SRAM memories (e.g., processor halting and code corruption). Caching was disabled to observe events occurring directly in SRAM memory through reading and writing of the memory content.

A software test routine executes continuously on the processor system, reading and writing the memory content.

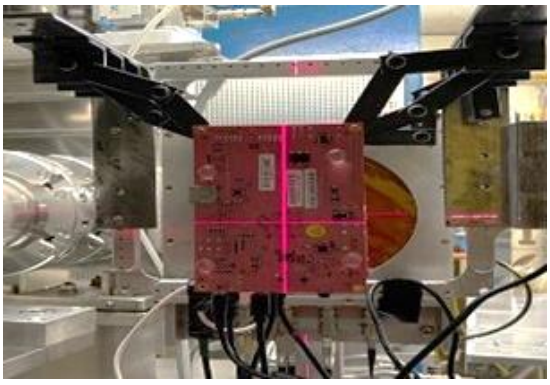

Fig. 1: Board exposed to the protons beam in the irradiation room.

The pseudo-code of the software routine is illustrated in Algorithm 1.

Algorithm 1 Online Test Routine

```
Initialization:
pattern_even ← all 0s, pattern_odd ← all 1s;
for each addr in memory_addresses do
    if addr is even then
        call write_mem at addr with pattern_even
    else:
        call write_mem at addr with pattern_odd
    end if
Test process:
while True do
    for each addr in memory_addresses do
        if addr is even then
            call check_value at addr with pattern_even and notify errors
            call write_mem at addr with pattern_odd
            call check_value at addr with pattern_odd and notify errors
        else:
            call check_value at addr with pattern_odd and notify errors
            call write_mem at addr with pattern_even
            call check_value at addr with pattern_even and notify errors
        end if
    end for
    call swap pattern_even with pattern_odd
end while
```

The routine writes new values in the memory, checking if the value written during the previous test loop has been corrupted. Additionally, it verifies that the current value has been written correctly and can be read correctly. When an erroneous value is detected, it is notified to a host computer connected through a serial connection. The software routine can identify both SEFI errors (e.g. a memory cell cannot be written or read correctly anymore) and soft errors, such as SEU and SEMUs.

B. Test Methodology

The board has been mounted on an adjustable frame in the irradiation room. The host computer running the experiment manager was placed in the control room and connected through a serial connection for collecting results and performing soft reset and programming the microprocessor with the executable code at the start and after the soft reset was needed. A power switch was present in the control room allowing to perform a manual power cycle if needed.

The design has been tested using different energy and fluxes. Table I reports the test conditions in the radiation test. for different energies.

TABLE I. RADIATION TEST CONDITIONS: ENERGY, FLUX AND FLUENCE.

Energy [MeV]	Flux [$cm^{-2}s^{-1}$]	Fluence [cm^{-2}]
16.04	$1.89 \cdot 10^{7}$	$2.17 \cdot 10^{10}$
29.31	$4.12 \cdot 10^{7}$	$1.70 \cdot 10^{11}$
50.80	$4.02 \cdot 10^{7}$	$1.94 \cdot 10^{11}$
69.71	$4.11 \cdot 10^{7}$	$6.70 \cdot 10^{10}$
101.34	$4.32 \cdot 10^{7}$	$1.86 \cdot 10^{11}$
151.18	$4.09 \cdot 10^{7}$	$1.23 \cdot 10^{10}$
200	$4.14 \cdot 10^{7}$	$1.97 \cdot 10^{11}$

The test routine executes on the hardware platform. It continuously reads and writes memory. The test routine periodically sends reports to the host computer about detected events (including memory addresses, type of event, occurring time, and erroneous values). On the host side, an experiment manager collects the information on the detected events and evaluates if the software routine is correctly running. If the test routine stops running, (e.g., as a consequence of microprocessor halting due to radiation effect) a soft reset is performed. If the device is not recovered by soft reset, a power reset was performed. Additionally, a soft reset and eventually, a power cycle is performed even when an unrecoverable error is detected (e.g., memory locations that cannot be written or read anymore, or device unavailability).

C. Proton Test Results

Radiation-induced events affecting on-chip SRAM memories have been evaluated. In this subsection, an overall report of events and bit cross-sections is provided. A finer classification of the detected events and their cross-section is reported in Section IV, along with the fault models associated with each event category. In Figure 2, the cross-section of detected Single Event Effects is reported. Events causing multiple errors (e.g., SEMUs or Burst Events) contribute as a single event to the SEE cross-section. Differently, in Figure 3, the cross-section of bit events is reported. In this second analysis, each radiation-induced modification of a bit value contributes to the bit cross-section value. The drop in the cross-section value visible in Figure 3 is due to the no occurrence of burst events at 150 MeV that heavily contribute to the bit error cross-section. Even if no burst event has been detected at 150 MeV, we think it is reasonable (coherently with other radiation test experiments [7]) to assume that these events could occur at these energies as well.

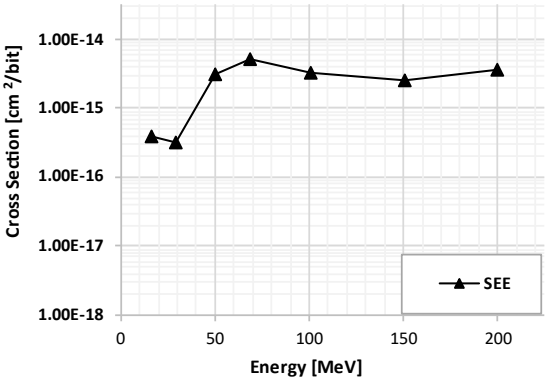

Fig. 2: SEE cross section of Zynq SRAM on-chip memory.

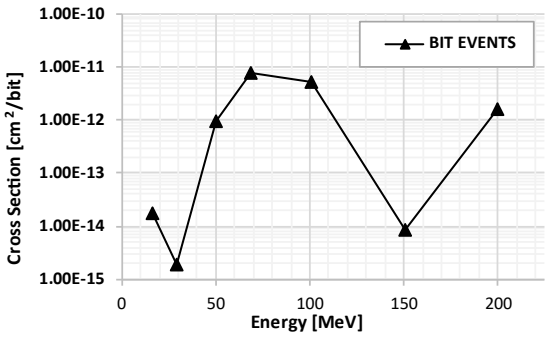

Fig. 3: Bit Error Cross section of Zynq SRAM on-chip memory.

IV. Fault Models

A detailed analysis of the events detected on the on-chip SRAM memory from the processor system side during radiation test experiments has been performed. In the current section, a set of fault models is proposed and discussed based on the effect detected in on-chip SRAM from the processor system side. These fault models provide a characterization of the events affecting the on-chip memory from the processor side to be used during reliability analyses based on simulation analysis, fault injection campaigns, and fault emulation. These methodologies can benefit from a realistic model of faults providing valuable data to be used as preliminary analysis in preparation for later radiation experiments or when radiation testing is not feasible.

A. *Single Event Upset*

An SEU causes a bitflip in the value stored in a memory cell. It has been the most observed event during the radiation experiment. Figure 4 reports the SEU cross-section during the different proton energy experiments. Cross-sections of radiation-induced transitions from 0 to 1 and from 1 to 0 have been also analyzed, showing similar ratios and distributions.

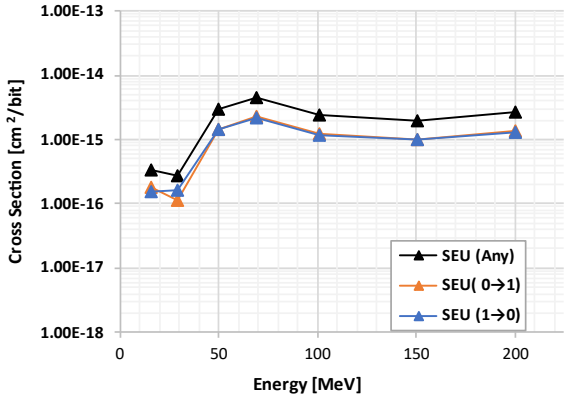

Fig 4: SEUs Cross Section of Zynq SRAM on-chip memory.

B. *Single Event Multiple Upsets*

A SEMU is a multiple event. It has been identified as a group of SEU occurring close in time and space. It has been the second most observed event. SEMU cross-section is reported in Figure 5. As for SEUs, faulty transitions showed similar ratios and cross-section values.

It is interesting to notice that SEMUs, in almost all the detected events, affected the same significant bits of some equally distanced memory words. To elaborate more, when a SEMU was detected in two or more memory words, the in-memory distance (i.e., the offset between the address of the locations) was constant among the locations affected by the same event (but it can vary for different events) and the same significant bit was corrupted. Occurrences of SEMUs affecting multiple bits of a single memory word have not been observed. The memory distance among words affected by SEMUs showed some recurring cases. An overview is reported in Table II. The number of different words affected by a single SEMU has been evaluated and the normalized occurrence of the number of different words affected by a single event but causing multiple upsets is reported in Figure 6.

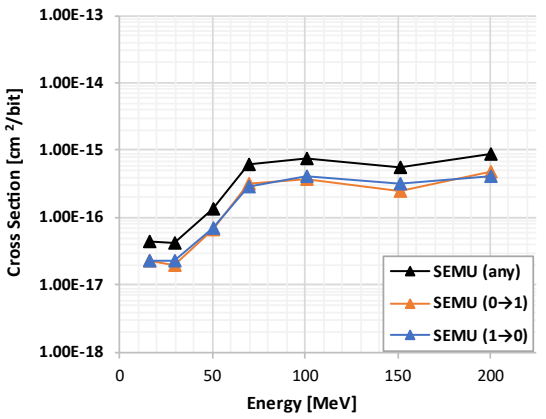

Fig 5: SEMUs Cross Section of Zynq SRAM on-chip memory.

Table II. Normalized Occurrence of In-Memory Distance of Bits Affected by Single Event Multiple Upsets

Address Offset of Bitflips in a SEMU	Normalized Occurrence
128	0.61
4	0.12
124	0.06
132	0.03
16	0.01
256	0.01
Others	Less than 0.01 each (0.16 total)

C. *Burst Events*

During the proton test, Burst Events occurred at a much lower rate than SEUs and SEMUs. However, they affected a large number of memory locations, corrupting many memory bits and words at once. Some burst events (referred to here as burst stuck-at) also prevent the memory to be read or written correctly, leading to SEFIs. A power cycle has been needed for returning to nominal behavior. We want to emphasize that the routine was able to distinguish burst events from Single Event Latch-up. In particular, burst events were only limited to a subset of the memory space, and usually (except for Burst Stuck-at) the memory continued to work normally in the following check loops of the software test routine.

1) *Burst Clear/Set*

As a result of an event, a large group of memory locations is corrupted. The affected bit value is now all 0s (clear) or all 1s (set). The memory is still working and can be written and read normally but the content is lost.

2) *Burst Errors*

As a result of an event, a large group of memory locations is corrupted. The event is similar to numerous bitflips affecting the memory.

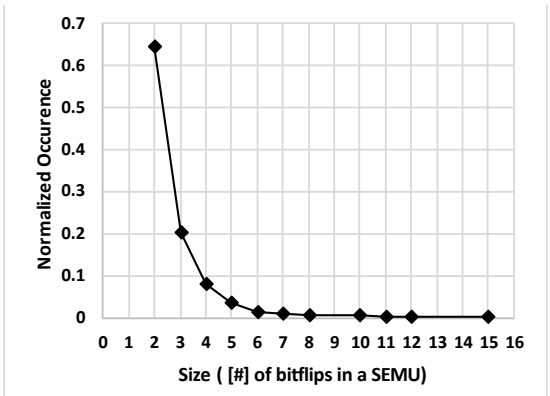

Fig 6: Normalized occurrence of different SEMU Sizes

3) Burst Stuck-at

As a result of an event, a large group of memory locations is corrupted. The event is similar to a Burst Clear/Set model but in addition, the value is stuck and writing operations have no visible effects. The distribution of the different burst events is illustrated in Figure 7. Few burst events have been observed compared to SEUs and SEMUs. The number of memory locations affected in a burst event has been found to vary. A general overview is provided in Table III. We would like to emphasize that although no burst event has been detected at 150 MeV, we believe it is reasonable that these events can occur at these energies as well. They did not occur during our experiments and this does not allow us to estimate a statistically significant cross-section value at this energy.

TABLE III. NORMALIZED OCCURRENCE OF THE NUMBER OF AFFECTED MEMORY LOCATIONS INVOLVED IN A BURST EVENT

Number of Affected Memory Locations	Normalized Occurrence
Less than 1000	0.16
Between 1000 and 10,000	0.62
More than 10,000	0.22

V. FAULT INJECTION ANALYSIS

In order to analyze the impact of the detected fault models on software applications, a group of fault injection campaigns has been executed. Four different bare-metal software applications have been evaluated. A fault injection campaign has been executed for each software application and proposed fault model pair.

A. Hardware Setup

As a hardware platform, the same system-on-chip used in the radiation test and already described in section III-A has been adopted. However, during the fault injection campaigns, the ARM core executes the software application under evaluation, and fault models are emulated in the on-chip SRAM memory where the program is loaded and stored to be executed. The fault emulation process is managed by an experiment manager running on a host computer connected by a serial link to the board.

B. Software Applications

Four different software applications have been evaluated against proposed fault models in the fault injection campaigns. They are:

MatMul: a group of squared matrices is multiplicated column by row. The resulting matrices are sent through the output channel.

Sobel: Sobel edge detection algorithm is performed on an input image. The resulting image is sent through the output channel.

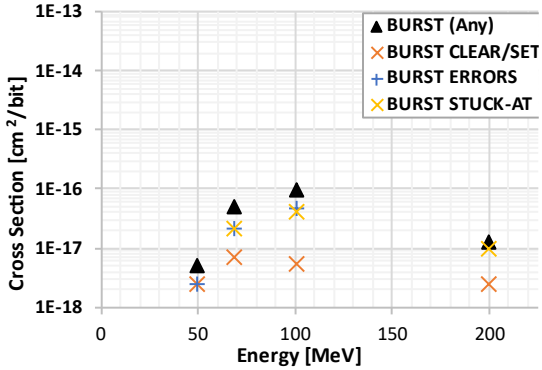

Fig 7: Burst Events Cross Section of Zynq SRAM on-chip memory.

Dijkstra: Dijkstra's algorithm is adopted for finding the shortest paths between two nodes in a graph. The paths and their costs are sent through the output channel.

Dhrystone: Dhrystone is a synthetic computing benchmark. It performs string processing tasks.

Table IV reports the in-memory size of the software applications.

TABLE IV. OVERVIEW OF THE SOFTWARE APPLICATIONS

Software Application	In-memory Size [bytes]
Matrix Multiplication	32,816
Sobel Edge Detection	49,260
Dijkstra Minimal Path	50,136
Dhrystone	59,564

C. Fault Injection Methodology and Fault Models

The fault injection campaigns have been executed by injecting fault models under evaluation in the on-chip SRAM memory. Each software application presented in section V-B has been evaluated against the suite of fault models reported in section IV. The PyXEL framework [17] has been extended for supporting SRAM memory fault injection. In particular, an experiment manager running on a host computer is in charge of generating the fault location and emulating the fault model on the memory of the device under test. The experiment manager performs result collection and categorization too. Errors are detected by comparing the output data with the expected output (i.e., the output of the applications when no faults are emulated in the on-chip SRAM memory).

The evaluated fault models are SEU, SEMU, and Burst Events. In fault injection campaigns involving the SEMU fault model, the size and memory distance characterizing the SEMU fault model are generated accordingly with the distributions shown in Section IV-B. The size and type of the burst fault model are based on data exposed in Section V-C. Each fault injection campaign consists of 10,000 fault injections. Fault locations are randomly generated during each campaign. Fault injection experiments are carried out independently, without fault accumulation (however multiple events such as SEMU are emulated as multiple accumulated faults in memory).

D. Fault Injection Campaigns Results

Results have been categorized into three groups: Masked, Silent Data Corruption, and Halt. A Masked outcome occurs when the fault does not produce any effect on the application output. Silent Data Corruption (SDC) outcome is defined as errors in the application output, detectable only by

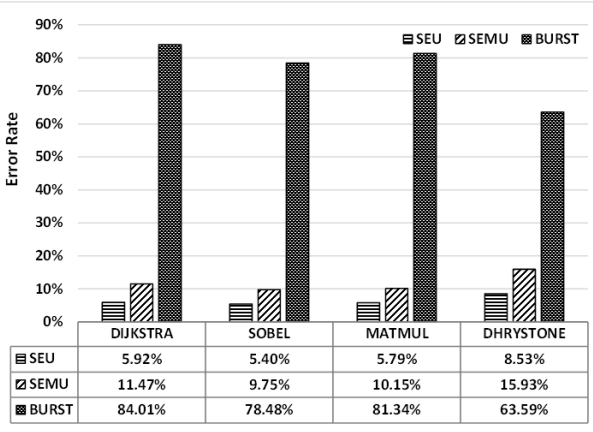

Fig 8: Overall Error Rate of the application for evaluated fault models

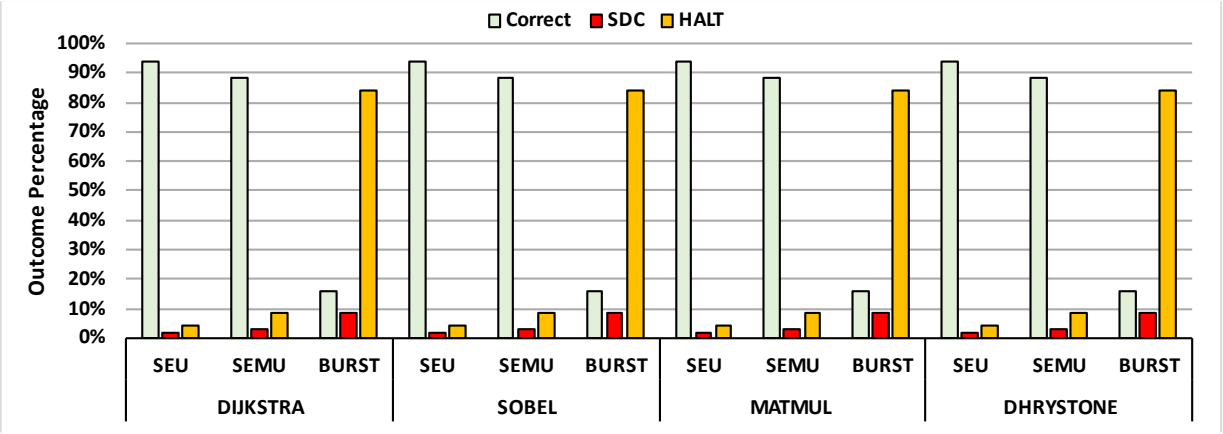

Fig 9: Application results categorization for different fault models

comparison with the results of the unfaulty execution. Finally, if the fault prevents the application from terminating due to processor or endless looping the error is categorized as a Halt error. Figure 8 reports the overall error rate of the evaluated software application against specific fault models. Figure 9 reports the percentage for each outcome associated with the specific fault model and software applications. Although the error rate varies slightly for different applications, the general trend is the same. The error rates increase slightly in SEMUs compared to SEUs and reach very high values for more destructive events such as burst events. However, it is interesting to notice that for burst events, as can be seen in Figure 9, the percentage of SDC increases only slightly, despite the heavy increase in error rates, which is mainly due to halt errors. Since the characteristics of SDC to pass silently is a big concern for system reliability, it is important to be aware that burst events lead mainly to halt errors, characteristics that combined with their lower cross-section will produce a lower rate of silent errors compared to what could have been expected for such an impacting event. However, they should still be considered due to the huge impact they have on system availability. Additionally, the percentage of halt outcomes to which applications appear to be susceptible for all the fault models should make designers consider the importance of finding solutions to decrease the occurrence of these types of effects, which although easy to detect at run time (unlike from SDCs) contribute greatly to the system total error rate.

VI. Conclusions

In this paper, an analysis of the effect of single events in the on-chip SRAM memory of a system-on-chip during a proton test experiment has been presented along with their fault models, including even rarer and often neglected effects such as SEMU and Burst faults. The reliability of a set of bare-metal software applications has been evaluated against the reported fault models through a comprehensive fault injection analysis. Results have shown as different events, according to their impact on the memory content, lead to different reliability scores or erroneous behavior.

References

[1] M. Pignol, "COTS-based applications in space avionics," 2010 *Design, Automation & Test in Europe Conference & Exhibition* (DATE 2010), 2010, pp. 1213-1219, doi: 10.1109/DATE.2010.5456992.

[2] S. Danzeca *et al.*, "Qualification and Characterization of SRAM Memories Used as Radiation Sensors in the LHC," in *IEEE Transactions on Nuclear Science*, vol. 61, no. 6, pp. 3458-3465, Dec. 2014, doi: 10.1109/TNS.2014.2365042.

[3] L. Dilillo, G. Tsiligiannis, *et al.*, (2016). Soft errors in commercial off-the-shelf static random access memories. *Semiconductor Science and Technology, 32(1), 013006.*

[4] M. Rezaei *et al.*, "Evaluation of a COTS 65-nm SRAM Under 15 MeV Protons and 14 MeV Neutrons at Low VDD," in *IEEE Transactions on Nuclear Science*, vol. 67, no. 10, pp. 2188-2195, Oct. 2020, doi: 10.1109/TNS.2020.3023287.

[5] Yuanming Wang, *et al.*, (2011). SRAM single event upset calculation and test using protons in the secondary beam in the BEPC. *Journal of Semiconductors, 32(9), 092001.*

[6] C. De Sio, S. Azimi, A. Portaluri and L. Sterpone, "SEU Evaluation of Hardened-by-Replication Software in RISC- V Soft Processor," 2021 *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems* (DFT), 2021, pp. 1-6, doi: 10.1109/DFT52944.2021.9568342

[7] L. M. Luza *et al.*, "Investigating the Impact of Radiation-Induced Soft Errors on the Reliability of Approximate Computing Systems," *2020 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2020, pp. 1-6, doi: 10.1109/DFT50435.2020.9250865.

[8] Azimi, S.; De Sio, C.; Rizzieri, D.; Sterpone, L. Analysis of Single Event Effects on Embedded Processor. *Electronics 2021, 10,* 3160. https://doi.org/10.3390/electronics10243160

[9] H. Quinn, *et al.*, "Single-Event Effects in Low-Cost, Low-Power Microprocessors," *2014 IEEE Radiation Effects Data Workshop (REDW)*, 2014, pp. 1-9, doi: 10.1109/REDW.2014.7004596.

[10] C. De Sio, S. Azimi and L. Sterpone, "An Emulation Platform for Evaluating the Reliability of Deep Neural Networks," *2020 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2020, pp. 1-4, doi: 10.1109/DFT50435.2020.9250872.

[11] C. De Sio, S. Azimi and L. Sterpone, "FireNN: Neural Networks Reliability Evaluation on Hybrid Platforms," in *IEEE Transactions on Emerging Topics in Computing*, doi: 10.1109/TETC.2022.3152668.

[12] D. M. Hiemstra and V. Kirischian, "Single Event Upset Characterization of the Zynq-7000 ARM® Cortex™-A9 Processor Unit Using Proton Irradiation," *2015 IEEE Radiation Effects Data Workshop (REDW)*, 2015, pp. 1-3, doi: 10.1109/REDW.2015.7336735.

[13] F. G. H. Leite *et al.*, "Ionizing radiation effects on a COTS low-cost RISC microcontroller," *2017 18th IEEE Latin American Test Symposium (LATS)*, 2017, pp. 1-4, doi: 10.1109/LATW.2017.7906762.

[14] M. Amrbar, F. Irom, S. M. Guertin and G. Allen, "Heavy Ion Single Event Effects Measurements of Xilinx Zynq-7000 FPGA," *2015 IEEE Radiation Effects Data Workshop (REDW)*, 2015, pp. 1-4, doi: 10.1109/REDW.2015.7336714.

[15] L. A. Tambara *et al.*, "On the Characterization of Embedded Memories of Zynq-7000 All Programmable SoC under Single Event Upsets Induced by Heavy Ions and Protons," *2015 15th European Conference on Radiation and Its Effects on Components and Systems (RADECS)*, 2015, pp. 1-4, doi: 10.1109/RADECS.2015.7365643.

[16] Yang, WT., Du, XC., Li, YH. *et al.* Single-event-effect propagation investigation on nanoscale system on chip by applying heavy-ion microbeam and event tree analysis. *NUCL SCI TECH* **32,** 106 (2021). https://doi.org/10.1007/s41365-021-00943-6.

[17] L. Bozzoli, *et al.*, "PyXEL: An Integrated Environment for the Analysis of Fault Effects in SRAM-Based FPGA Routing," *2018 International Symposium on Rapid System Prototyping (RSP)*, 2018, pp. 70-75, doi: 10.1109/RSP.2018.8632000.