High-energy Neutrons Characterization of a Safety Critical Computing System

Andrea Fedi[1], Marco Ottavi[2], Gianluca Furano[3], Antimo Bruno[1], Roberto Senesi[5], Carla Andreani[5], Carlo Cazzaniga[6]

***Abstract*—This article presents use of a neutron beam for error injection in safety-critical Commercial Off-the-Shelf (COTS) based platform GeminiX implemented on System on Chip (SoC) FPGA (Field Programmable Gate Array). The results represent an important indication of the resilience of the safety critical system showing a full coverage of soft errors caused by atmospheric neutrons.**

I. INTRODUCTION

The pervasive use of electronic devices in many embedded control applications involving the lives of human beings makes safety of paramount importance. Safety-critical systems are embedded systems that could cause injury or loss of human life if they fail or encounter errors. Flight-control systems, automotive drive-by-wire, railway control systems, nuclear reactor management, or operating room heart/lung bypass machines naturally come to mind [1][2][3]. Emerging IoT market, especially in home energy management, is increasing the number of potentially hazardous control systems and future self-driving cars are already cause of concern. Safety is strictly connected to the concept of risk. Indeed each application has its own level of risk that can be accepted in order to declare the system *safe*[4][5]. Safety-related systems need to obtain specific certifications to be able of handle risky situations: the more the application is critical, the more the certification has harder requirements. Hardware and software must be designed following mandatory directives.

On the other hand it is well known that the constant technology scaling combined with the ubiquitous presence of electronic devices makes the consequences of interactions with ionized particles more and more relevant also to consumer electronics causing both permanent and transient effects caused by the charge injected by the particles in the device[6]. Transient effects affecting memories cause the so-called Single Event Upsets (SEU) which cause a memory element to change the value stored in it and thus potentially causing a serious and dangerous disruption in the correct operation of a digital computing system.

This paper analyses a test case of the Hardware/Software safety critical platform GeminiX [7][8][9][10]: the contribution of this paper is to investigate the behaviour of this COTS system GeminiX, not specifically designed for radiation robustness, but very well suited for safety functions, under critical conditions, such as neutron-induced soft errors.

The rest of the paper is organized as follows: in Section II we present the safety-critical platform GeminiX, its architecture and the hardware (GeminiX-Cores) and the software (GeminiX-OS) it is composed of. In section III we illustrate the experiment carried out at ISIS facility, in U.K., while in section IV and V we illustrate the data extracted from the test and we draw the conclusions.

II. DESCRIPTION OF THE SYSTEM UNDER TEST

The purpose of this section is to introduce the readers to the safety-critical platform GeminiX, its architecture and SoC implementation as well as to describe the System under test which has been irradiated under neutron beam.

A. GeminiX-Platform

The GeminiX-Platform is an embedded virtual platform developed by Neat s.r.l. which performs safety critical applications. It consists of two independent systems (Node A and Node B) which execute the same safety-related functions.

GeminiX-Platform is not intended to be a redundant system, i.e. cold standby, hot standby or TMR. A failure in a subsystem which belongs to a Node (A or B) is considered a fatal error and this implies the system to enter a safe state. If this happens, the other Node does not keep running as the only working unit, because its behaviour cannot be checked by another Node in order to assure that no hardware failures are present.

GeminiX-Platform is built with a dual diverse electronic structure based on *composite fail-safety* with *fail-safe comparison*.

With *composite fail-safety* is meant that each safety-related function is performed by at least two items (the two nodes). Each of these items shall be independent from all others, to avoid common-cause failures. With *fail-safe comparison* is meant that the two nodes synchronize themselves at precise instant of time and cross-check their output data.

Each node of GeminiX is able to terminate or disable the whole system independently from the other, using an interrupt signal or other countermeasures. SW execution and output

[1]Andrea Fedi and Antimo Bruno are with Neat S.r.l., Rome, Italy andrea.fedi@neat.it, antimo.bruno@neat.it

[2]Marco Ottavi is with University of Rome Tor Vergata, Department of Electronic Engineering, Rome, Italy ottavi@ing.uniroma2.it

[3]Gianluca Furano is with ESTEC - ESA (European Space Agency), Keplerlaan 1 2201AZ Noordwijk, The Netherlands gianluca.furano@esa.int

[5]Roberto Senesi and Carla Andreani are with University of Rome Tor Vergata, Department of Physics, Rome, Italy roberto.senesi@uniroma2.it, carla.andreani@uniroma2.it

[6]Carlo Cazzaniga is with Rutherford Appleton Laboratory-ISIS, Didcot, Oxon OX11 0QX, U.K. carlo.cazzaniga@stfc.ac.uk

978-1-5386-0362-8/17/$31.00

results for CPU A and B respectively are runtime cross-checked for synchronization and consistency verification. The failure of a processor causes the system to enter a safe state.

GeminiX includes base software (GeminiX-OS) and design hardware components (GeminiX-Cores) that are independent of the final hardware and that can be used as a building block for SIL4 capable systems, i.e. GeminiX can be implemented on different architectures according to the requirements of final customers.

B. GeminiX architecture

Each GeminiX Node is composed of the following components:

- Processing Unit
- Dedicated RAM
- Dedicated Mass Memory
- GeminiX-Cores
- A system bus interconnects all of these elements together

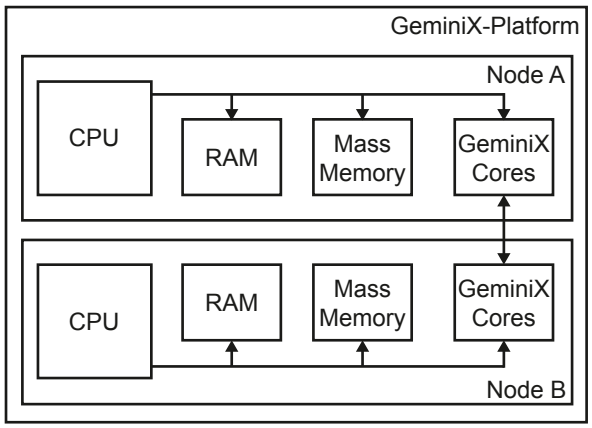

Fig. 1. GeminiX-Platform

The Processing Unit is the Master of the bus and all the other devices (dedicated RAM, dedicated Mass Memory and GeminiX-Cores) are the Slaves and are memory mapped in the address space of the processor to specific addresses. The two nodes exchange and cross-check their data only through a proprietary bus which connects the two GeminiX-Cores.

C. GeminiX-Cores

GeminiX-Cores is composed of a set of VHDL/VERILOG modules which are implemented on FPGA devices in order to accomplish specific functions of the GeminiX-Platform. GeminiX-Cores implements an hardware accelerator for the GeminiX-Platform, i.e. improves the execution of specific algorithms by allowing greater concurrency and parallelism typically on dedicated hardware.

It includes diagnosable components that implement the many safety related measures, such as:

- A system to control failures in Dedicated RAM during operation
- A passive Memory Protection Unit, to implement tasks spatial segregation
- A time-window Watchdog, to implement tasks time segregation
- A cross communication channel, with synchronization capabilities
- A DES signature calculator, to check the Mass Memory to avoid data corruption in it. The signature code previously calculated is verified against the newly recalculated code: if an error is identified, the safe state is enforced
- A cross-power monitor and a bus monitor

D. GeminiX-OS

GeminiX-OS is the GeminiX base software, written in MISRA C, that implements a real time OS-like environment, independent from the specific hardware. GeminiX-OS main features are:

- MISRA C 2004, with coding rules and diagnostic coverage suitable for IEC 61508 and EN 50128 up to SIL4
- H/W segregation of tasks: time segregation (via watchdog) and space segregation (via MAS)
- SW Defensive Programming (assertion and data check before use)
- Controlled execution flow (token passing)
- $64\,\mathrm{bit}$ code protection of firmware on NV-MEM (CBC-MAC) each $1\,\mathrm{KB}$ block
- Complete documentation package following safety standards
- Complete test environment available

III. Experimental Test Setup

The experiment was carried out at the ISIS neutron source [11] which is located at the STFC Rutherford Appleton Laboratory (Harwell campus, Didcot, U.K.). Neutrons are produced at ISIS by the spallation process [12]: a heavy-metal target (tungsten) is bombarded with pulses of highly energetic protons, generating neutrons from the nuclei of the target atoms. The acceleration process is composed of two steps: first H^- ions are injected into a linear accelerator (LINAC). The beam is converted to protons by a $0\,3\mu$m thick aluminium oxide stripping foil and then accelerated in a synchrotron. The high-energy proton pulses travel into two different beam lines, strike the tungsten target and corresponding pulses of neutrons are freed by spallation. The resulting neutron beam reaches several instruments, including ChipIr.

ChipIr [13] is one of the first instruments outside of US aimed at study the effects of neutron radiation on electronic devices. The instrument offers the user to perform highly accelerated tests as one hour being equivalent to exposing microchips to high-energy neutrons for hundreds to thousands of years in the real environment. Such accelerated tests are designed to cause Single Event Effects in electronics.

ChipIr's main features are:

- Neutron beam up to $800\,\mathrm{MeV}$ (thermal and fast neutrons)
- Neutron flux $>10^6\,\mathrm{cm}^{-2}\mathrm{s}^{-1}$
- Adjustable, collimated, uniform and square beam (for this experiment, $70\times70\,\mathrm{mm}^2$ has been used)

- Beam's differential energy spectrum matching the one of the atmospheric spectrum
- Independent shutter, i.e. ChipIr beam can be shut down while the accelerator is running

The Device Under Test irradiated in this experiment is the Xilinx Zynq-7000 SoC XC7Z045-2FFG900C mounted on a ZC706 Evaluation Board, which hosts GeminiX Node B. The Evaluation Board is a PCI Express board which has been connected through its PCIe connector to an Asus Motherboard which hosts an Intel Core i7-6700. This setup implements GeminiX-Platform running Dual Node.

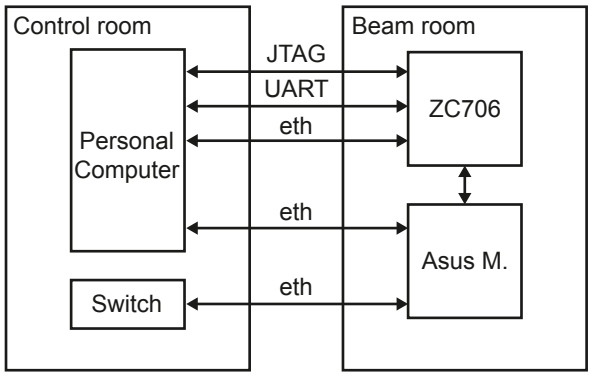

Fig. 2. Test setup

The following test setup has been used:

- A Personal Computer for data logging during testing and for remotely control the Asus Motherboard and the Xilinx Evaluation Board
- An Asus Motherboard on which runs GeminiX Node B
- A Xilinx Evaluation Board on which runs GeminiX Node A
- A switch for remote reset

The application program which runs on the machine is a basic GeminiX service called MAIN-TEST, which continuously performs Abraham test on memories, checks the right functionality of all peripherals, makes temporal cross-checks with watchdogs and verifies the hardware integrity of the whole system.

All console logs and PL readback files have been saved and analysed in order to study the behaviour of GeminiX in a neutron-rich environment. In particular, GeminiX-OS adopts many strategies in order to discover damages and failures in hardware itself to avoid any hazardous behaviour from a safety point of view. If GeminiX-OS discovers any failure, it shuts down the entire system and actualizes procedures that arrange the system itself in a safe state.

Analysis that have been done includes:

- verification that GeminiX-OS detected any failure produced by SEE
- indexing of the type of error that GeminiX-OS detected in comparison with the real SEE the neutron radiation has produced

IV. Analysis of Results

Data have been collected on 13th of March 2017 and consist of 52 log files coming from each GeminiX Node.

During the experiment, The fluence of the ChipIr neutron beam has been measured by a diamond sensor. Data are shown is Figure 3.

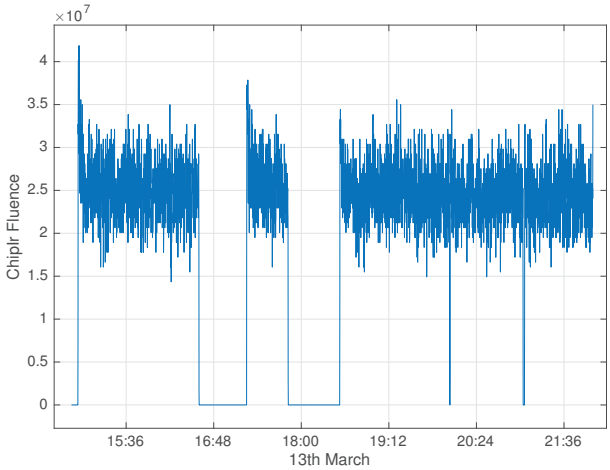

Fig. 3. ChipIr neutron beam fluence during the experiment

The average value is:

$$\langle Fluence \rangle = 2.48 \times 10^7 \, \mathrm{cm}^{-2} \tag{1}$$

In all of 52 runs, one of the two GeminiX Node discovered a failure in its hardware and in all of 52 runs the other node, in which the failure didn't happen, noticed that problem occurred in the other node.

First parameter extracted is the Mean Time To Failure (MTTF), independently from the type of failure. Histogram in Figure 4 shows the number of Failures (N.o.F.) versus the TTF.

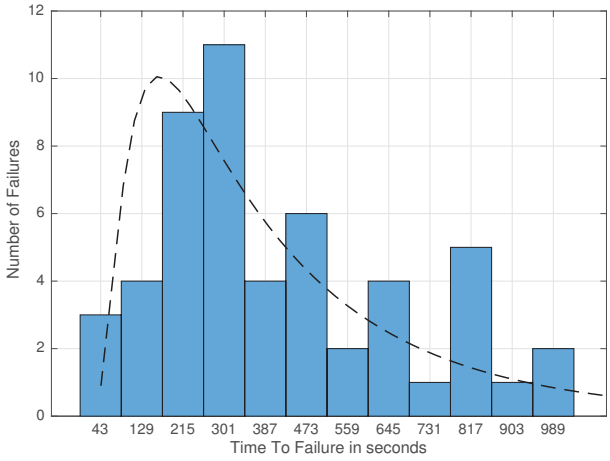

Fig. 4. TTF histogram

The MTTF calculated is:

$$MTTF = 421.26\,\mathrm{s} \approx 7\,\mathrm{min} \quad (2)$$

while the median value is:

$$322\,\mathrm{s} \approx 5.36\,\mathrm{min} \quad (3)$$

The measured data have been fitted by a Landau distribution, which resembles a Gaussian distribution but with a null lower tail and a longer upper tail.

Registered Failures have been indexed in accordance with the errors they have generated in GeminiX. Results are given in Table I.

TABLE I
FAILURES REPORTED BY GEMINIX

Node	Subsystem	N.o.F.	Description
B	DDR	12	Failed to perform operations on DDR
B	PL Shared Memory	8	Invalid semaphore value on Shared Memory
B	PL Shared Memory	1	Shared Memory test failed
B	PL Register File	5	Invalid mirrored value
B	PS ARM	12	Data abort exception
B	PS/PL	4	Interrupt time-out
A	Mass Memory	1	Failed to perform operations on Mass Memory
A	PL Shared Memory	6	Invalid semaphore value on Shared Memory
A	PL Register File	3	Invalid mirrored value
Total		**52**	

It's clear that it has been detected more failures on Node B in comparison to Node A ($81\,\%$ versus $19\,\%$) because not only its GeminiX-Cores, but also the Processor Unit and its DDR are directly exposed to the beam. Some failures have been detected on Node A too, since its GeminiX-Cores is implemented in the same SoC's PL and, eventually, all the electronics in beam room is exposed to radiation.

In particular, the subsystems that have shown higher sensitivity to radiation are the Processing Core (ARM CPU inside SoC) and DDRAM ($54\,\%$), immediately next to the latter in Xilinx Evaluation Board.

Instead, time to failure values of every subsystem are shown in Table II. Processing System is the one with lower Time To Failure, which indicates that it is the most vulnerable component to neutron radiation.

After the experiment, no lasting effects on the failed parts have been detected. All the hardware has been analysed with proper diagnostic tools which did not report permanent failures or damages on electronics. Indeed, every board kept working normally after a full reset.

TABLE II
TTF FOR EACH GEMINIX SUBSYSTEM

Node	Subsystem	Times	Average TTF (s)
B	DDR	12	576
B	PS	16	223
B	PL Shared Memory	9	571
B	PL Register File	5	383
A	PL Shared Memory	6	470
A	PL Register File	3	327
Total		**51**	

V. CONCLUSIONS

We tested in a neutron-rich environment the safety-critical COTS platform GeminiX. The experiment allowed to collect worthwhile data about the robustness of GeminiX in a neutron-rich environment, where the system has been hit by a massive dose of neutron radiation. Clearly, the experiment represents an accelerated test which does not relay on a practical situation. Since GeminiX performed well under these conditions, being able to recognize all failures in its hardware due to bitflips in PL configuration memory, we can assert that the system could assure an high level of safety in every practical situation where neutron radiation doses are very smaller than the one used in this test.

REFERENCES

[1] Q. V. E. Hommes, "Assessment of the iso 26262 standard, road vehiclesfunctional safety," 2012.

[2] "En 50129 railway applications: Safety related electronic systems for signalling," 2003.

[3] L. Volchansky, "Standards in aviation safety (avs)," in *2016 Integrated Communications Navigation and Surveillance (ICNS)*, pp. 1–5, April 2016.

[4] K. Suyama, "Functional safety analysis of safety-related systems using majority decision according to iec 61508," in *2003 European Control Conference (ECC)*, pp. 1720–1725, Sept 2003.

[5] R. Bell, "Iec 61508: functional safety of electrical/electronic/ programme electronic safety-related systems: overview," in *IEE Colloquium Control of Major Accidents and Hazards Directive (COMAH) - Implications for Electrical and Control Engineers (Ref. No. 1999/173)*, pp. 5/1–5/5, 1999.

[6] R. D. Schrimpf, K. M. Warren, D. R. Ball, R. A. Weller, R. A. Reed, D. M. Fleetwood, L. W. Massengill, M. H. Mendenhall, S. N. Rashkeev, S. T. Pantelides, and M. A. Alles, "Multi-scale simulation of radiation effects in electronic devices," *IEEE Transactions on Nuclear Science*, vol. 55, pp. 1891–1902, Aug 2008.

[7] Neat s.r.l., "Geminix reference hw design," 2015.

[8] Neat s.r.l., "Geminix-cores architecture," 2015.

[9] Neat s.r.l., "Geminix-cores detailed design," 2015.

[10] Neat s.r.l., "Geminix - geminix-os," 2015.

[11] "The isis accelerator." http://www.isis.rl.ac.uk/accelerator/, 2006.

[12] N. Watanabe, "Neutronics of pulsed spallation neutron sources," *Reports on Progress in Physics*, vol. 66, no. 3, p. 339, 2003.

[13] "The chipir instrument." http://www.isis.stfc.ac.uk/instruments/chipir/chipir8471.html, 2007.