ADS_0321021252-ESR_019 v01

Online detection and diagnosis for radiation-induced errors in COTS microprocessors EXECUTIVE SUMMARY REPORT

	Name / Role	Date	Signature
Written:	Borja Verdasco	28/04/2023	
Reviewed:	Manuel Peña	28/04/2023	
Approved:	Úrsula Gutierro	28/04/2023	

CHANGE CONTROL

ISSUE	DATE	DESCRIPTION
01	28/04/2023	Creation

CONTENTS

List of figures

List of tables

1. Overview

1.1. Trends and assessment for COTS microprocessors

Nowadays high-end microprocessors are needed in many fields including Space applications. Missions are constantly increasing in their complexity and so the computational load of the on-board microprocessors. This tendency justifies the interest in the use of COTS (Commercial Off-The-Shelf) microprocessors in space applications, provided that sufficient error detection or mitigation is achieved.

1.2. About the trace

The trace interface is a resource which is commonly found in modern ARM microprocessors. It is intended to provide support for debugging and profiling tasks. Trace interface is, by design, capable of exporting information about processor behavior without disturbing execution.

1.3. Objectives

The main objectives within this project are to expand the TRACE Checker IP support to a wider range of ARM processors and devices and, also, to increase its TRL level from a proof-of-concept TRL3 performed at academic level to a higher TRL5 to be industrially offered to customers.

1.4. Hardware identification

The following devices have been selected to demonstrate the operation of the TRACER under heavy ion irradiation:

- Xilinx Zynq-7000 SoC device with ARM Cortex-A9 processor and both ITM and PTM trace protocols.
- Microchip SAMV71Q21RT device with ARM Cortex-M7 processor and both ITM and ETMv4 instruction trace protocols.

1.5. Applications identification

The following applications have been selected as benchmarks to be running on the target processing devices during heavy ion irradiation:

- Matrix Multiplication: the initial tests should be accomplished with small, reduced complexity and controllable benchmarks so that experiments could be easily controlled to detect and correct any possible misbehavior. This application computes the multiplication of two matrices of a given size and produces another matrix as a result. It is quite intensive in both branch execution and data computation.
- NIR-HAWAII-2RG BM algorithm: this application is provided by ESA as a benchmark for on-board computers. It processes the raw image frames coming from the HAWAII-2RG Teledyne near infrared detector to process and detect cosmic rays. This code performs complex operations with large dataset generating a high computational load.

2. TRACER IP

2.1. IP description

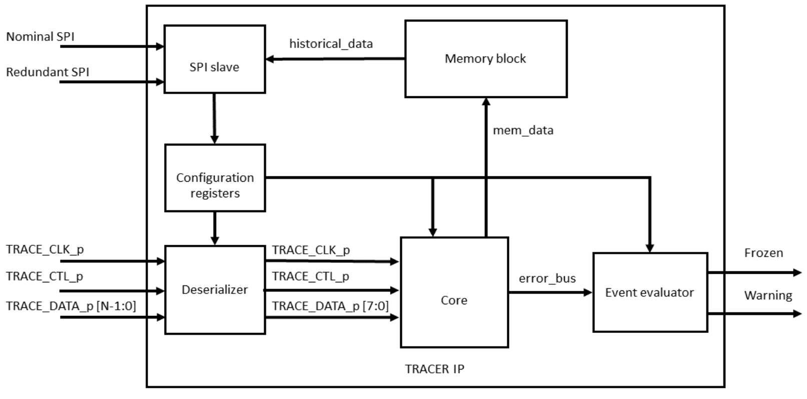
The Trace Real-Time Analyzer to Check processor Errors under Radiation (TRACER) is an IP devised as a feasible solution for both detecting and diagnosing errors on a microprocessor during execution, including radiation-induced errors. Therefore, it stands as a pragmatic approach to harden processing systems onboard spacecraft.

To achieve this, the TRACER IP handles information produced by the trace port unit of the monitored processor. Trace data is processed online by the IP, analyzing the processor behavior at real-time, what results in low latency error detection. Even more valuable, it does so without halting the processor (non-invasive monitoring). Hence, there are no associated overloads or performance penalties.

TRACER IP provides both data and instruction trace analysis capabilities. Data trace analysis is checked via ITM monitoring. Conversely, instruction trace analysis is checked via PTM or ETMv4 monitoring.

TRACER IP consists in a pure Register-Transfer Level (RTL) design with no dependency on the technology in which it is instantiated. Certainly, it can be instantiated in whichever FPGA device. Moreover, the maximum frequency of the processing system trace interface will exclusively depend on the routing capabilities of the FPGA device and the success of signal integrity in the external hardware setup between the microprocessor TPIU and the FPGA pins.

TRACER IP receives the trace bus interface as input to extract information about the processing system operation. Configuration registers can be accessed through SPI. Historical information about the trace data stream is gathered on the internal memory block. Eventually, frozen and warning signals will be raised if an error is detected. Figure 1 illustrates a functional block diagram.



N = 1, 2, 4 or 8 bits

Figure 1: TRACER IP Block Diagram

2.2. Processor errors management

2.2.1. Error detection through data tracing observability

TRACER IP is able to successfully decode and analyze data trace which is generated by an Instrumentation Trace Macrocell (ITM). Actually, an ITM produces different types of packets which provide valuable information about timestamping and software data through writing to stimulus registers.

Stimulus registers form a composite group of 32 registers which are virtually addressed. Whenever the user application performs a write operation to any of the stimulus registers address, ITM generates a SWIT packet indicating the written value and the stimulus port number.

Therefore, any instrumented code may produce such a data trace stream which eventually outputs a key value related to a critical mathematical computation or algorithm result that shall be checked by the TRACER IP. The concept is to validate the instantaneous value of a processor variable before it may have disruptive consequences on the execution flow.

2.2.2. Error detection through instruction tracing observability

TRACER IP is able to successfully decode and analyze instruction trace which is generated by a Program Trace Macrocell (PTM) or Embedded Trace Macrocell (ETMv4). Despite each protocol has a different format, both protocols produce different types of packets which provide valuable information about timestamping, program counter address value, exceptions, context tracing…

TRACER IP decodes all the trace packets produced by PTM or ETMv4 to consistently follow the processor execution flow. The information that is extracted to monitor the processor regards the program counter (PC) address value.

By means of following the program counter address value, it can be observed the code flow that the processor followed. The TRACER IP can detect unexpected jumps or branch condition results in the execution as well as the incorrect timely execution of a periodic task.

2.2.3. Error diagnosis

TRACER IP provides the possibility of recording historical data for further analysis purposes. In fact, the status of the processor before the error occurred is as significant as detecting the error and diagnose its source.

TRACER IP offers the opportunity to allocate FPGA resources to store historical information received from trace data stream. The presence and size of this memory block is configurable by the user. Once an error is detected, the frozen signal is activated, and the TRACER IP does not capture trace data until a reset is performed.

Historical information is intended to be preserved within the TRACER IP memory block so that it may be retrieved if a critical error is detected during the processor execution flow. The information that is stored is directly the most recent trace data processed by any of the implemented checker resources.

Once a critical error is detected, TRACER IP operation is halted. Then, the user may retrieve historical information to get to know in detail the source and nature of the detected error. This might help to diagnose why the error occurred during the execution flow of the processor.

3. Validation under heavy ion irradiation

3.1. Hardware Test Setup

3.1.1. Setup for Microchip SAMV71Q21RT as DUT

A SAMV71Q21RT decapsulated microcontroller assembled on the SAMV71 board was radiated. It was supplied through NGE100 PSU connected to a PC which handles configuration and control. Power supply provided both 3.3V DC and 1.2V DC (internal microcontroller core) individually. The TRACER IP was implemented on a separate Zybo-Z7 board.

The trace information from SAM to IP was provided by a flat twisted cable from the SAMV71 connector to Zybo board.

For sending the diagnosis and events to PC, two USB cables were connected to a PC:

- From Zybo board, a micro-USB cable was connected to the programming USB port, including power supply and serial port communication capabilities (main way for monitoring and diagnosis).
- From SAMV71 board, a USB-to-UART cable was be connected to SAMV71 GPIO, including only serial port communication capabilities. (For double diagnosis check, without supply voltage, only with TX and RX data signals and GND for reference).

In addition, as the DUT was tested with two different FW, an additional USB cable was connected to the DUT SAMV71 board and PC to allow FW changes. This USB cable only supplies the program interface between PC and core to be radiated, but does not supply power to the DUT, that means it does not affect to power supply for detecting SEL.

3.1.2. Setup for Xilinx XC7Z010-1CLG400C SoC as DUT

A XC7Z010-1CLG400C decapsulated SoC assembled on the Zybo Z7 board was radiated. It was supplied thought NGE100 PSU connected to the PC which handles configuration and control. Power supply provided 5V DC monitoring current consumption. At the same time, 4 different core voltages from the SoC (1V, 1V35, 1V8, 3V3) were monitored thanks to TiePie oscilloscope connected through x4 coaxial cable. The TRACER IP was implemented on a separate Zybo-Z7 board.

The trace information from SoC to IP was provided by differential signals using twisted cables between both boards.

For sending the diagnosis and events to PC, two USB cables were connected to a PC:

- From IP Zybo board, a micro-USB cable was connected to the programming USB port, including power supply and serial port communication capabilities (main way for monitoring and diagnosis)
- From DUT Zybo board, a USB-to-UART cable was connected to ZYNQ GPIO, including only serial port communication capabilities (for double diagnosis check, without supply voltage, only with TX and RX data signals and GND for reference).

In order to test with two FW versions, this board allows to load a FW program through two different memory banks (either SD card or QSPI FLASH), which are selectable by a jumper.

3.2. Radiation Strategy

The main objective of the radiation campaign is to demonstrate the suitability of the TRACER IP to observe, detect and diagnose errors on COTS processors execution through monitoring them by the trace interface.

The processor is executing a certain software benchmark in order to represent a computational load on the SoC. The processor includes an ARM CoreSight trace subsystem configured to provide all necessary information to the IP module in order to monitor, evaluate and diagnose any error occurred during radiation test. In parallel, the software benchmark includes redundant information to double-check the results of the performed computation (including a golden reference) and reporting the health status of the execution to an external control PC through a serial port.

On other hand, TRACER IP is monitoring the execution of the DUT processor using trace information. The TRACER IP is implemented in the programmable logic (PL) region of a Zynq SoC for convenience (though it is not exposed to radiation) on a Zybo Z7 board (IP board). The processor available on the Zynq device of the IP board is programmed to export the IP status and diagnosis information whenever the IP reports an error on the DUT.

In this way, errors are double-checked either by the IP and the DUT processor itself to confirm and provide enough information when an error occurs because of radiation.

The beam is on during the whole time, including processor rebooting after an error, to speed-up the test. Boot errors are expected to be low, due to the short boot time compared to the error rate. As the goal of the test is to characterize for errors in the benchmark, any error occurring at boot time will be discarded.

Both IP module and processor are providing the mentioned information through serial port via USB connected to a specific SW tool through an PC. The SW collects all feedback information from IP and processor and store it on a timestamped log file.

SEL effects are monitored by using a programmable power supply as well as a Handyscope HS6 TIEPIE oscilloscope as transient recorder. No specific test runs are dedicated to analysing SEL effects. In this experiment, the relevance of detecting SEL effects is tied to the prevention of damage to the equipment.

SEU effects are exhibited on the trace data stream. They may result in an erroneous computation that corrupts the benchmark output. Also, these events can lead to an unexpected jump of the program counter address value such that the processor execution turns abnormal, getting unpredictable results, or even hanging the processor.

SEFI effects are exhibited when the processor has not performed a recurrent task for a while so that the associated watchdog timer has overflowed.

4. Test Sequence

In Table 1, it is shown the test sequence that was followed during the irradiation campaign at UCL – Heavy Ion Facility (Belgium).

RUN	DUT	TEMP (ºC)	ION	Energy (MeV)	LET (MeV cm2/mg)	TILT (degrees)	EFF LET (MeV cm2/mg)	TEST	FLUX (ions/(cm2 *s))	TIME (seconds)	OBSERVED EVENTS (#events)	TID (krad)	Acc. TID (krad)
1	1 (FW1)	25	^{13} C $^{4+}$	131	1,3	0	1,3	SET/SEU	500	1843.033	54	1,73E-02	0,017
2	1 (FW2)	25	^{13} C $^{4+}$	131	1,3	0	1,3	SET/SEU	400	1262.779	53	9,48E-03	0,027
3	4 (FW1)	25	^{13} C $^{4+}$	131	1,3	0	1,3	SET/SEU	4000	1920.545	42	1,44E-01	0,144
4	4 (FW2)	25	^{13} C $^{4+}$	131	1,3	0	1,3	SET/SEU	1500	2034.248	57	5,73E-02	0,201
5	4 (FW1)	25	^{22} Ne $^{7+}$	238	3,3	0	3,3	SET/SEU	2000	1646.978	28	1,59E-01	0,361
6	4 (FW2)	25	^{22} Ne $^{7+}$	238	3,3	0	3,3	SET/SEU	500	1716.854	39	4,15E-02	0,402
7	1 (FW1)	25	^{22} Ne $^{7+}$	238	3,3	0	3,3	SET/SEU	500	1279.04	49	3,09E-02	0,058
8	1 (FW2)	25	^{22} Ne $^{7+}$	238	3,3	0	3,3	SET/SEU	200	1076.038	54	1,04E-02	0,068
9	2 (FW1)	25	^{13} C $^{4+}$	131	1,3	0	1,3	SET/SEU	500	2132.909	48	2,00E-02	0,020
10	2 (FW2)	25	^{13} C $^{4+}$	131	1,3	0	1,3	SET/SEU	400	1175.631	53	8,82E-03	0,029
11	5 (FW1)	25	^{13} C $^{4+}$	131	1,3	0	1,3	SET/SEU	4000	1901.728	48	1,43E-01	0,143
12	5 (FW2)	25	^{13} C $^{4+}$	131	1,3	0	1,3	SET/SEU	1500	2158.046	91	6,07E-02	0,203
13	5 (FW1)	25	^{22} Ne $^{7+}$	238	3,3	0	3,3	SET/SEU	2000	1643.793	42	1,59E-01	0,363
14	5 (FW2)	25	^{22} Ne $^{7+}$	238	3,3	0	3,3	SET/SEU	500	855.367	91	2,07E-02	0,383
15	2 (FW1)	25	^{22} Ne $^{7+}$	238	3,3	0	3,3	SET/SEU	500	1031.372	43	2,49E-02	0,054
16	2 (FW2)	25	^{22} Ne $^{7+}$	238	3,3	0	3,3	SET/SEU	200	984.298	53	9,52E-03	0,063

Table 1: Test Sequence as run

Ions used from UCL heavy ion High Penetration (HP) cocktail are listed in the table below.

Ion species	**Energy (MeV)**	**Range in Si (um)**	**LET (MeV/cm^2/mg)**
^{13}C^{4+}	131	269.3	1.3
^{22}Ne^{7+}	238	202.0	3.3

Table 2: Selected High Penetration (HP) cocktail

5. Radiation results

This section is intended to present the results obtained from the conducted radiation test as well as describe and analyse the exhibited behaviour of the TRACER IP and the monitored DUTs.

5.1. Experiment overview

Consistency is dually checked both by the DUT itself and the TRACER IP (see section 3.2). Thus, the errors can be classified as follows:

- Error DAT: each of the duplicated operation branches has output a different result.
- Error SDC: both operation branches differ from the golden reference.
- Error TMO: absence of DUT communications for an excessive period of time.
- Error only IP: corresponds to events that the TRACER IP is alerting on, but DUT does not.
- Error COM: corresponds to a communication error in any of the serial ports.

5.2. Experiment results

DUT	SAMV71Q21RT		ZYNQ	
ion	C4+ LET = 1.3 MeV/cm2/mg	Ne7+ LET = 3.3 MeV/cm2/mg	C4+ LET = 1.3 MeV/cm2/mg	Ne7+ LET = 1.3 MeV/cm2/mg
DAT	96	89	87	68
Det DAT	96	89	87	68
SDC	0	1	0	0
TMO	0	0	0	1
Det TMO	0	0	0	1
Only IP	4	1	0	0
COM	2	0	1	0
Cross-section (all errors)	$5.62\cdot10^{-5}$ $(4.57\cdot10^{-5}, 6.83\cdot10^{-5})$	$8.73\cdot10^{-5}$ $(7.03\cdot10^{-5}, 1.07\cdot10^{-4})$	$5.88\cdot10^{-6}$ $(4.71\cdot10^{-6}, 7.25\cdot10^{-6})$	$9.82\cdot10^{-6}$ $(7.64\cdot10^{-6}, 1.24\cdot10^{-5})$
Cross-section (undetected)	- $(0, 2.07\cdot10^{-6})$	$9.60\cdot10^{-7}$ $(2.43\cdot10^{-8}, 5.34\cdot10^{-6})$	- $(0, 2.49\cdot10^{-7})$	- $(0, 5.25\cdot10^{-7})$

Table 3: Radiation test results over MMULT benchmark

DUT	SAMV71Q21RT		ZYNQ	
ion	C4+ LET = 1.3 MeV/cm2/mg	Ne7+ LET = 3.3 MeV/cm2/mg	C4+ LET = 1.3 MeV/cm2/mg	Ne7+ LET = 1.3 MeV/cm2/mg
DAT	105	105	112	110
Det DAT	105	105	47	46
SDC	0	0	0	1
TMO	0	1	3	4
Det TMO	0	1	3	4
Only IP	0	0	0	0
COM	1	0	0	0
Cross-section (all errors)	$1.05\cdot10^{-4}$ $(8.60\cdot10^{-5}, 1.27\cdot10^{-4})$	$2.35\cdot10^{-4}$ $(1.92\cdot10^{-4}, 2.84\cdot10^{-4})$	$1.81\cdot10^{-5}$ $(1.49\cdot10^{-5}, 2.17\cdot10^{-5})$	$5.60\cdot10^{-5}$ $(4.63\cdot10^{-5}, 6.73\cdot10^{-5})$
Cross-section (undetected)	- $(0, 3.69\cdot10^{-6})$	- $(0, 8.16\cdot10^{-6})$	$1.02\cdot10^{-5}$ $(7.89\cdot10^{-6}, 1.30\cdot10^{-5})$	$3.17\cdot10^{-5}$ $(2.44\cdot10^{-5}, 4.04\cdot10^{-5})$

Table 4: Radiation test results over NIR-HAWAII benchmark

5.3. Experiment conclusions

Most of the occurring events during the test were related to data corruption. This fact is coherent since the tested benchmarks are mainly computationally demanding what makes them more susceptible to data errors than program flow errors. It is also observable that the cross section of each device increases when the ion energy is increased but also when the complexity of the executed application is increased.

No SET/SEL effects occurred during radiation tests.

SEU/SEFI effects were detected by TRACER IP as they result in program flow or data access errors in the processor. Moreover, TRACER IP is able to report errors on any of the instantiated trace checker modules that analyze ITM, PTM and ETMv4 protocols respectively.

Experiment results show that data accesses on ARM processors can be instrumented through the ITM and TRACER IP is able to monitor it. Also, the program flow of any ARM processor provided with PTM or ETMv4 instruction tracing capabilities can be monitored during execution. Furthermore, TRACER IP provides the capability of retrieving historical information such that the processor flow before the error occurrence can be gathered for diagnosis purposes.

The TRACER IP was able to detect all errors except in the case of the NIR-HAWAII benchmark on the Zynq device. A closer look to this experiment reveals that the order of checks was inverted by the compiler. While in the other cases data were first compared and then sent to the ITM, in this case, data were first sent to the ITM, then read again from the memory and finally compared internally. Thus, it is possible that the ITM gets correct data, but the data gets corrupted before the internal check is done. This result shows the importance of paying attention to compilation options and compiler results that may introduce subtle differences in the error detection process.

Finally, it can be stated that TRACER IP is able to observe and diagnose errors on ARM processors that implement the trace interface. Future works may extend the trace protocols that the TRACER IP is capable of decoding and analyzing (maybe ETMv4 data trace protocol). This would make the IP suitable for other ARM processors families for which it currently does not provide support.