1964-2014

→ SERVING EUROPEAN
COOPERATION
AND INNOVATION

ESTEC experience for Flash-based FPGAs in Space: design and verification guidelines for critical applications

Gianluca Furano, R. Jansen, G. Magistrati, K. Marinis, A. Menicucci, D. Merodio-Codinachs, M. Rovatti and
C. Urbina-Ortega

European Space Research and Technology Centre (ESA)
Noordwijk, The Netherlands

Space FPGA Users Workshop, 2014
ESTEC - 18 September 2014

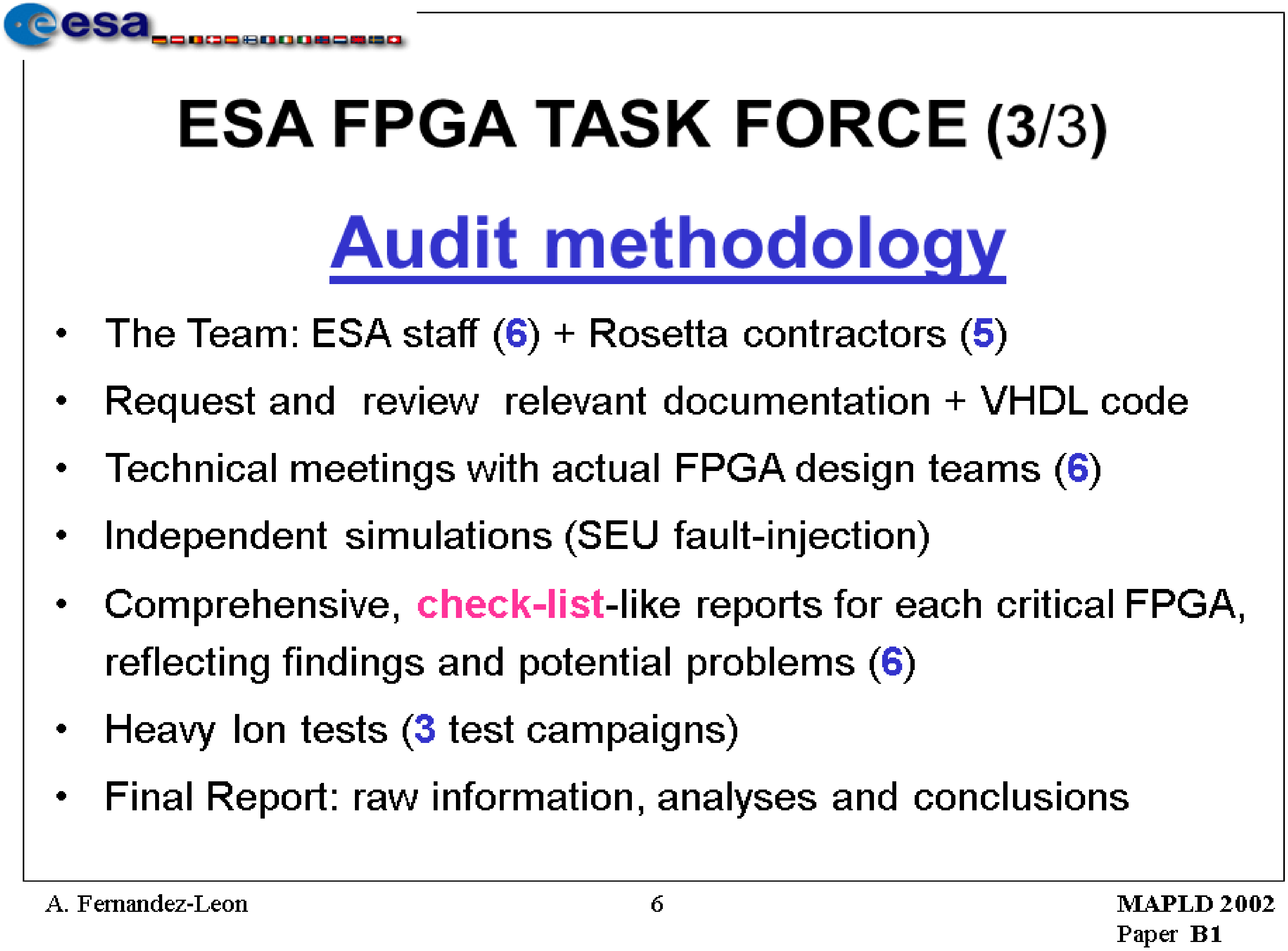
European Space Agency

www.esa.int

How will we spend the next 20 minutes

- Why Space FPGA design and development world is changing
- Radiation Hardness Assurance (RHA) policy for FPGAs
  - Trends for FPGA use in space (ESA)
- The specific case for FLASH FPGA
  - HZE irradiation results
  - Expected SEE rates in space (compared with RTAX)
  - Role of TMR
  - (Formal) Verification of TMR and other RHBD techniques
  - We are flying it to MARS (with CNES, SYDERAL)
- Conclusions and food for thought

Let's have a look at the past. ROSETTA.



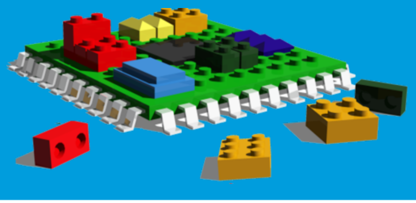
ESA FPGA TASK FORCE (3/3)

Audit methodology

- The Team: ESA staff (6) + Rosetta contractors (5)
- Request and review relevant documentation + VHDL code
- Technical meetings with actual FPGA design teams (6)
- Independent simulations (SEU fault-injection)
- Comprehensive, check-list-like reports for each critical FPGA, reflecting findings and potential problems (6)
- Heavy Ion tests (3 test campaigns)
- Final Report: raw information, analyses and conclusions

A. Fernandez-Leon 6 MAPLD 2002 Paper B1

Ongoing Trends



- The size, the expanded functionalities and the large selection of building blocks for the available space grade programmable logic devices are allowing safe and convenient replacement of ASICs in several space applications in P/F and P/L units.
  - Even with the increasing FPGA device cost, the break-even point between ASIC and FPGA is moving higher (we now put it at ~ 15/20 pieces for commercial projects)
  - On the other hand, the complexity, the expanded functionalities and the related cost of space designs, added to the always present schedule constraints has also increased the pressure on designers and reviewers of such systems.

Simple extrapolation of success of previous projects can not ensure that new designs will be flawless !

Radiation Hardness Assurance (RHA) policy for FPGAs

- In the past at ESA we validated porting of the LEON3-FT core on the RTAX2000S. The design under ion beam proved to operate reliably, thanks to the fault-tolerant design of the LEON processor core.
  - SANDIA has done recently a similar work on Xilinx

- Unfortunately the validation of the radiation techniques of a complete digital design on the FPGA <u>is an exception rather than a rule</u>.
- Many designs with radiation effects protection techniques have not been validated and their effectiveness in space relies only on the underlying RHA of the bare device.

  The potential effects of SEE/SEU on the operation of the design, like in FSMs, are at times not fully appreciated.

- The current situation is that no extensive validation campaigns are requested even though the FPGA could contain a micro-controller or sequencer with hard coded program

Radiation Hardness Assurance (RHA) policy for FLASH FPGAs - Challenges

- RTP3 tests have demonstrated how the TID degrades propagation delay through the pass transistors that provide connections between logic modules and routing tracks
  - At a low dose rate of 1 Rad/minute, (more representative than the 40 krad/minute dose rate used in prior testing), a 10% prop delay increase was observed at a TID level up to 40 kRad or 15% prop delay increase at a TID level up to 55 kRad.
  - The manufacturer has updated design software to include prop delay derating to account for this increase in simulation and STA.

- For SEE, situation is much more complex.
  - It is not only single SEUs in register logic and SRAM cells that might need to be mitigated. SETs, SEFIs, double bit SEU and IO bank upsets have entered the scene, which makes the SEE-aware design more demanding.

Radiation Hardness Assurance (RHA) policy for FLASH FPGAs - Challenges

- We were told yesterday (Microsemi) that built-in hardness of coming RTG4 devices allows a straight implementation of non hardened (at RTL or at netlist level) logic, thus relying only on device's robustness.
- Historically, immunity to soft errors is considered a requirement that may need a grade of over-design.
- In a world where even ground-level applications are suffering a greater numbers of radiation effects as FPGA process technologies advance, critical functions such as those for control, high-reliability communications and highly dependable manoeuvres can benefit from automated built-in protection against soft errors.

- So, don't do it (ESA's opinion).

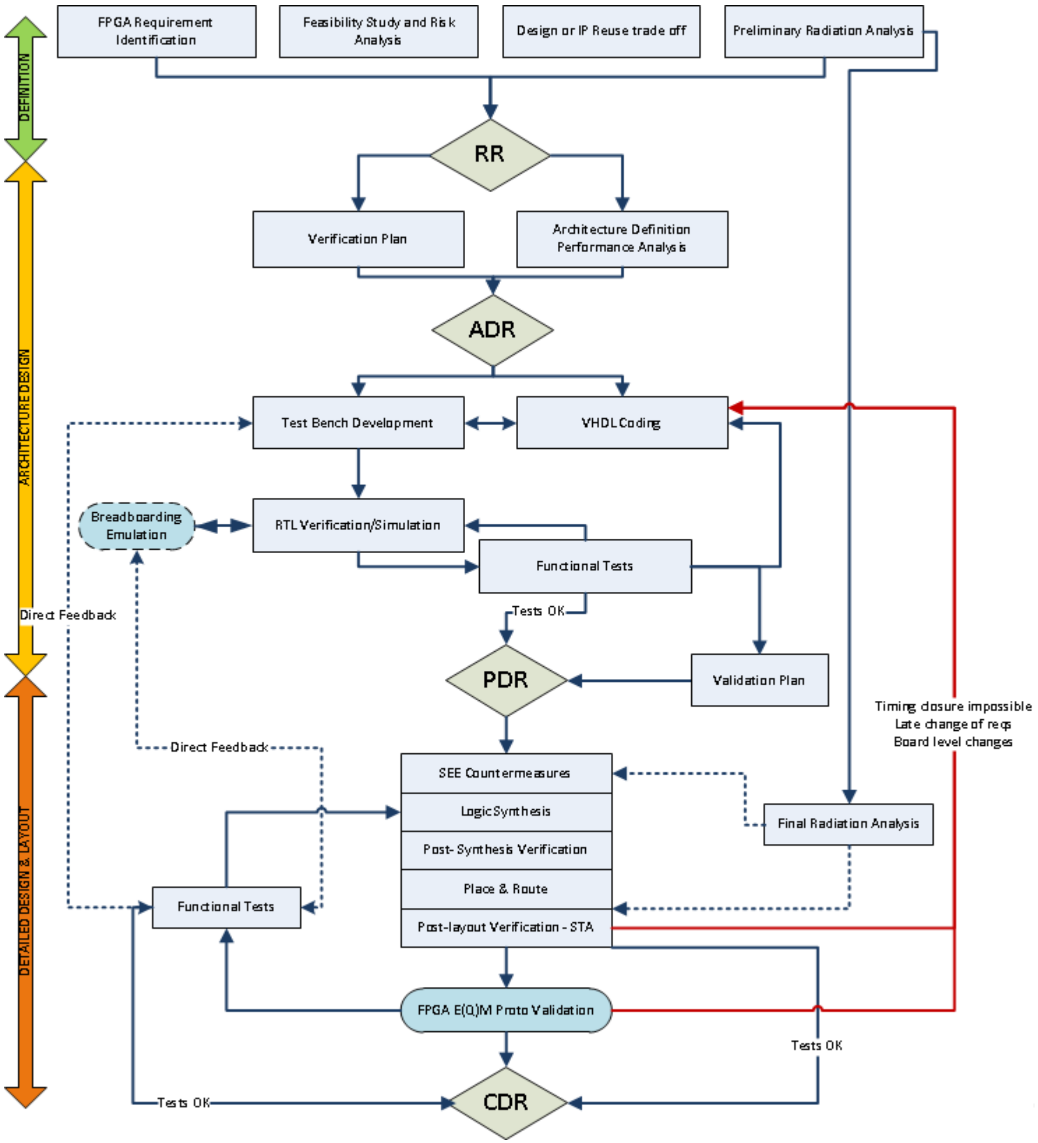
Conclusions (halfway)

- Given the current adoption of FPGA in payload as well as platform systems and the large number of not validated “radiation tolerant” designs in FPGAs with respect to its mitigation effectiveness or radiation sensitivity, **a criticality analysis with regard of the application is highly recommended**.
- Based on the level of the criticality of the intended application to the mission, **different levels of validation of the design could be envisaged**. A similar approach has been adopted at ESA for the software development in the ECSS-Q-ST-80C.

WE ADDED A NEW PERFORMANCE TEST, BUT LEARNED THAT THE TEST ITSELF IS FLAWED.
NOW OUR PRODUCT FAILS OUR OWN TESTS AND OUR CUSTOMERS ARE ASKING TO SEE THE TEST RESULTS.
DO I HAVE PERMISSION TO FAKE THE TEST DATA?
I DIDN'T EVEN KNOW DATA CAN BE REAL.
Dilbert.com DilbertCartoonist@gmail.com
8-11-10 ©2010 Scott Adams, Inc./Dist. by UFS, Inc.

Proposed dev flow for for Microsemi RT-ProASIC family based design

- ProASIC allows more design interactions.
- In circuit reprogrammability shall be exploited to reduce development risks
- Verification tasks can go parallel
- More Design and verification cycles may be needed on complex designs
- Dedicated path for 3rd party IPs



FLASH FPGAs - Heavy Ion irradiation results

We did a dedicated, design dependent and dynamic (up to 200 MHz) RTP3 proton, ion and TID test with remarkable results :

1) PLLs are sensitive to PLL lock signal SEFI and to SET. Asymptotic cross-section is below 10^{-5} cm^2 with LET_{th} around 1.8 MeV·cm^2/mg.
2) UFROM: No error was observed up to a LET of 55 MeV·cm^2/mg (^{131}Xe) and a total cumulated fluence of 1.36 × 10^7 p/cm^2.
3) Configuration Flash: It is not sensitive to SEE. However, its programming part (Charge Pump and In-System Programming) is sensitive to SEU, and to TID effects.
4) No SEL observed up to a LET of 55 MeV·cm^2/mg (^{131}Xe), a cumulative fluence of 10^7 p/cm^2 and with temperatures up to 125 C, bias voltages up to 1.65 V for the core voltage and 3.6 V for the input/output voltage.
5) Very limited statistics were accumulated for SEFI.
   - Only one event was detected with LET of 55 MeV·cm^2/mg.

[1] M. Grandjean, "HRX/SEE/0303 A3PE3000L SEE Test Report," Hirex Engineering, Aug. 2011.

[2] C. Poivey, M. Grandjean, and F. Guerre, "Radiation Characterization of Microsemi ProASIC3 Flash FPGA Family," in Radiation Effects Data Workshop (REDW), 2011 IEEE

FLASH FPGAs - Heavy Ion irradiation results

The Weibulls for SEU in registers show that a 100x improvement in SEU resilience can be achieved with TMR (up to 25 MHz).

ProASIC3L Registers and TMR Registers are not sensitive to proton-induced SEUs.

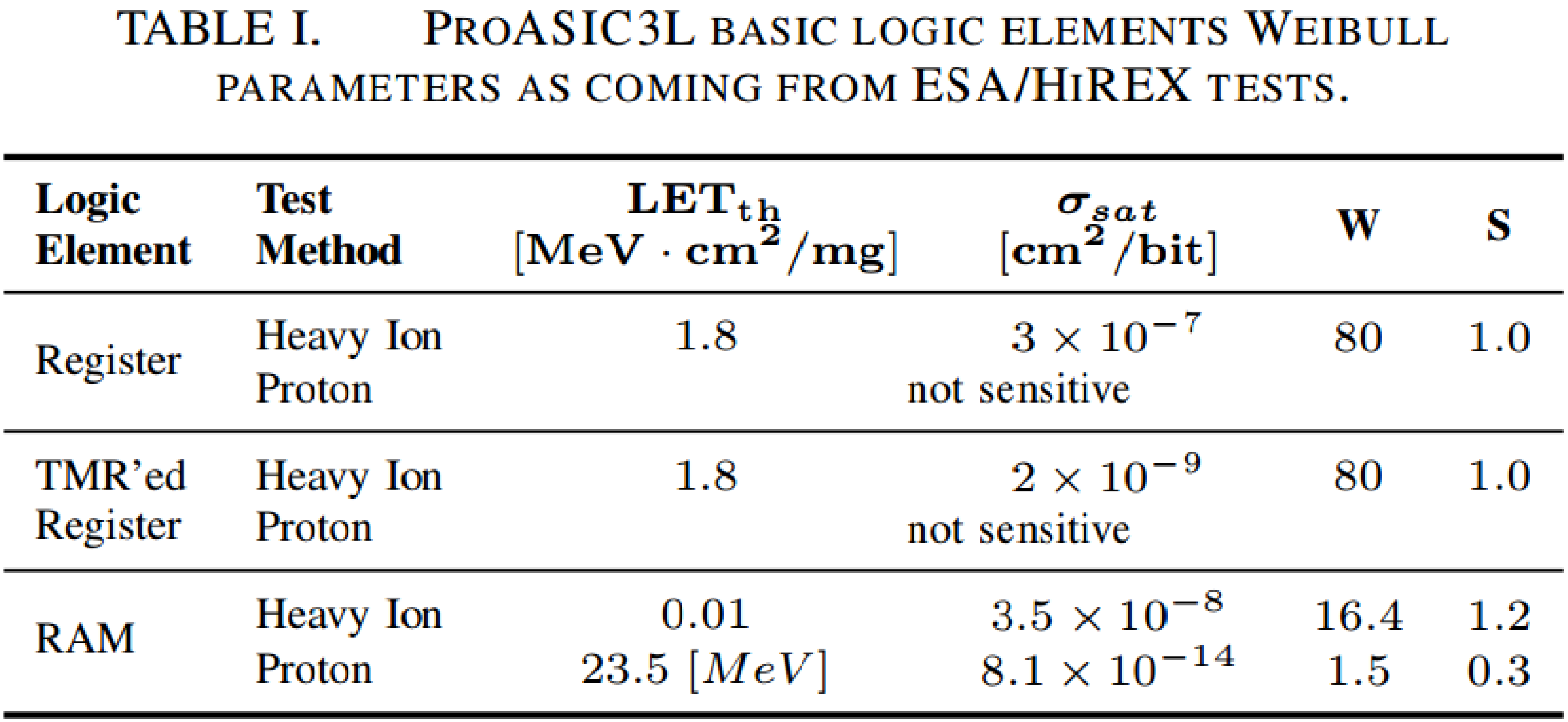


TABLE I. PROASIC3L BASIC LOGIC ELEMENTS WEIBULL PARAMETERS AS COMING FROM ESA/HIREX TESTS.

Logic Element	Test Method	LET_{th} $[\mathrm{MeV} \cdot \mathrm{cm}^2/\mathrm{mg}]$	σ_{sat} $[\mathrm{cm}^2/\mathrm{bit}]$	W	S
Register	Heavy Ion	1.8	3×10^{-7}	80	1.0
	Proton	not sensitive			
TMR'ed Register	Heavy Ion	1.8	2×10^{-9}	80	1.0
	Proton	not sensitive			
RAM	Heavy Ion	0.01	3.5×10^{-8}	16.4	1.2
	Proton	$23.5\ [MeV]$	8.1×10^{-14}	1.5	0.3

FLASH FPGAs – Simulated SEU rates in space

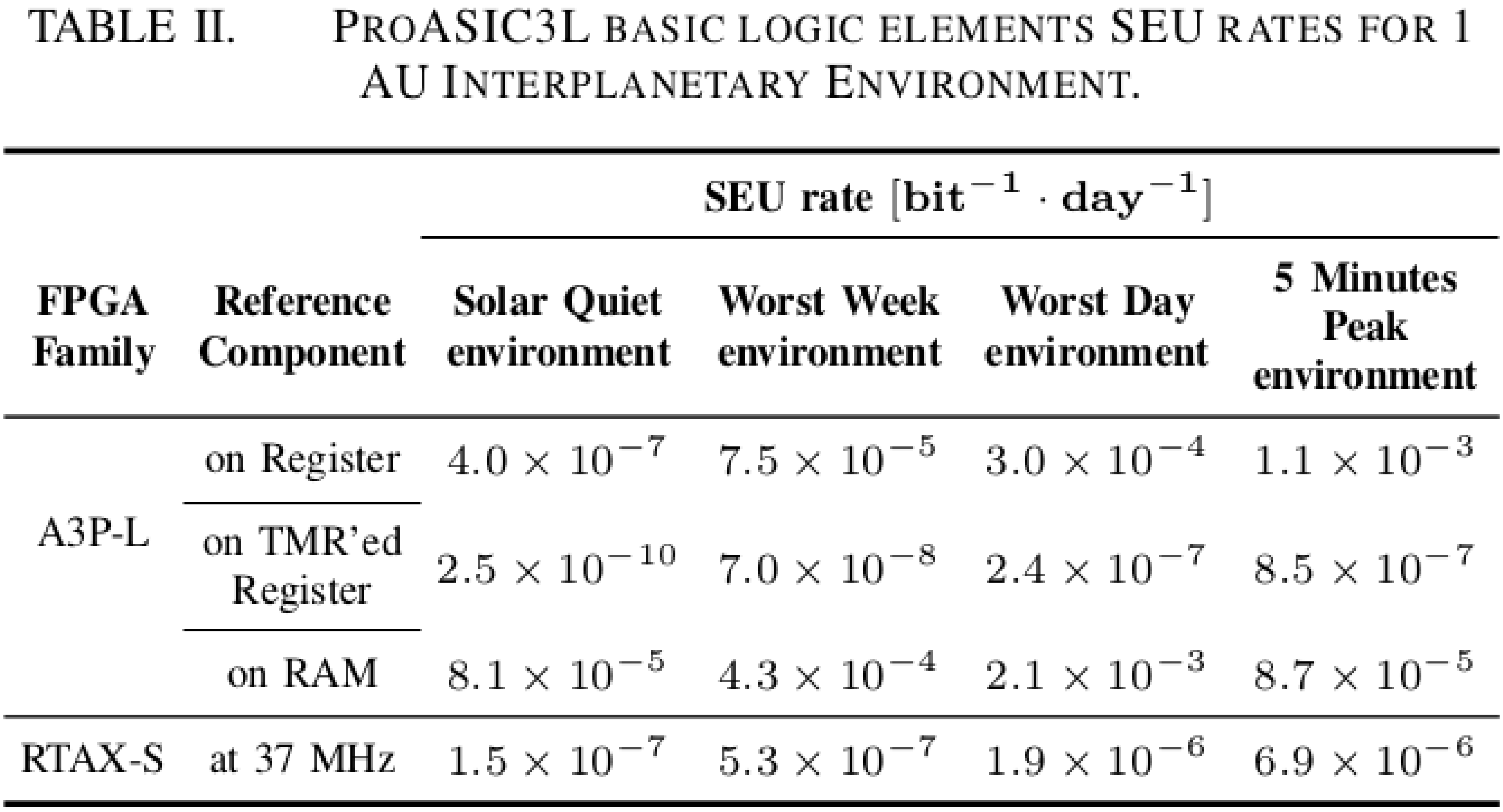


TABLE II. PROASIC3L BASIC LOGIC ELEMENTS SEU RATES FOR 1 AU INTERPLANETARY ENVIRONMENT.

FPGA Family	Reference Component	SEU rate $[\mathrm{bit}^{-1} \cdot \mathrm{day}^{-1}]$			
		Solar Quiet environment	Worst Week environment	Worst Day environment	5 Minutes Peak environment
A3P-L	on Register	4.0×10^{-7}	7.5×10^{-5}	3.0×10^{-4}	1.1×10^{-3}
	on TMR'ed Register	2.5×10^{-10}	7.0×10^{-8}	2.4×10^{-7}	8.5×10^{-7}
	on RAM	8.1×10^{-5}	4.3×10^{-4}	2.1×10^{-3}	8.7×10^{-5}
RTAX-S	at 37 MHz	1.5×10^{-7}	5.3×10^{-7}	1.9×10^{-6}	6.9×10^{-6}

FLASH FPGAs – RHBD Techniques

Several techniques can be applied, including incremental combinations.

Since IP core commercialization strategy not always eases the access to the source code of the design, so it is necessary to know the limits of each technique and its entry point in the design flow (and how to verify it!).

At Register Transfer Level

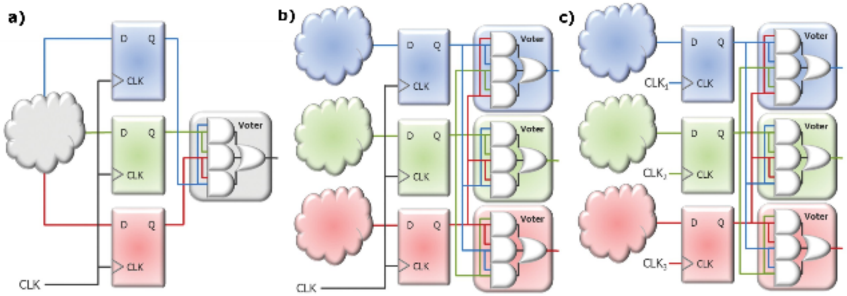
1) Safe Finite State Machine Coding (may be introduced by synthesizer)

2) 3-Hamming distance enhancement in FSMs (same as above)

3) I/O ports triplication

4) Output Control Loops

5) EDACs and scrubbing on memory banks



At Netlist Level

1) Sequential logic Triple Modular Redundancy (sTMR)

2) Local TMR

3) Global TMR

4) Combinatorial Cells with Feedback as storage (*NOT SUPPORTED IN ProASIC !*)

5) Guard Gates Filtering (*for SET limitation, not necessary below 30 MHz*)

FLASH FPGAs – RHBD Techniques cost

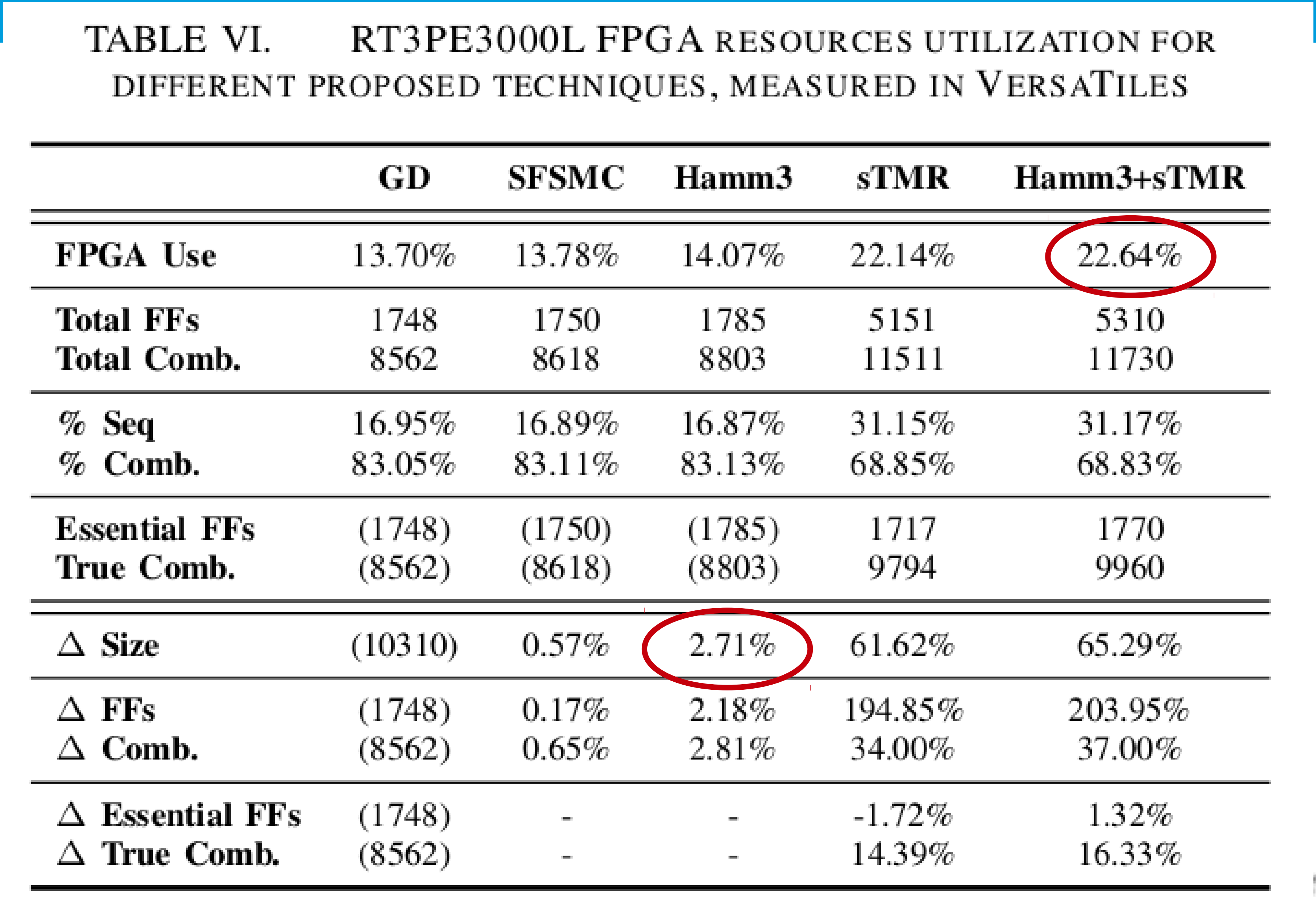


TABLE VI. RT3PE3000L FPGA RESOURCES UTILIZATION FOR DIFFERENT PROPOSED TECHNIQUES, MEASURED IN VERSATILES

	GD	SFSMC	Hamm3	sTMR	Hamm3+sTMR
FPGA Use	13.70%	13.78%	14.07%	22.14%	22.64%
Total FFs	1748	1750	1785	5151	5310
Total Comb.	8562	8618	8803	11511	11730
% Seq	16.95%	16.89%	16.87%	31.15%	31.17%
% Comb.	83.05%	83.11%	83.13%	68.85%	68.83%
Essential FFs	(1748)	(1750)	(1785)	1717	1770
True Comb.	(8562)	(8618)	(8803)	9794	9960
Δ Size	(10310)	0.57%	2.71%	61.62%	65.29%
Δ FFs	(1748)	0.17%	2.18%	194.85%	203.95%
Δ Comb.	(8562)	0.65%	2.81%	34.00%	37.00%
Δ Essential FFs	(1748)	-	-	-1.72%	1.32%
Δ True Comb.	(8562)	-	-	14.39%	16.33%

Formal verification for RHBD techniques

In the spirit of "not trusting the tools blindly" Formal Verification methods (e.g. FormalPro from Mentor, as presented by TAS) are necessary to confirm that the resulting layout netlist maintains full functional equivalence to the original RTL netlist.

Since different TMR/hardening techniques are possible, it should be highlighted that a TMR'ed netlist is not (Boolean) logically equivalent to the original netlist, because of the added logic.

That's one of the main problems with applying formal verification methods to TMR designs.

The designs should still be functionally equivalent though ;-).

However, while a formal verification flow for TMR seems to be supported for some FPGA technologies (e.g. Xilinx, Altera) this does not seem to be the case for ProASIC3.

Formal verification for RHBD techniques

The synthesis compilation report needs to be carefully checked to confirm that the safe FSM logic is properly built for all FSM state vectors.

- Often happens that in some instances the safe logic is not implemented, e.g. in complete state vectors.
- I see this as another argument for 3-hamming distance FSM encoding, together with error accumulation probability due to non-feedback of TMR registers in ProASIC.

	Hamming-3 Error Detection / Correction in FSM	Safe FSM
	Automatic error detection and correction of 1-bit state error	Automatic error detection and reset
What Happens Upon Error	Error corrected automatically and FSM functions as normal	FSM goes to a default or reset state as specified in the user's RTL in the "others" clause

Future work

- Further study on RTP3 SEFI behaviour for LETs above 55 MeV·cm^2/mg.
  - Most ESA missions have a SEFI/SEL threshold at 60 MeV·cm^2/mg.
- Study about synergy of total dose effects, stress-induced leakage current (read stress), and temperature and power supply variations with SEU rates/thresholds.
  - We *kind of guess* that the single-event upset cross section of FLASH devices is sensitive to cumulated total dose.
- Characterization of SEE/SEU effects at 1.5 V and 1.2 V Core Supply Voltages.
- Radiation tests and long duration low dose rate tests (~ 1 rad/min), in biased and unbiased conditions of 'real world' designs, with head to head comparison of different hardening schemes
  - Yes, reprogramming...
- Characterization of SEE/SEU effects at different clock speeds for complex designs.

Future work

- All the above for RTG4 ...

Challenges

RTG4™

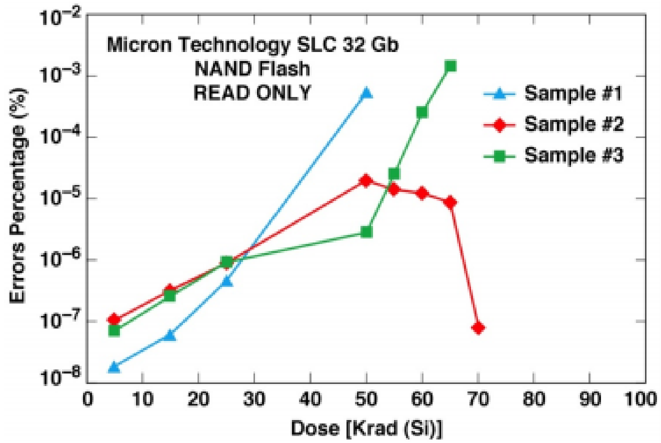


Figure 4.2.1-1. Percentage of bit errors versus dose for Micron Technology 32-Gb SLC NAND flash memories in No Refresh mode.

RTAX-S / DSP

RT ProASIC3

RTSX-SU

Possibilities

Conclusions + Food for thought

In the spirit of SEFUW, I list here some open issues

- Use of 3rd party IPs is on the rise
- We (as Agency) need to give (well substantiated) guidelines on applicability of RTL/Netlist RHBD techniques for IP+Device combinations
- Criticality level of Device+IP+Usage is a system level issue that shall be tackled early in development
- "FDIR" and failure propagation at IP/block level inside a SoC shall be dealt with at architectural level.

- Quote from a famous guy

FPGAs should be forbidden in space applications until the designers learn how to design with them.

(S. Habinc, now Aeroflex, then at ESA/ESTEC).

esa

50 1964-2014

→ SERVING EUROPEAN COOPERATION AND INNOVATION

Would you like to know more?

Visit www.esa.int

European Space Agency