ACCEDE | ESCCON
2025
Seville - Spain
25 to 27th March
ALTER | esa

LOCKSTEP-BASED SEE MITIGATION APPROACH FOR COTS SOC FPGAS

ESA OSIP PROJECT

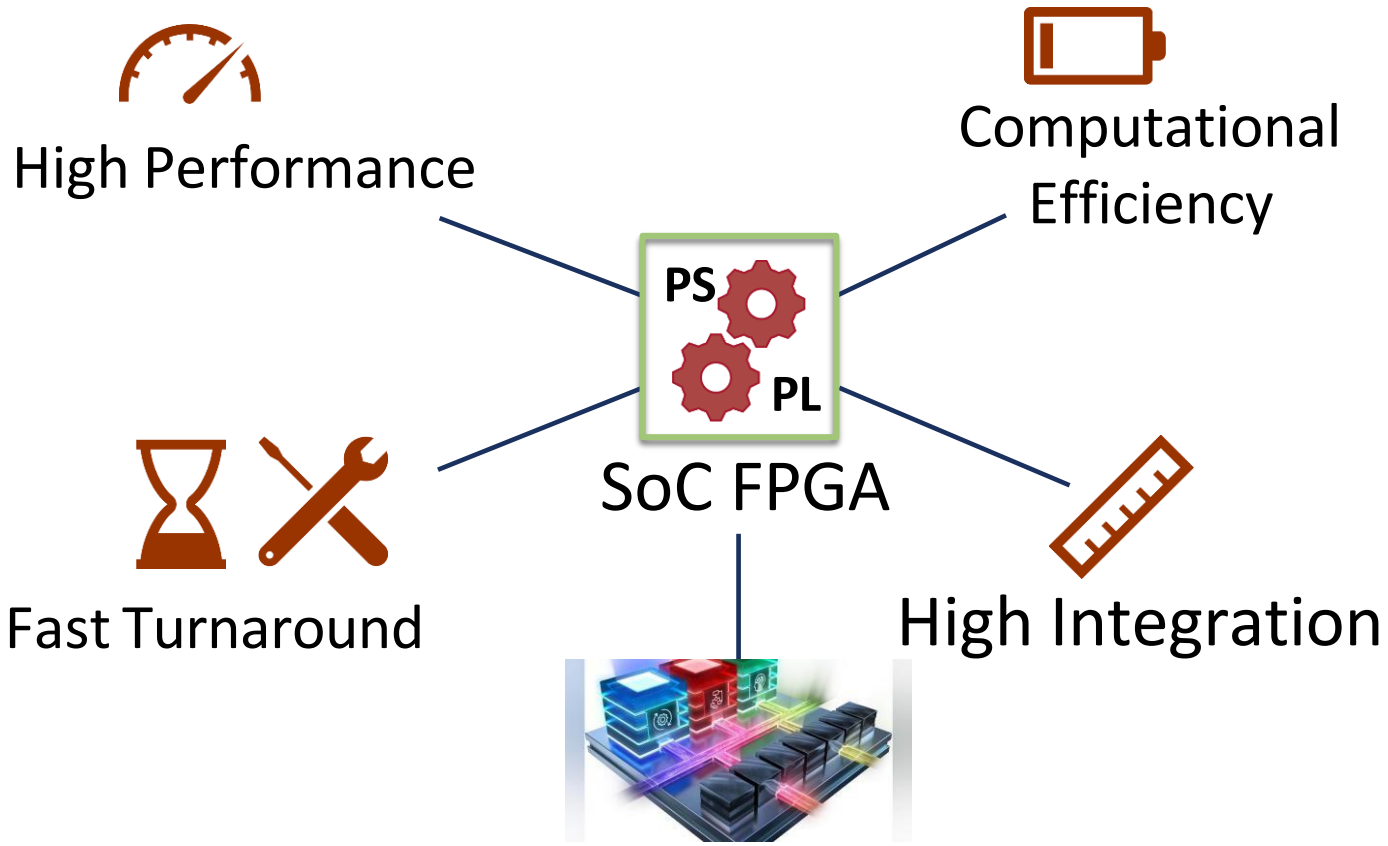
Dimitris Agiakatsikas (presenter), Vasileios Vlagkoulis, Aitzan Sari, Mihalis Psarakis (University of Piraeus, GR)
Maria Kastriotou (STFC, Rutherford Appleton Laboratory, UK)
Antonis Tavoularis, Gianluca Furano (ESA, ESTEC, NL)

SolidKosmos

esa BUSINESS INCUBATION CENTRE Greece

UNIVERSITY OF PIRAEUS RESEARCH CENTER
Spin-off

COTS SOC FPGAS IN SPACE

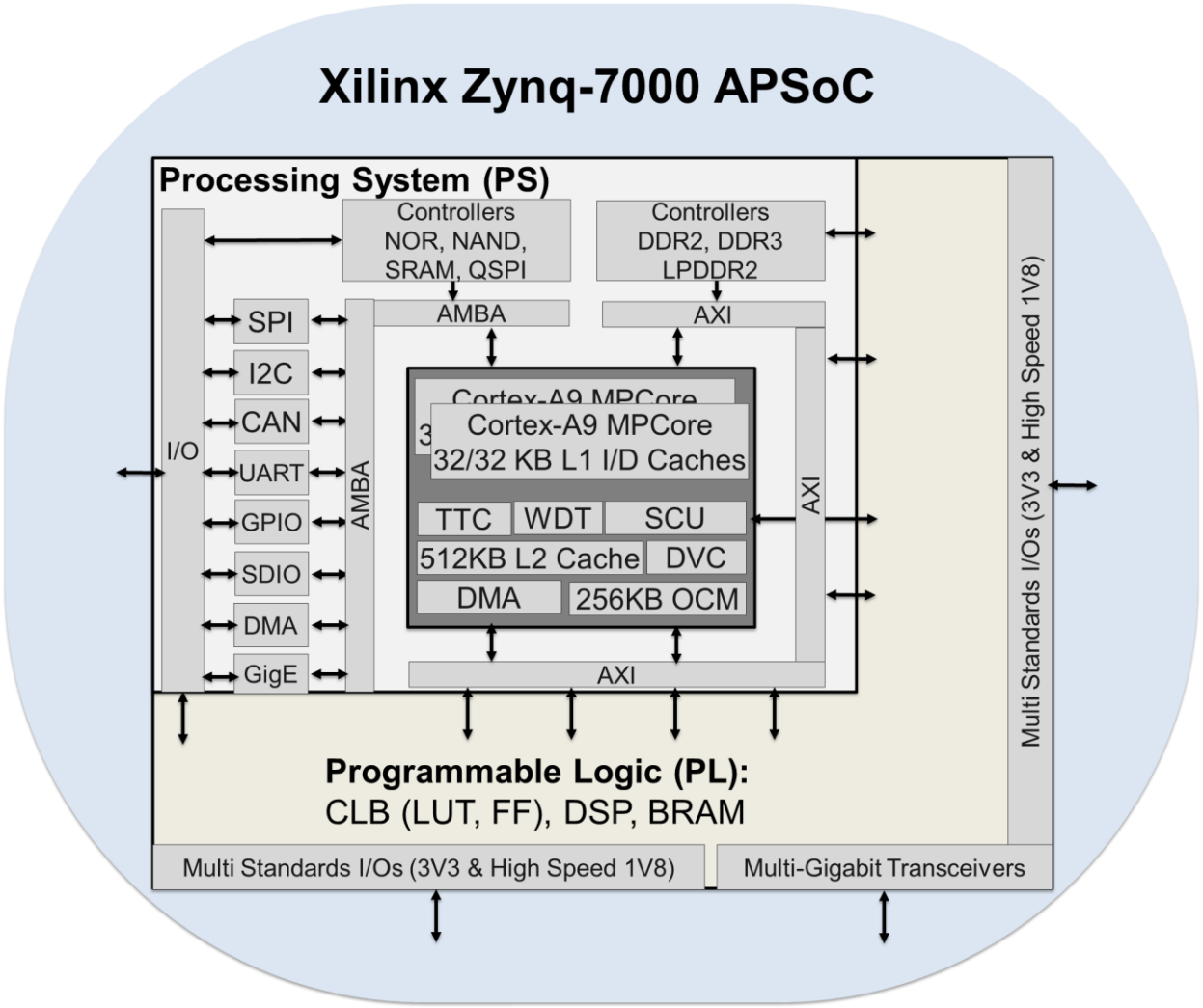


Companies Using AMD-Xilinx SoC FPGAs

- Aerospacelab
- CesiumAstro
- EnduroSat
- GomSpace
- Innoflight
- KP Labs
- NOVI LLC
- Novo Space
- Ramon Space
- SwRI
- Trident Space
- Xiphos

2024 NASA State-of-the-Art Small Spacecraft Technology Report.

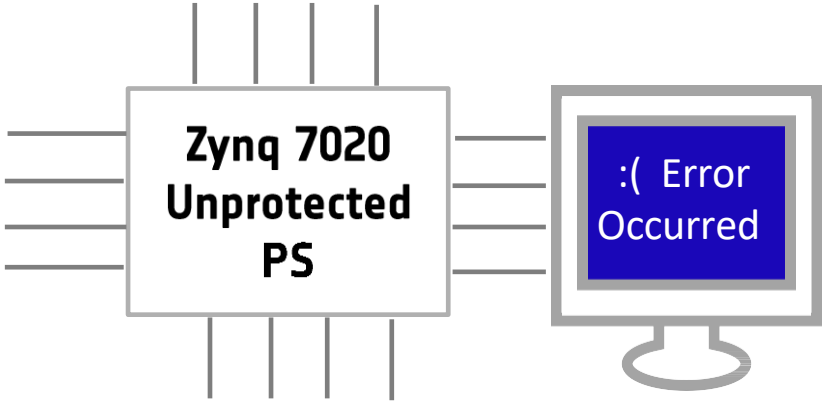
POPULAR COTS SOC FPGA



- Processing System (PS):
  - Single- or **dual-core ARM Cortex-A9 processor**
  - Level-1 per core
    - 32 KB Instruction Cache (L1-I)
    - 32 KB Level-1 Data Cache
  - Shared
    - 512 KB Level-2 Data Cache (L2)
    - 256 KB On-Chip Memory (OCM)
  - Rich I/O peripheral set (e.g., CAN, SPI, DDR controller)
- Programmable Logic (PL): Artix-7 or Kintex-7

PROBLEM: THE PS IS VULNERABLE TO RADIATION EFFECTS

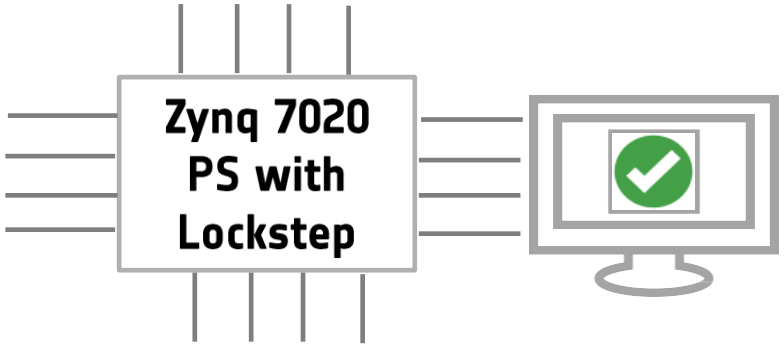
- Heavy-ion and proton radiation experiments show that the PS is vulnerable to
  - SDCs
  - System Unresponsiveness (Crashes)
- Disabling caches
  - Improves reliability
  - At the cost of performance penalty (up to 20x for some applications)

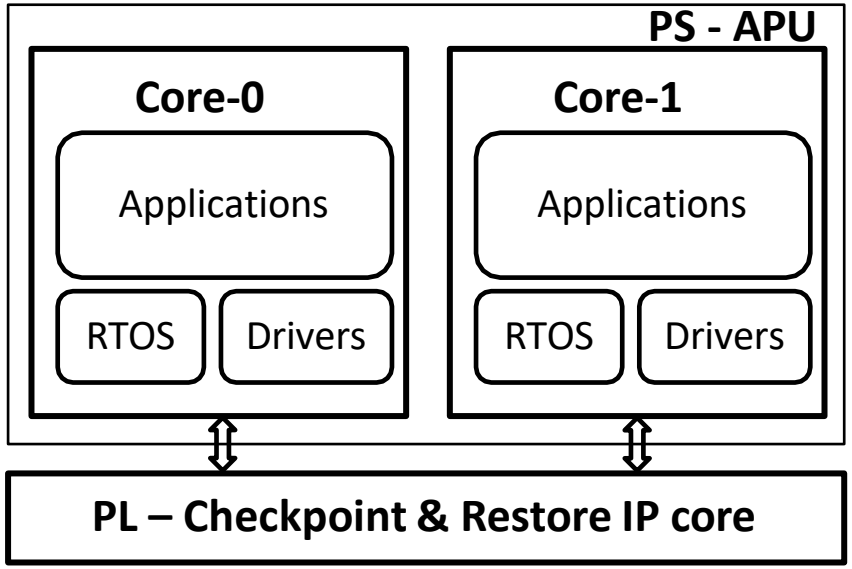


Challenge

- **How can we develop reliable applications with the processing system (PS) of a COTS SoC FPGA?**

OUR SOLUTION: LOCKSTEP WITH CHECKPOINT AND RESTORE

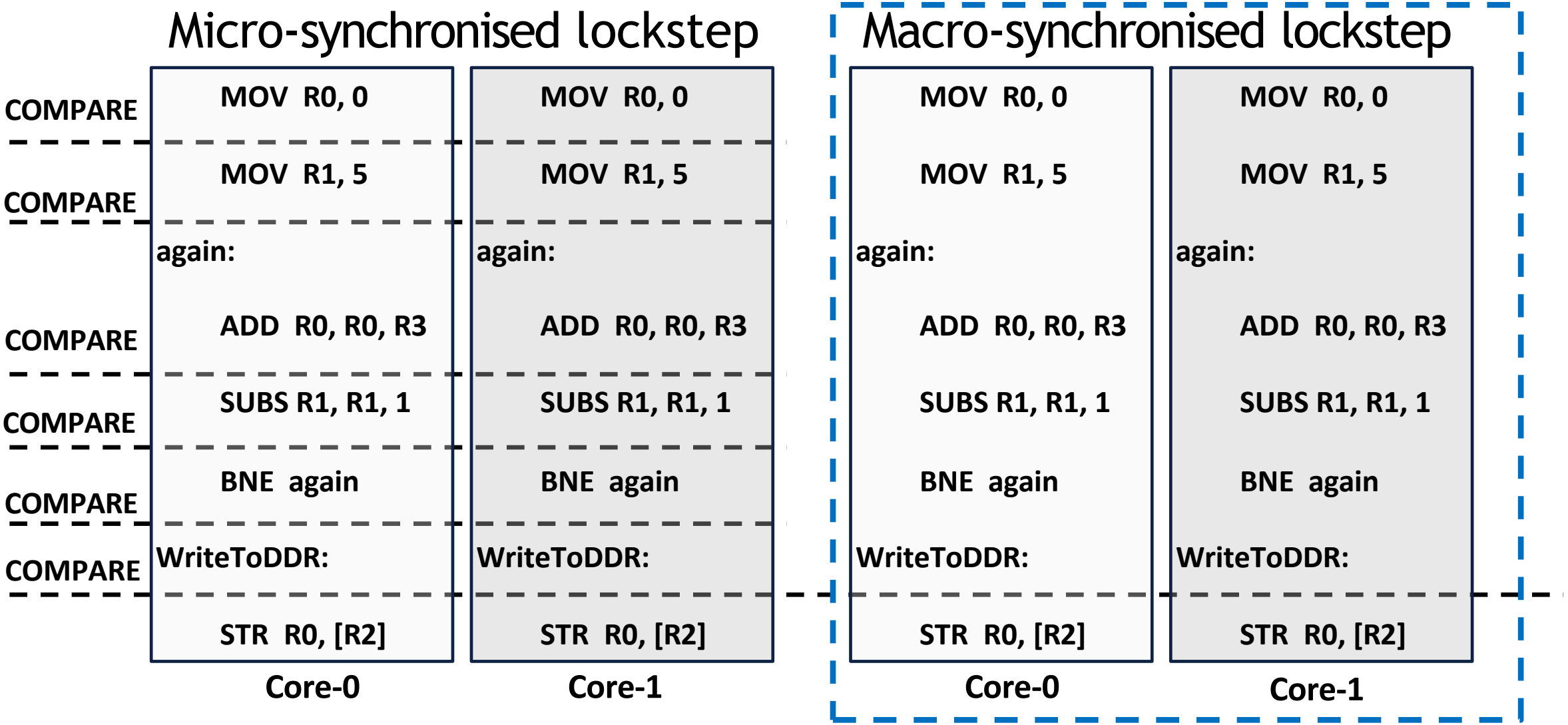




Compared to state-of-the-art, our solution improves:

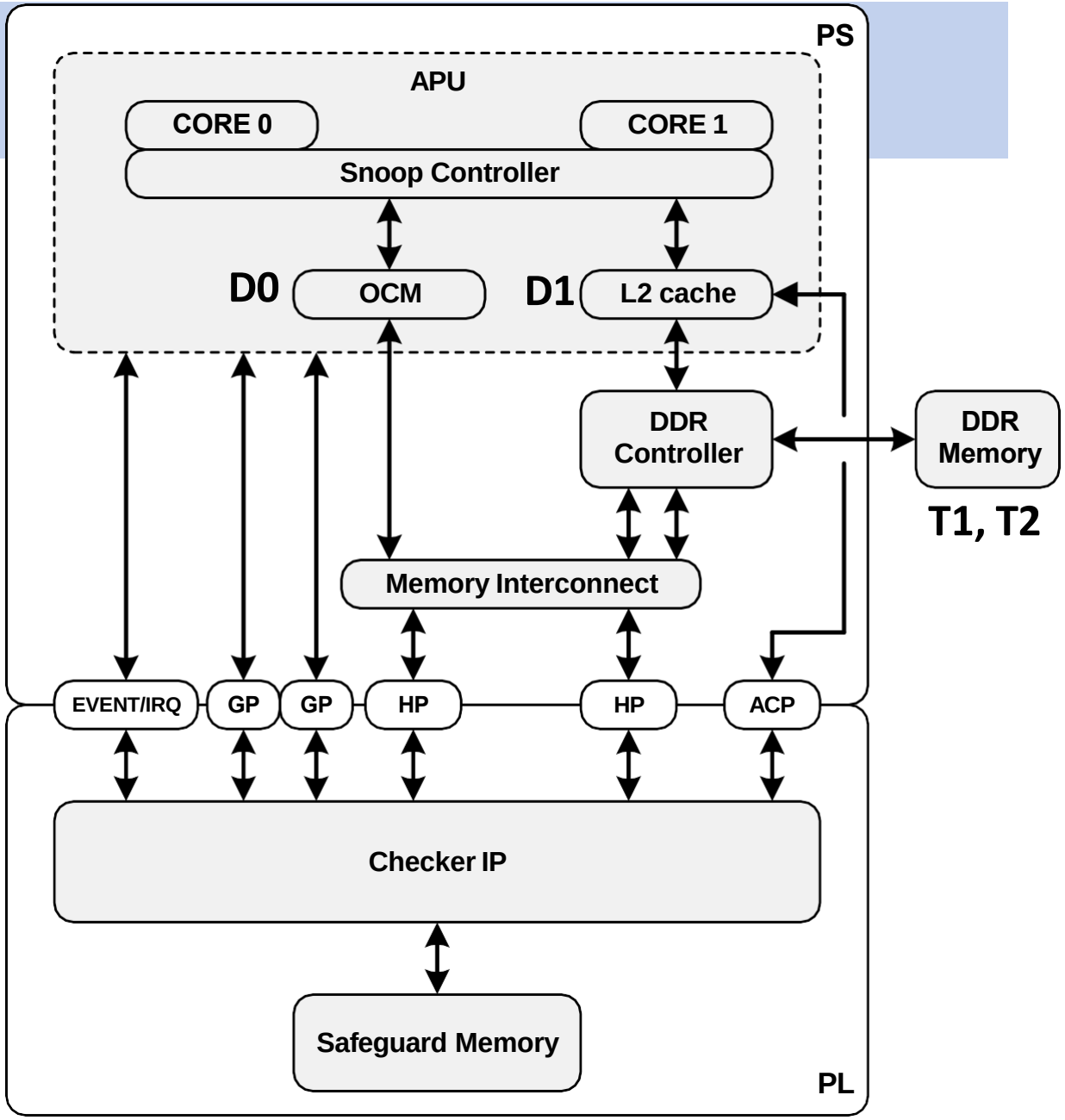
- Fault-coverage → Can detect errors in the RTOS kernel space
- Common-mode errors → We map checkpoint data to (isolated) physically separate memories
- Performance overhead→ Caches enabled, HW-based Checkpoint & Restore

OPERATING PRINCIPLE: MACRO SYNC LOCKSTEP EXECUTION



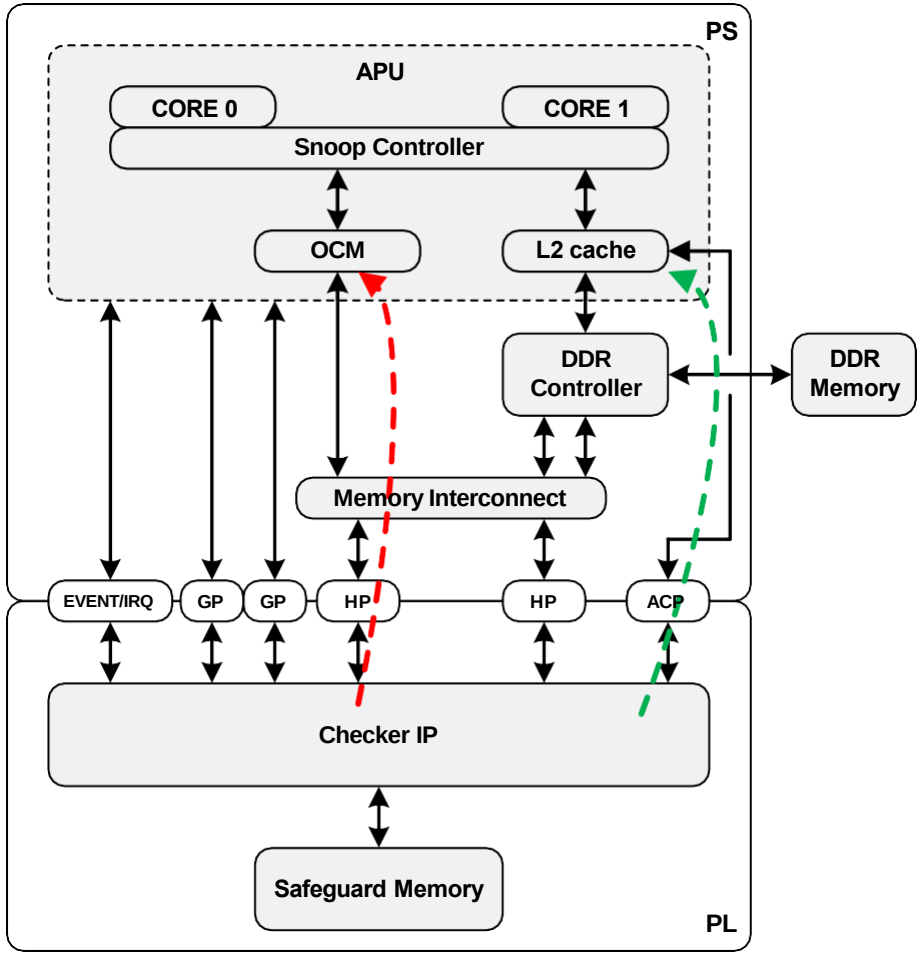
ARCHITECTURE OVERVIEW

- Each core runs in AMP mode with a copy of the OS/Application (same binary)
- Physically separate data memories:
  - D0 (Core-0 data) → OCM (256KB)
  - D1 (Core-1 data) → L2 (256KB)
- Shared code memory:
  T0, T1 (Core0 & Core1 code) is mapped on DDR (Error detection → Data comparison)
- Checker IP Access Ports:
  - Core0 → HP
  - Core1 → ACP

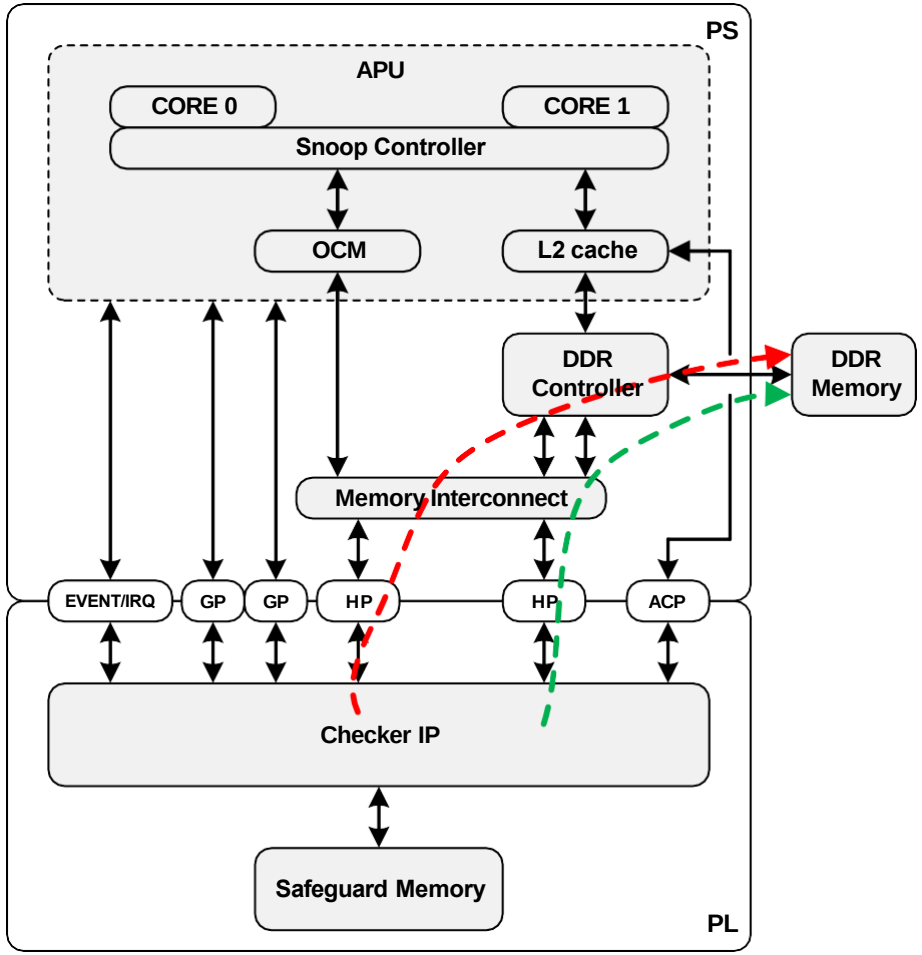


D1 & D2 CAN ALSO MAP TO DDR FOR MORE MEMORY DATA

- D0 (Core-0 data) → OCM (256KB)
- D1 (Core-1 data) → L2 (256KB)



- D0 (Core-0 data) → DDR
- D1 (Core-1 data) → DDR

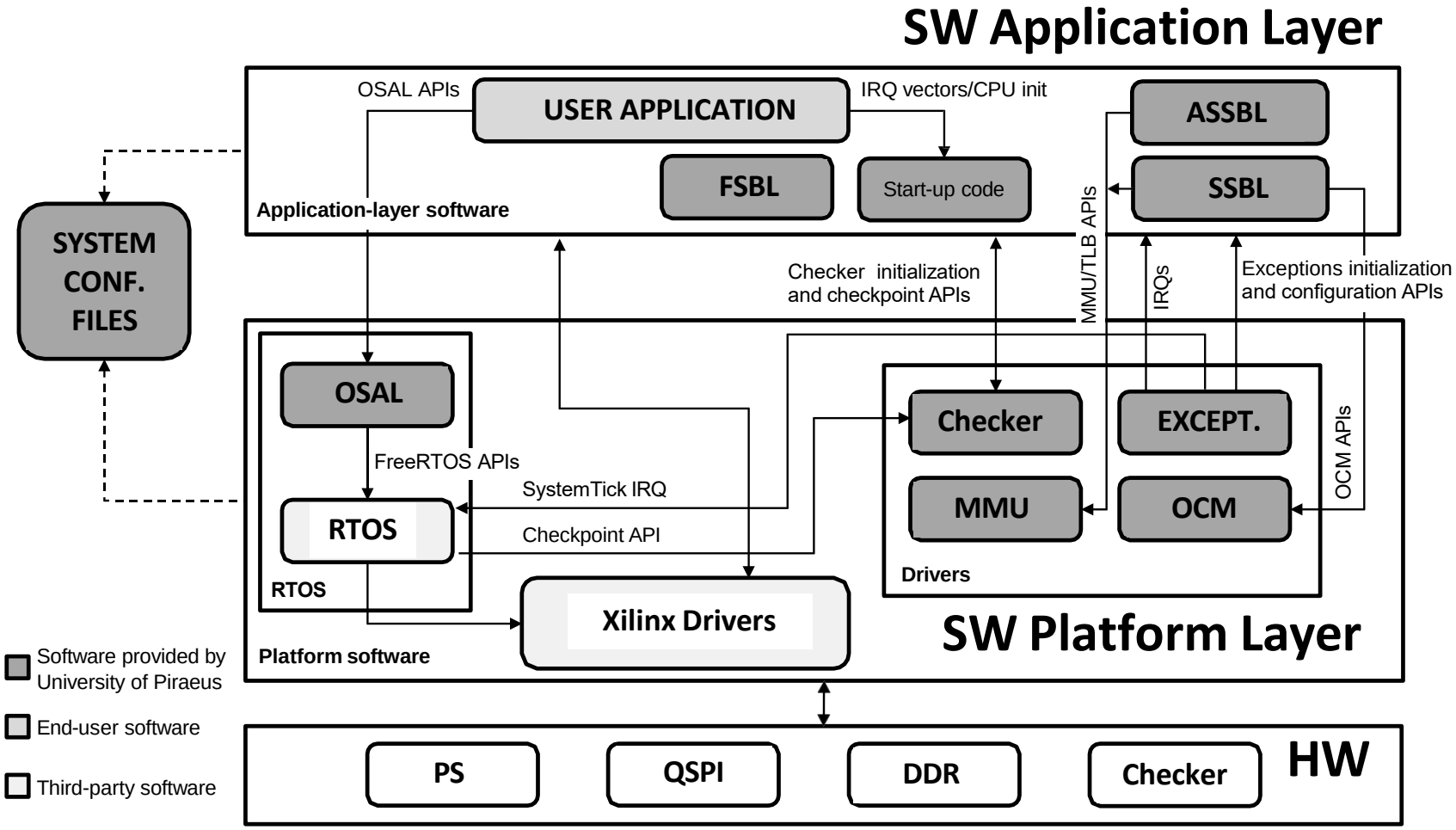


SOFTWARE ARCHITECTURE

CUSTOM SW | USER SW | THIRD PARTY SW

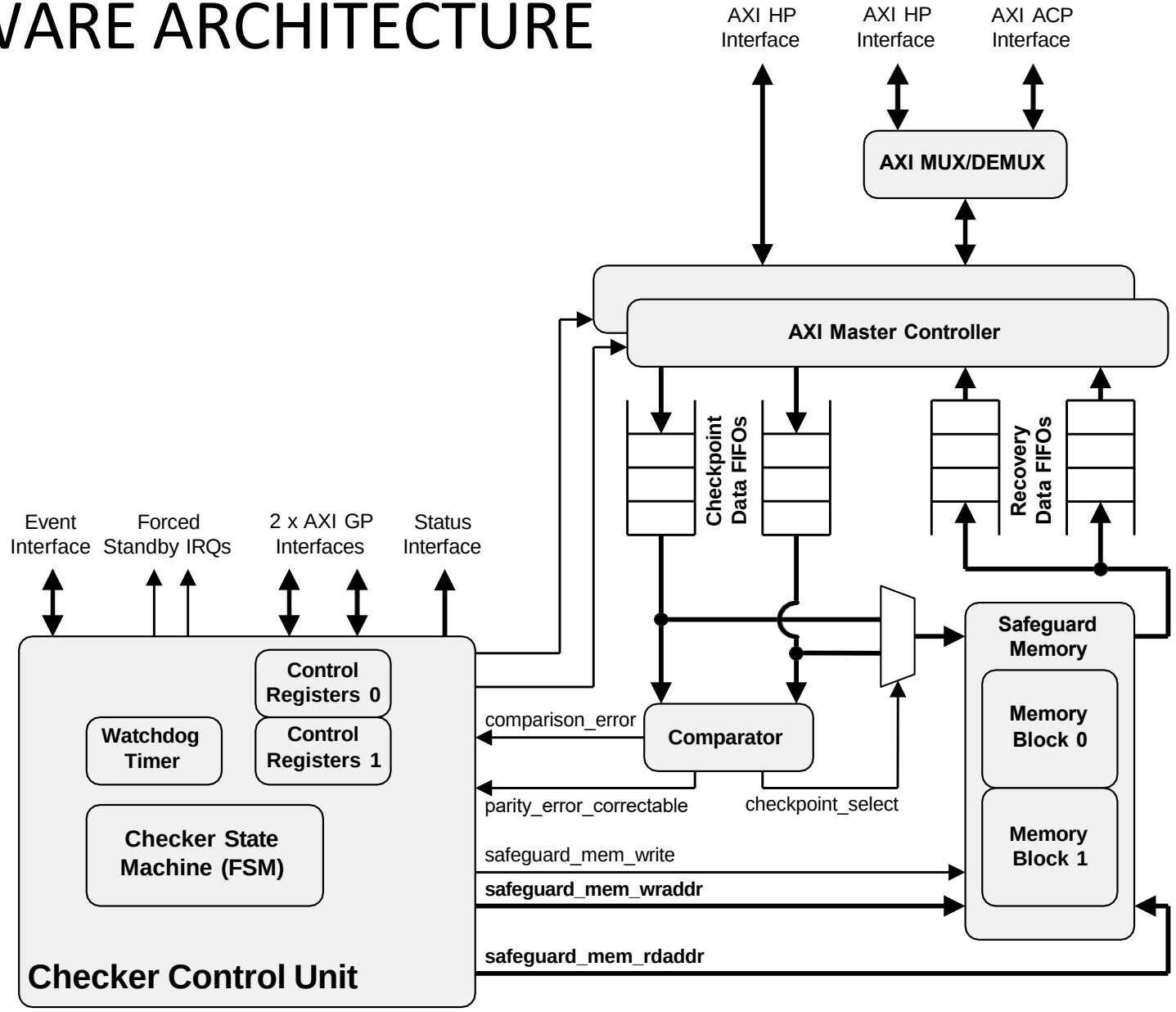
Custom SW

- Application Layer
  - Start-up code (ASM)
  - FSBL
  - Auxiliary SSBL (ASSBL)
  - SSBL
- Platform Layer
  - OSAL
  - Checker Drivers



CHECKER IP CORE: HARDWARE ARCHITECTURE

- AXI Master Controller
  - R/W access to APU Data memories
- AXI MUX/DEMUX
  - Core0,1 data in L2, OCM
  - Core0,1 data in DDR
- Comparator
  - Detects errors
- Safeguard Memory (TMR)
  - Ping-pong architecture
- Checker Control Unit
  - FSM
  - Watchdog times
  - Control registers



POST-ROUTING IMPLEMENTATION RESULTS (ZYNQ-7020)

Checker IP (No Safeguard Memory)			
Version	**#LUTS**	**#Regs**	**Freq (MHz)**
Simplex	881 (1%)	1771 (1%)	250
TMR*	7561 (14%)	5523 (5%)	180
*Used Synplify® Distributed TMR			

Complete design: Checker + Safeguard mem + SEM			
Version	**#LUTS**	**#Regs**	**#BRAM**
TMR+ECC	10545 (20%)	5523 (6.8%)	140 (100%)
Checker: TMR protected Safeguard mem: ECC protected			

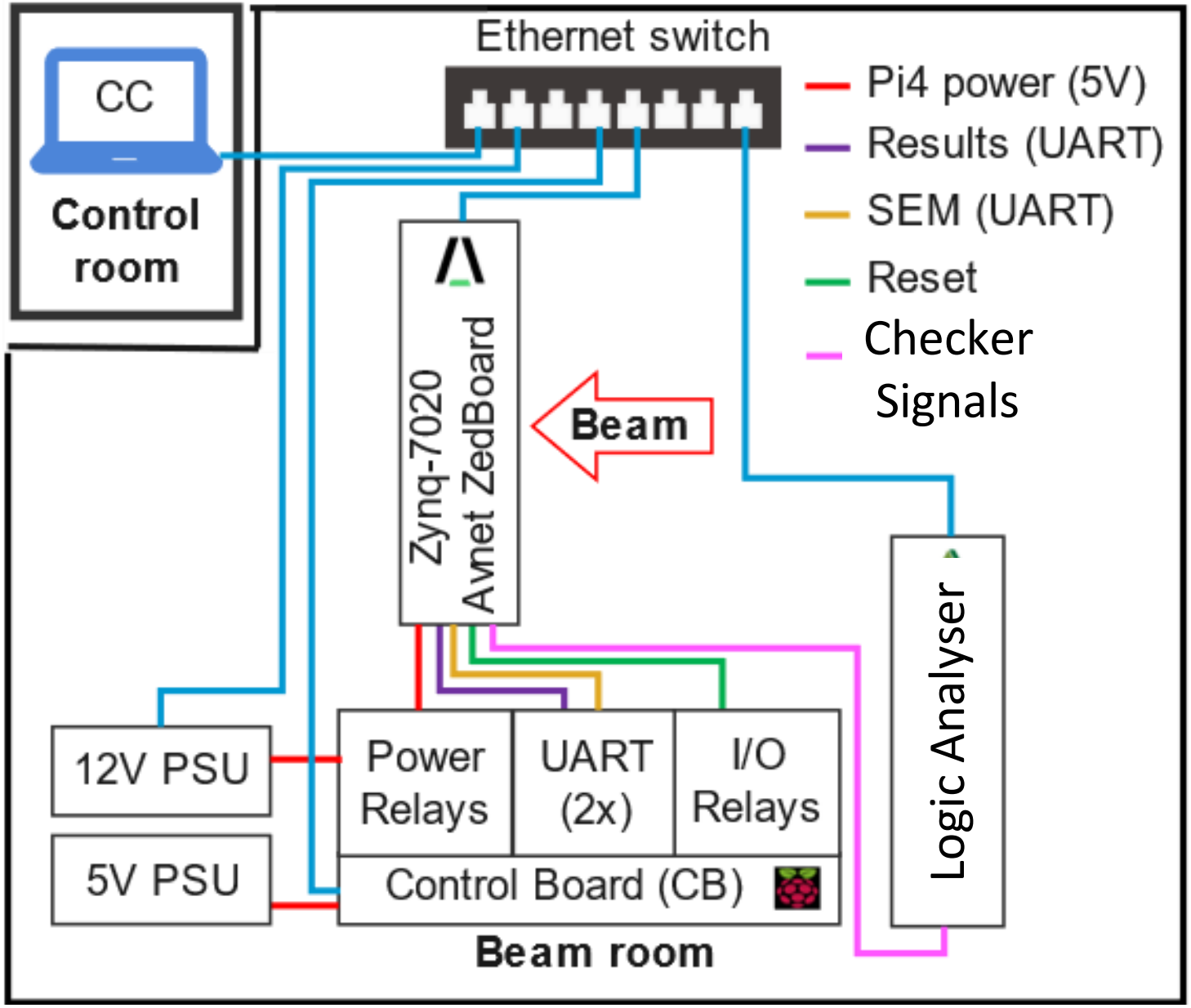
NEUTRON RADIATION EXPERIMENTS
CHIPIR, STFC, RUTHERFORD APPLETON LABORATORY, UK

Beam characteristics

- Energy: > 10 MeV
- Flux: 5 x 10^6 neutrons per cm^2 per second
- Fluence: 3.06 x 10^{10} neutrons per cm^2
- Duration: 102 minutes

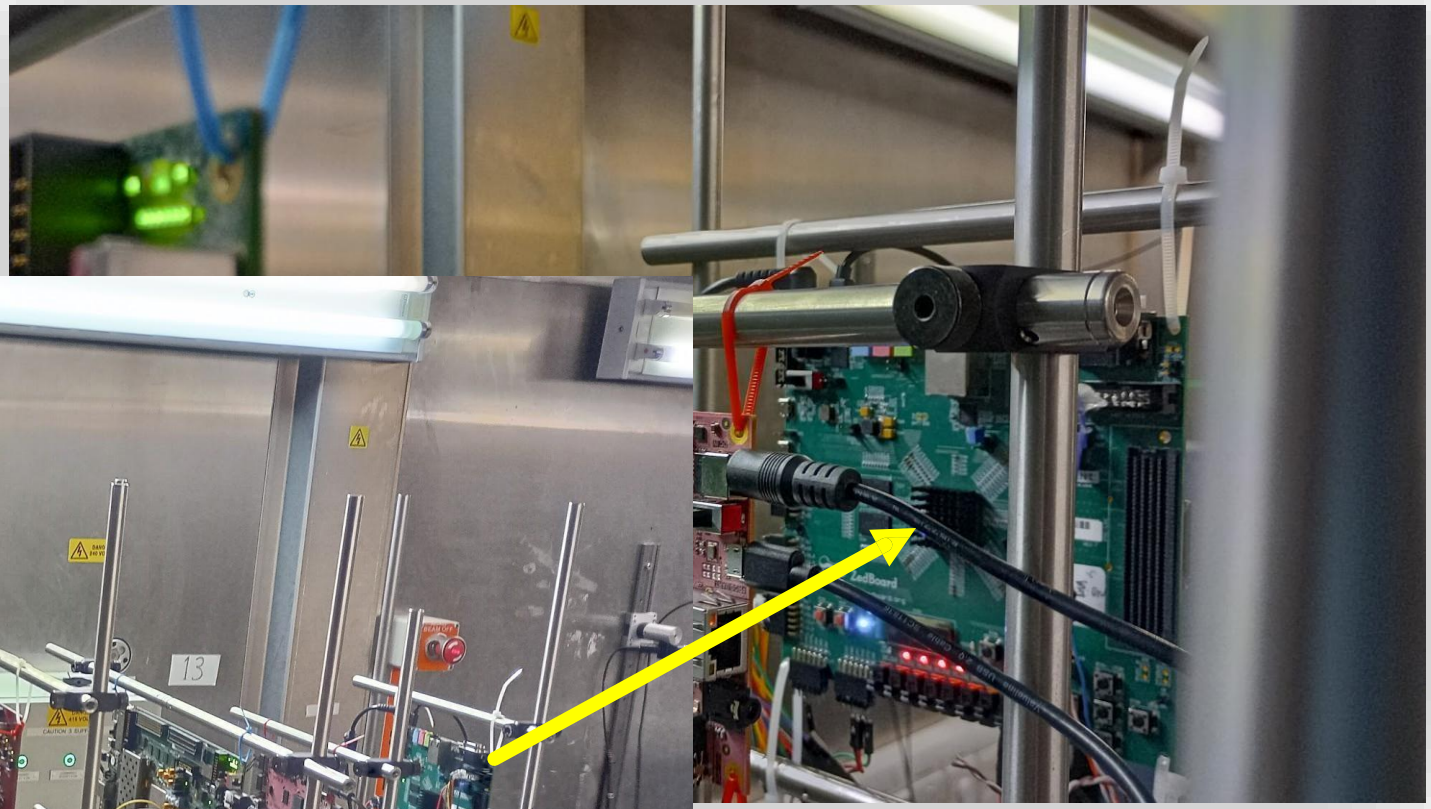
EXPERIMENTAL SETUP

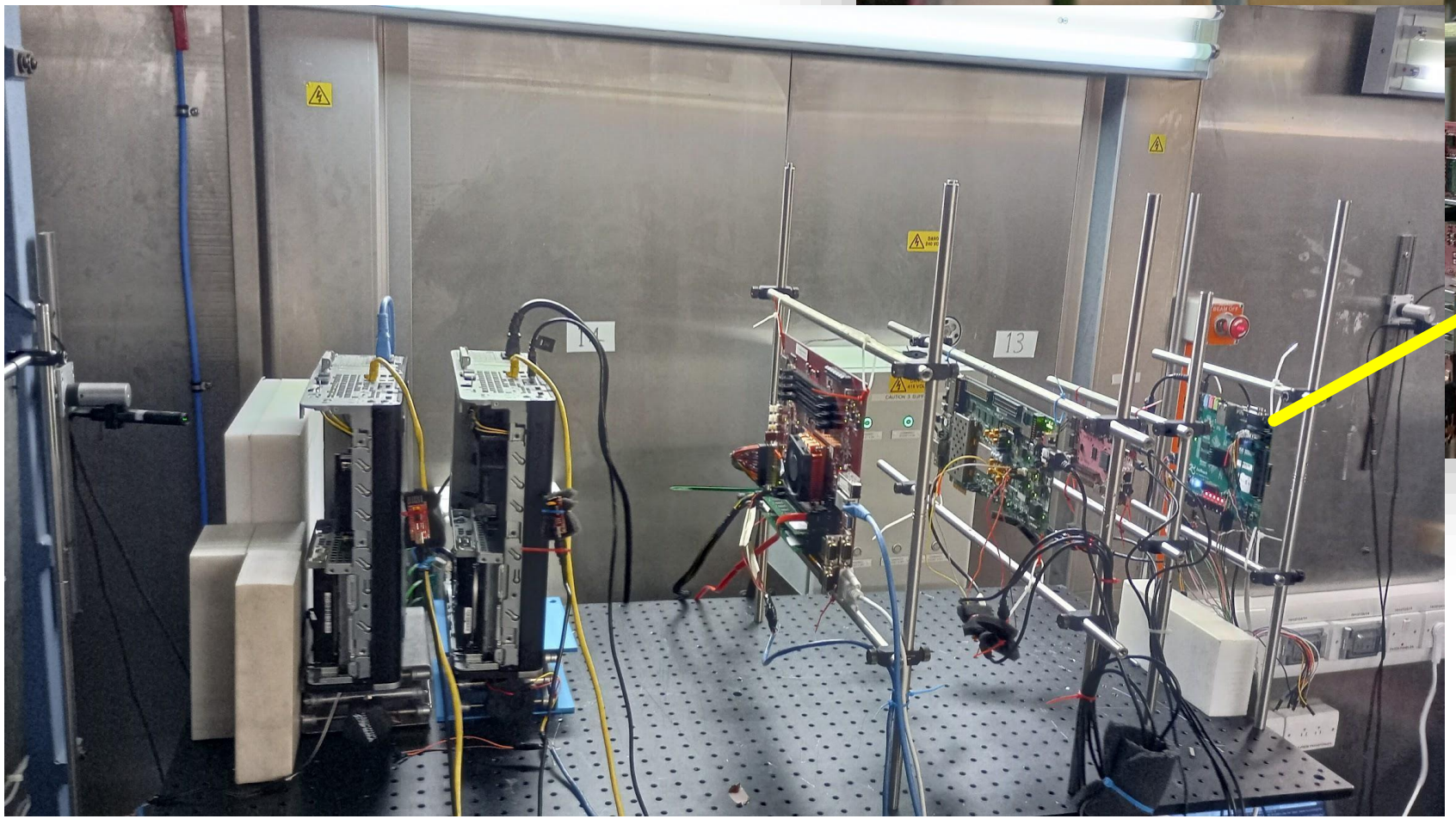
- 2x UART
  - SEM
  - Checker results
- Logic Analyser
  - Monitors Checker IP
- Control Board
  - Captures Results
  - Power C



SolidKosmos

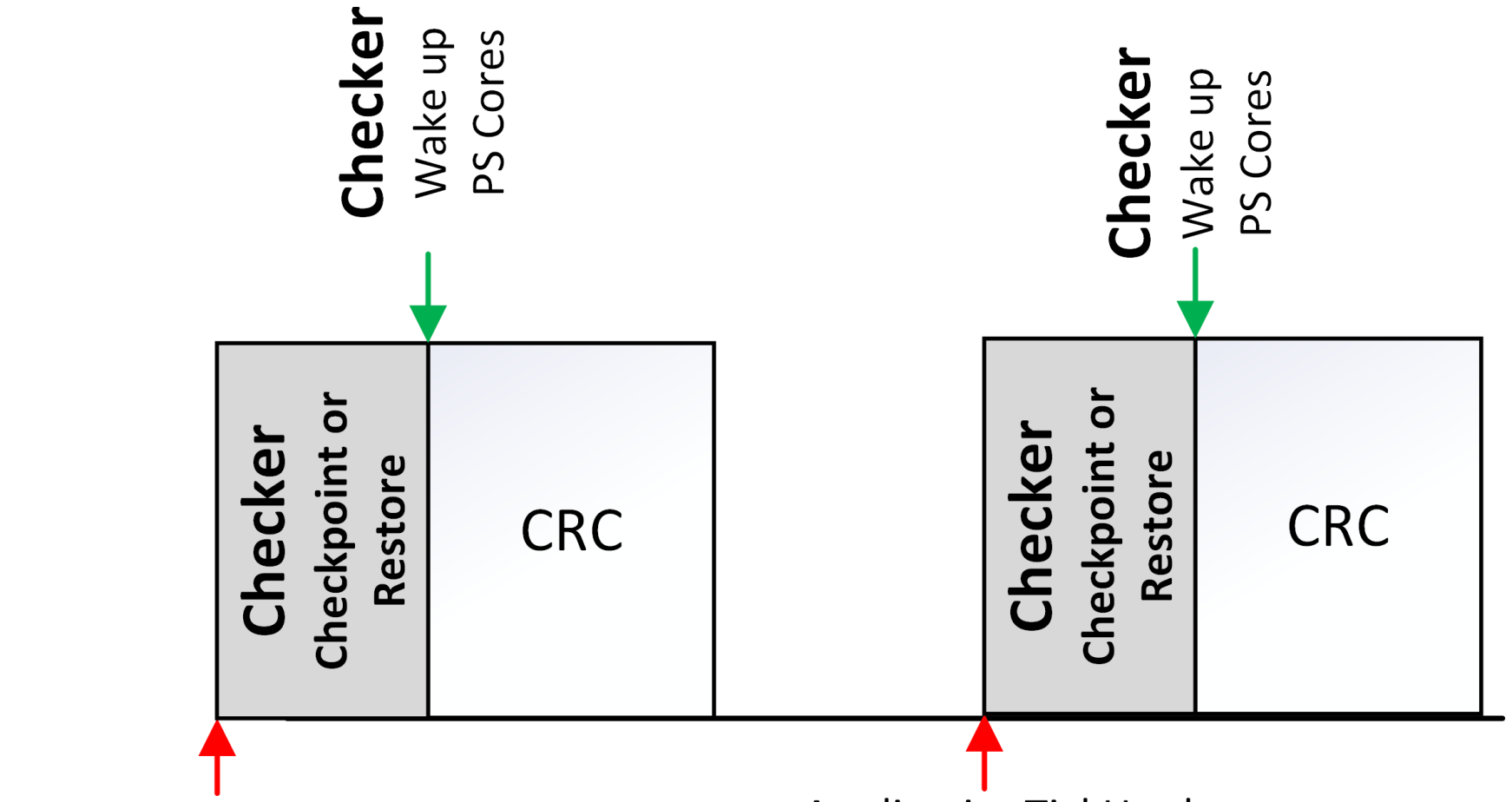
ZEDBOARD IN THE BEAM ROOM





BENCHMARK

- Macro-sync lockstep exec.
- CRC from MiBench
- Checkpoint and Restore

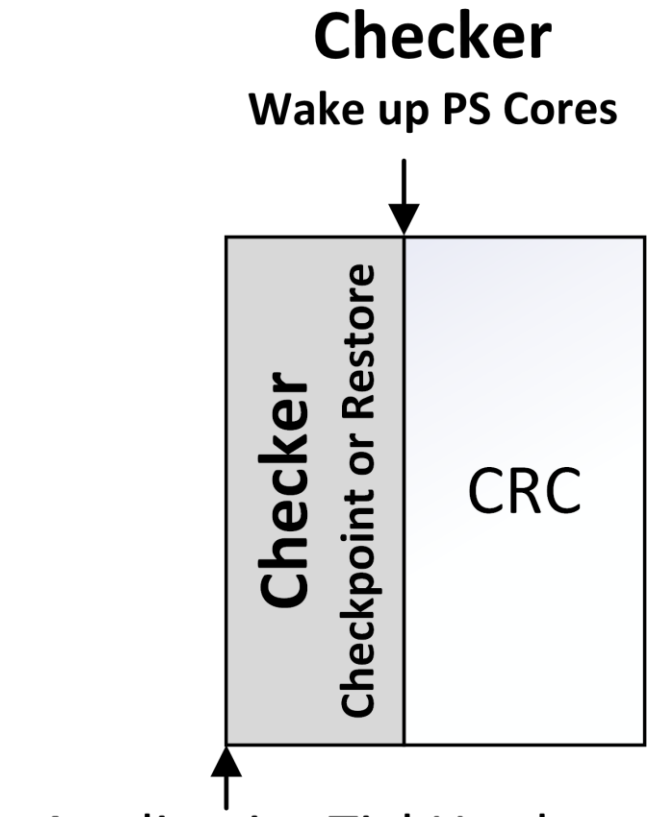



```
vApplicationTickHook
{
   // PowerSave Mode
    __asm (WFE)
}
```

```
vApplicationTickHook
{
   // PowerSave Mode
    __asm (WFE)
}
```

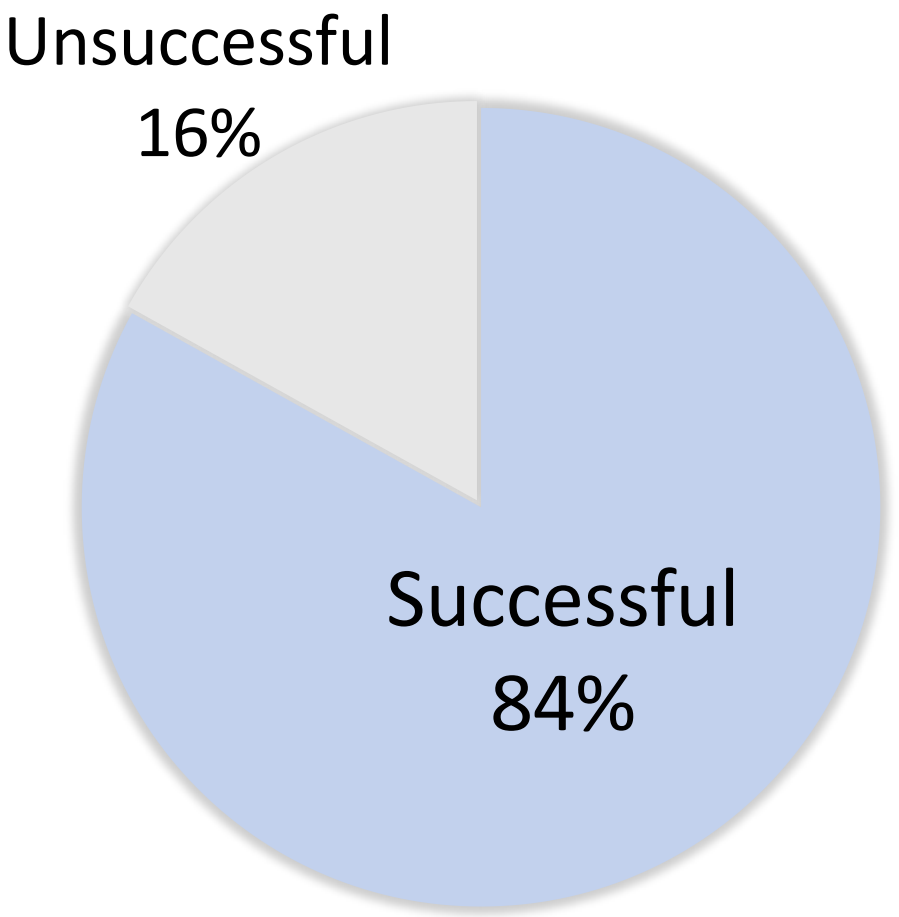
PERFORMANCE ANALYSIS

- CRC Execution: 22 ms
- Error Detection : < 750 us
- Error Correction: 750 us
- Error Recovery: ≤ 1.5 ms
- Critical task slack must be > 1.5 ms
- Overhead: 0.75% to 7.5%
  (For SysTick 10-100 ms)



NEUTRON RADIATION RESULTS

Event Classification	#Event
Fault free execution	18,519
Successful error recovery with rollback	101
Unsuccessful error recovery with rollback	1
Successful error recovery with rollforward	115
Unsuccessful error recovery of “axi parity corrected” event with rollforward	43
Total Benchmark Executions	18,779



THANK YOU!

Let's Discuss How We Can Collaborate to Make COTS FPGA Designs More Reliable

Site: www.solidkosmos.gr

Email: sales@solidkosmos.gr

SolidKosmos

UNIVERSITY OF PIRAEUS
RESEARCH CENTER
Spin-off

esa BUSINESS INCUBATION CENTRE Greece