SAND2017-2897C

Implementation of a Loosely-Coupled Lockstep Approach in the Xilinx® Zynq®-7000 All Programmable SoC for High Consequence Applications

GOMACTech 2017

Session 9.3

22 March 2017

Ryan David Kral

rdkral@sandia.gov

Sandia National Laboratories

Albuquerque, New Mexico, USA

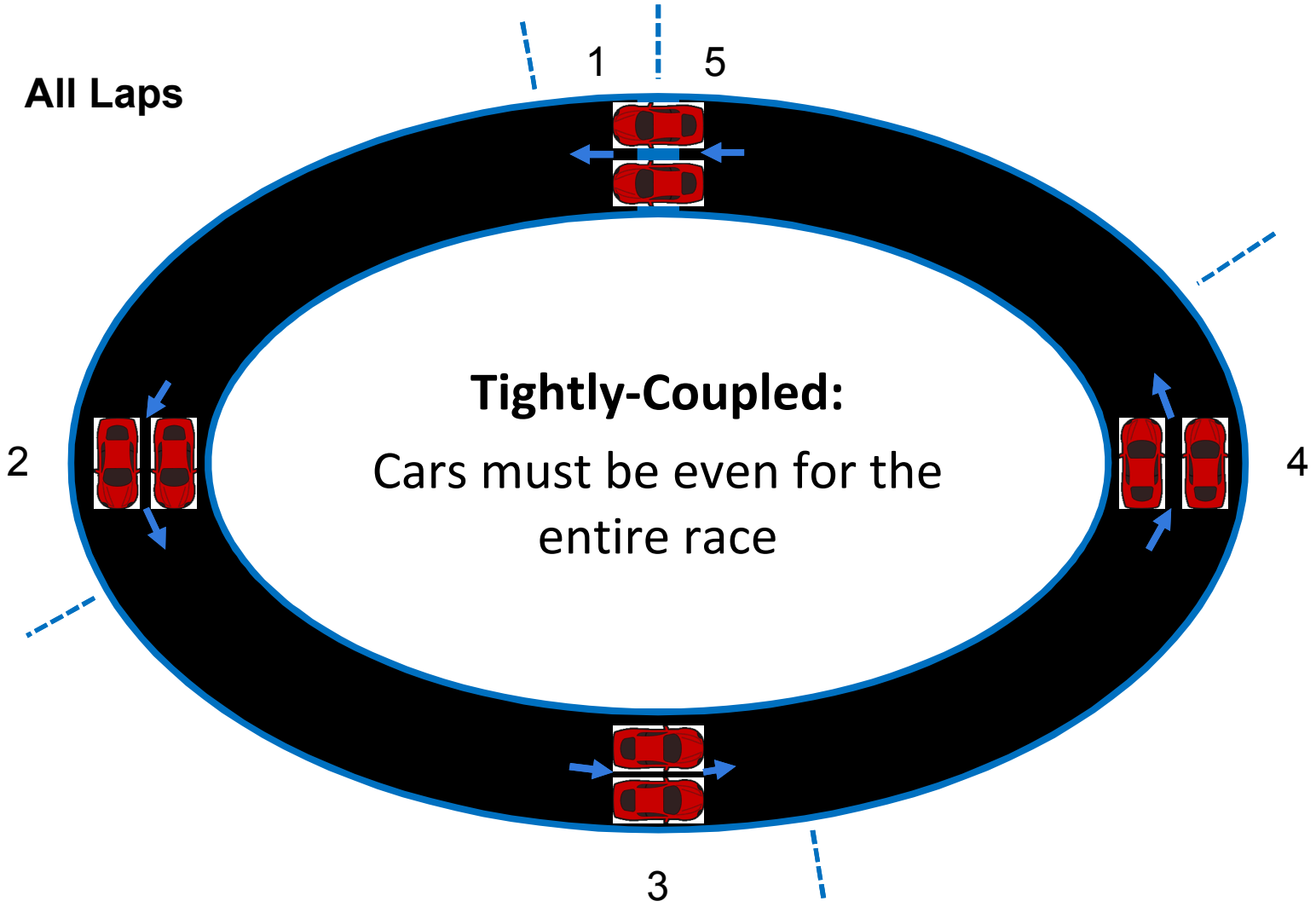
Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Overview

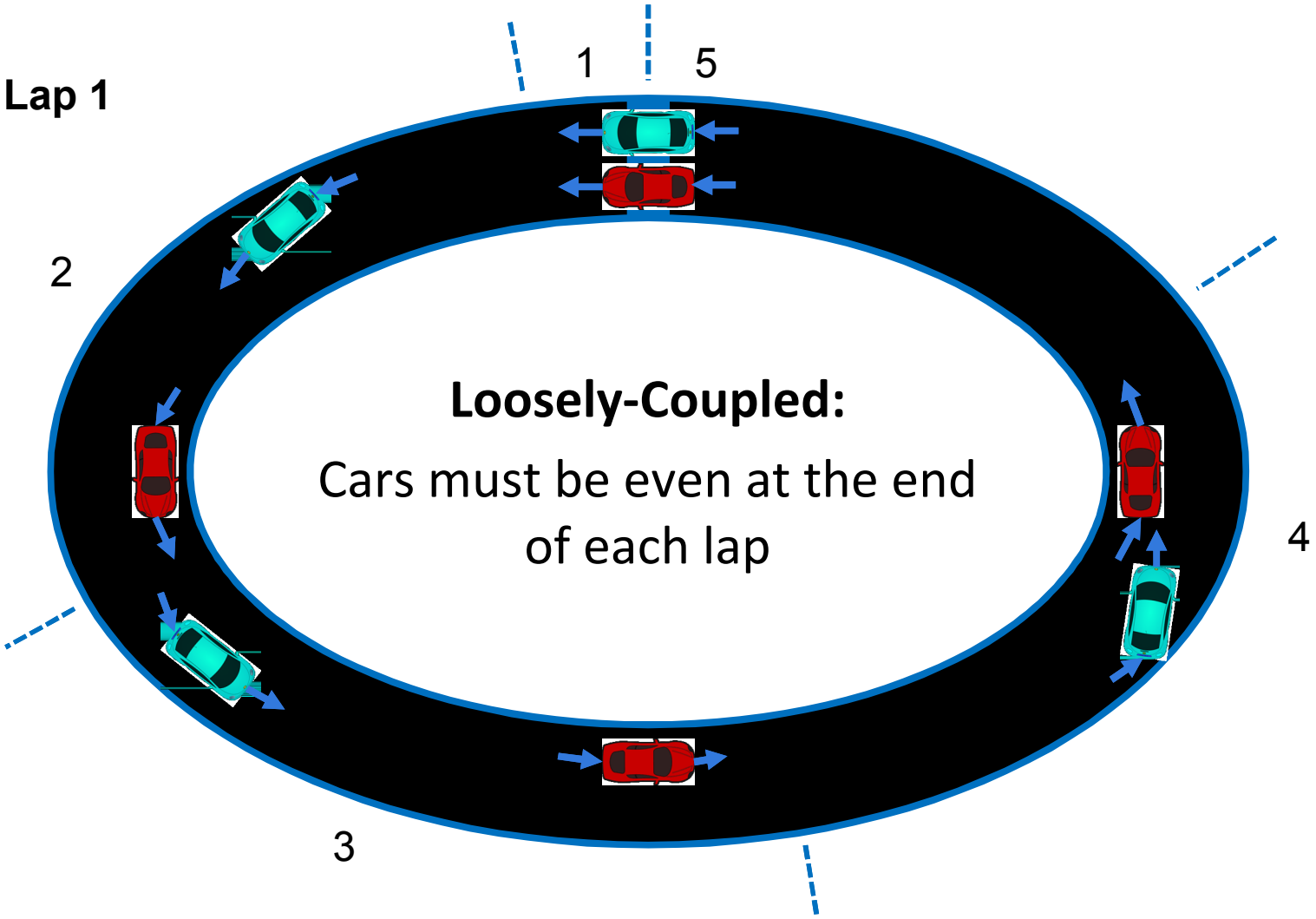
Sandia National Laboratories

- **What:** Develop and implement a loosely-coupled lockstep architecture using the Zynq-7000 System on a Chip
- **Why:** To increase information assurance in a widely used System on a Chip
- **How:** Create the Transaction Checker Architecture which contains a programmable logic comparator that verifies the peripheral accesses of two CPUs running identical code.

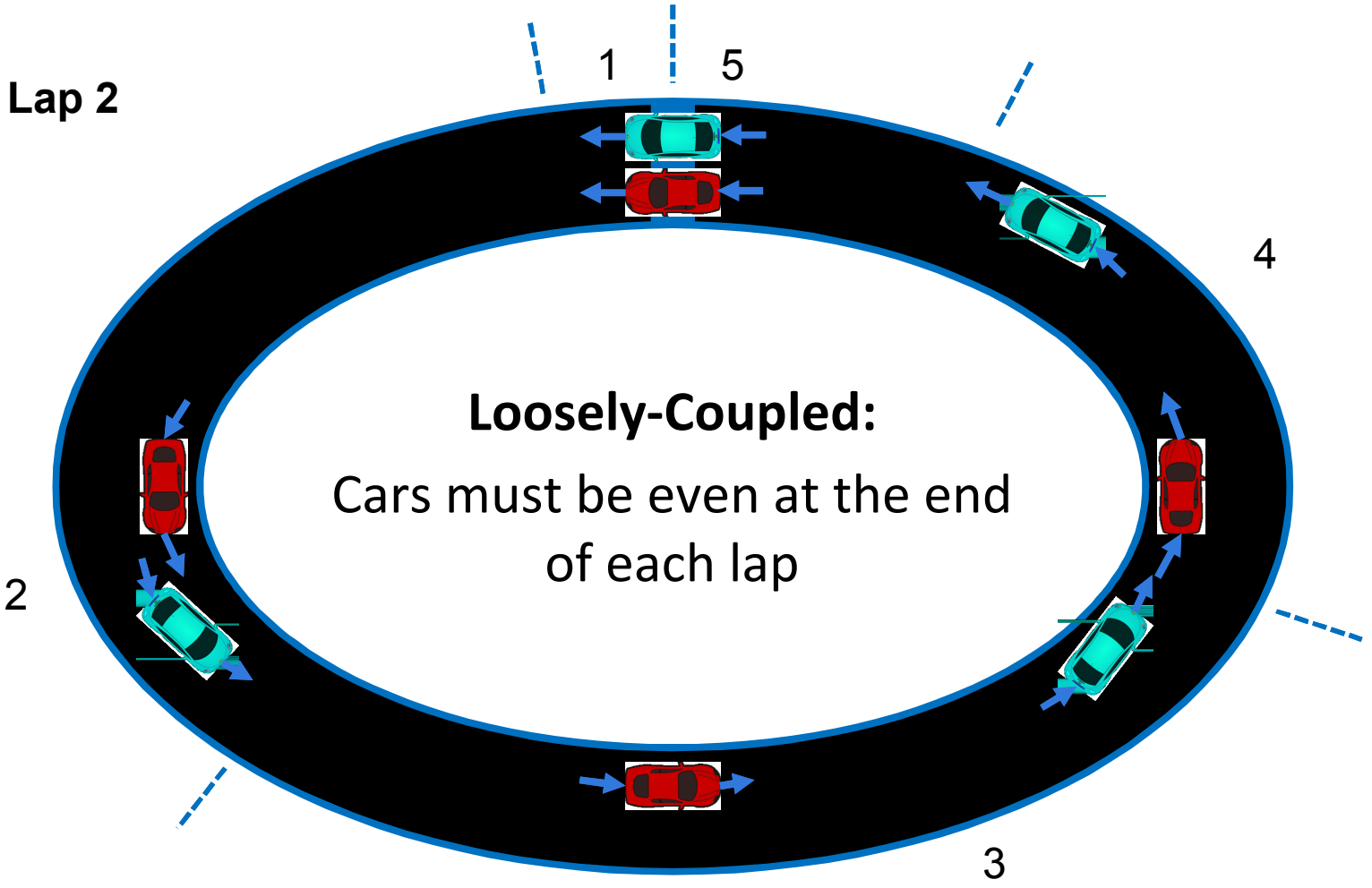
Tightly vs. Loosely-Coupled Lockstep



Tightly vs. Loosely-Coupled Lockstep



Tightly vs. Loosely-Coupled Lockstep



Tightly vs. Loosely-Coupled Lockstep in Computer Architecture

Sandia National Laboratories

Tightly-Coupled

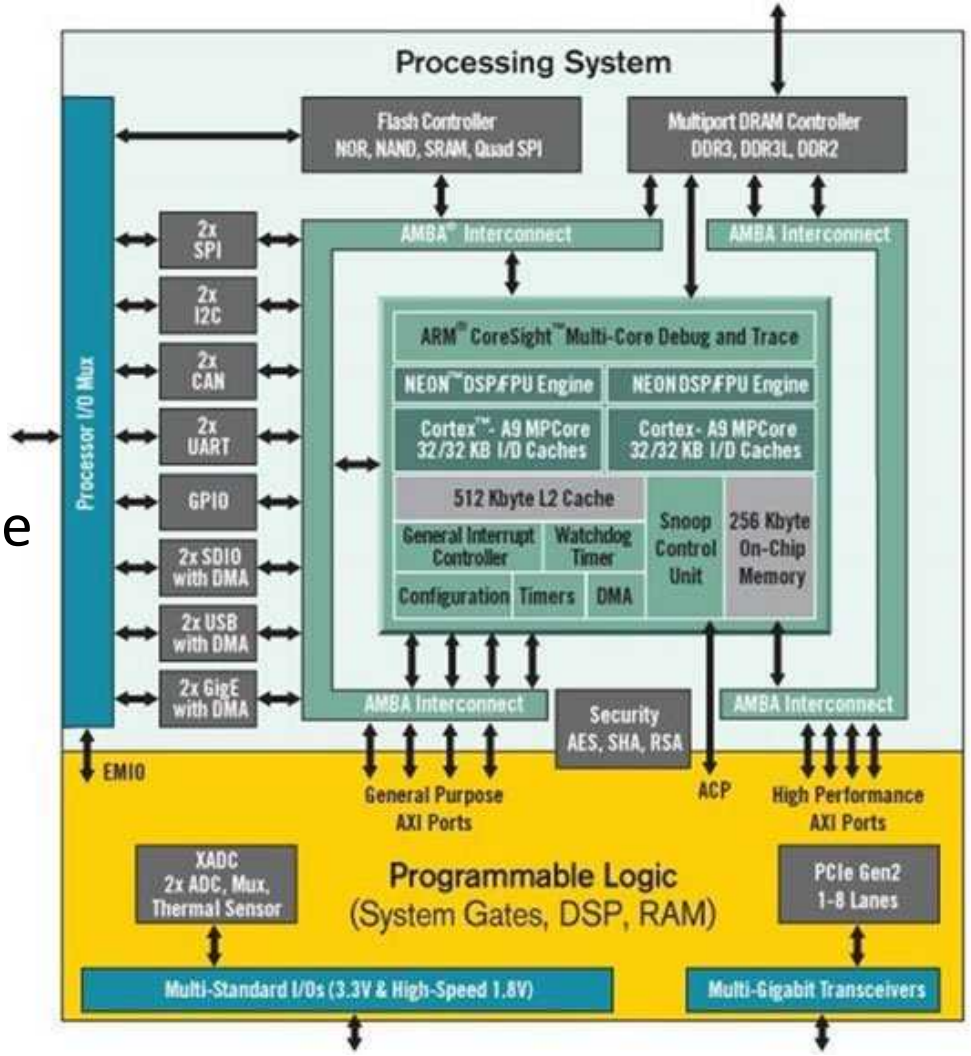
- Requires specialized hardware
- Consistent behavior throughout
- Each instruction is compared before execution

Loosely-Coupled

- Increases hardware flexibility
- Consistency at key checkpoints
- Each peripheral access is compared before entering or exiting the system

Xilinx Zynq-7000 SoC

- Dual-core ARM Cortex-A9 Processing System (PS)
- Programmable Logic (PL)
- PS-PL AXI communication interfaces
- Input/Output Peripherals are accessible from the CPUs or the PL

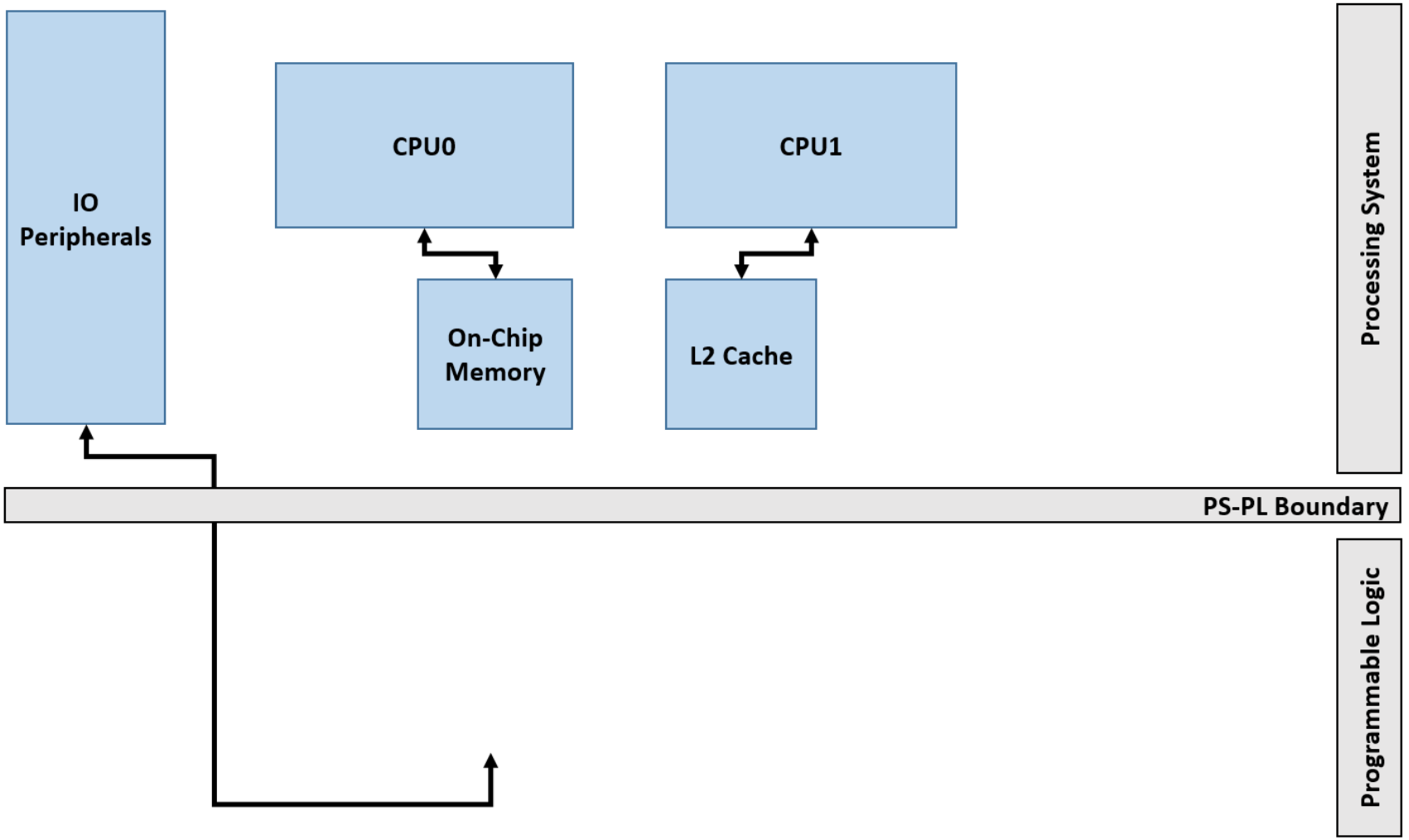


Processing System Configuration

Sandia National Laboratories

- Processor and Memory
  - Each CPU is configured to run identical code from separate memories
    - CPU0 runs from On-Chip Memory
    - CPU1 runs from L2 Cache
  - Memory Management Unit and Snoop Control Unit
    - Prevent CPUs from accessing each other's memory
    - Prevent CPUs from accessing peripherals
- IO Peripherals (IOP)
  - Register reads and writes involving these peripherals are routed exclusively through the PL

Transaction Checker Architecture



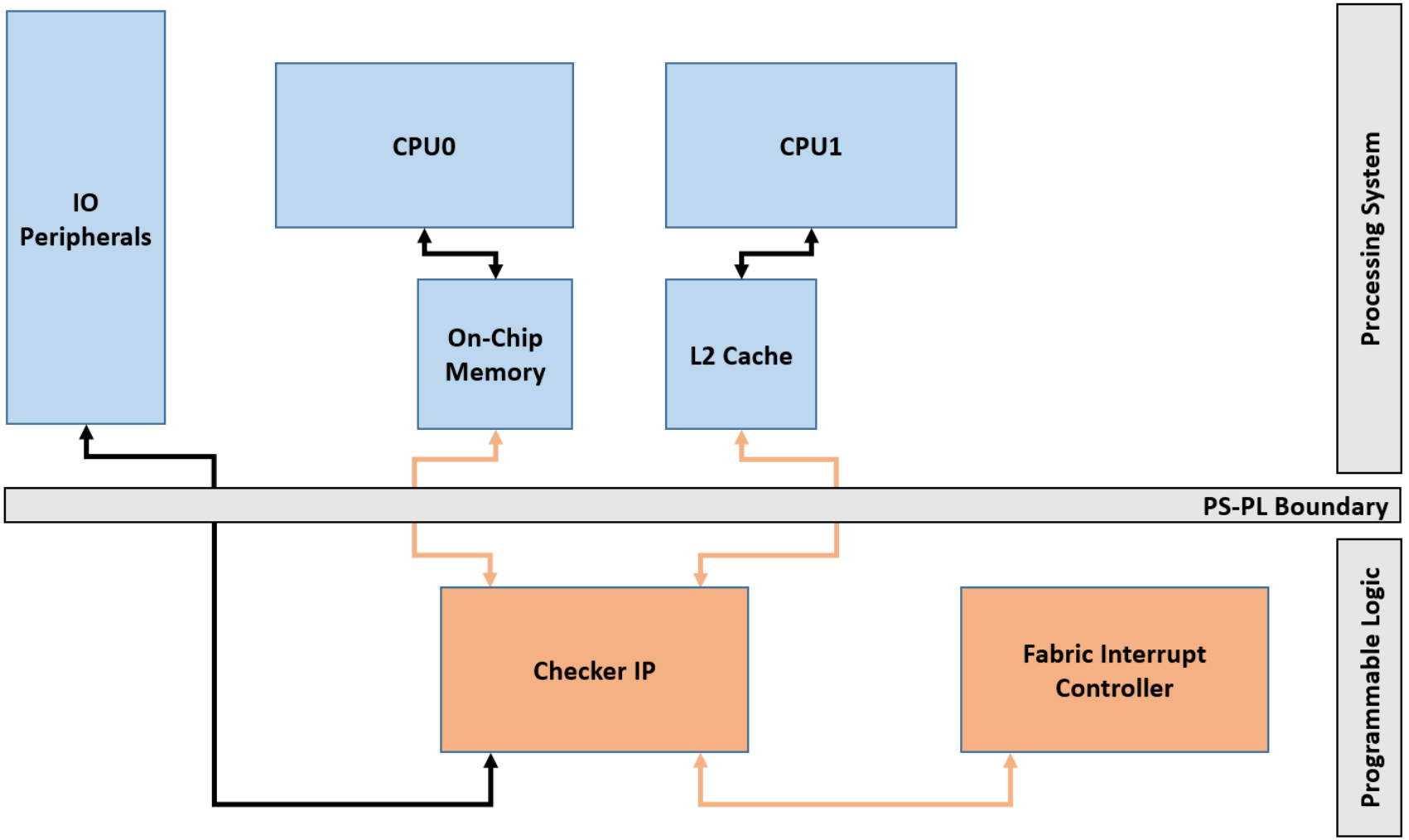
Peripheral Transactions

Sandia National Laboratories

- Shadow Registers
  - Dedicated, 80-byte memory banks for each CPU
  - Control, address, data, and status for a peripheral access are specified in these memories

- Checker IP Functions
  1. Compare the dedicated shadow registers between the CPUs
  2. Perform the peripheral accesses described by the CPUs
  3. Interact with a Fabric Interrupt Controller (FIC)
  4. Detect and report error conditions

Transaction Checker Architecture



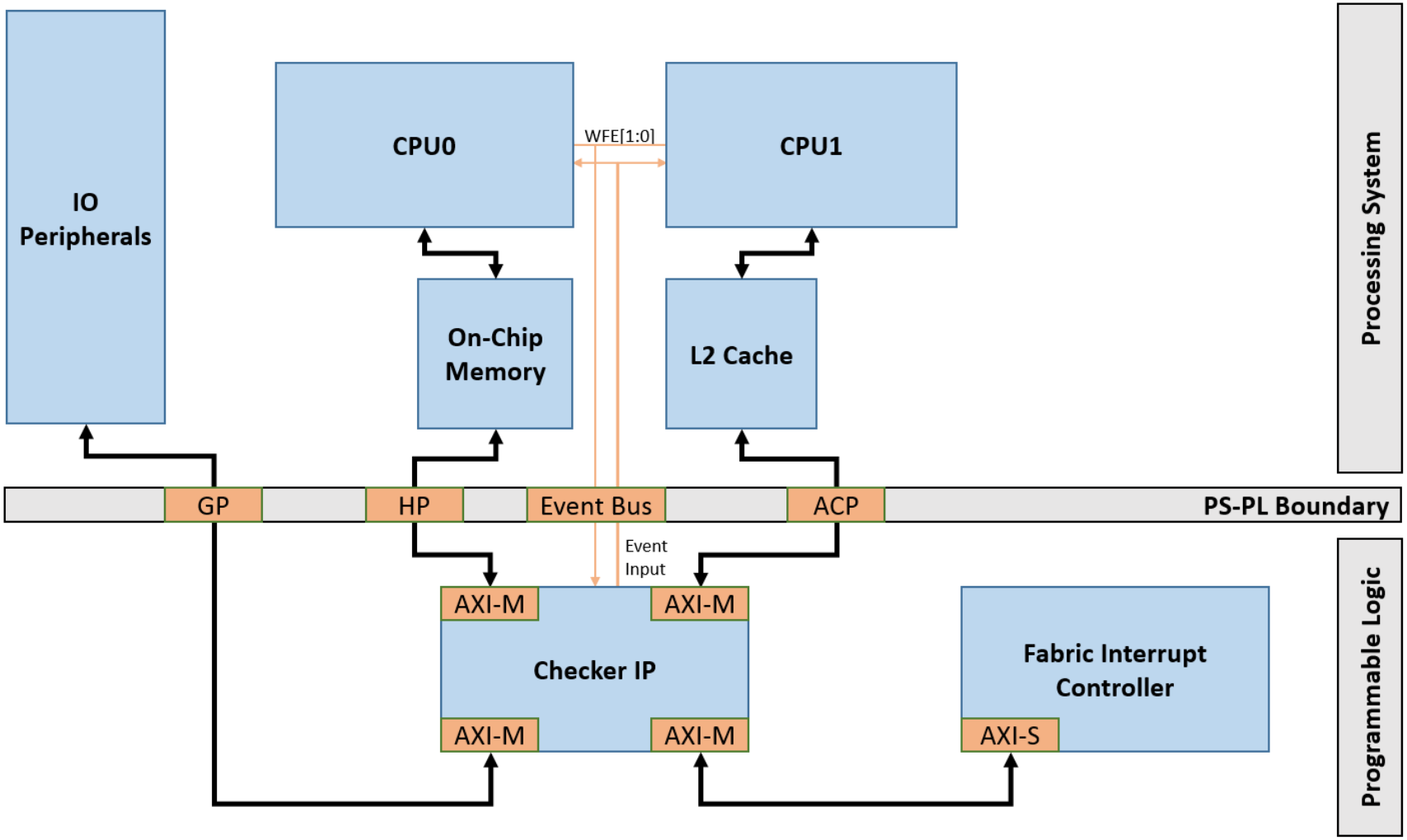
Communication at PS/PL Boundary

Sandia National Laboratories

- Processor Event Bus provides start and end mechanisms for a transaction
  - Wait For Event (WFE) – CPU halts execution and Checker IP starts
  - Event Input – Checker IP ends and processors resume execution

- AXI communication is used for PS⇔PL⇔IOP data transfer
  - 64-bit interfaces between the CPUs and Checker IP
  - 32-bit IO peripheral interfaces

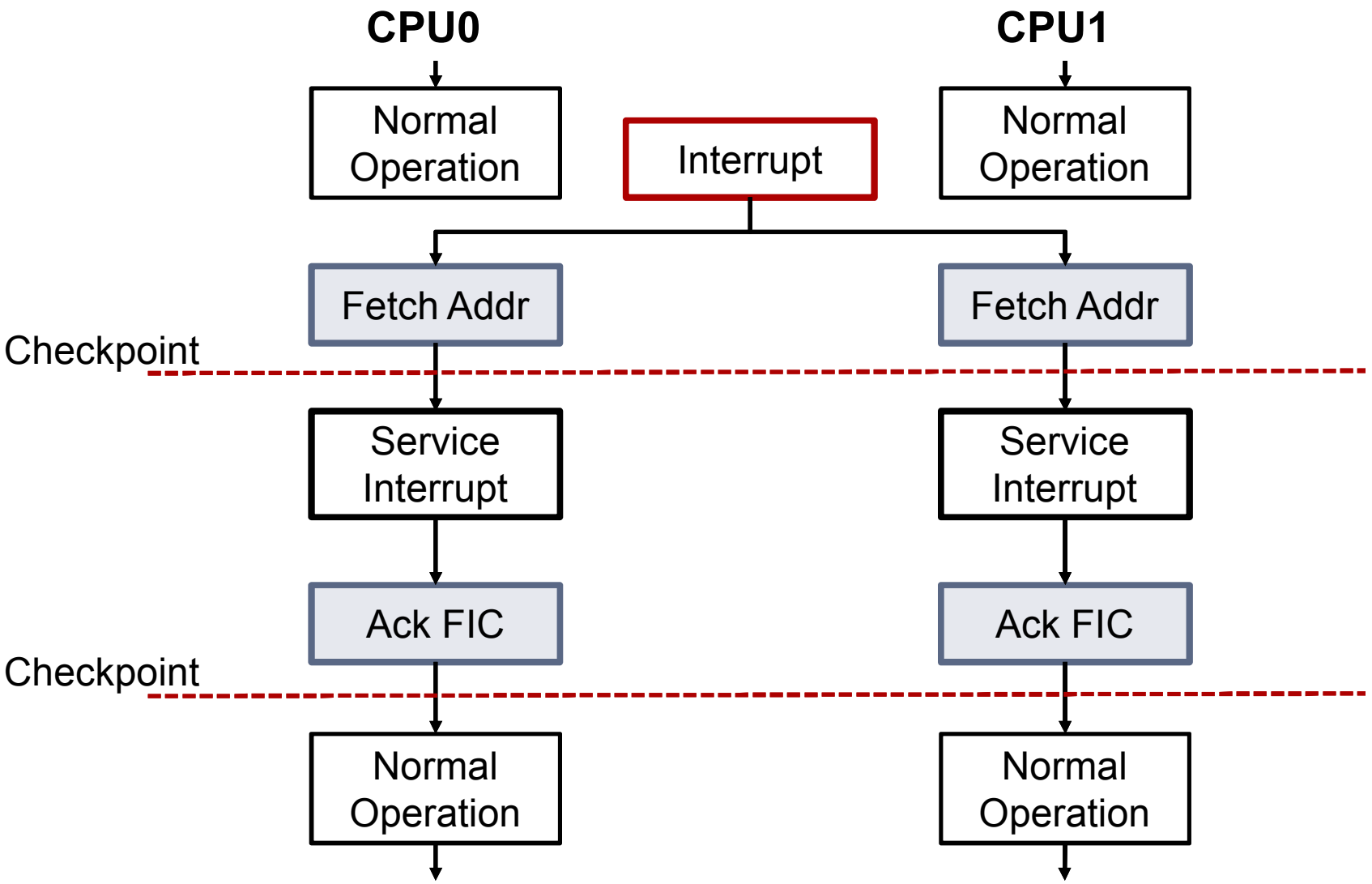
Transaction Checker Architecture



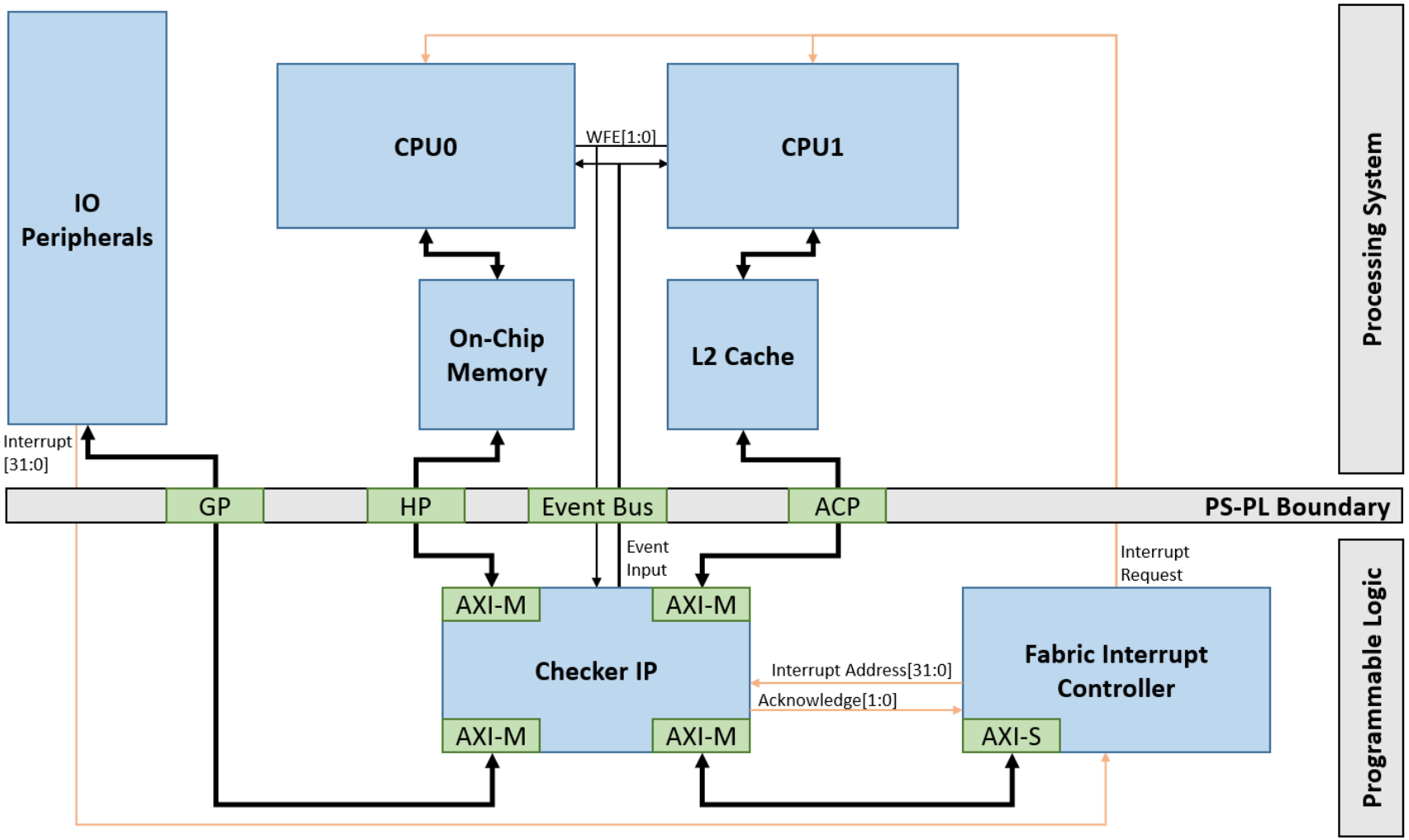
Interrupt Handling

- Both CPUs must service every interrupt
- CPUs cannot access peripherals directly
  - They must go through the Checker IP to access the Fabric Interrupt Controller

Interrupt Handling

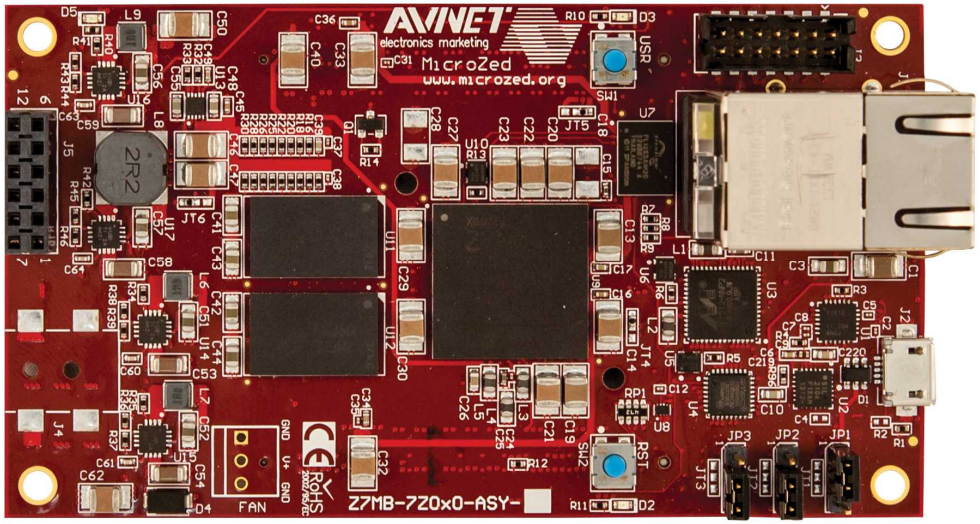


Transaction Checker Architecture

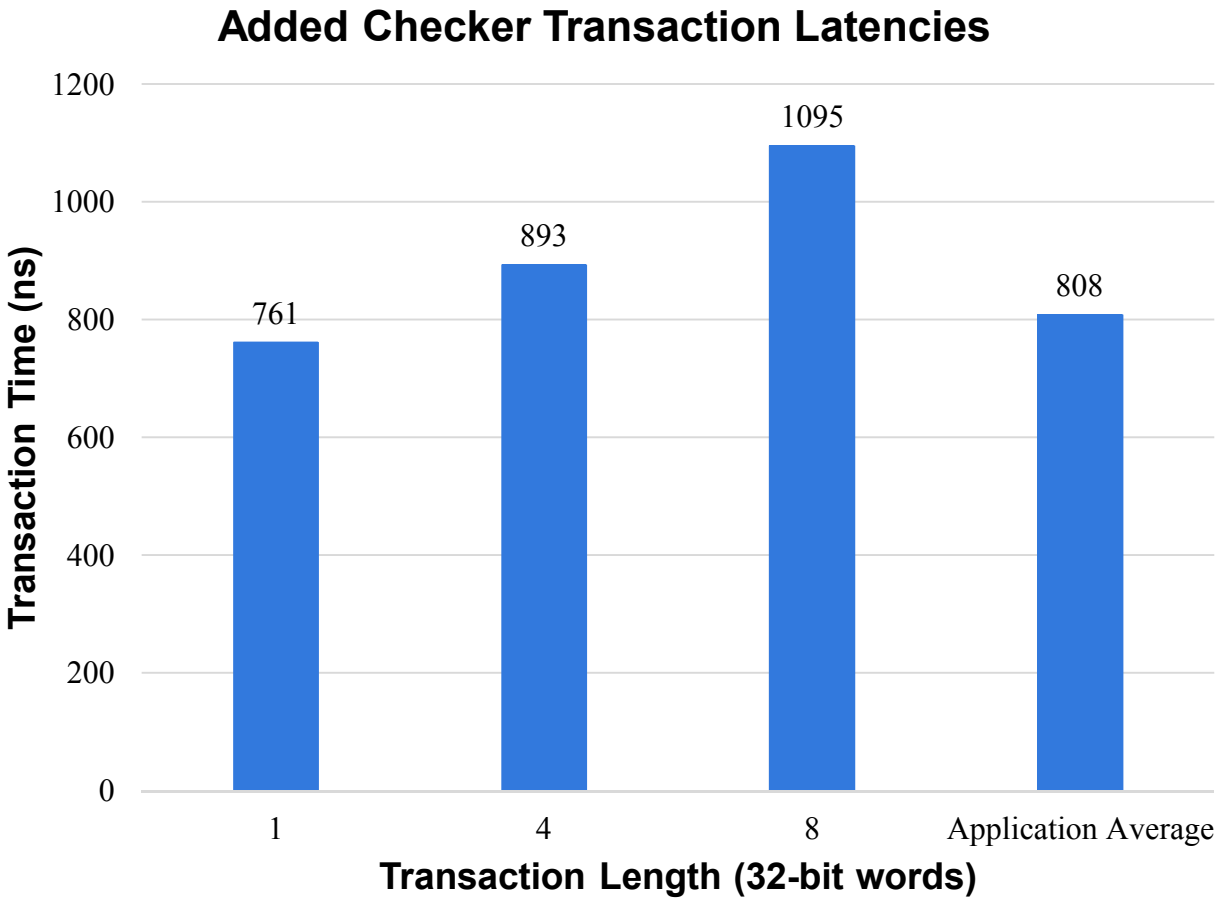


Results – Hardware Testing

- Simulated RTL and implemented in hardware
- GPIO and UART were configured and used for testing of reads, writes, and interrupts



Results – Latency Measurements

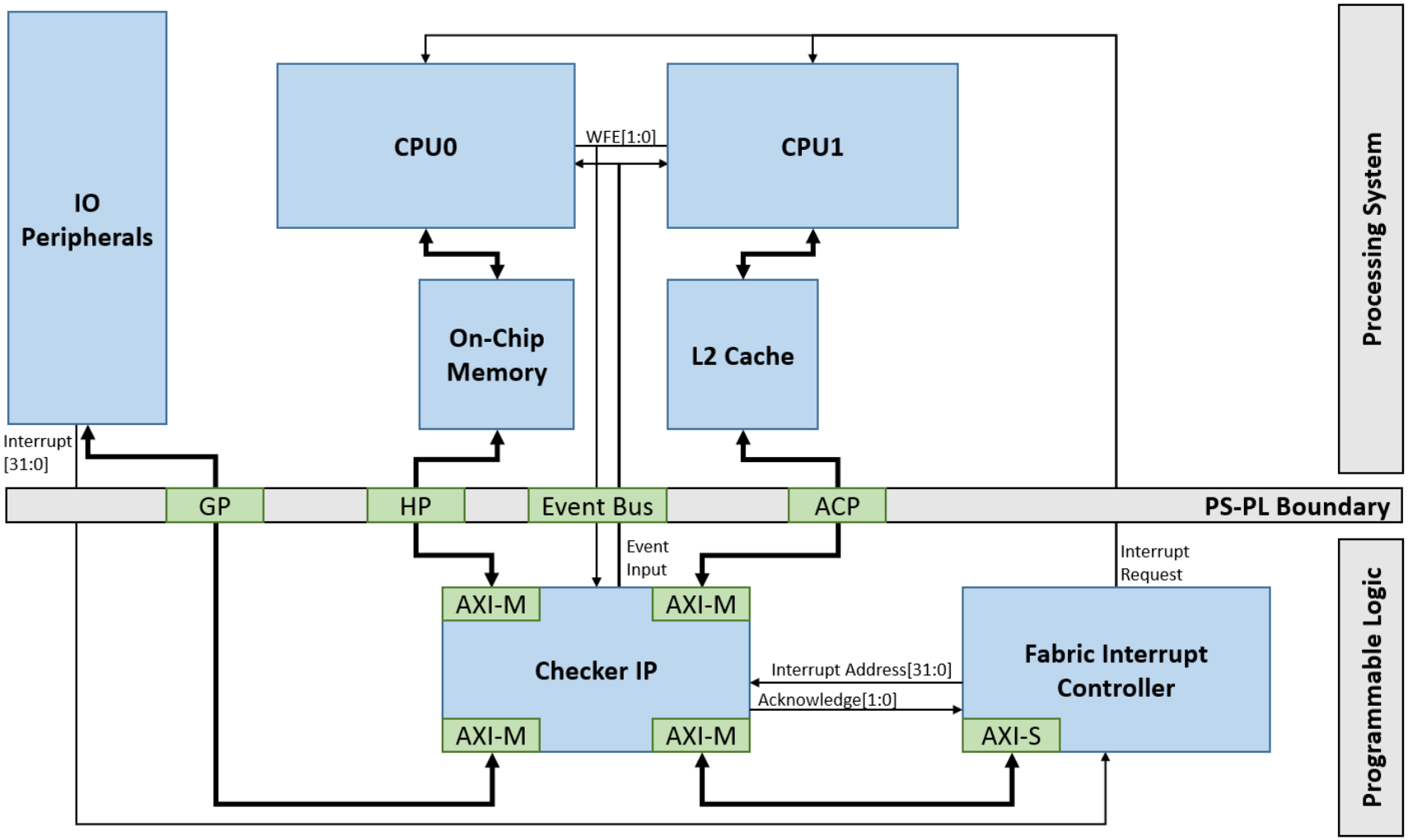


Speeds from 42-233Mbit/sec depending on transaction length

Future Work

- Optimize for speed
  - Only tested PL at 100MHz
  - Parallelize major functions
- Analyze failure modes
  - Only checking for timeouts and failed comparisons
- Implement additional redundancy and error handling

Questions?


IO Peripherals
CPU0
WFE[1:0]
CPU1
On-Chip Memory
L2 Cache
Processing System
Interrupt [31:0]
GP
HP
Event Bus
ACP
PS-PL Boundary
Event Input
Interrupt Request
AXI-M
AXI-M
Checker IP
AXI-M
AXI-M
Interrupt Address[31:0]
Acknowledge[1:0]
Fabric Interrupt Controller
AXI-S
Programmable Logic