CSE 237D: SoC Security
Project Specification

Mahima Rathore | Richa Pallavi

Project Charter:

Project Overview

Extension of the CEP architecture

The Common Evaluation Platform (CEP) is intended as a surrogate System on a Chip (SoC) allowing users to test a variety of tools and techniques.

The Common Evaluation Platform (CEP) was developed to enable and facilitate the evaluation of various integrated circuit (IC) security-enhancing design and fabrication techniques across a variety of DoD sponsored research and development programs. The CEP is a mission-relevant and license-unencumbered System on Chip (SoC) design with representative scale and features such that it can serve as a surrogate for trusted US Government designs. The CEP is an entirely open-source benchmark design that features:

- Scale: Sufficient SoC complexity to stress and challenge defensive design techniques
- Diversity: DoD Mission-relevant surrogate modules that offer diversity of digital computation functions.
- Releasability: Open-source license compatibility permits free distribution to any performer seeking to evaluate a defensive technique.
- Extensibility: Modular approach to design that offers easy adaptation to meet emerging and future evaluation objectives

In summary, the CEP is a DoD-relevant surrogate SoC for IC security technology assessments, and the SETs within the CEP serve as the basis for evaluating the performance and efficacy of those security enhancing technologies.

Project Approach

CEP architecture itself defines just a simple bus architecture for the hardware accelerators, in which the hardware accelerators do not have direct access to memory, instead, the processors are in charge of moving the data for them (hardware accelerators are slaves on the bus).

The step to address to extend the architecture would be:

- Extend each hardware accelerator with a high-performance full AXI master Interface. This mainly means developing an AXI machine with burst capabilities and integrating the machine with the code of each hardware accelerator in the system.
- We would also need to choose/develop a data AXI Interconnect.

- Develop a target shared scratchpad memory for the hardware accelerators.
- Integrate everything in the CEP architecture.

Once the extended architecture is ready, the first thing we want to do is extend the AXI interconnect to implement a configurable memory access control system. This would allow us to set boundaries in the memory access on each hardware accelerator. We want the boundaries to be customizable, so we would extend the AXI Interconnect with a configuration port to be customizable by the firmware. We would also likely develop a simple driver to set the registers in the AXI Interconnect.

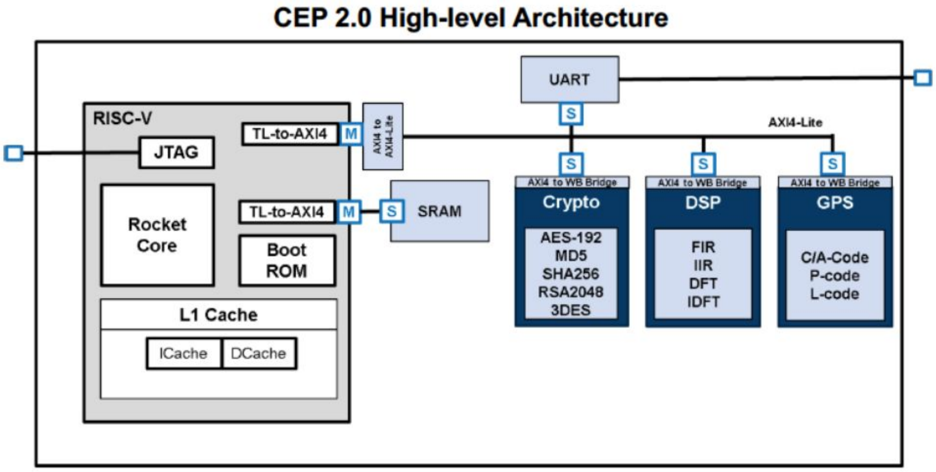

Figure 1: CEP 2.0 High-level Architecture

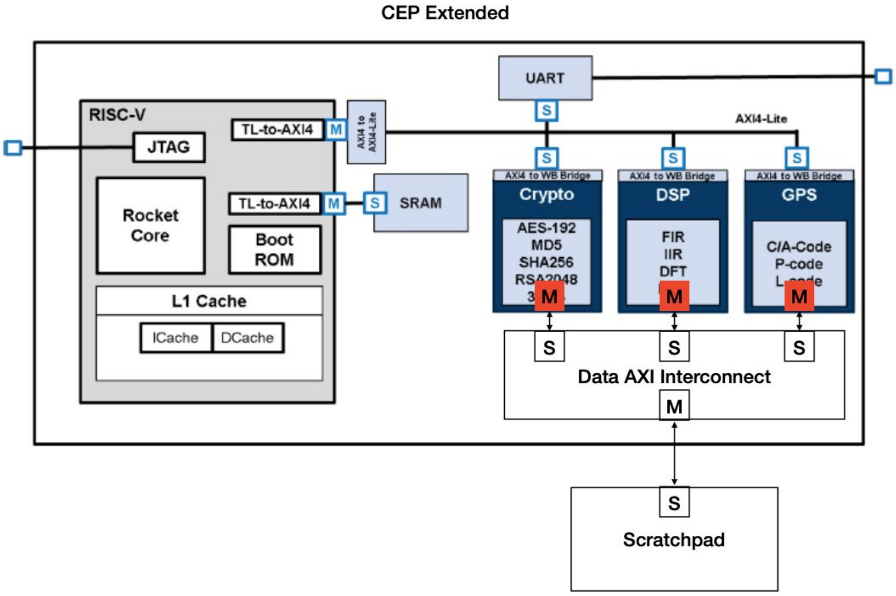

Figure 2: CEP Extended

Project Objectives, Milestones and Major Deliverables

OBJECTIVES AND MILESTONES:

- Extend each hardware accelerator with a high-performance full AXI master Interface. This mainly means developing an AXI machine with burst capabilities and integrating the machine with the code of each hardware accelerator in the system.
- Development of an AXI Interconnect (full AXI). Basic functionalities (routing, burst support). For simplicity, we suppose that the transactions are served in-order.
- Choose or develop a target shared scratchpad memory for the hardware accelerators.
- Integrate everything in the CEP architecture

GOALS OF THE PROJECT FOR THIS QUARTER:

- Development & verification of AXI masters.
- Development & verification of an AXI interconnect.
- Development & verification of target/slave.

POTENTIAL LONG TERM GOALS:

- Integration of all masters and slaves with the AXI interconnect.
- Extend the AXI Interconnect with a configuration port to be customizable by the firmware

DELIVERABLES:

1. 04/23/2020 : Project Specification Document
2. 05/01/2020 : Report presenting the build & simulation results
3. 05/11/2020 : Report presenting code-design & details of the AXI master module
4. 05/20/2020 : Report presenting code-design & details of the AXI Interconnect module
5. 05/29/2020 : Report presenting code-design & details of the AXI slave module
6. 06/05/2020 : Final Report

Constraints, Risk and Feasibility

- Issue we are facing currently is to have access to the server and setup the build. This initial setup might take a few days.
- The AXI architecture design is itself quite complicated and we might face some unexpected challenges while developing or integrating these machines with our SoC architecture.
- The above mentioned challenge might derail us from our scheduled track and we might slip off the schedule.
- Development of masters ,slaves and interconnect needs to be verified. We might have to develop the testbench to verify all the modules with ongoing development.

- Complete development & integration are possible only after the development and verification of all modules which could be tight in this schedule.

Group Management:

TEAM:

- Richa Pallavi & Mahima Rathore.
- We both will be working hand in hand with each deliverable.

WEEKLY WORK SCHEDULE FOR TEAM:

- Meetings every Monday to discuss and create a detailed daily plan for the week for achieving the decided milestones. In addition, this will be helpful in estimating schedule slips and effectively counteracting them in time.
- In case of any prominent difficulty encountered, meetings within the week (mostly Wednesdays) for brainstorming and overcoming the problem to ensure continued progress. Otherwise, regular emails to communicate the progress on the milestones.
- Final meeting on Friday evening to discuss the current status of the deliverables of the week and to plan work for the weekend to ensure that the milestones for the week are completed.

MODE OF COMMUNICATION:

- The main mode of communication will be through meetings and the decisions will be made through discussion and consensus.
- The frequent meetings and micro-planning will help us know when we are off schedule and immediately allow us to deal with the same through efficient replanning.
- We will also be using a Gantt progress monitor so that we are always aware of the amount of work left and the time for the same.

Project Development:

MAJOR DEVELOPMENT ROLES:

Our major development roles include developing verilog modules for AXI interconnect, masters and slaves. Both of us will be working on them together.

HARDWARE AND SOFTWARE REQUIREMENTS:

We are using Xilinx Vivado, Quartus & Modelsim softwares. They are all available to us. We also need a linux platform, which is in the works.

TESTING PROCEDURE:

For testing, we will have a simple verification environment setup to test the AXI designs.

DOCUMENTATION PROCEDURE:

Documentation will be done in the form of a report which will contain detailed description of how each deliverable was achieved, what challenges we faced and how they were resolved. We will demonstrate our work with simulation reports wherever possible. Documentation is integrated within the deliverable at the end of each milestone.

Project Schedule:

Milestone 0 - A complete plan for the project SoC Security after understanding the past developments within the project. Requires a detailed discussion with project leads Francesco & Armita.

Weekly Milestones:

- Understand the current progress of the SoC progress - meeting with project leads.
- Read documentation on firmware security with security policies, AXI protocol & development of fair interconnect for AXI.
- Prepare a quarter-long plan for this project and get it reviewed by the project leads.

Deliverable: Project Specification Document

Due on: 04/23/2020, Thursday

Milestone 1 - Demonstrating working simulation & successful build of the current SoC - CEP Architecture.

Weekly Milestones:

- Figure out the issues related to software and platform required for this project, report them & get them resolved asap.
- Get the set up ready following all prerequisites for working on CEP.
- Build the CEP SoC architecture.

Deliverable: Report presenting the build & simulation results

Due on: 05/01/2020, Friday

Milestone 2 - Development & verification of AXI Masters & complete test-planning for it.

Weekly Milestones:

- Set up project web presence for better information exchange.

- Integrate an AXI full master machine with the CEP hardware accelerators and verify this integrated module - using the burst feature allowed by the AXI standard!
- Integrate the provided AXI master machine code with the CEP hardware accelerators to make them able to issue requests for transactions.

Deliverable: Report presenting code-design & details of the developed module.

Due on: 05/11/2020, Monday

Milestone 3 - Development & verification of AXI Interconnect & complete test-planning for it.

Weekly Milestones:

- Use the skeleton code provided by francesco to integrate with CEP and propose to integrate the memory access control.
- Integrate an access control mechanism on the AXI Interconnect (Multi-memory region). We want hardware accelerators to access just a limited portion of the memory.

Deliverable: Report presenting code-design & details of the developed module.

Due on: 05/20/2020, Wednesday

Milestone 4 - Development and verification of AXI Slaves & complete test-planning for it.

Weekly Milestones:

- Understand the AXI Slave module w.r.t. the interface it communicates with in the CEP SoC and its proposed functionality.
- Integrate a slave configuration port and registers to the AXI Interconnect to set the memory boundaries.

Deliverable: Report presenting code-design & details of the developed module.

Due on: 05/29/2020, Friday

Milestone 5 - Integration of AXI Modules developed.

Weekly Milestones:

- Develop a verification environment for the AXI Modules with testbench, drivers and monitors.
- Complete the verification by running the test cases and debugging any failures.
- Debugging and fixing design for the failures.

Deliverable: Report presenting the verification summary.

Due on: 06/05/2020, Friday

Milestone 6 - Develop a final report for the project.

Weekly Milestones:

- Develop the final report for this project explaining in detail each milestone accomplished, challenges faced and how they were resolved.

Deliverable: Final Report

Due on: 06/10/2020, Wednesday

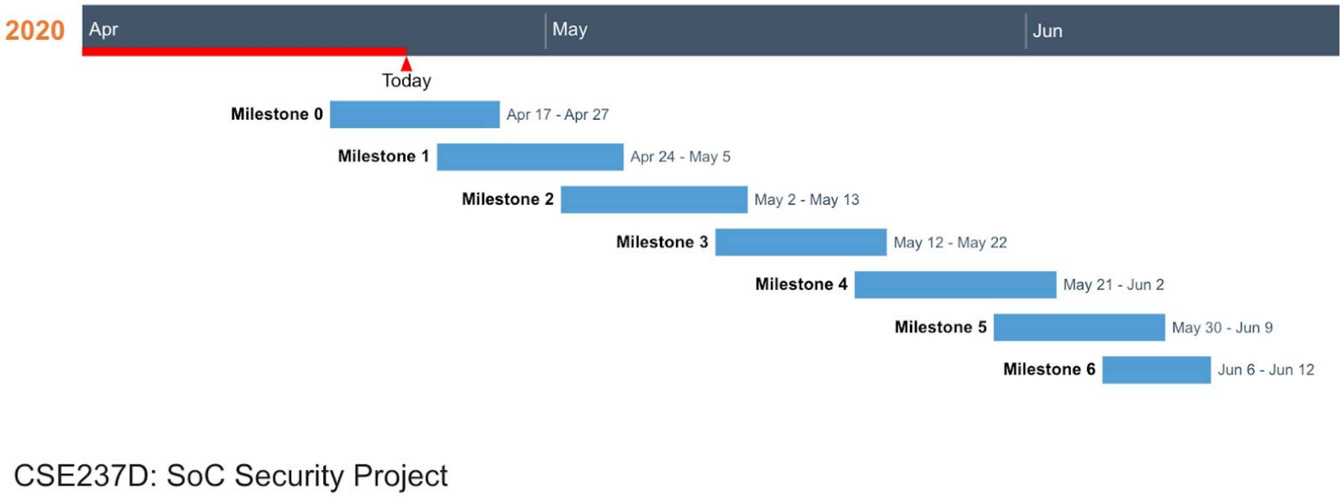

Figure 3: Gantt Chart