EMDALO TECHNOLOGIES

Embedded Software Solutions

QEMU-based Hardware Modelling of a Multi-Hart RISC-V SOC

(with execution contexts free from interference)

Daire McNamara / Dr Ivan Griffin

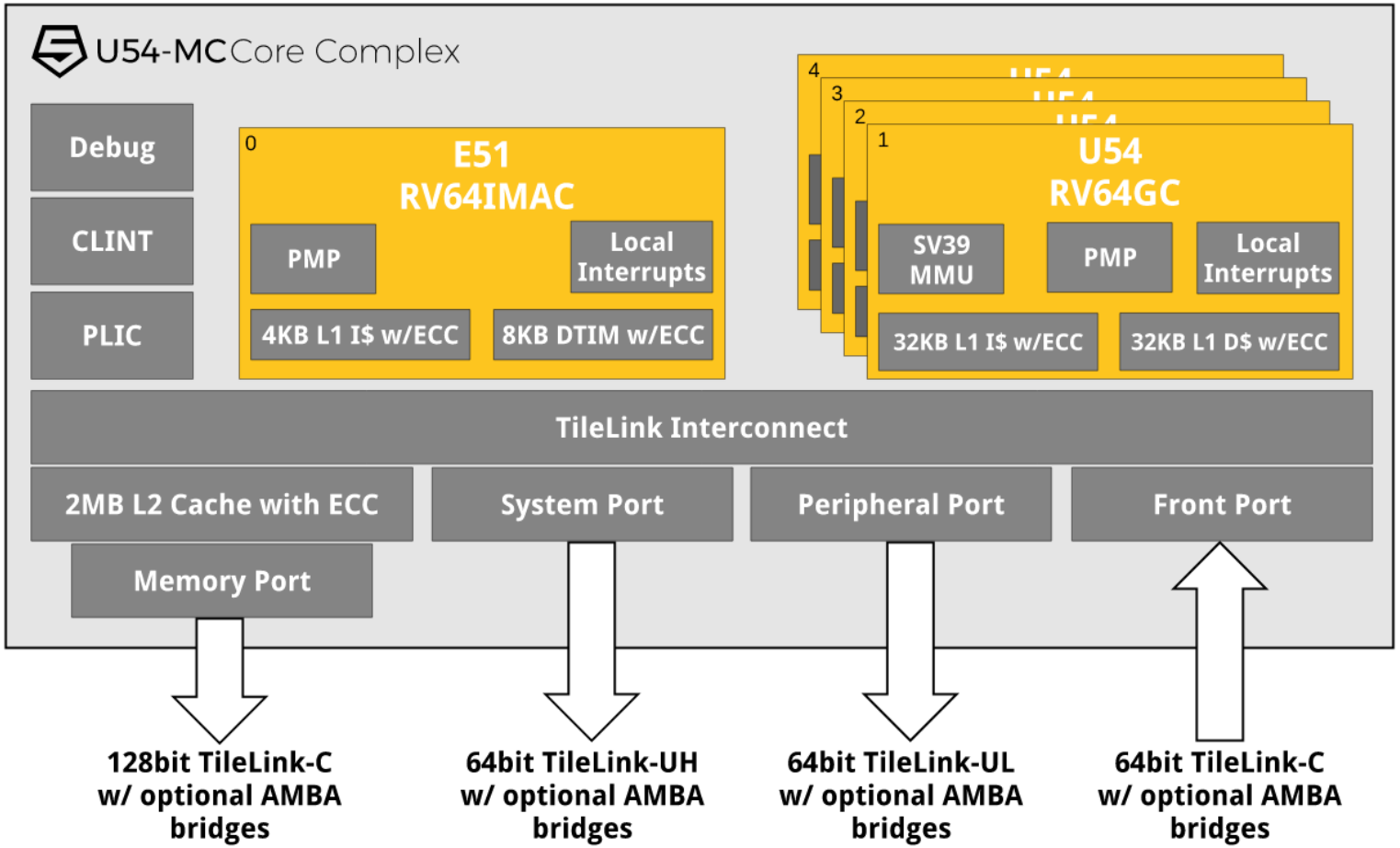
2017-11-22

Agenda

- SOC with Execution Contexts free from Interference
  - E51 and Securing Firmware Services
- QEMU for modelling

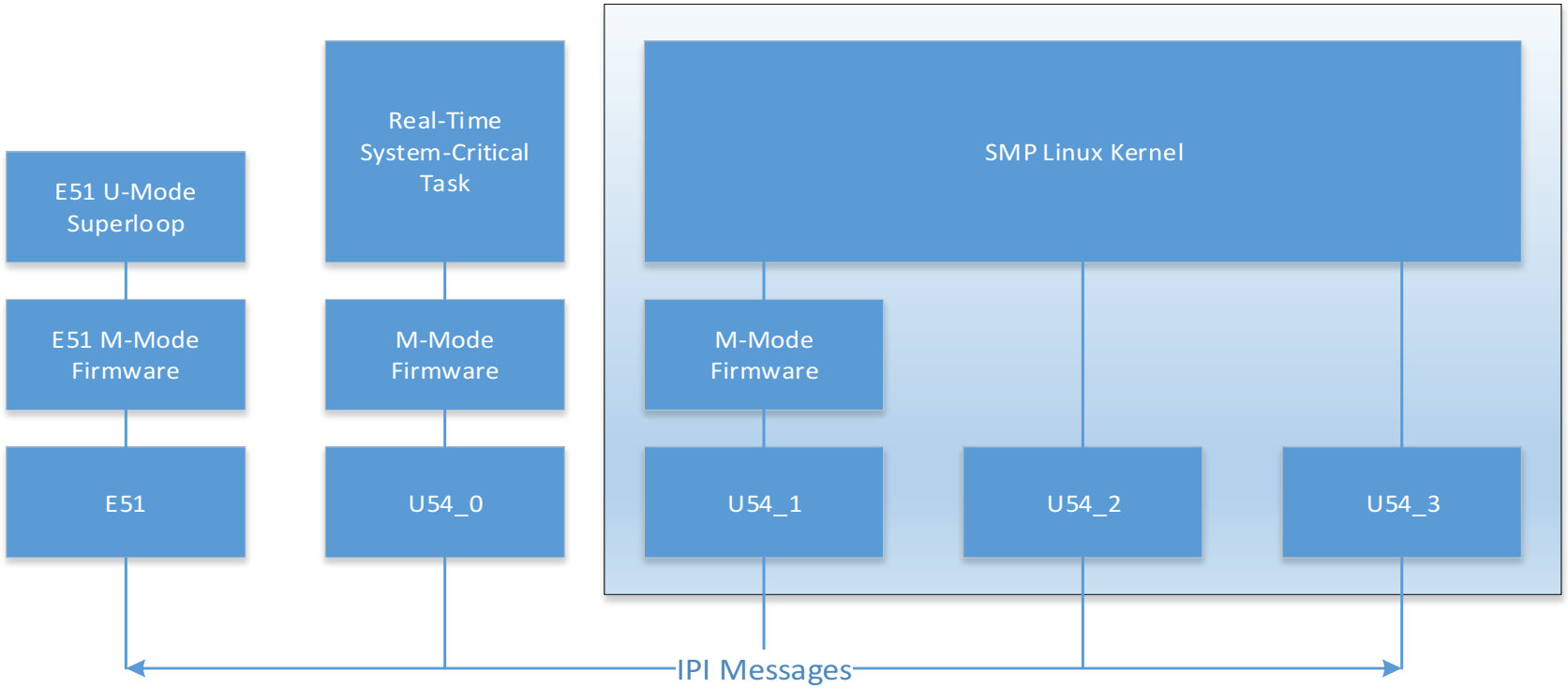
EMDALO TECHNOLOGIES
Embedded Software Solutions

SOC with Execution Contexts free from Interference



EMDALO TECHNOLOGIES
Embedded Software Solutions

SOC Firmware Architecture



- E51 provides services to other U54 Harts:
- E51 is now critical.
- Must be as fault tolerant as possible

E51: Superloop Benefits

- E51 services/peripheral drivers are implemented as event-driven state machines
- State machines are described via a structure and states are named
- Time-triggered schedules can be created to prioritise one state machine over another.

Emulator Required

- To implement and test these firmware services prior to real hardware, we needed a software emulator of the SOC…
- Enter QEMU…
  - User
  - System
  - System provides closest model of the SOC, however user provides ability to instrument and debug Firmware Services code.
- Supports RISCV based architectures
- Needed some extensions to support U54 MC

EMDALO TECHNOLOGIES
Embedded Software Solutions

Modified RISCV QEMU

- Aspects extended for QEMU:
  - Privilege Specification updates (1.9.1 to 1.10)
  - Hart synchronisation (IPIs)
  - Hart communication (shared memory)
  - PMPs partially modelled (more later)
  - PLIC, CLINT, local interrupts
  - Added support for managing contexts of multiple harts
  - L1/L2 cache configuration register writes/reads
  - L1 ITIM/DTIM behaviour

EMDALO TECHNOLOGIES
Embedded Software Solutions

U54-MC QEMU General Points

- Allows us to accelerate SoC software development
- Supports RISC-V 64 only (at the moment)
- Hasn't been up-streamed to main RISCV QEMU github repo yet
- Current status: pretty much functionally complete
  - Can boot Linux to console and interact
  - A little slow; takes about 15 minutes

EMDALO TECHNOLOGIES
Embedded Software Solutions

Adding 1.10 Privilege Specification

- Extended QEMU to support 1.10 of the privilege specification
  - MCAUSE values on page faults are different for virtual and physical access attempts
  - PMP scheme has been implemented
  - Virtual memory configuration move from MSTATUS register to sptbr register
  - SFENCE.VMA instruction added
  - Polarity of PUM bit in SSTATUS is inverted
  - Other minor changes

EMDALO TECHNOLOGIES
Embedded Software Solutions

Multi-HART QEMU

- Extended QEMU to partially support concept of HARTs
  - Each HART in QEMU is provided with an individual HARTID
- Memory is shared between Harts
  - Implemented PMP in QEMU to limit this behaviour, if required
- Support for PMP related CSRs
  - Support for parsing PMP rules
- PMP Enforcement Logic
  - Currently called from riscv_cpu_handle_mmu_fault

EMDALO TECHNOLOGIES
Embedded Software Solutions

U5 Coreplex Interrupts

- PLIC
  - Extended QEMU's ability to raise and lower machine external and supervisor external interrupts
  - Added a driver to QEMU for PLIC
- CLINT
  - riscv_rtc.c adapted for U5 Coreplex mtime related structure
  - Inter-processor Interrupt (IPI) support added

EMDALO TECHNOLOGIES
Embedded Software Solutions

Future Plans

- Improve speed
- Add vectorisation for local interrupts
- Add device tree support
- Add support for QOM
- Remote control of real hardware
  - FPGA developers can control their FPGA on real hardware from U54 MC running on QEMU
- Clean up and upstream

EMDALO TECHNOLOGIES
Embedded Software Solutions

Summary

- We are developing secure/safe firmware for a U54-MC Coreplex based SOC design
- In order to validate and verify this firmware, we needed to add capabilities to the RISC-V QEMU port
- This QEMU code is being made available to the community…

EMDALO TECHNOLOGIES
Embedded Software Solutions