RISC-V Trusted MCU for Functional Safety Applications

Abdoulaye Berthe[1]*

[1]Low Power Futures IBM Innovation Space - 3600 Steeles Ave. East, E171, Markham, ON L3R 9Z7

Abstract

This paper presents a RISC-V Trusted microcontroller unit (MCU) architecture for functional safety applications. The proposed architecture targets both ASIC and FPGA implementations. The architecture is based on asymmetrical dual core configuration to enable efficient power saving and hardware isolation mechanisms to support Trusted Execution Environment (TEE) and integrated Secure Element (SE). The application core in the architecture implements various reliability and redundancy features including, protocol hardening, fault detection and alerts. Bus protocol hardening, fault detection and parity check on memories have been extended to the entire architecture to ensure reliable operations across the MCU. The architecture also includes a security engine with advanced cryptographic services and secure key management using a Physical Unclonable Function.

Introduction

The recent development and maturation of RISC-V Instruction Set Architecture (ISA) implementation has led to the design and fabrication of low-cost and power-efficient System On Chip (SoC), using RISC-V processors for IoT (Internet Of Things) end points [1][2]. The SoC usually comprises a small processor, one or multiple non volatile and volatile memory banks, and a rich set of peripheral interconnected with standard SoC interconnect buses such as the Open Bus Interconnect (OBI), the Advanced eXtensible Interconnect (AXI) and the Advanced Peripheral Bus (APB). Wired or wireless communication peripherals are sometime included to enable communication with external devices. While most of the effort has so far focused on IoT endpoints used in consumer electronics; there is a growing opportunity in the automotive and industrial application space. These new opportunities are fuelled by the developments of industrial automation, autonomous driving and connected vehicles. Each of which has more stringent requirements in terms of security and functional safety. In addition to the automotive and industrial applications safety standards defined respectively in the ISO26262 and IEC 61508; several new standards have recently been defined to address the specific security needs of applications in industrial automation and automotive, including the ISO/SAE 21434 for road vehicles and the ISA/IEC 62443 for industrial automation and control systems.

In this work, we introduce a RISC-V Trusted micro controller unit (MCU) architecture for functional safety applications. The proposed architecture is extensible and targets both Application Specific Integrated Circuit (ASIC) and Field Programmable Gate Array (FPGA) implementations of secure MCU for automotive and industrial applications. The architecture targets the two least stringent (Automotive Safety Integrity Level) ASIL readiness: ASIL A and ASIL B. The architecture is built around two RISC-V processors in a big-little configuration to enable efficient power saving and hardware isolation. The architecture includes a micro-DMA (uDMA), with a rich set of associated peripheral for communication with off-chip components, and an embedded FPGA (eFPGA) to extend the functionalities of the device after manufacturing.

The proposed RISC-V Trusted MCU architecture includes an immutable Root of Trust (RoT), an integrated Secure Element (SE), a security engine with advanced cryptographic services, and a Physical Unclonable Function (PUF) for advanced cryptographic key management. The PUF and the boot ROM (Read Only Memory), together provide an immutable RoT used to ensure the authenticity of the firmware code or eFPGA bitstream stored in Flash before running it on the target device.

The new architecture is currently being implemented on both FPGA and ASIC in the context of the OpenHW Group CORE-V Trusted MCU Project. The FPGA prototype is expected to be completed in early Q2 2023 and the ASIC fabrication is planned for Q4 2023. The remainder of this paper is organized as follows, we first present an overview of the proposed architecture then the security and functional safety features supported followed by a section on the use cases and applications before concluding.

Architecture

Figure 1 presents an overview of the proposed RISC-V Trusted MCU architecture.

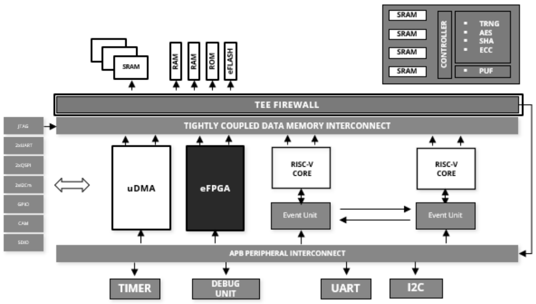

Figure 1 RISC V Trusted MCU Architecture

The architecture comprises two cores: the secure core on the right-hand side and the application core on the left, each core is a master and is connected to an event unit for interrupt management. The two other masters in the architecture are the uDMA and the eFPGA. To the uDMA is associated a rich set of peripherals, including UART, I2C, etc. for faster memory to peripheral and peripheral to memory accesses and low power mode of operation. The four masters in the architecture are connected to memories via a Tightly Coupled Data Memory (TCDM) interface. The TCDM is connected to the TEE firewall. The firewall acts as an isolation hardware; only programmable by the secure core, to prevent other masters in the architecture to access unauthorized memory location or restricted addresses in the peripheral memory map. The Static Random Access Memory (SRAM), Flash, boot ROM and all peripheral in the system are memory mapped; they are thus accessed via memory read and write instruction from the masters. The security engine on the upper right provides advanced cryptographic services and key management functionalities. Its functions include hashing, symmetric and asymmetric cryptographic algorithm acceleration, true random number generation and a secure key obfuscation and regeneration.

The interconnection shown in Figure 2 represents the implementation of the RISC-V Trusted MCU architecture in the context of the CORE-V Trusted MCU Project. The upper part of the system represents the secure subsystem, and the lower part represents the application subsystem.

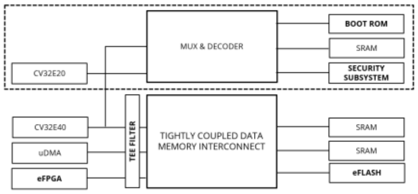

Figure 2 TCDM Interface to Memory Interconnect

Features

The new architecture includes both security and functional safety feature detailed below.

Advanced Security

The advanced security features in the architecture include:

- Trusted Execution Environment: the secure core and the security engine are used to perform secure boot. This process involves regenerating cryptographic keys inside the secure subsystem to perform signature verification on the firmware stored in eFlash.
- Memory isolation: the TEE filter which is only configured by the secure core ensure memory isolation vis a vis the other master in the architecture.
- The security engine provides advanced cryptographic service for application running on the secure core. The application core accesses the security engine via inter processor communication using an SRAM mailbox.
- Secure key management: The PUF in the security engine is used to regenerate keys from helper data generated during the obfuscation phase. Helper data are not security sensitive because only the device that is used during the obfuscation can regenerate the key from the helper data.

Integrity and Reliability

The reliability features in the architecture are an extension of the reliability features included in the application core, namely data independent timing, bus protocol, register file and program counter hardening. Some important reliability functions have been extended to rest of the system, including bus protocol hardening, bus protocol fault detection and Error Correction Check (ECC) on all memories in the system to increase the reliability across the system. Referring to the Autosoc framework presented in the [3] the new architecture can be divided into various blocks, including a safety island, a security block, an infrastructure block etc.

Use Cases and Applications

The RISC-V Trusted MCU architecture presented in this paper enable various use cases, including secure boot, secure debugging and secure firmware upgrade in industrial automation and automotive applications.

Conclusion

In this paper, we have presented an extensible RISC-V Trusted MCU architecture for functional safety application. The proposed architecture is currently being implemented on FPGA and ASIC in the CORE-V Trusted MCU Project and will be verified by the mean of Software-Based Self-Test (SBST) for ASIL readiness.

References

[1] P. D. Schiavone et al., "Arnold: An eFPGA-Augmented RISC-V SoC for Flexible and Low-Power IoT End Nodes," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 4, pp. 677-690, April 2021, doi: **10.1109/TVLSI.2021.3058162.**

[2] A. Pullini, D. Rossi, G. Haugou and L. Benini, "µDMA: An autonomous I/O subsystem for IoT end-nodes," 2017 27th International Symposium on Power and Timing Modeling, Optimization and Simulation (PATMOS), Thessaloniki, Greece, 2017, pp. 1-8, doi: **10.1109/PATMOS.2017.8106971.**

[3] F. A. da Silva et al., "Special Session: AutoSoC - A Suite of Open-Source Automotive SoC Benchmarks," 2020 IEEE 38th VLSI Test Symposium (VTS), San Diego, CA, USA, 2020, pp. 1-9, doi: **10.1109/VTS48691.2020.9107599.**