

MC2101: A RISC-V-based Microcontroller for Security Assessment and Training

Author: Luca DALMASSO

Advisor: Paolo Ernesto PRINETTO

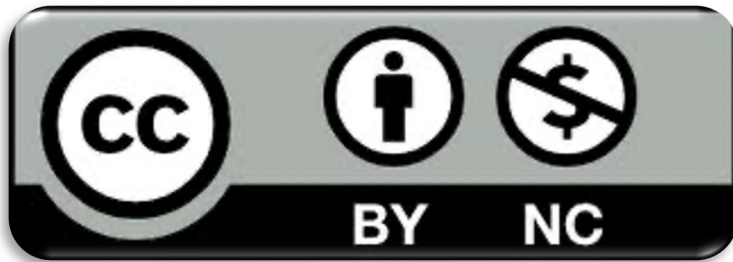
Co-Advisor: Gianluca ROASCIO



License & Disclaimer

License Information

This presentation is licensed under the
Creative Commons BY-NC License



To view a copy of the license, visit:
<http://creativecommons.org/licenses/by-nc/3.0/legalcode>

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Outline



- Introduction
- MC2101 Microcontroller
 - Architecture
 - Peripherals
- Experimental Results
- Conclusions

Introduction

4

- Embedded systems are massively used as edge devices in:
 - Safety-critical applications
 - Cars, Aircrafts, Trains, Medical equipment, ...
 - Business-critical missions
 - Industrial automation, telecommunications, ...
- Key benefits:
 - Real-time reliable
 - Low manufacturing cost
 - Low power consumption
 - Require minimal human intervention on the field

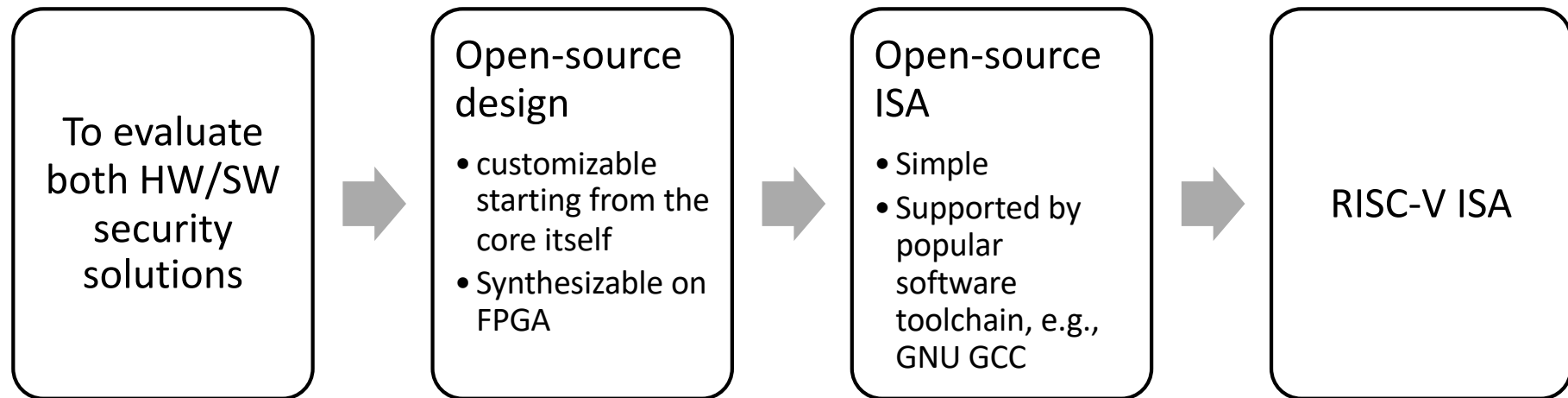
Introduction

5

- Such devices must be secure and reliable
- Problem:
 - Built-in device security is minimal
- Research Solution:
 - Software-based techniques
 - Can be easily tested outside the operating environment with a proper software toolchain
 - Hardware-based solutions
 - Require a CPU architecture description to be physically tested
 - Most famous architectures are licensed (Intel, ARM) and not accessible to research
 - Production of new silicon (e.g., ASIC) is unaffordable

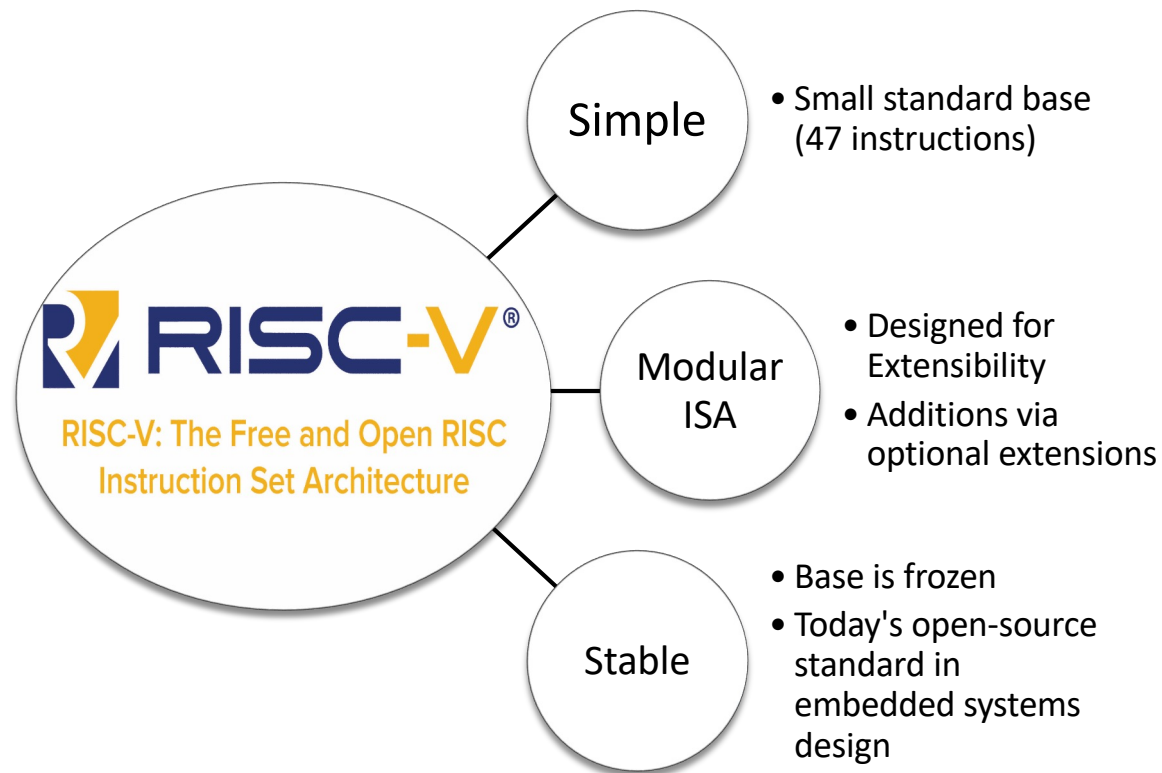
Introduction

6



Introduction

7



Introduction

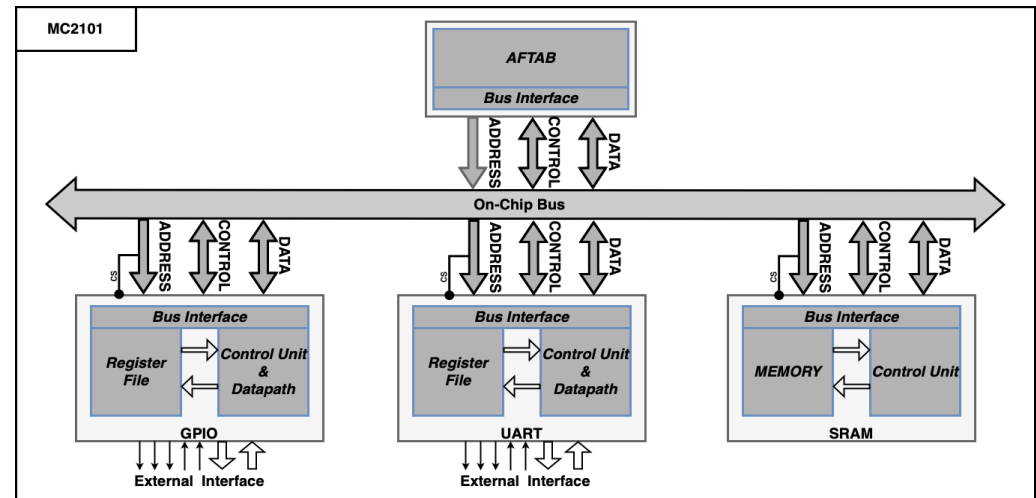
8

- *Purpose of the thesis work*: design MC2101, a modular, extensible and synthesizable embedded system to be used as a reliable platform for:
 - Integrate and evaluate security solutions for embedded/IoT domain
 - Run real applications
 - Teaching microcontrollers architecture
 - Security training activities for students and professionals
 - E.g., Capture-the-Flag challenges

MC2101 Architecture: overview

9

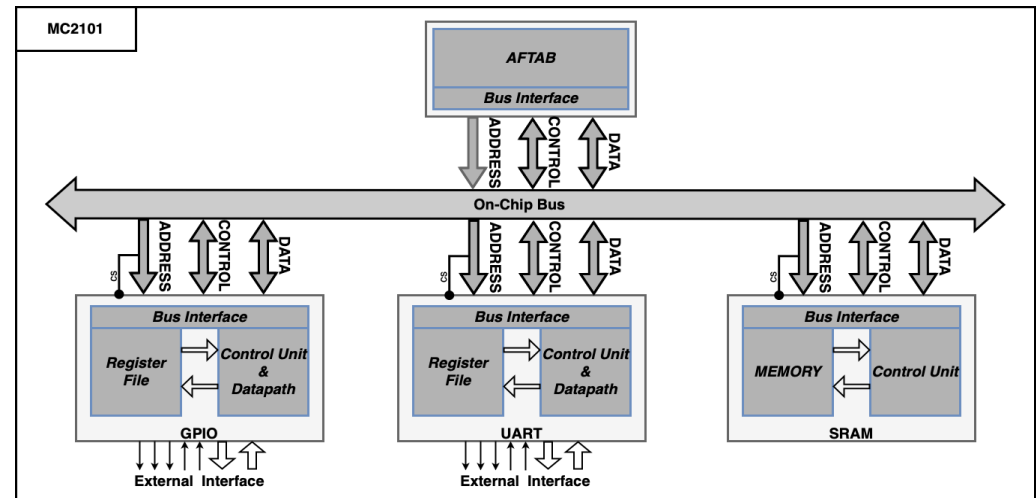
- The microcontroller includes:
 - A 32-bit RISC-V processor: **AFTAB**
 - Designed at PoliTO and developed by University of Tehran
 - Sequential core
 - RV32IM Subset RISC-V ISA
 - Integer base + Multiplication and Division Extension
 - Subset of privilege extension for interrupts and exceptions
 - Master of the BUS
 - Access peripherals and RAM in memory mapped mode.



MC2101 Architecture: overview

10

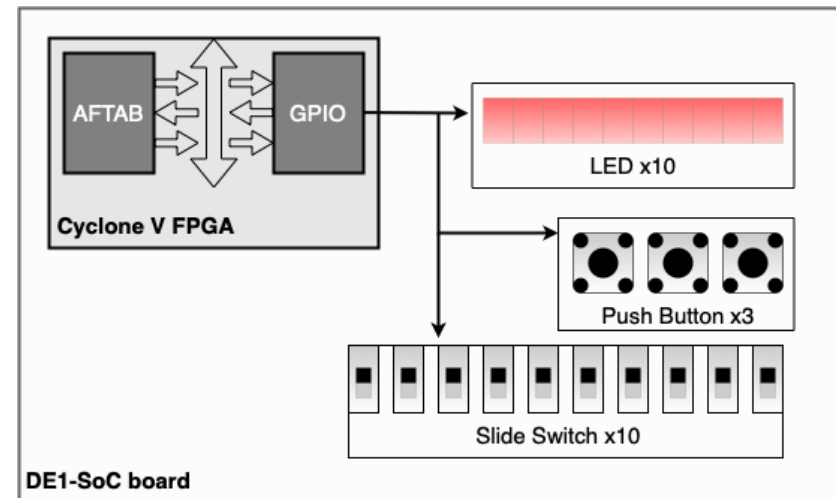
- Single BUS interconnecting the processor with memory and peripherals
 - Supports multi-cycle R/W operations
 - Control signals for interrupts
 - Control signals for transfer response
- Minimal set of peripherals designed to provide all necessary I/O functions
 - GPIO, UART



MC2101 Architecture: GPIO

11

- General Purpose Input Output (GPIO) peripheral
 - Present in every microcontroller
 - Designed to manage incoming and outgoing digital signals
 - Controlling physical pins
 - Bit-banging operations
- The logic and the software library designed allow to:
 - configure pins direction
 - read/write pins logic state
 - enable interrupt on each input pin
 - configure interrupt triggering behavior



MC2101 Architecture: UART

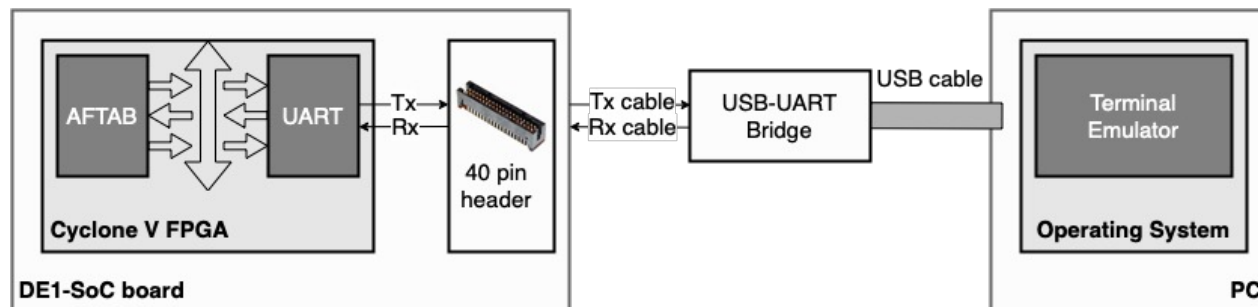
12

- The UART module designed for MC2101 provides a receiver-transmitter pair
 - Configurable with different speeds
 - Supporting different data widths
 - Parity codifications
 - Information status for different error conditions:
 - Overrun Error, Frame Error, Break Interrupt
 - Prioritized interrupts
 - Buffered communications
 - Two dedicated hardware FIFO's

MC2101 Architecture: UART

13

- Communication channel between PC and the microcontroller synthesized on FPGA
 - Uart Tx and Rx are bridged to USB
 - Through a PC terminal, it is possible to send/receive characters
 - Software libraries integrate *scanf* & *printf* functions



Experimental Results

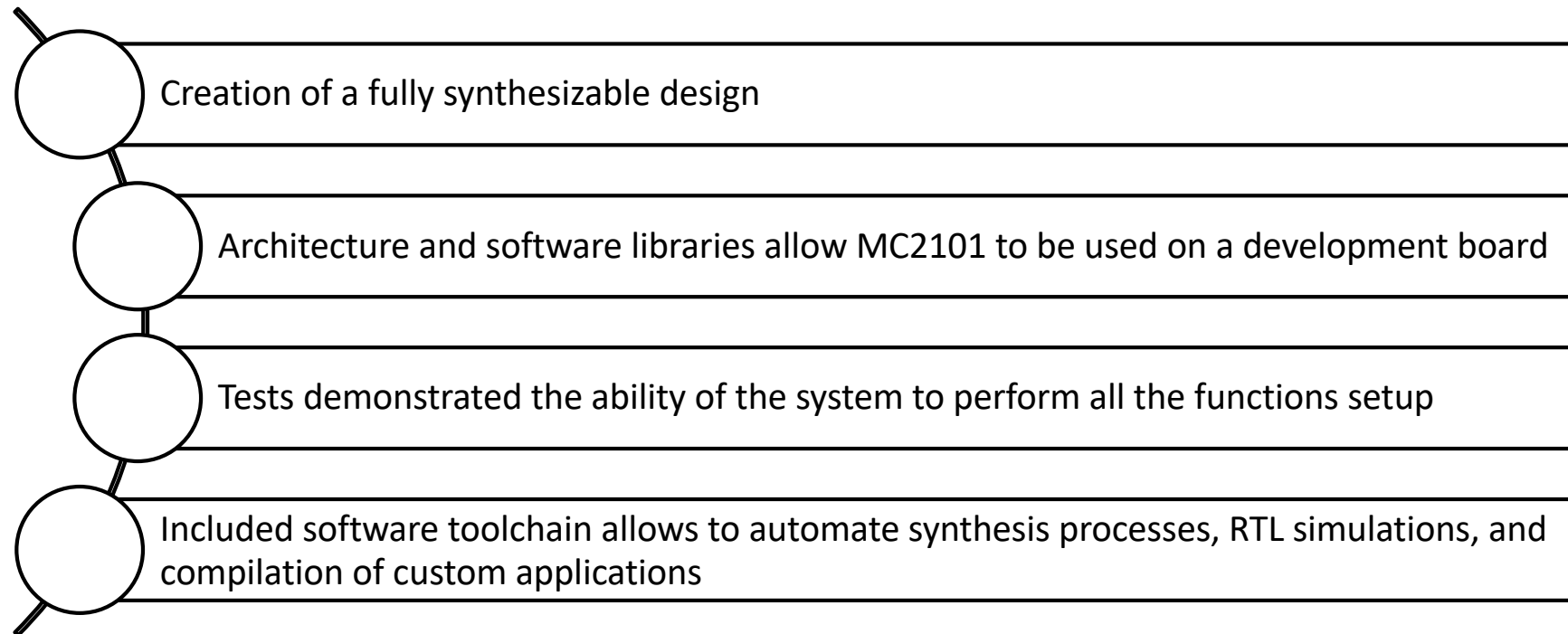
14

- Synthesized on Cyclone-V FPGA using Quartus 21.1 software
- Very small percentage of available resources is used
 - Great deal of freedom for future developments

Resource Name	Used Amount	Total Amount	Percentage Used
ALM	2628	32070	8%
FF	3443	64140	5%
PIN	36	457	8%
M10K Memory Bits	131072	4065280	3%
M10K Blocks	16	397	4%

Conclusions

15



Thanks for your attention!

