Making VeeR EL2 Caliptra 2.0-ready: enhanced functionalities, verification and documentation

Open Hardware Mini Summit 2024, Vienna, 2024-09-19
Karol Gugala, kgugala@antmicro.com

antmicro

ANTMICRO

- Founded in 2009, dedicated to commercial adoption of open source in the hardware space, Platinum CHIPS Alliance member
- We provide end-to-end engineering services, software/hardware co-design, advanced tools and strategic R&D for high-tech
- Developing, adapting and integrating open source ASIC and FPGA tooling and IP
- Tools for synthesis, linting, formatting, simulation and co-simulation, hardware-software co-design, chip design verification, CI and automation

antmicro

VEER FAMILY

- Open source production-grade 32 bit RISC-V core family hosted by CHIPS Alliance
- Come in three variants - EL2, EH1 and EH2
- Developed under CHIPS Alliance
- All the code available in repositories in CHIPS GitHub organization

antmicro

VEER EL2

- Smallest core from VeeR family
- RV32IMC-compliant RISC-V core with branch predictor
- 4-stage, scalar, in-order pipeline
- Used in Caliptra
- Supports AXI and AHB bus interfaces
- Code available on GitHub

antmicro

CALIPTRA

- Open source Root of Trust
- Collaboration between Google, Nvidia, Microsoft and AMD within CHIPS Alliance (spec lives in OCP, implementation is developed in CHIPS)
- By default meant to be integrated with a larger SoC, with concrete plans from several member companies
- Reuses a number of OpenTitan peripheral cores

antmicro

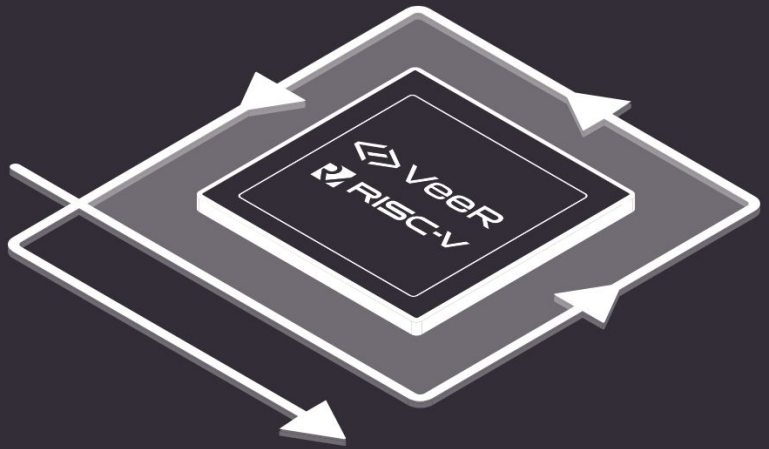
CALIPTRA AND ANTMICRO

- Focus on enabling open source collaboration on Caliptra for both current project partners and external adopters
- Took over cleanup and maintenance of the VeeR core family, primarily EL2, making sure it's on par
- Encouraging more industry collaboration around RTL with open source tools:
  - unifying development and verification flow with open source tools
  - providing system-level testing and integration
  - maintaining public-facing CI

antmicro

CALIPTRA 1.0 (1.1)

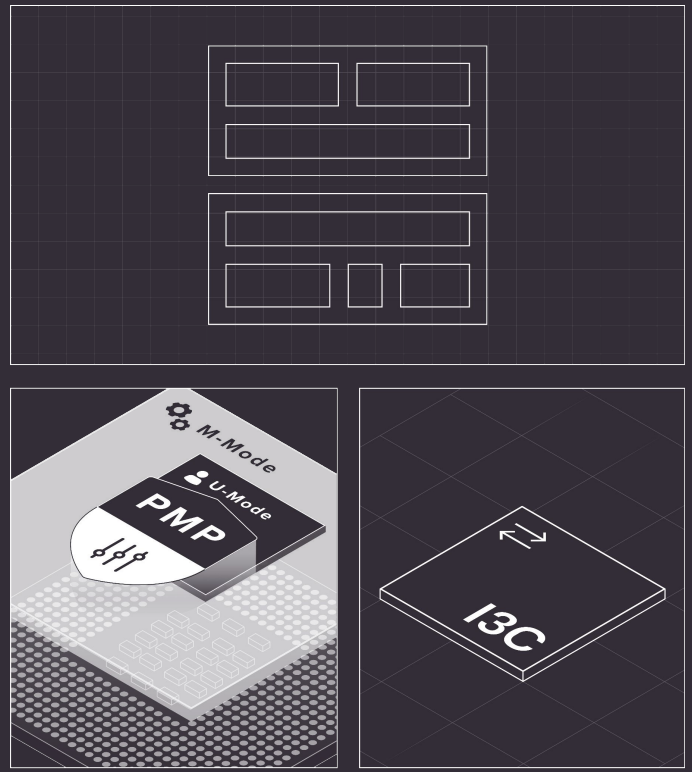
- Fully functional RoT IP block and software you can integrate with your SoC
  - Non-secure part of the SoC communicates with Caliptra using a mailbox
  - Implements a number of attack mitigations (discussed in the docs)
- Open-source RTL and verification code
- Register file generated from SystemRDL
- Watch last year's presentation



antmicro

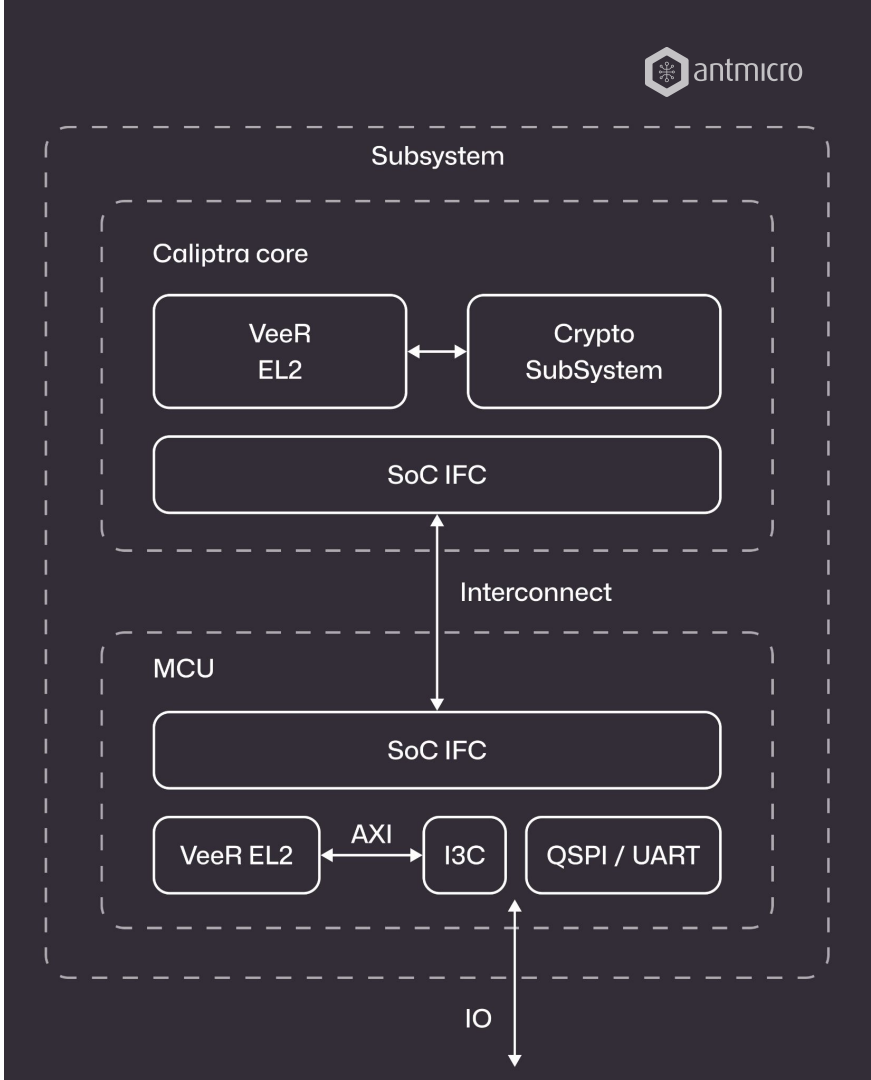
TOWARDS CALIPTRA 2.0

- Introducing Caliptra Subsystem
  - Standalone SoC with Caliptra core and Manufacturer Control Unit
- User Mode support in VeeR-EL2
  - SmePMP
  - TockOS port utilizing User Mode
- Open source I3C Core
  - Integrated with Caliptra MCU subsystem
  - Generic I3C core, within Caliptra used to provide functionalities needed for OCP Recovery Flow



CALIPTRA MCU SUBSYSTEM

- Code on GitHub: github.com/chipsalliance/caliptra-ss
  - Under ongoing development
- The Subsystem is a standalone SoC design implementing:
  - Caliptra core
  - A general purpose CPU (also VeeR EL2)
  - Peripherals allowing integration of the chip (QSPI, UART, Fuses)
  - I3C core
- AXI based interconnect (Caliptra core uses AHB) with access control

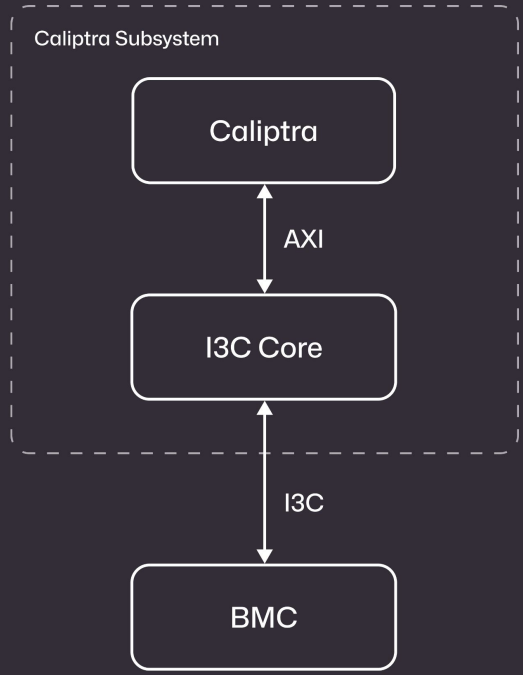


antmicro

OPEN SOURCE I3C CONTROLLER

New peripheral developed by Antmicro as necessary for the MCU Subsystem

- Open source I3C core implementing both host and target functionalities
- The I3C core can be connected as a subordinate on either AHB or AXI bus
- Base I3C functionality is extended with I3C CSRs handling needed for the OCP recovery flow
- Apache 2.0 licensed code is available on GitHub
  - The core itself is still under development



antmicro

VERILATOR

UVM

bus interface
AXI

OPEN SOURCE AXI BUS VERIFICATION

- To verify Caliptra subsystem we needed an AXI verification flow that we can publicly share and run in public CI
- axi-vip package from Western Digital provides the required functionality, but there was no open source simulator where we could run tests using it
  - The package uses a number of SystemVerilog features like clocking blocks in virtual interfaces or inline random variable control
  - None of those were supported in open source simulators

	Total	Pass	Fail	Skip
Branch: 'axi-vip'	2	2	0	0

antmicro

IMPROVING VERILATOR

- As you may know we have an ongoing effort on improving on SystemVerilog support in Verilator
  - The goal of this work is to be able to use packages like axi-vip in an open source flow
- Extended Verilator to support missing SystemVerilog features to be able to do verification with axi-vip
- Built upon our previous milestones on the road to UVM support in Verilator
  - UVM testbenches
  - Constrained randomization
- Added axi-vip to our Verilator verification test suite

VERILATOR

UVM

bus interface
AXI

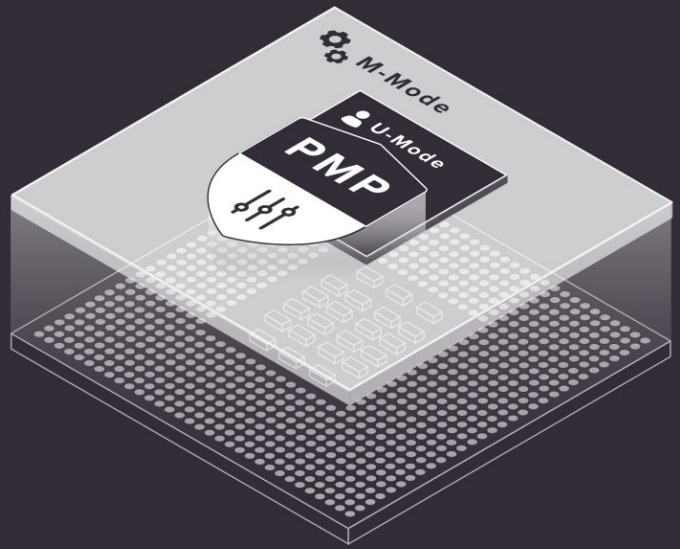
	Total	Pass	Fail	Skip
Branch: 'axi-vip'	2	2	0	0

antmicro

VeeR RISC-V

EXTENDING THE RISC-V VEER EL2 CORE

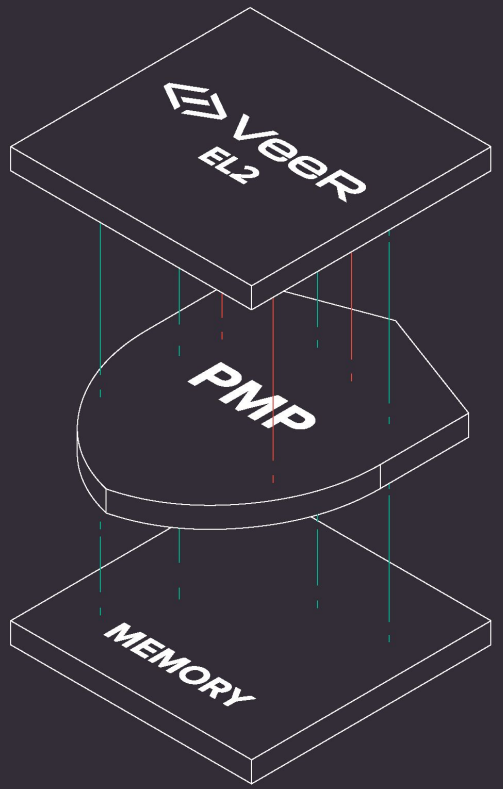
- Added User mode support to VeeR EL2
- Extended standard CSRs already present in VeeR EL2
  - `misa`, `mstatus`
- Introduced new CSRs required by User mode
- U-mode-specific performance counters
- Logic required to switch between modes



antmicro

EXTENDING THE RISC-V VEER EL2 CORE

- Updated PMP behavior to account for U-mode
- Added extended PMP support according to the Smepmp specification
- Software and simulation infrastructure
  - Verified the support with Verilator, RISCV-DV, Tock and Renode
- More details in the blog article



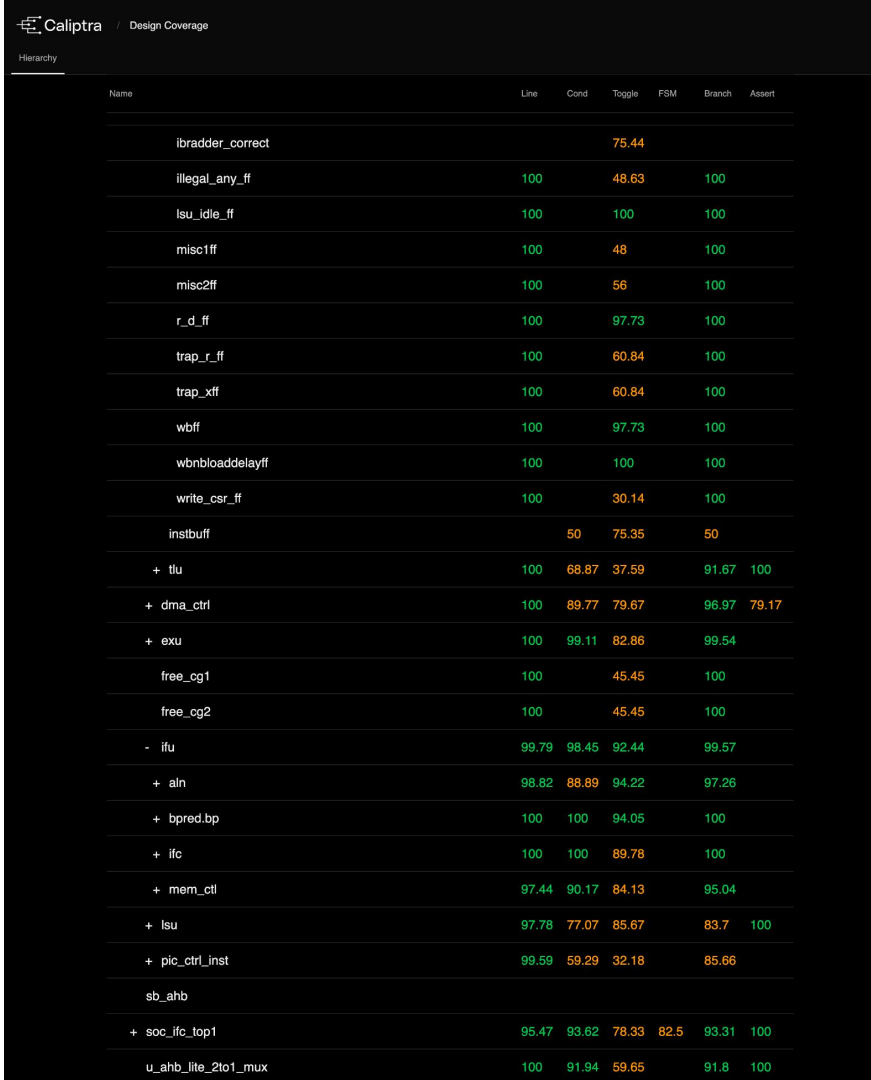
antmicro

TOCK SUPPORT

- Secure embedded operating system implemented in Rust
- Supports RISC-V privilege spec (M, S and U modes)
- VeeR-EL2 support is done, in the upstreaming process
  - One PR merged, two are past review and got ACKs, to be merged soon
  - libtock-c/pull/464
  - tock/pull/4118
  - tockloader/pull/117

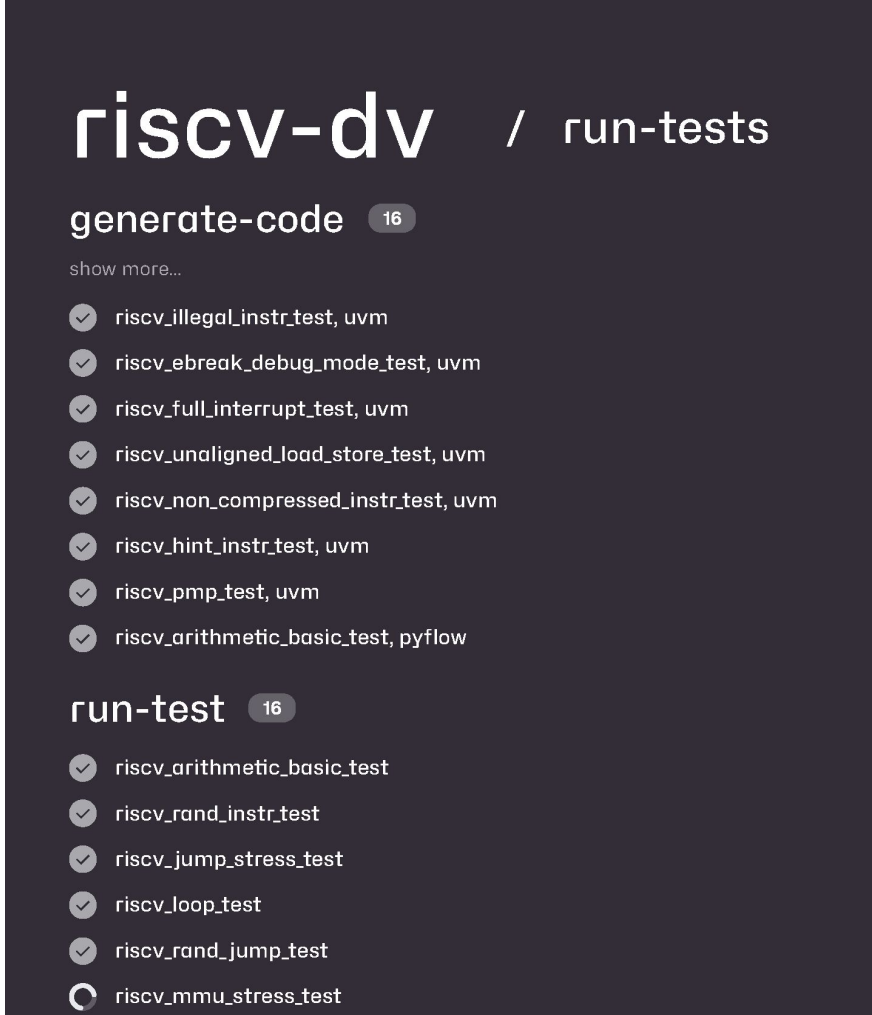
IMPROVED VERIFICATION COVERAGE

- Improved verification coverage and new coverage visualizations
  - Coverage dashboard
  - Verification tests dashboard
- Automated CI generating the reports
- Coverage dashboard is now included in the public documentation
- More in the blog article



RISCV-DV FOR VEER VERIFICATION

- Open source RISC-V verification suite
  - Runs randomized instruction streams on a CPU under test and compares the output with ISS simulation
- Extended with User mode and PMP tests
- Included in VeeR-EL2 CI
- Results included in the coverage dashboards
- Renode support

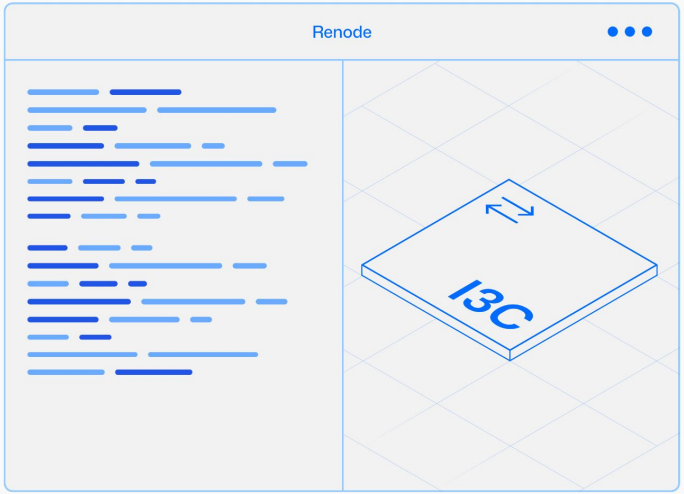


antmicro

RENODE SIMULATION MODELS FROM SYSTEMRDL

- To speed up generation of the co-simulation verification environment we've extended renode with RDL support
- We can now generate C# peripherals models with register definitions
  - This flow is used in the I3C core verification
  - Will be extended to other Caliptra cores
- See tomorrow’s presentation to learn more on Renode and its co-simulation capabilities

RENODE™



DOCUMENTING COMPLEX SYSTEMS

- System Designer is an interactive portal aggregating Antmicro's open source methodologies, workflows and tools
  - Check it out at designer.antmicro.com
- Explore Caliptra SoC's structure, RTL and verification artifacts from a block diagram perspective
  - Diagram created with the Topwrap toolkit for connecting individual HDL modules into full designs

Caliptra SoC

VENDOR

Caliptra

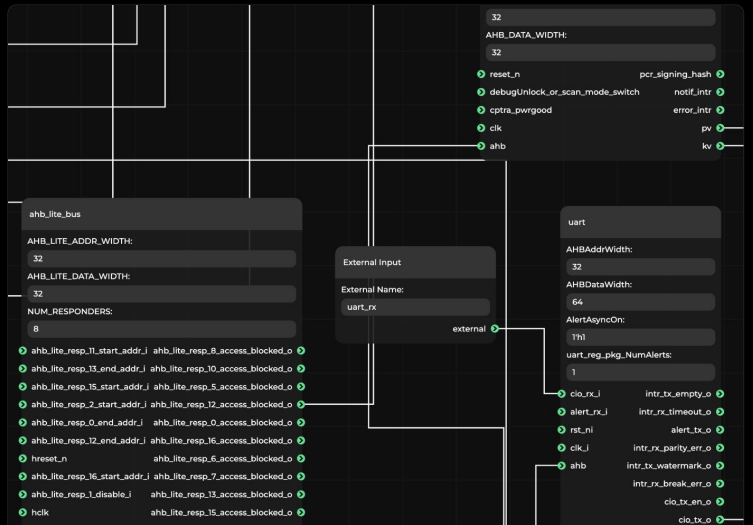
DESCRIPTION

Root of Trust for Measurement block, enabling Identity, Measured Boot, and Attestation capabilities

Peripherals 6 total

Block Diagram

Edit in System Designer



THANK YOU
FOR YOUR ATTENTION!