Scale4Edge

Success Story:

The Scale4Edge Hardware Verification and Validation Ecosystem for RISC-V Platforms

For a commercially successful development of edge devices for a wide range of applications, a whole ecosystem of tools and hardware components is mandatory. Ensuring the safe, secure, and reliable design and operation of these devices is an indispensable, but challenging requirement for many of these applications. The Scale4Edge project aims to address this challenge by enabling a comprehensive RISC-V-based ecosystem that helps ensure the correct and secure functioning throughout the whole design process and lifetime of an edge system: The ecosystem encompasses tools for functional verification—both using virtual prototypes in an early stage of development and using formal methods—, security verification, software-based self-test (SBST), and system visualization and debugging. With the development of this hardware verification and validation ecosystem, the Scale4Edge project aims to create optimized and reliable edge devices that meet the high demands of modern industries.

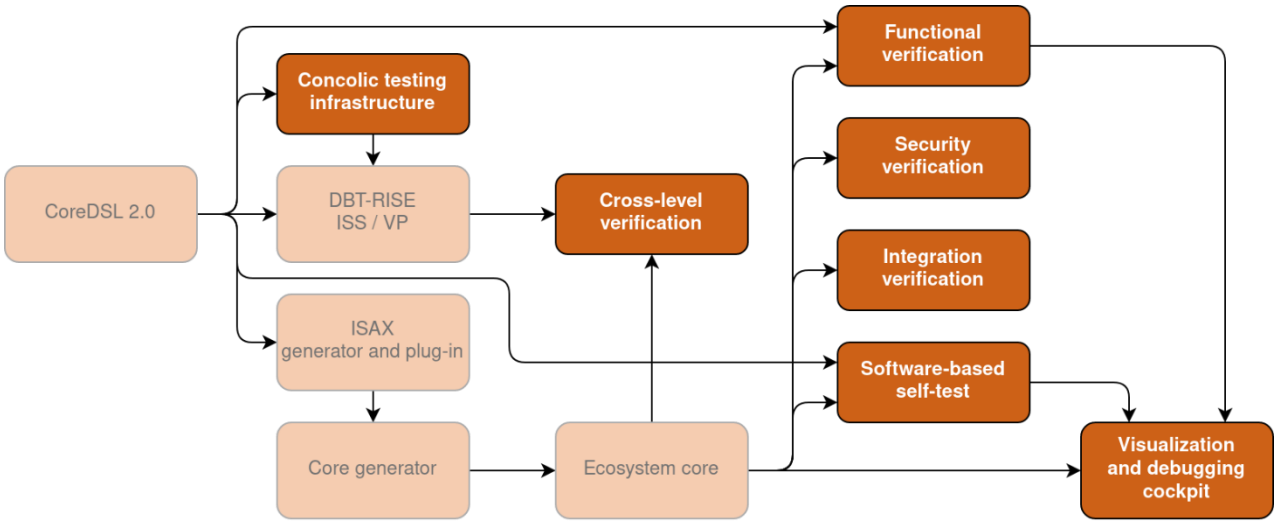

Figure 1: The Scale4Edge Hardware Verification Ecosystem

The Scale4Edge project has made significant strides in hardware verification and validation for RISC-V platforms, with multiple partners contributing to its success. The components of the hardware verification ecosystem are shown in Figure 1. The **University of Bremen** developed a comprehensive cross-level verification approach and a concolic testing infrastructure. **Siemens EDA**—an associated partner—created new functional verification tools for processor verification while the **University of Kaiserslautern-Landau** (*RPTU)* focused on formal security analysis with Unique Program Execution Checking (UPEC). The **FZI Research Center for Information Technology** (FZI) devised methods for specifying, generating, and verifying hardware properties in System-on-Chip (SoC) platforms, with the **University of Freiburg** and **Concept Engineering** contributing to in-field monitoring and testing (SBST) as well as debugging and visualization tooling. The collaborative efforts of the project partners around the Scale4Edge ecosystem core, developed by **MINRES** according to the ISO 26262 safety standard, resulted in a comprehensive hardware verification and validation flow with award winning methods and industry-proven EDA tools.

CoreDSL 2.0—a domain-specific language for instruction set architecture (ISA) description—and the Scale4Edge ecosystem core are key components on which the verification methods and tools of the project partners have been applied and evaluated. In the early stages of a hardware design flow, virtual prototypes and abstract functional models are paramount to ensure the correct behavior of a complex system such as a RISC-V core. This is where the **cross-level verification** approach comes into play to detect implementation errors early and achieve high coverage very quickly. The Scale4Edge cross-level processor verification approach generates infinite instruction streams and tightly couples an instruction set simulator (ISS) to the ecosystem core RTL code via an in-memory communication interface. This co-simulation of a concrete implementation of the RISC-V core against the functional reference model in the ISS enables a comprehensive test approach where we have rapidly achieved high RTL coverage of the ecosystem core. In addition, **concolic testing** is an emerging automated software testing technique that combines symbolic and concrete program execution and can be easily used in virtual HW/SW prototypes. The concolic testing engine has been successfully used to uncover over 10 previously unknown bugs in RIOT OS, a popular open-source operating system for embedded IoT devices.

Scale4Edge

This work has been developed in the ZuSE project Scale4Edge. Scale4Edge is funded by the German ministry of education and research (BMBF) (reference numbers: 16ME0122K-16ME0140+16ME0465). The authors are responsible for the content of this publication.

The Scale4Edge ecosystem core is more than a micro-architectural implementation of the RISC-V ISA, it is a specialized core instance of a highly configurable and customizable core design generator. Generator-based hardware design is currently very popular in agile hardware development and provides a powerful solution for streamlining SoC design by enabling rapid synthesis of virtual and evaluation prototypes early in the development cycle. Within the verification ecosystem, the FZI has developed a novel and lightweight **verification approach for generator-based hardware designs**. Using a domain-specific language for formal property specification called CHIPS, generic properties are specified directly in hardware generators, synthesized into concrete assertions in the RTL code and formally checked by commercial verification tools. Our approach was applied during integration of the ecosystem core into the highly popular Rocket Chip SoC generator, where we were able to prove lightweight integration properties using Bounded Model Checking (BMC) without the need for extensive simulation prior to synthesizing the SoC into an FPGA prototype.

Ensuring the correctness of a complete system involves verifying hardware at the lowest RTL level, including custom instructions and registers, which can be a challenging task. **Formal verification** and automation are crucial for success, as they can provide exhaustive verification and enable easy core customization while ruling out adverse influence on processor behavior when adding hardware customizations. To that end, Siemens EDA developed a Processor Verification App to formally verify the RTL implementation against the official formal specification of the RISC-V ISA. We automatically extract a register map from the core implementation and generate a set of assertions for all instructions and registers, which are then formally verified. Siemens EDA's Processor Verification App proves correct behavior of all instructions and registers, shows the absence of any unexpected instructions or registers or quickly analyses root cause failures with an automatically generated counterexample. In addition to the ecosystem core, we applied our Processor Verification App to the OpenHW Group CORE-V CV32E40P v2 project with 300+ custom instructions from the XPULP extension, identifying numerous RTL issues.

Motivated by the wide-spread concerns regarding the security of computing systems and SoCs, the Scale4Edge ecosystem comprises novel methods for **formal security analysis**. By using our unique program execution checking (UPEC) approach, dozens of previously unknown security breaches have been found in several open-source RISC-V designs (Rocket Chip, BOOM, Pulpissimo, Ariane, Ibex, OpenTitan). We conducted extensive experiments on two ecosystem cores. Both cores were previously verified thoroughly using state-of-the-art simulation based on randomized assembly tests from the RISC-V-DV framework. Still, UPEC detected five bugs that were missed by these assembly tests. The bugs affected access control and occurred in corner cases involving special access control configurations when targeting specific memory addresses. Such scenarios are pathological for any randomized assembly test. The work on UPEC received high international recognition, as attested to by the DAC Best Paper Award 2022 and the Intel Hardware Security Academic Award 2022.

Extending verification to in-field monitoring and testing strengthens the dependability guarantees of the system. **Software-based self-tests** (SBSTs) allow detection of faults caused by defects that have been introduced during production or through aging. The University of Freiburg actively develops methods for automatic SBST generation. The SBST programs run on the processor during idle times or in regular, defined intervals and perform computations that make effects of faults detectable as test result. The test result is validated, and appropriate measures are taken if faults are present. Fault simulations of an automatically generated SBST program targeting the arithmetic logic unit (ALU) and register file on an RISC-V RV32I core in the Scale4Edge ecosystem shows that it is possible to achieve a stuck-at test coverage for these modules of 99.76% and 96.36% respectively. Future work will focus on shortening the test program and covering components that require complex SBST behavior to test. In cooperation with Politecnico di Torino, the SBST research is extended to circuit switching activity generation and burn-in testing.

Scale4Edge's hardware verification ecosystem not only provides tools to detect errors and to generate test programs, but also the powerful **hardware visualization and debugging cockpit** StarVision PRO by Concept Engineering. It supports hardware descriptions from system level (e.g., in SystemVerilog), register-transfer level and gate level (e.g., in VHDL or Verilog) down to transistor level. The user can interactively explore the design hierarchy and extract useful information like clock trees, annotate the schematics with simulation data and error traces and much more. Extensions developed as part of the Scale4Edge project include the possibility to analyze power management structures as defined in UPF, which is particularly important for low-power edge devices, and to visualize test coverage.

Cont@ct:
MINRES Technologies GmbH | Eyck Jentzsch | eyck@minres.com | https://www.edacentrum.de/scale4edge/

Further Scale4Edge partners and sub-contractors

This work has been developed in the ZuSE project Scale4Edge. Scale4Edge is funded by the German ministry of education and research (BMBF) (reference numbers: 16ME0122K-16ME0140+16ME0465). The authors are responsible for the content of this publication.