In the final year of the project, all work packages have progressed to completion

WP2 & WP3 – Design of a silicon Root-of-Trust and Trusted Execution Environment

Within the first two years of the project the final Root-of-Trust (RoT) was already developed, however in the last year in the context of the WP2, the **RoT Library for SPIRS Platform** was presented to ease the access to the HW modules of the RoT.

The **Trusted Execution Environment** (TEE) was also finished, so in the last year, the WP3 task was devoted to complete the design of software TEE running on top of open RISC-V hardware, the usage of the silicon RoT to provide a secure boot flow, and continuous support for the development of Trusted Applications.

WP4 – Integration into network infraestructures

The activities are focusing on integrating TEE and RoT into networking infrastructures to meet the growing connectivity demands of Internet of Things (IoT) devices. The integration of IoT devices with networks poses challenges, such as insecure communication protocols and limited device resources. SPIRS addresses these challenges with a solution based on RISC-V technology, combining TEE (Keystone) and RoT for secure data exchange in IoT environments.

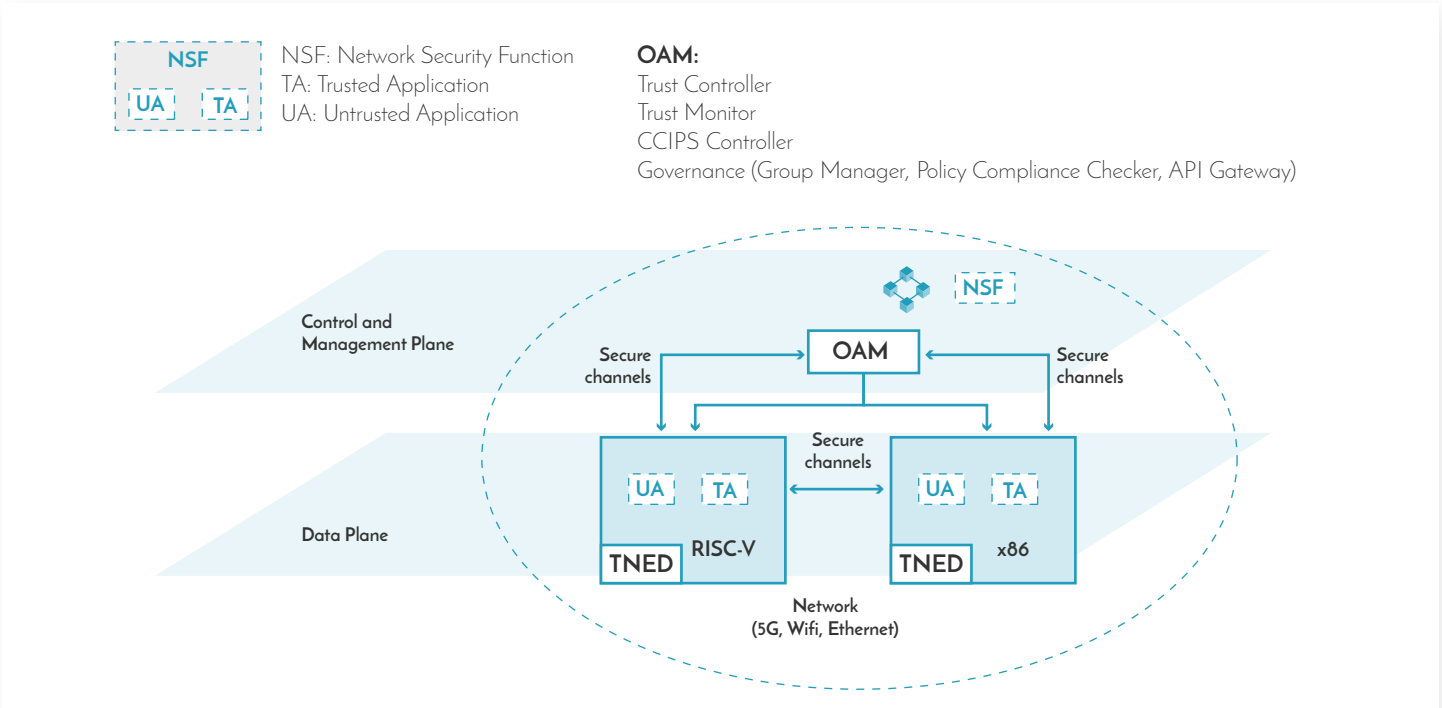

Figure: Trusted Network Environment for Devices (TNED) conceptual solution.

The SPIRS Project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement N° 952622

Follow us

The TNED solution leverages

- NFV/SDN principles to enable secure connectivity across different architectures, such as RISC-V and x86, which are common in cloud and data centers.
- Network Operation, Administration, and Management (OAM) principles, enabling monitoring and orchestration of network security functions (NSF) via Kubernetes and containers.
- Trust management ensures remote attestation services for integrity verification using TEE frameworks like Keystone and Enarx.
- A compliance solution was added to evaluate the security policies defined by the operator and one identity management solution, including traceability using DLT technology.

Applications developed for use cases in 5G connectivity and Industry 4.0 included SDN-based IPsec VPN solutions, data transfer forwarders, and firmware exchange tools.

The TNED system is designed for future scalability, supporting additional applications and microprocessor architectures beyond the current use cases.

WP5 – Platform integration

The final version of the **SPIRS platform**:

- Resolved key issues identified during testing, such as applications freeze on the Spritz processor caused by instruction incompatibility by upgrading the processor to a newer version of the **CVA6.**
- Integrates the **final RoT** developed in WP2 that significantly reduces the power consumption and improves the overall area efficiency on the FPGA.
- Incorporates the **secure boot ROM** developed in WP3 of the project.

The final design maintained the high security standards of the platform while optimizing resource efficiency, resulting in a power consumption of only 2.578W and using 58.21% of the available area in the FPGA prototype implementation.

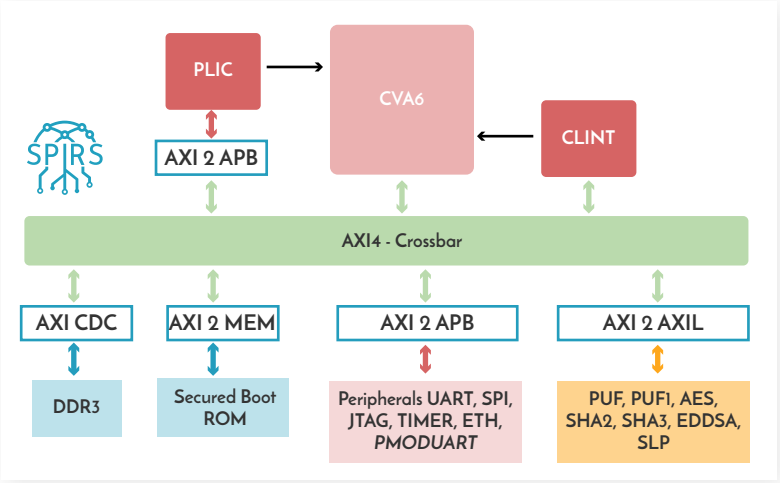

Figure: Block diagram of the final version of the SPIRS Platform.

The final SPIRS platform was rigorously tested and validated, ensuring that all components functioned correctly. The platform securely booted using the boot ROM from WP3, followed by loading a Linux operating system, establishing an Ethernet connection, and running multiple RoT software applications.

An automated generation methodology for the platform has been also developed in WP5. This methodology streamlines the creation process of the platform, reducing development time and increasing reproducibility.

The SPIRS Project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement N° 952622

Follow us

Final VLSI integration of a lightweight RoT

The performance of the building blocks of the RoT manufactured in the preliminary RoT VLSI integration has been evaluated by characterizing and testing them on the lab.

A second ASIC has been manufactured also in a TSMC technology. The new design is based on the lessons learned during the first ASIC RO-PUF and ASCON modules including new features and modifications as follows:

- A redesign of the PUF, as an ID generator and TRNG, was made, as well as an HDA module for key post-processing.
- The ASCON module has also been redesigned to include the variants for standardization of the Ascon Family according to the latest NIST updates. The ASCON-128 and ASCON-Hash versions are implemented since the operations performed by both algorithms similar, making it appropriate to include them in a single design. Additionally, hardware countermeasures against side-channel attacks (SCA) and fault injection attacks (FIA) have been designed for the ASCON. Both ASCON implementations, with and without countermeasures, have been included for comparison purposes.
- Access to the PUF-HDA and ASCON blocks is handled by a register level communication interface.
- A glitch detector is included as a System Level Protection (SLP) mechanism against FIA.

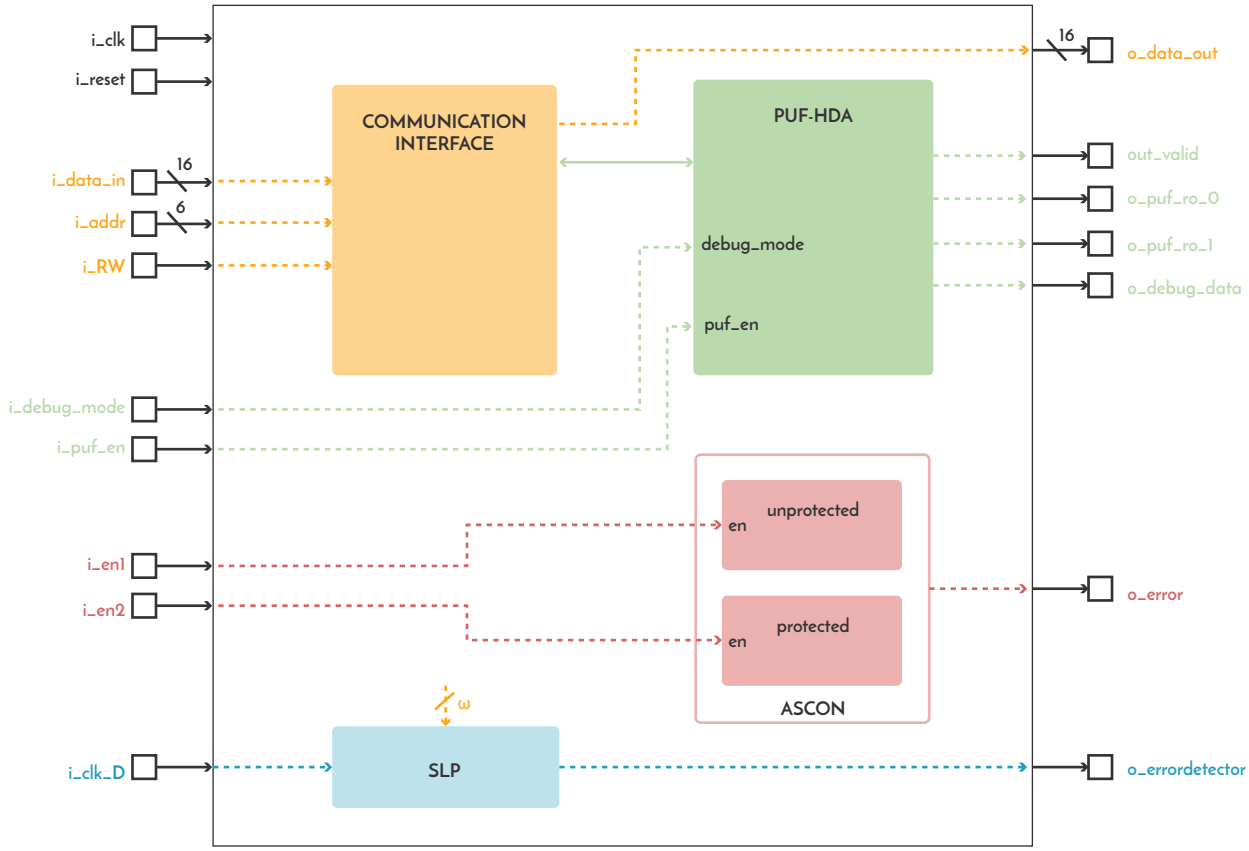

Figure: Blocks and I/Os in the Final VLSI integration of a lightweight RoT.

The SPIRS Project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement N° 952622

Follow us

WP6 – Platform Validation

This WP was devoted to validate the platform. The validation allows to ensure that the security solutions developed were practical, reliable, and actually useful across various real-world applications.

5G Use Case: SPIRS is deployed within a Public Network-integrated Non-Public Network (PNI-NPN) to secure wireless connectivity for enterprise devices such as IoT systems and robots. Leveraging a zero-trust approach, the platform establishes an end-to-end IPsec overlay between two SPIRS TNEDs, ensuring secure communication and data protection across both local enterprise networks and remote monitoring through the 5G core infrastructure.

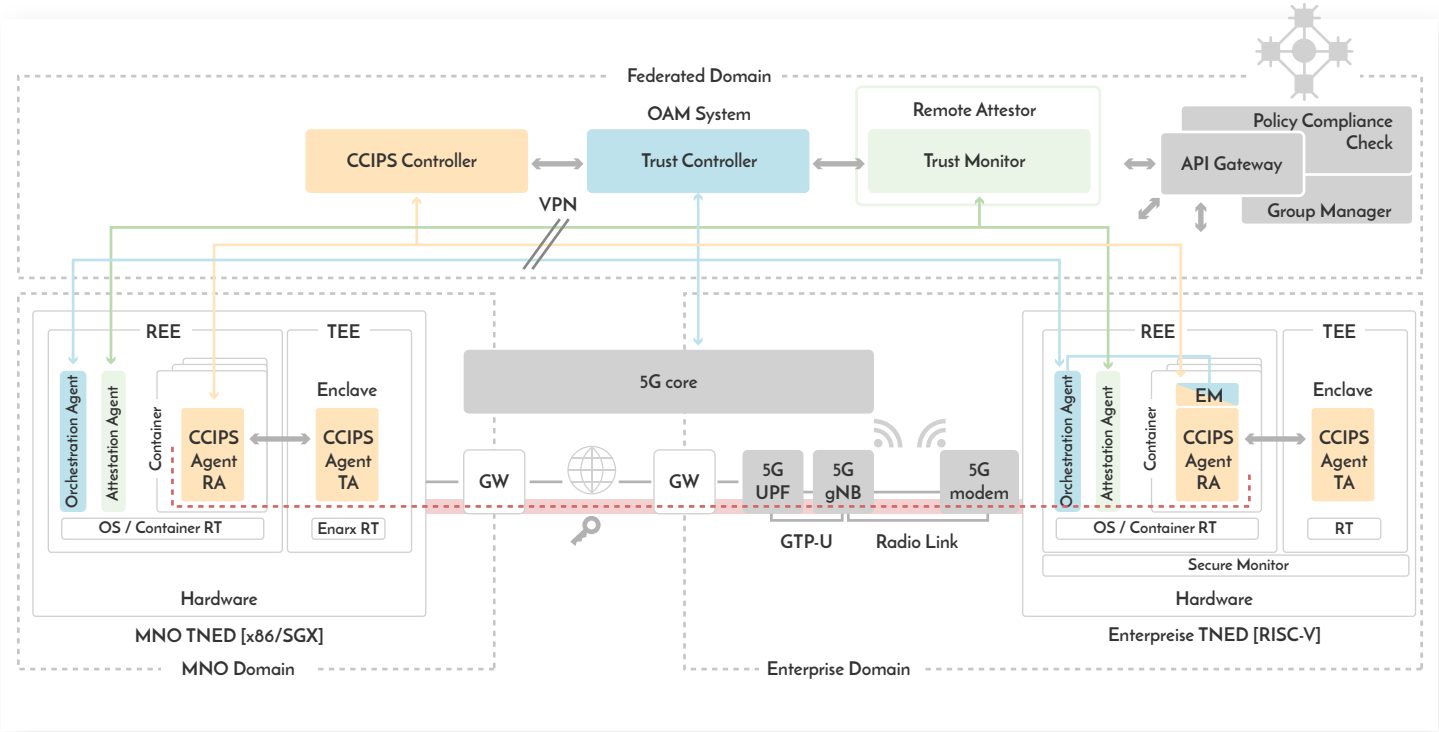

Figure: 5G setup for the validation of SPIRS zero-trust enablers.

Industry 4.0 Use Case: The attestation and privacy enhancement mechanisms together the SPIRS TEE and HW RoT enable to produce a secure network gateway for Industry 4.0 IoT devices. Those validated are the Trust in Manufacturing Machine, where the SPIRS platform is installed at the physical machine of a production line and protects the data for the MES Server, and the Secure Firmware Exchange that protects the firmware produced by customers and monitor the accesses during the final stage of the production.

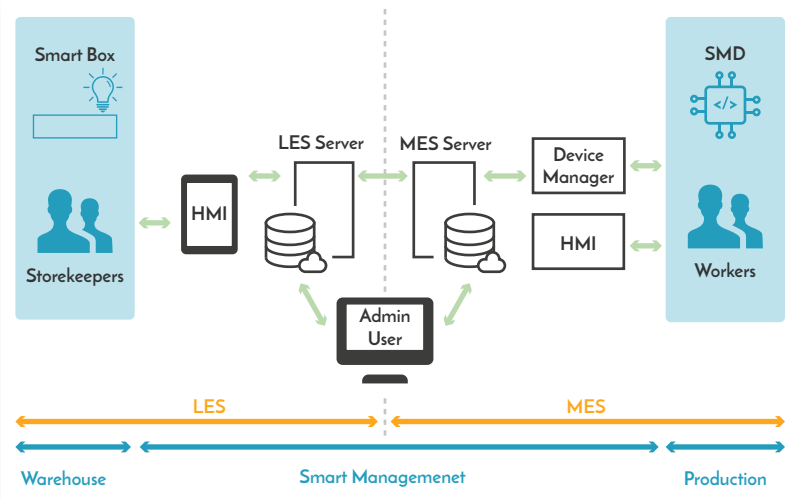

Figure: Schematics of the Industry 4.0 use case in SPIRS.

The SPIRS Project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement N° 952622

Follow us

A Proof-of-concept of the SPIRS governance scheme both Industry 4.0 and 5G Network use cases have been provided. The SPIRS governance scheme is mainly determined by the privacy respectful identity management developed in the project and the Distributed Ledger Technology (DLT) protocols for the gathering and recording of activity and security events. SPIRS supports two different options for DLT that are accessible through the API Gateway: the IOTA Tangle and Hyperledger fabric. For identity management, the group signatures library developed in SPIRS allows the definition of operational roles related to the Industry 4.0 and 5G Network use cases.

The **validation phase** was essential in demonstrating that SPIRS is not just a theoretical or lab-based solution but one that can be placed in real-world environments, proving its adaptability. This is particularly important as both Industry 4.0 and 5G environments are highly dynamic, with new devices and processes newly created. The ability of the SPIRS platform to adapt to these changing environments was a critical outcome of the validation process, together with the enhancement to the security of the processes involved in the various use cases.

WP7 – Dissemination and exploitation of results

A summary of the total of dissemination activities in numbers:

11 publications in peer-reviewed international journals

28 participations in peer-reviewed conferences

44 talks in workshops, seminars, webinars, summer-schools

1 whitepaper

Communicating and promoting SPIRS during the project life-time:

- Organization of the SPIRS Final Workshop
- Participation in Security Research Event (SRE) 2023
- 12 promotional videos
- 5 blogposts
- 6 Press releases, 1 radio interview, 1 TV interview
- 10 participations in outreach activities for general audience
- Active participation in social media

SPIRS consortium meetings for 3rd year

Description	How	When
Management Committee meeting	Online	December 2023
Intermediate meeting	Hybrid-Barcelona (Spain)	February 2024
Intermediate meeting	Hybrid-Tessalonika (Greece)	June 2024
Industrial Advisory Board meeting	Online	September 2024

The SPIRS Project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement N° 952622

Figure: SPIRS booth in SRE 2023 (October 2023).

Figure: SPIRS meeting in Barcelona (February 2024).

Figure: SPIRS meeting in Tessalonika (June 2024).

The SPIRS Project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement N° 952622

Follow us