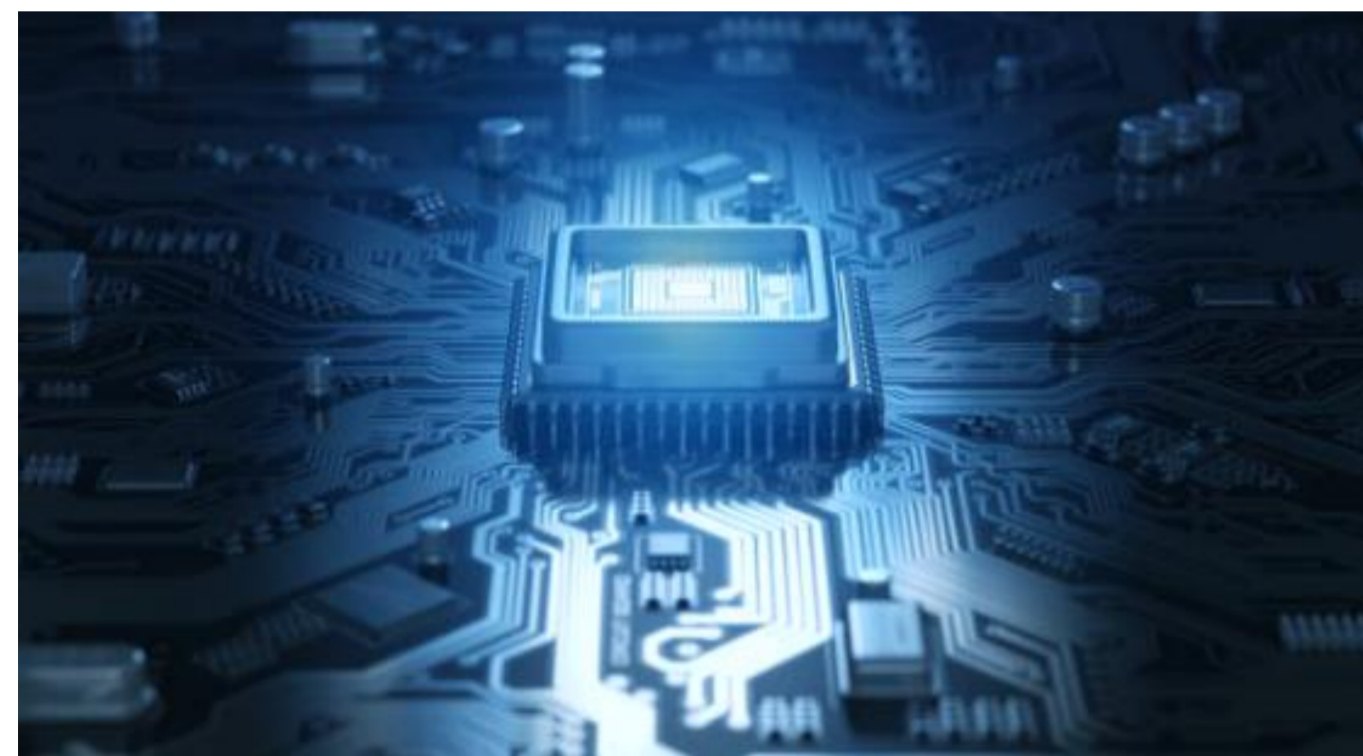


Mission

The **REWIRE** project envisions a holistic security management framework that can safeguard IoT environments during the whole spectrum of their lifecycle, from the Design to the Runtime phases.



REWIRE will define and leverage advanced and lightweight attestation mechanisms to enable the establishment of trust relationships in next generation Systems-of-Systems based on trust assertions and indisputable evidence.

Approach

REWIRE will be a 4-layered security sandbox that offers a harmonized toolchain to efficiently protect IoT deployments during their entire lifecycle.

It relies on the following core pillars:

- Provable secure cryptographic protocols, definition of customized instruction set
- Firmware & software security updates and patching validation
- Runtime attestation for verification of IoT devices' operational assurance using customizable lightweight TEEs
- Blockchain-assisted AI-based misbehaviour detection in distributed fashion

Use Cases



Smart Cities: Secure device on-boarding, collaborative threat and misbehaviour detection, and software and firmware updates for critical IoT devices



Automotive: Ensure the correct authentication and authorisation, prior to receiving the software updates to assess the trust level of unreliable sources.

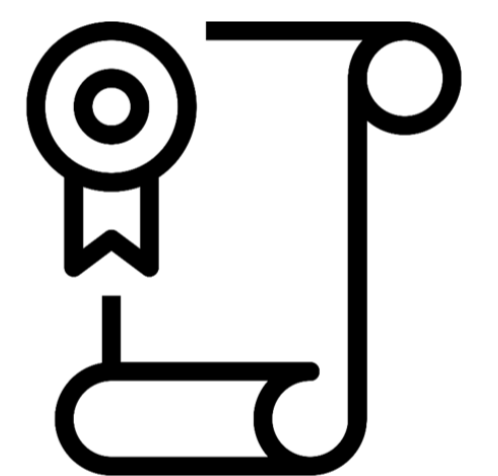


Smart Satellites: deployment and isolation of applications, services, software and security patches on a spacecraft in a secure manner.

Standardisation

Planned outcomes include the development of **standardization** proposals to push the state of the art in **cryptographic constructions** towards secure device execution, **formal hardware verification, dynamic and runtime trust assurance** in heterogeneous environments, **firmware and software integrity analysis** in connected devices, **secure and trust-aware data auditing** based on blockchain.

They will involve the technical committees of relevant standards bodies:



TCG, ISO/IEC JTC 1/SC 27, ISO/IEC JTC1/WG13, TIES/SWG-03, CEN, ETSI

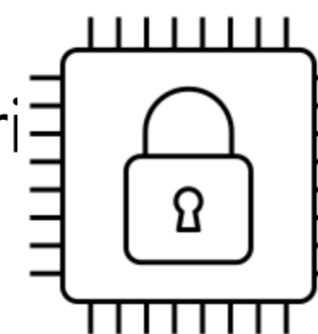
Main Goals



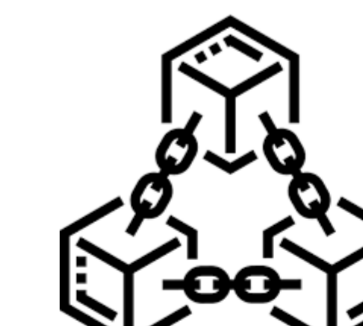
Compositional Assurances through Formally Verifiable HW-Security & Crypto Design Models



Firmware & Software Integrity Verification



Customizable TEE for In-Chip Security & Trust Assurance



Secure & Trust-Aware Auditing for Software Updates through Blockchain

Contact Information

Web: www.rewire-he.eu

Email: skazazis@ubitech.eu



@RewireProject



@rewire-horizoneu-project

Project Coordinator and Scientific Lead: UBITECH



This project has received funding from the European Union's Horizon Europe. Views and opinions expressed are those of the REWIRE consortium authors only and do not necessarily reflect those of the European Union or its delegated Agency DG CNECT. Neither the European Union nor the granting authority can be held responsible for them.