REWIRE

REWiring the CompoSItional Security VeRification and AssurancE of Systems of Systems

Newsletter Issue 2 | April 2023

Welcome to REWIRE Newsletter!

REWIRE is a 3-year Research and Innovation Action, started during October 2022, and funded under Horizon Europe.

REWIRE envisions a **holistic framework for continuous security assessment** and management of open-source and open-specification hardware and software for IoT devices, throughout their **entire lifecycle**, under the **zero-trust** concept, adhering to the **security-by-design** principle and providing **cybersecurity certification**.

In this issue

- Workshop on requirements and reference architecture
- Synergies & Liaisons with other projects
- Scientific publications
- Events
- REWIRE blog
- Learn more

Our newsletter is published every 3 months, offering updates on project achievements and results.
Subscribe here to receive REWIRE newsletter at your inbox.

Funded by the European Union

Disclaimer: Views and opinions expressed are those of the REWIRE consortium authors only and do not necessarily reflect those of the EU or its delegated Agency DG CNECT. Neither the EU nor the granting authority can be held responsible for them.

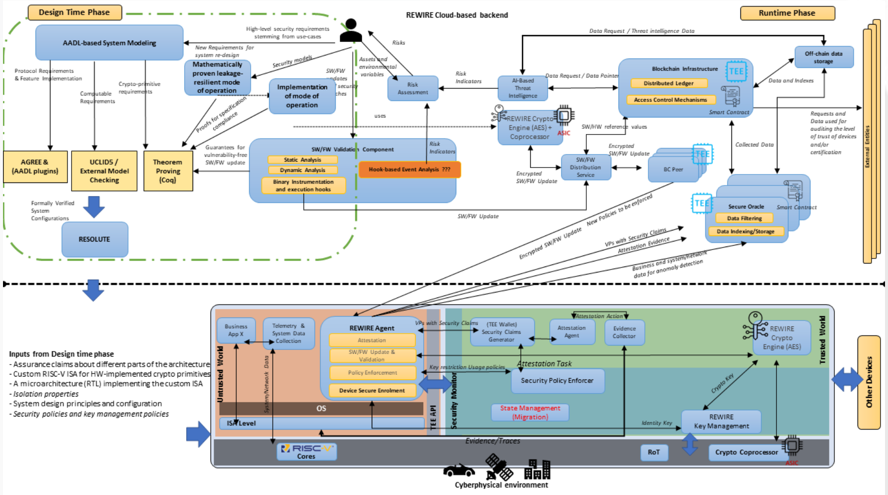
Eliciting REWIRE requirements and Reference Architecture

REWIRE Architecture and Requirements definition Workshop

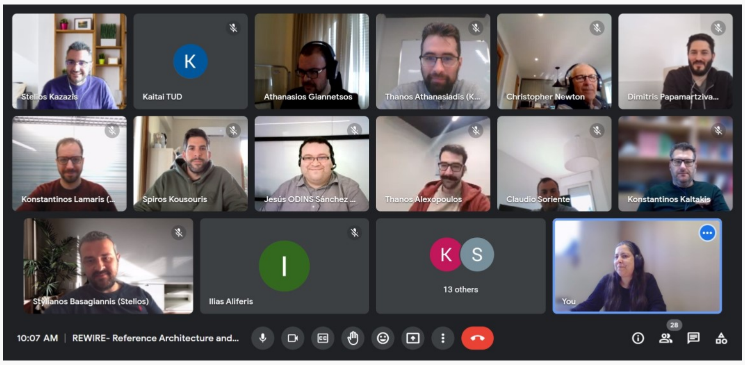
REWIRE consortium partners came together on March 23rd 2023 in a virtual workshop that aimed at eliciting the project requirements and designing the Reference Architecture to address them. The agenda of the meeting was divided into two parts, one for the discussion of the requirements, and one for the architecture. The aim of the workshop was to conclude the definition of REWIRE requirements and to flesh out the interactions between the components of the architecture.

During the first part of the workshop, the participants walked through the requirements to decide which ones were mandatory or optional. They clarified the purpose of each requirement and made the mapping with the technical components and technologies to be used to meet each requirement.

For the Reference Architecture, the ongoing discussions concern **design-time** for formal hardware and crypto, as well as the architecture for run-time. For the **run-time** part, each component's interactions have been defined as to achieve its operational objective in REWIRE.


Design Time Phase
AADL-based System Modeling
High-level security requirements stemming from use-cases
New Requirements for system re-design
Protocol Requirements & Feature Implementation
Computable Requirements
Crypto-primitive requirements
Mathematically proven leakage-resilient mode of operation
Security models
Implementation of mode of operation
Proofs for specification compliance
Guarantees for vulnerability-free SW/FW update
AGREE & (AADL plugins)
UCLID5 / External Model Checking
Theorem Proving (Coq)
Formally Verified System Configurations
RESOLUTE
SW/FW updates / security patches
Assets and environmental variables
Risks
Risk Assessment
Risk Indicators
uses
SW/FW Validation Component
Static Analysis
Dynamic Analysis
Binary Instrumentation and execution hooks
Hook-based Event Analysis ???
SW/FW Update
REWIRE Cloud-based backend
Runtime Phase
Data Request / Threat intelligence Data
AI-Based Threat Intelligence
Data Request / Data Pointer
Blockchain Infrastructure
TEE
Distributed Ledger
Access Control Mechanisms
Smart Contract
Off-chain data storage
Data and Indexes
REWIRE Crypto Engine (AES) + Coprocessor
ASIC
SW/HW reference values
Encrypted SW/FW Update
SW/FW Distribution Service
BC Peer
Collected Data
Requests and Data used for auditing the level of trust of devices and/or certification
External Entities
Secure Oracle
Data Filtering
Data Indexing/Storage
Encrypted SW/FW Update
New Policies to be enforced
VPs with Security Claims
Attestation Evidence
Business and system/network data for anomaly detection
Inputs from Design time phase
- Assurance claims about different parts of the architecture
- Custom RISC-V ISA for HW-implemented crypto primitives
- A microarchitecture (RTL) implementing the custom ISA
- Isolation properties
- System design principles and configuration
- Security policies and key management policies
Untrusted World
Business App X
Telemetry & System Data Collection
System/Network Data
REWIRE Agent
Attestation
SW/FW Update & Validation
Policy Enforcement
Device Secure Enrolment
OS
ISA Level
TEE API
Security Monitor
VPs with Security Claims
Key restriction Usage policies
(TEE Wallet) Security Claims Generator
Attestation Action
Attestation Agent
Evidence Collector
Attestation Task
Security Policy Enforcer
State Management (Migration)
REWIRE Crypto Engine (AES)
Crypto Key
Identity Key
REWIRE Key Management
Trusted World
Other Devices
Evidence/Traces
RISC-V Cores
RoT
Crypto Coprocessor
ASIC
Cyberphysical environment

Ongoing technical discussions focus on capabilities for application instrumentation/ hooks, repackaging, and vulnerability detection on different Operating Systems (OS) or Real-time OS (RTOS). Additionally, Keystone Trusted Execution Environment (TEE) and its isolation capabilities, key management, support of attestation, and TEE Wallet, are being investigated. Another architectural component under consideration is the TEE Wallet and support of attestation, verifiable credentials and software / Firmware update. Also, the partners discussed interactions and data flows to be supported by the Secure Oracles, as well as the attestation schemes and evidence collector. Finally, one point of discussion is AI approaches to be followed for the misbehavior detection.



Overall, the meeting was productive, and the participants made progress on the requirements and architecture for the REWIRE project. The next steps include the finalisation of the requirements and architecture and moving to the design and development phase of the project.

Funded by the European Union

Disclaimer: Views and opinions expressed are those of the REWIRE consortium authors only and do not necessarily reflect those of the EU or its delegated Agency DG CNECT. Neither the EU nor the granting authority can be held responsible for them.

Synergies & Liaison with other projects

CROSSCON: a Cross-platform Open Security Stack for Connected Devices

CROSSON aims at designing a new open, modular, highly portable, and vendor-independent IoT security stack that can run on highly heterogeneous devices.
https://crosscon.eu/

PUZLE: Towards a Sophisticated SIEM Marketplace for Blockchain-based Threat Intelligence and Security-as-a-Service

The PUZZLE project implements a highly usable cybersecurity, privacy and data protection management marketplace targeted at SMEs&MEs.
https://puzzle-h2020.com/

CERTIFY: aCtive sEcurity foR connecTed devIces liFecYcles

CERTIFY defines a methodological, technological, and organizational approach towards IoT security lifecycle management.
https://certify-project.eu/

ORSHIN: Open-source ReSilient Hardware and software for Internet of thiNgs

ORSHIN is creating the first generic and integrated methodology, to develop secure network devices based on open-source components while managing their entire lifecycle.
https://horizon-orshin.eu/

CONNECT: Continuous and Efficient Cooperative Trust Management for Resilient CCAM

The vision of CONNECT is to address the convergence of security and safety in CCAM by assessing dynamic trust relationships and defining a trust model and reasoning framework.
https://horizon-connect.eu/

SecOPERA: Secure OPen source software and hardwaRe Adaptable framework

SecOPERA will provide a one-stop hub for complex OSS/OSH solutions offering to designers, implementers, operators and open-source HW/SW developers the means to analyse, assess, secure/harden and share open-source solutions as these are integrated in an overall complex product within a networked connected environment.
https://secopera.eu/

Funded by the European Union

Disclaimer: Views and opinions expressed are those of the REWIRE consortium authors only and do not necessarily reflect those of the EU or its delegated Agency DG CNECT. Neither the EU nor the granting authority can be held responsible for them.

Publications, Events & Media

Scientific publications

We present below the list of papers submitted and accepted during the period January-March 2023 that carry acknowledgement of REWIRE project. For the complete list of research papers, please visit https://www.rewire-he.eu/publications/.

◊ Felipe Lisboa Malaquias, Georgios Giantamidis, Stylianos Basagiannis, Simone Fulvio Rollini, Isaac Admundson. *Towards a methodology to design provably secure cyber-physical systems*, The 27th Ada-Europe International Conference on Reliable Software Technologies (Ada-Europe 2023), Lisboa, Portugal. Accepted.

Events

REWIRE @ HiPEAC2023 Conference

Our colleagues from project partner Collins Aerospace participated in the industrial exhibition which run in parallel with the HiPEAC2023 Conference., where REWIRE has been displayed in a technical poster. Read more at https://www.rewire-he.eu/rewire-presented-in-the-hipeac2023-conference/.

REWIRE presented in the IoT Solutions World Congress 2023

Our colleagues from project partner OdinS participated in IoT Solutions World Congress (IOTSWC) 2023, where they distributed REWIRE promotional material and discussed the objectives and aim of the project with other event participants. Read more at https://www.rewire-he.eu/rewire-presented-in-the-iot-solutions-world-congress-2023/

REWIRE at Embedded World 2023

Our colleagues from project partner KENOTOM, participated with a booth in embedded world Exhibition & Conference 2023 and promoted REWIRE. Read more at https://www.rewire-he.eu/rewire-at-embedded-world-2023/.

#REWIREBlog

Here is the list of blog entries for period January-March 2023. Stay tuned with our informative and insightful posts at https://www.rewire-he.eu/blog/.

◊ REWIRE behind the Scenes, by Dr. Stylianos Kazazis, UBITECH (March 15, 2023)

◊ Addressing the risk of physical-level attacks in the IoT adversarial context, by Dr. François Koeune, UCLouvain (March 30, 2023)

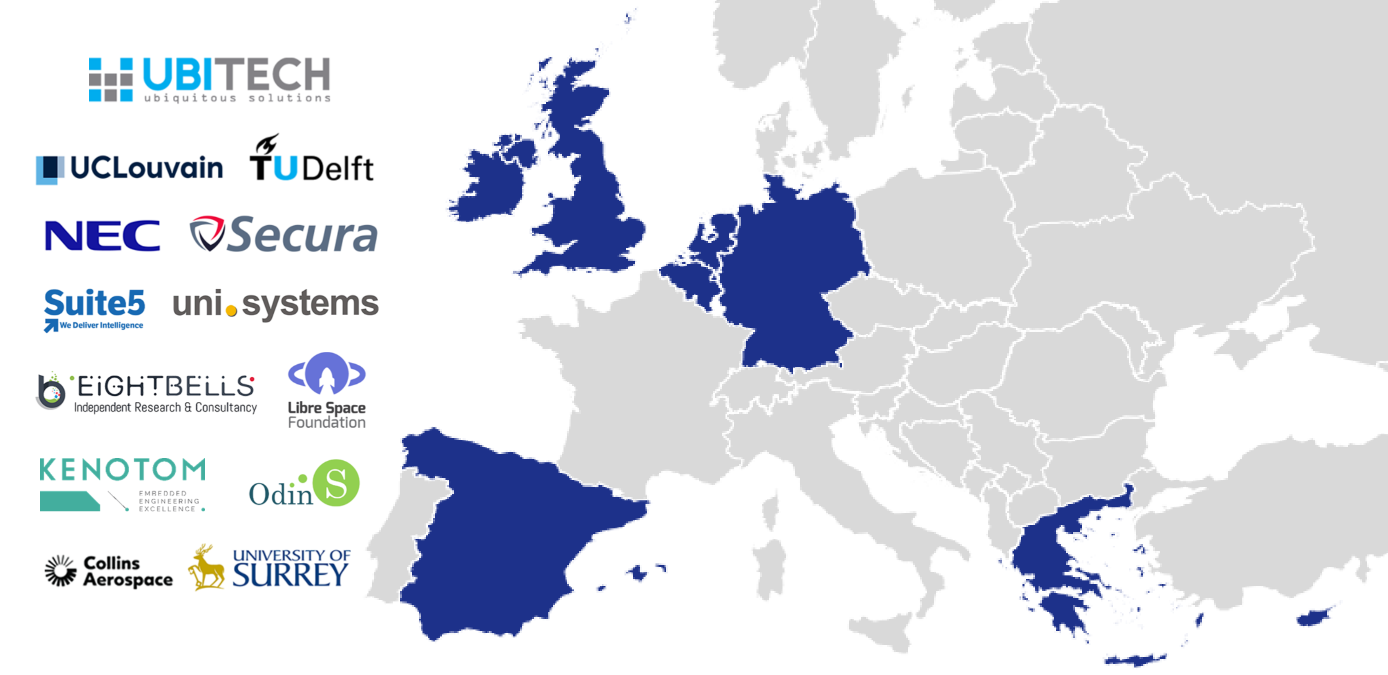
Funded by the European Union

Disclaimer: Views and opinions expressed are those of the REWIRE consortium authors only and do not necessarily reflect those of the EU or its delegated Agency DG CNECT. Neither the EU nor the granting authority can be held responsible for them.

At a glance

Rewire consortium

REWIRE brings together 13 partners form 8 European countries, providing all the required expertise for achieving the project's ambitious objectives.


UBITECH ubiquitous solutions
UCLouvain
TU Delft
NEC
Secura
Suite5 We Deliver Intelligence
uni.systems
EIGHTBELLS Independent Research & Consultancy
Libre Space Foundation
KENOTOM EMBEDDED ENGINEERING EXCELLENCE
OdinS
Collins Aerospace
UNIVERSITY OF SURREY

Fact Sheet

Title	Rewiring the Compositional Security Verification and Assurance of Systems of Systems Lifecycle
Acronym	REWIRE
GA No	101070627
Start	01 October 2022
End	30 September 2025
Budget	4.158.961 €
EU Fund	4.158.961 €
Topic	HORIZON-CL3-2021-CS-01-02
Scheme	RIA - Research and Innovation action

rewire-he.eu   rewire-horizoneu-project   @RewireProject   @REWIRE-HE-project

REWIRE newsletter is published every three months, offering the latest news and advances of the project!
Subscribe here to receive REWIRE newsletter at your inbox.

Funded by the European Union

Disclaimer: Views and opinions expressed are those of the REWIRE consortium authors only and do not necessarily reflect those of the EU or its delegated Agency DG CNECT. Neither the EU nor the granting authority can be held responsible for them.