REWIRE

REWiring the ComposItional Security VeRification and AssurancE of Systems of Systems

Newsletter Issue 12 | September 2025

Welcome to the 12th 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

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

End of the REWIRE Project

Athens, September 30, 2025

After three years of intense research, innovative ideas, and a fruitful collaboration among 14 partners, the REWIRE Project has successfully concluded its mission to reinforce Europe's cybersecurity posture in the age of the great rise of the IoT ecosystem and trusted computing. With its final activities wrapped up this September, REWIRE delivers a legacy of ground-breaking new technologies, exploitable innovations and unique research outcomes for the open-source communities that upgrade cybersecurity and trustworthiness of the EU digital ecosystems.

In a globally interconnected world, with the rise of the IoT and pervasive Edge Computing we witness the continuous transformation of societies, industries and economies. Although, this transformation also leads to the escalation of emerging cyber risks: such as the fragmentation of trust anchors, HW and SW vulnerabilities, and growing cyberattacks that target essential services in major and critical industries. REWIRE partners managed successfully to address these challenges with a common vision: to create an interoperable, trustworthy computing continuum that extends from edge devices to cloud services, integrating new trust models and extensions, lightweight attestation mechanisms, and automated risk assessment into practical solutions for real-world applications.

By combining expertise in trusted execution environments (TEE), formal verification, AI-driven anomaly detection, secure blockchain infrastructures, and verifiable credentials, the REWIRE partners advanced both scientific knowledge and practical deployment pathways, contributing actively with core innovations and a suite of real-world exploitable results. At the heart of REWIRE's success is the advanced portfolio of tools and demos developed during this adventurous journey. As a result, in three years, REWIRE managed to develop a portfolio of innovative KERs and outcomes, demonstrating the impact of the research in three Smart verticals (Smart Cities, Smart Automotive and Smart Satellites), in order to ensure that results moved beyond the laboratory, REWIRE validated its technologies in high-impact demonstrators. These demonstrators not only validated REWIRE technologies but also engaged industry stakeholders, creating pathways for exploitation and up-scale.

To this end, the REWIRE's legacy is not only technological, but also strategic. The project has directly contributed to Europe's cybersecurity policy frameworks by aligning fully with NIS2 Directive. Its innovations support compliance with these regulations by offering concrete mechanisms for risk management, certification, and resilience in the face of evolving hybrid threats.

As REWIRE closes, but the technologies and knowledge it generated are expected to fuel new research directions and new uptakes. In the words of the consortium: *"REWIRE has shows that cybersecurity for the IoT requires a continuum of trust — from design to deployment, from cloud to edge, and from the lab to the market. Our project has served this foundation."*

Funded by the European Union

REWIRE Interview Series

Interview #5: Annika Wilde (Rhur University Bochum)

During the interview, Annika explores key perspectives on cybersecurity challenges in modern computing architectures, with a particular focus on trusted execution environments for enhanced security. The discussion highlights open-source innovations in RISC-V and open hardware security, alongside strategies for defending against hardware-exploiting attacks. Special attention is given to REWIRE's impact on safety-critical systems, its role in implementing sustainable security, and the significant progress and achievements it has made in advancing hardware resilience.

Watch the full interview here: https://www.youtube.com/watch?v=5G-6rkxwvnE

Interview #6: Samira Briongos (NEC Labs Europe)

Samira discusses the most expert perspectives on the urgent cybersecurity challenges in critical systems, focusing on trusted computing and remote attestation methodologies. She explores open-source advancements in RISC-V and hardware security, while also addressing strategies for protecting against hardware-exploiting attacks. Furthermore, Samira emphasizes the importance of implementing sustainable security through the REWIRE approach and concludes with final thoughts on shaping the future security landscape.

Watch the full interview here: https://www.youtube.com/watch?v=IMgwhaWfDDM

Funded by the European Union

New Joint White Paper

REWIRE joined forces with 5 EU-funded projects for a new white paper!

Title: Gain insights into the latest empirical Cyber Security trends and results from Horizon Europe Funded Projects: A joint White Paper from AI4CYBER, CERTIFY, CROSSCON, ENCRYPT, REWIRE and TRUSTEE.

Executive Summary:

In recent years, the significance of cybersecurity has grown exponentially in an increasingly digital world. This white paper represents a collaborative effort to consolidate insights from eight distinct European projects, all funded to address the evolving cybersecurity landscape. Within these pages, we aim to provide valuable insights into each project's objectives, use cases, high-level architecture, and the pivotal technologies that will be harnessed to safeguard our digital ecosystem. By shedding light on these initiatives, we intend to equip various stakeholders with the most current information necessary to tackle emerging cybersecurity challenges effectively.

In today's interconnected world, the rapid expansion of digital data has ushered in an era of unprecedented innovation and convenience. However, it has also brought forth an array of cyber threats that jeopardize the security and privacy of sensitive information across critical domains such as healthcare, finance, and entertainment. These challenges have necessitated the development of robust solutions that not only enhance data security but also ensure compliance with stringent regulations like the General Data Protection Regulation (GDPR).

The European Union has recognized the urgency of addressing these cybersecurity challenges, leading to the initiation of eight groundbreaking projects, each committed to advancing the field of cyber security. This joint white paper aims to provide an overview of these projects and their objectives, shedding light on their significance in shaping the future of data protection and cybersecurity. The domain of cybersecurity has evolved rapidly in response to the increasing digitization of critical sectors, exposing vulnerabilities that necessitate innovative solutions. With digital data becoming the lifeblood of industries, the need for privacy-preserving technologies has become paramount.

To address challenges and limitations related to cybersecurity, the projects discussed in this white paper are poised to embark on several basic research directions.

Read the full white paper on the REWIRE website: xxxxxxxxxxxxxxxx

Funded by the European Union

REWIRE Blog Highlights

#REWIRE Blog

We are excited to share that the REWIRE project now hosts a total of 61 blog articles. These articles reflect the vibrant activity, research insights, and domain knowledge generated by the REWIRE team and partners over the project's lifetime. The blog series covers a wide array of themes, illustrating how REWIRE touches multiple facets of cybersecurity, hardware resilience, and trustworthy computing. Below is a snapshot of key topic areas:

- Risk Assessment & Architecture
- Update, Migration & Key Management
- Zero-Touch Onboarding, Enrollment & Trust Concepts REWIRE's mechanisms for automating secure onboarding
- Formal Verification, Integrity & Hardware Attacks
- Application Use Cases & Domains
- AI, Trust, Legal & Ethical Dimensions

We present below the most recent blog articles which were published on the REWIRE website and social media during the past few months. For the complete list of blog articles, please visit https://www.rewire-he.eu/blog/.

- **REWIRE Risk Assessment – Automotive Use Case**

In order to demonstrate the implied relevance in real world use cases, REWIRE applies its risk assessment framework to the automotive sector, one of the most demanding areas for cybersecurity. Modern vehicles are essentially computers on wheels, with dozens of interconnected Electronic Control Units (ECUs), complex firmware, and constant communication with external networks.

- **Instantiation of REWIRE MSPL-based Security Policies**

Risk assessment is only valuable if it leads to effective enforcement. Once risks are identified and prioritised, systems must be able to translate these insights into concrete security actions. The REWIRE Project achieves this through the Multi-level Security Policy Language (MSPL), a flexible and expressive framework for defining, instantiating, and enforcing policies across multiple system layers.

- **REWIRE SW/FW Vulnerability Analysis**

Modern systems are only as secure as their software and firmware. Vulnerabilities in these layers have been at the root of some of the most devastating cyberattacks, from ransomware outbreaks to targeted intrusions in vehicles and aircraft. Identifying and managing these vulnerabilities requires both technical depth and organisational agility. The REWIRE Project addresses this need with a dedicated Software/Firmware Vulnerability Analysis (SFVA) framework, integrated into its broader risk assessment architecture.

- **The Types of Keys within the REWIRE Ecosystem**

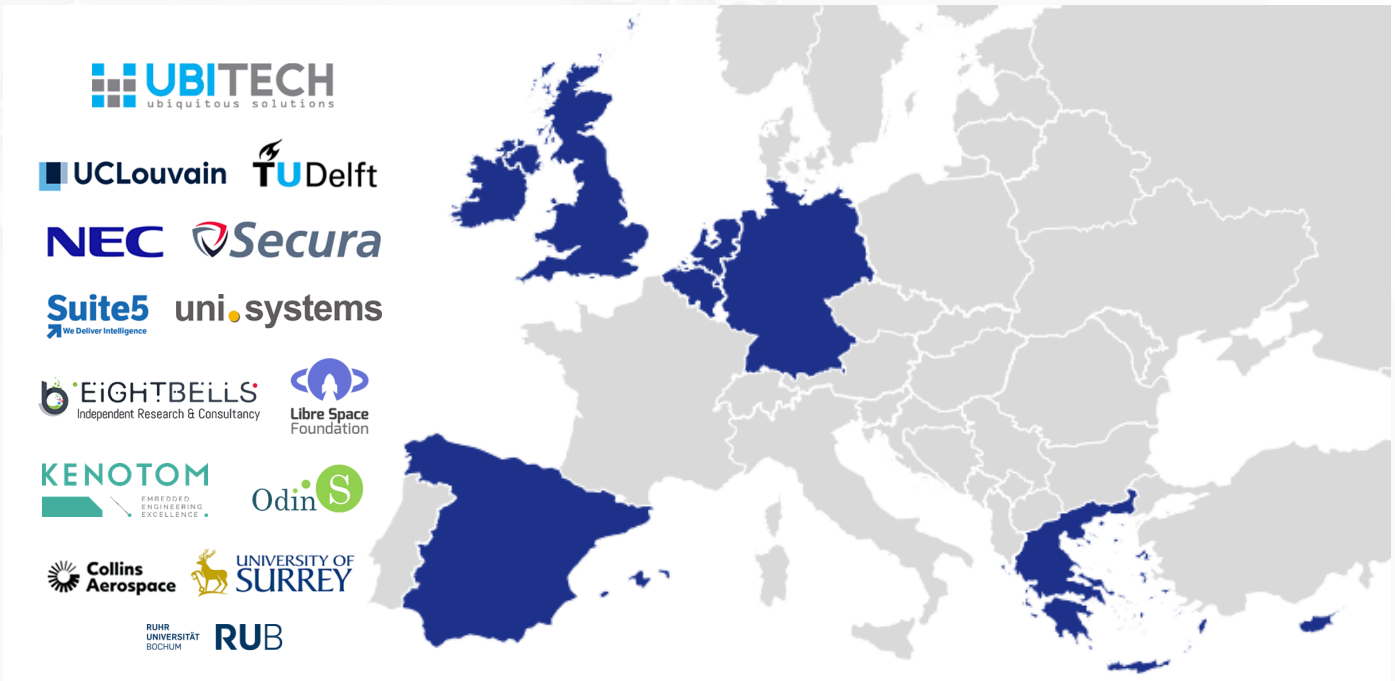
Cryptography is only as strong as the management of its keys, and poor practices can undermine even the most secure algorithms. The REWIRE Project addresses this challenge by introducing a Harmonised Key Management (HKM) framework designed to unify cryptographic interfaces, secure the entire key lifecycle, and enable crypto-agility across multiple platforms. By embedding a Key Management System (KMS) into the Security Monitor—the most trusted component of the system—REWIRE ensures that critical assets are managed securely, even though this slightly increases the Trusted Computing Base.

Funded by the European Union

At a glance

Rewire consortium

REWIRE brings together 14 partners form 8 European countries, providing all the required expertise for achieving the project's ambitious objectives.



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