REWiring the ComposItional Security VeRification and AssurancE of Systems of

Newsletter Issue 9 | May 2025

Welcome to the 9th 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**.

Our newsletter is published periodically 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.

REWIRE Workshop on Trustworthy AI

RERWIRE & CONNECT co-organise a Workshop on Trustworthy AI

Date: 25-26 March 2025

Location: Holm Centre, Frankfurt Airport.

Host: CONNECT and **REWIRE** Horizon Europe projects

The Workshop on Trustworthy AI, brought together leading experts and stakeholders from diverse AI-related fields to explore the evolving challenges and future directions of AI trustworthiness. This The workshop was co-organized by the CONNECT Horizon Europe project and the REWIRE HorizonEU Project, reflecting a strong commitment to fostering trustworthy AI across Europe,

Day 1 Highlights

The opening day of the workshop featured insightful presentations and engaging panel discussions that addressed key challenges surrounding AI trustworthiness. Participants and speakers delved into important topics such as the reliability of data in CCAM and related fields, focusing on issues like data integrity, data space frameworks, and standardization. The discussions also covered trust across the AI system lifecycle, including AI explainability, bias mitigation, the role of NLP models, and safety concerns. Additionally, the use of AI in 6G and ITS domains was explored, emphasizing the need for secure systems, distributed machine learning, and resilience in AI-driven technologies. The expert speakers gave their valuable insights and to all participants for their active engagement and thoughtful contributions, which greatly enriched the dialogue

Day 2 Highlights

On the second day of the workshop, participants engaged in an interactive working session aimed at fostering in-depth dialogue on the future of AI trustworthiness. Using a rotating table format, attendees switched groups every 20 minutes to address pre-set questions from various perspectives. This approach encouraged the exchange of diverse viewpoints and expertise to uncover key challenges and potential solutions. Moderators then compiled and presented the main takeaways, offering a clear summary of the most important insights gathered. A major outcome of the workshop is the creation of a roadmap for AI trustworthiness, informed by the rich discussions and contributions during the session. This roadmap will guide ongoing conversations, future research initiatives, and policy development in the area of trustworthy AI.

REWIRE Ethics and Legal Roadmap

The significant role of REWIRE Ethics and Legal Roadmap by Ubitech

The present blog post provides an interplay analysis between the concepts of trust and ethics within the REWIRE project, emphasizing the concept of trust from a user's perspective. More specifically, the REWIRE's roadmap sets out the context in which we examine the dimensions and determinants that affect the trust that humans can understand. Since the REWIRE framework and the design of the MVP establish an innovative trusted System-of-Systems (SoS), its value offering for the end-users focuses on cybersecurity and trust extensions. To this end, despite its technical standpoint, the project manages to provide strong trust evidence, including but not limited to Integrity, Safety, Consistency, Usability, Verifiability, Transparency, Accuracy, Privacy, Security, Reliability, etc.

Figure 1 showcases and describes the roadmap from the definition of Trust and Trustworthiness concepts within the REWIRE Framework to the Mapping of Trust Relationships, the Assessment of Trustworthiness with the Compute Continuum, and the Final Validation and Testing. This roadmap establishes a framework for evaluating trust and trustworthiness across complex, layered technological ecosystems involving both human and machine stakeholders. The iterative approach starts with broad conceptual definitions and gradually narrows down to practical applications and validations across specific use cases (within the context of REWIRE, Smart Cities, Smart Automotive and Smart Satellites).

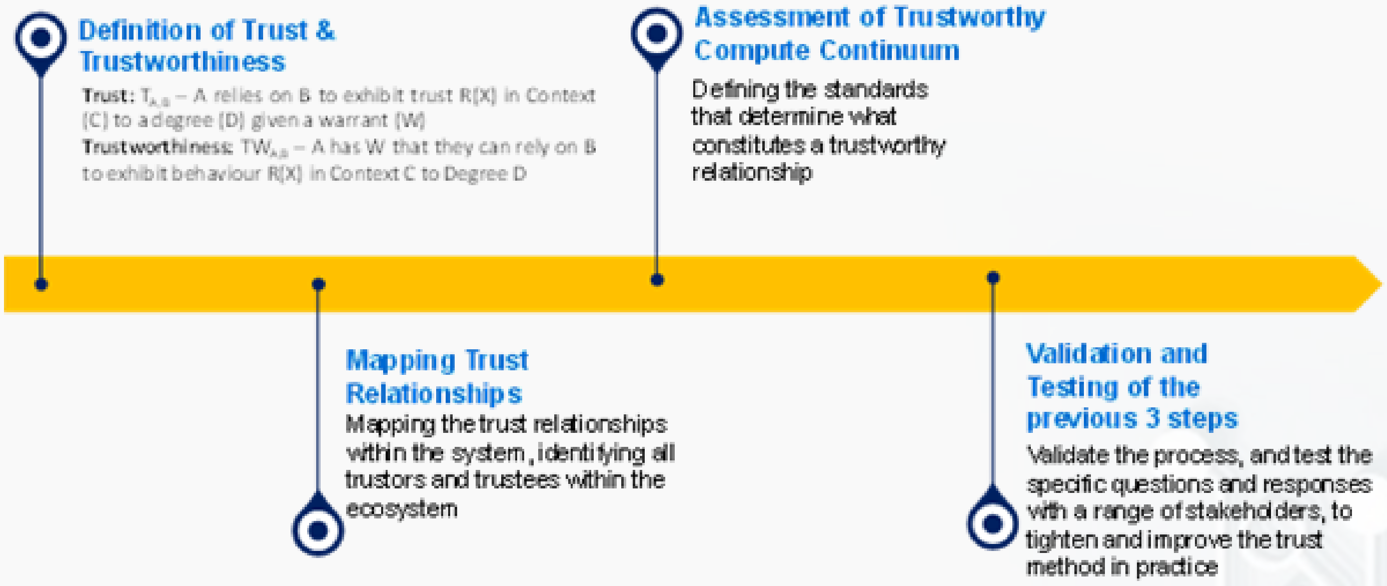

Definition of Trust & Trustworthiness
Trust: $T_{A,B}$ – A relies on B to exhibit trust R[X] in Context (C) to a degree (D) given a warrant (W)
Trustworthiness: $TW_{A,B}$ – A has W that they can rely on B to exhibit behaviour R[X] in Context C to Degree D
Assessment of Trustworthy Compute Continuum
Defining the standards that determine what constitutes a trustworthy relationship
Mapping Trust Relationships
Mapping the trust relationships within the system, identifying all trustors and trustees within the ecosystem
Validation and Testing of the previous 3 steps
Validate the process, and test the specific questions and responses with a range of stakeholders, to tighten and improve the trust method in practice

Figure 1: Roadmap for the Ethical and Legal Dimensions of REWIRE project

In the context of REWIRE, we envision performing a qualitative analysis of the type of evidence that a trust assessment framework needs to have for achieving high accuracy and at the same time be ethically sound and to evaluate if the REWIRE TCB can enable such mechanisms. More specifically, REWIRE offers a systematic approach to evaluating trust in complex, distributed computing environments.

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.

REWIRE Ethics and Legal Roadmap

The framework is ethically grounded, technically rigorous, and designed to evolve with stakeholder input, making it adaptable for a wide range of applications in the Compute Continuum.

To this end, REWIRE stresses that ethical and social aspects of trust must be understood alongside technical ones, and these concepts need to be tailored for different use cases. n addition, REWIRE incorporates mechanisms such as attestation to verify trustworthiness. accuracy tracking, and compliance with privacy standards such as GDPR. Finally, the last step guarantees that the REWIRE Framework is robust, adaptable, and practical. It is also the foundation for defining a “Required Trust Level” (RTL) for both components and systems. Overall, this level integrates ethical principles, technical evidence, and stakeholder insights to determine whether trust in a component is justified.

This includes assessing if devices can operate robustly and safely, communicate accurately, and remain free from external interference. In addition, REWIRE adapts these principles to System-of-Systems, focusing on embedded systems and IoT elements. For instance, technical robustness includes ensuring systems are secure, resilient, and accurate, while data governance ensures lawful, ethical processing of personal and non-sensitive data. Tables outline how systems can self-assess their performance against these values, covering aspects like penetration testing, fallback mechanisms,

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.

REWIRE Blogs & Demos

#REWIRE Blog

We present below the 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 Framework at Work** by UBITECH

The REWIRE project defines a comprehensive architectural framework composed of two distinct operational phases: the Design-time Phase and the Runtime Phase. These phases together ensure robust security, integrity, and resilience of critical software and hardware systems across their entire lifecycle, combining both proactive and reactive security measures from the initial design to operational deployment. Read more at: https://www.rewire-he.eu/putting-the-rewire-framework-at-work/

REWIRE Demo Videos

REWIRE has produced several demo videos with the work that has been undertaken. For the complete list of videos, please visit https://www.rewire-he.eu/media-kit/demo-videos/

♦ **UBITECH, explores the integration of Fabric Private Chain code (FPC)**
The demo showcases how Fabric Private Chaincode (FPC) is being utilized within the REWIRE framework to enable secure and privacy-preserving lifecycle management of embedded systems.

♦ **SUITE5 presents the AI-based misbehavior detection engine**
The demo developed as part of the REWIRE project Work Package 4, designed to enhance trust in embedded systems and improve the identification of anomalous behavior in cooperative environments.

♦ **UBITECH secures Device Lifetime Management with REWIRE's Attestation Engine**
The demo presents the mechanisms behind attestation protocols, showcasing our project's approach to secure device onboarding, runtime verification, and key management.

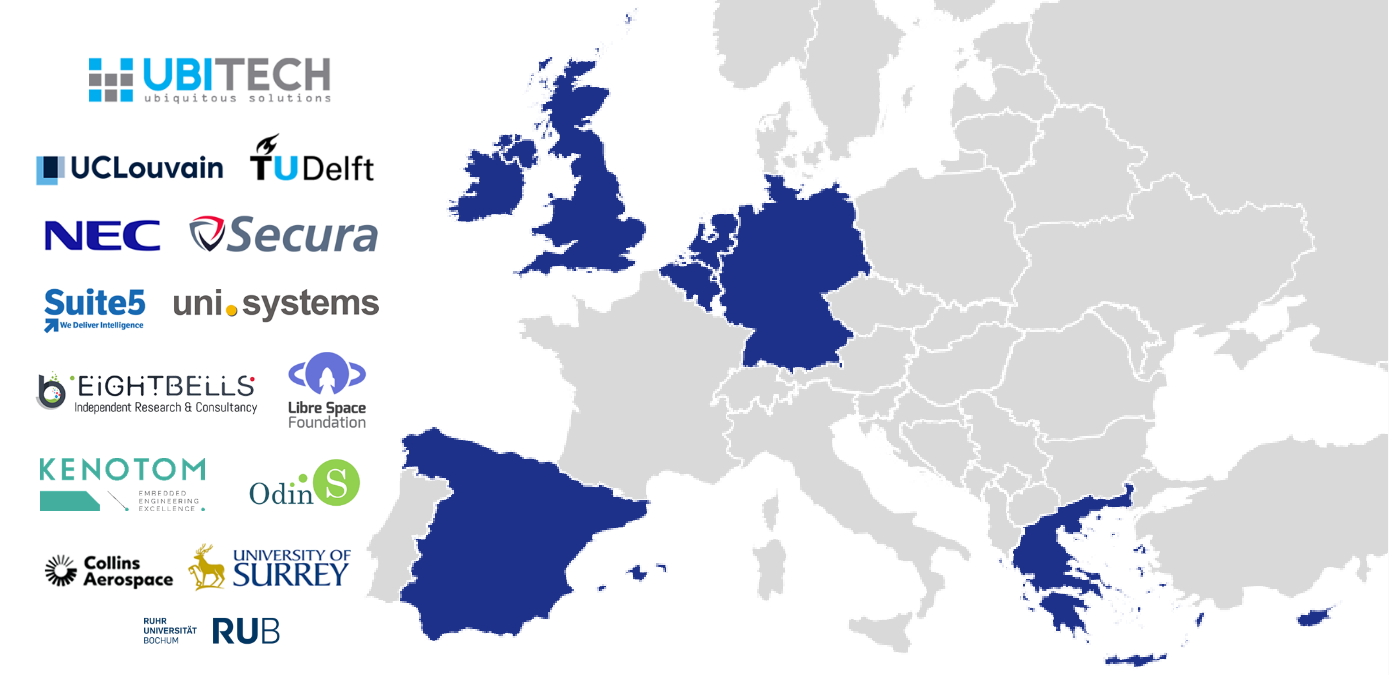
Funded by the European Union

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 14 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
RUHR UNIVERSITÄT BOCHUM
RUB

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.