



REWIRE

REWIRE: Re-Wiring the Compositional Security Verification and Assurance of Systems Life-Cycle

INFOCOM WORLD 2023,
ATHENS, 14 DECEMBER, 2023



Alexandros DIMOS, 8Bells LTD



EiGHtBELLs

Independent Research & Consultancy

EIGHT BELLS TODAY

 EIGHT BELLS LTD is based in Nicosia, Cyprus and Athens, Greece

 Specializing in Defence, Security, Space, Telecommunications, Cybersecurity, eHealth and Environmental Protection, with disruptive IT solutions

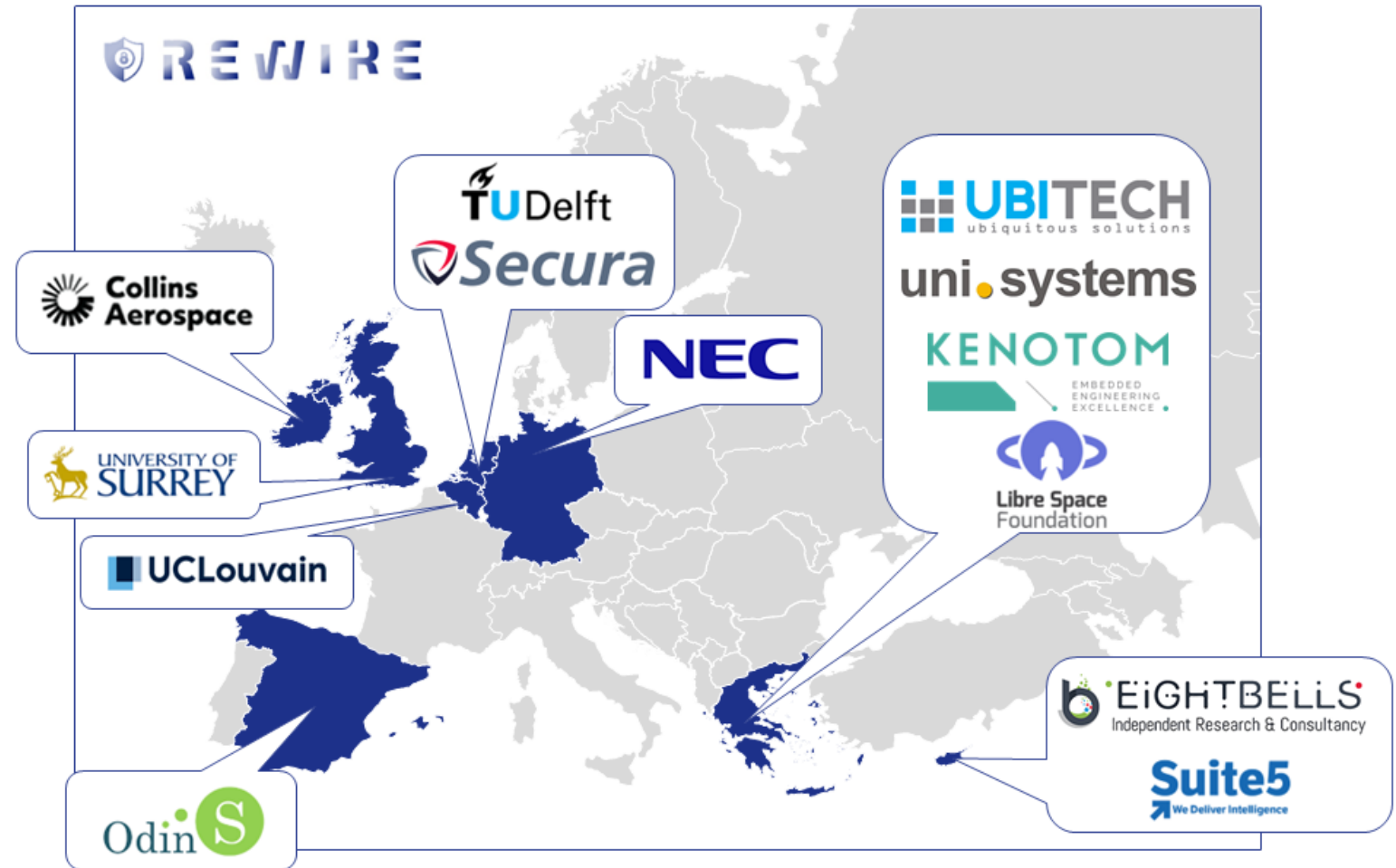
 Our technical capabilities include Systems & Network Engineering, Cloud computing, Privacy, Security & Data Protection and Software development

 Eight Bells, following a specific development plan, invests in high value-added staff by creating new job positions.

The Consortium

13 partners from 8 EU countries:

- 3 x Industrial partners
- 3 x Service providers
- 4 x Research Institutes and Universities
- 3 x SMEs



At a glance



REWIRE: Re-Wiring the Compositional Security Verification and Assurance of Systems Life-Cycle.



REWIRE aims to provide a **holistic framework for continuous security assessment and management** throughout the entire lifecycle of IoT devices under the zero-trust concept, while at the same time adheres to the **security-by-design principle**



Horizon Europe – Work Programme 2021-2022 | **Increased cybersecurity 2021**

Call: HORIZON-CL3-2021-CS-01 | **Topic:** HORIZON-CL3-2021-CS-01-02 | **GA Number:** 101070627

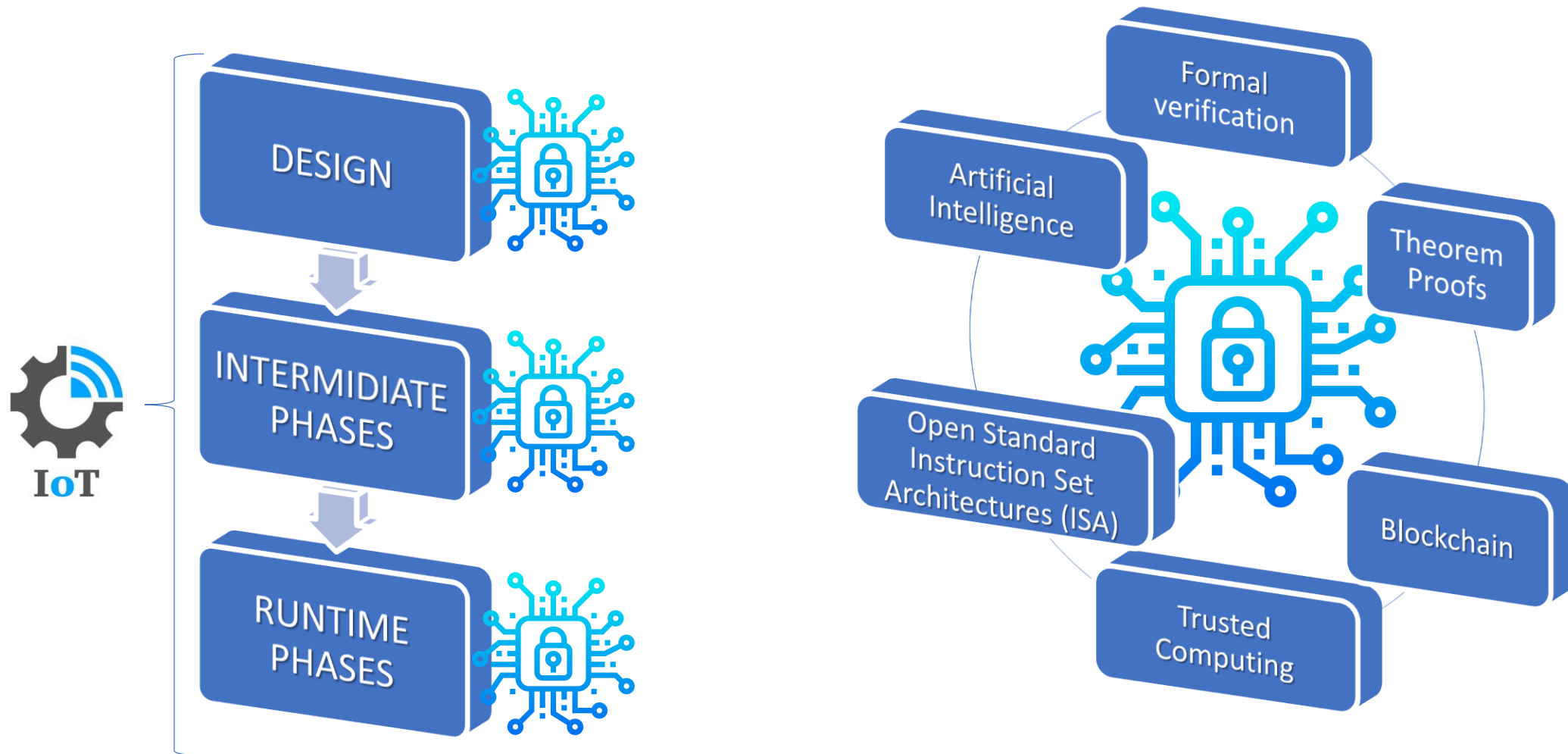


Duration: October 2022 – September 2025



Funding Scheme: Research & Innovation Action | **Budget:** € 4.158.961 | **EU contribution:** € 4.158.961

Vision: “Never Trust, Always Verify”

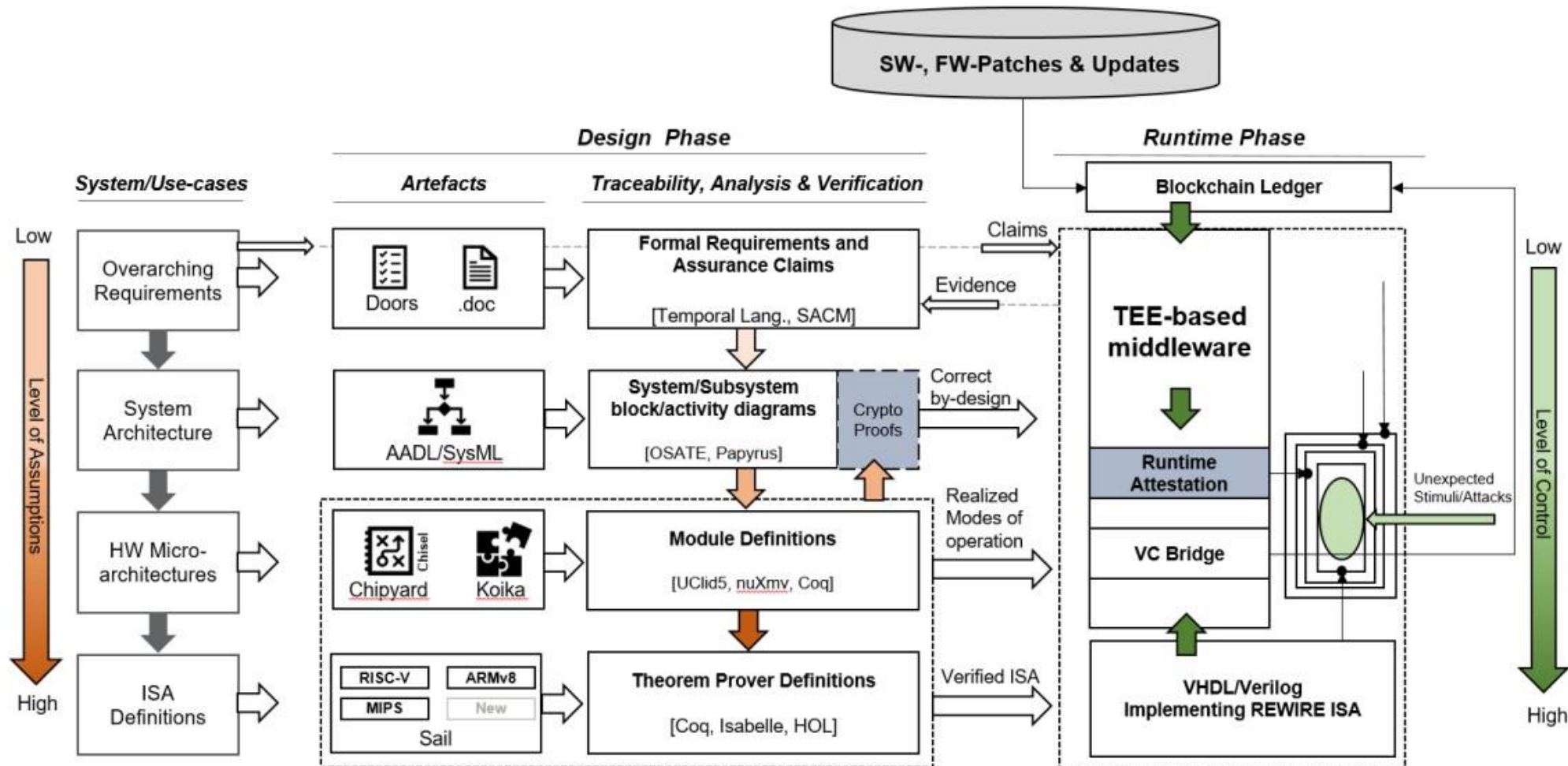


4-Layer Toolchain Workflow

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

- ≡ Formal verification of cryptographic protocols.
- ≡ Firmware (FW) & software (SW) security updates and patching validation.
- ≡ Runtime attestation for verification of IoT devices' operational assurance.
- ≡ Blockchain-assisted AI-based misbehavior detection in distributed fashion.

4-Layer Toolchain Workflow



Objectives

- ③ **Continuous security assessment and management of IoT devices throughout the entire lifecycle (bootstrapping, commissioning, operation, upgrade) under zero-trust conception.**
- ③ **Security-by-design through verified open-source software and open standard hardware designs for attack surface minimization.**
- ③ **Runtime monitoring of IoT trustworthiness through cryptographically verifiable security proofs and efficient attestation.**
- ③ **Cyber Security situational awareness in heterogeneous IoT environments through auditable security patch management and misbehavior detection.**
- ③ **Trust-aware continuous authentication and authorization for the secure communication and identity management in IoT ecosystems.**
- ③ **Simulation, Validation & Evaluation of REWIRE Framework in the field of Smart Cities, Smart Satellites and Smart Automotive.**
- ③ **Communication, exploitation and standardization strategy for adoption of REWIRE outcomes.**

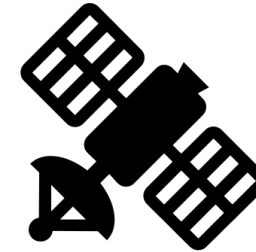
Use Cases



**Smart Cities for
Empowering Public
Safety.**



**Adaptive In-Vehicle
Software & Firmware
Patch Management &
Software Functions
Migration.**



**Smart Satellites Secure
Software Updates for
Spacecraft
Applications &
Services.**

Impact

- 1. Strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies.**
- 2. More resilient digital infrastructures, systems and processes.**
- 3. Increased software, hardware and supply chain security.**
- 4. Secured disruptive technologies.**
- 5. Smart and quantifiable security assurance and certification shared across the EU.**
- 6. Reinforced awareness and a common cyber security management and culture.**

Thank you for your attention!

Alexandros Dimos, R&D Engineer
alekos.dimos@8bellsresearch.com

Stay In Touch!



<https://www.rewire-he.eu/>



[REWIRE Project](#)



<https://twitter.com/RewireProject>