Secure OPen source softwarE and hardwaRe Adaptable framework

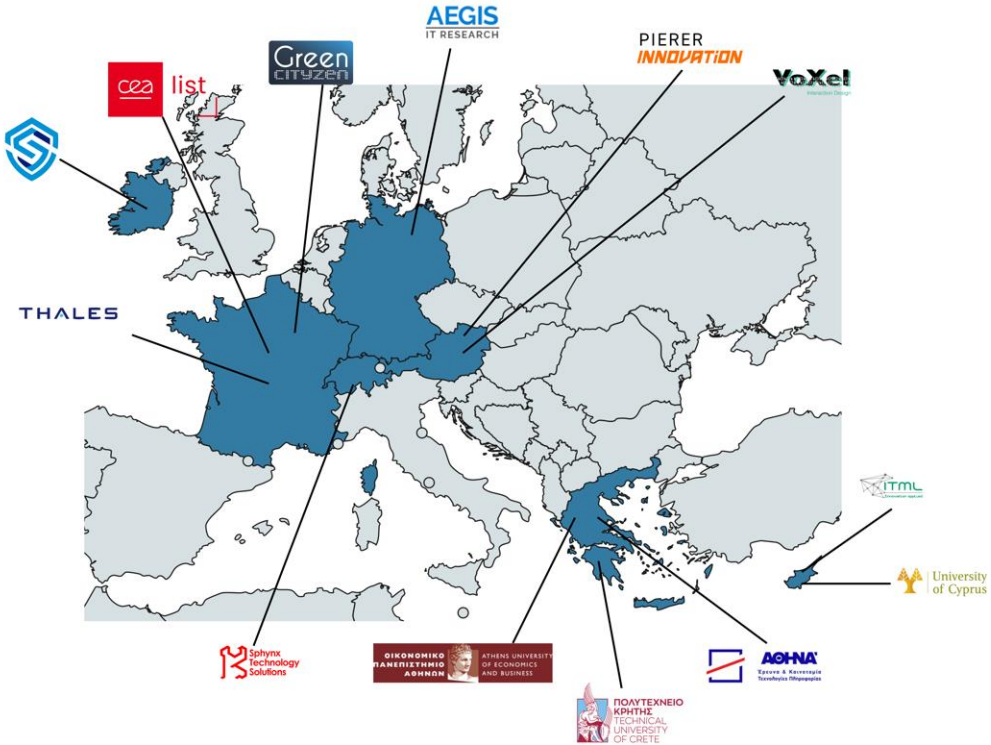
SecOPERA Presentation

CEA List

December 10th, 2025

SecOPERA Consortium

1. POLYTECHNEIO KRITIS (**TUC**)
2. AEGIS IT RESEARCH GMBH (**AEGIS**)
3. ATHINA-EREVNITIKO KENTRO KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS (**ISI**)
4. UNIVERSITY OF CYPRUS (**UCY**)
5. SECURITY LABS CONSULTING LIMITED (**SLC**)
6. ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER (**AUEB**)
7. PIERER INNOVATION GMBH (**PINNO**)
8. THALES SIX GTS FRANCE SAS (**THALES**)
9. COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (**CEA**)
10. IOTAM INTERNET OF THINGS APPLICATIONS AND MULTI LAYER DEVELOPMENT LTD (**ITML**)
11. VOGL SIMON (**VoXel**)
12. GREENCITYZEN (**GREEN**)
13. SPHYNX TECHNOLOGY SOLUTIONS AG (**STS**)



13 Partners from 7 Countries: *Greece, Germany, Cyprus, Ireland, Austria, France, Switzerland*

Project Identity Card

SecOPERA

Secure OPen source softwarE and hardwaRe Adaptable framework

Project Consortium: 13 partners

Project Type:
Research & Innovation Action

Duration: 36 Months

Start Date: 1 January 2023

Total Budget: €4,581,135

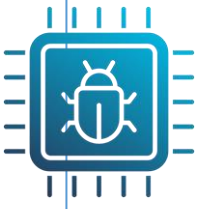
Motivation

Open-source code

Cannot be trusted out of the box and lacks appropriate security guarantees

Diverse code bases

Static analysis tools often fail in the vastly diverse open-source landscape



Non-verified hardware solutions

Similar to OSS open-source hardware lacks security guarantees and can be prone to vulnerabilities or even contain malware (e.g. Hardware Trojans)

Challenges

SecOPERA

1

Open-source solution security

- Hard to justify in the current business interconnected market
- Lacks security guarantees

2

Third-party components need to be assessed in terms of security

3

Open-source cognitive models are already deployed

- Without security assurance
- Without guarantees against possible sensitive information leakage

Our mission

SecOPERA will provide a one-stop hub for complex open-source software and open-source hardware (OSS/OSH) solutions delivering to system designers and operators and OSS/OSH developers and testers the means to analyse, assess, secure/harden, and share open-source solutions.

The SecOPERA hub will offer an open-source framework supporting the DevSecOps lifecycle and generate solutions along with appropriate, verifiable security guarantees.

Objectives

- Provide a complete **security auditing-testing toolbox**
- Research and develop **security hardening** and **enhancement** of open-source solutions
- Deliver **adaptable security** solutions for the open-source community
- Establish the **SecOPERA hub** with a **pool** open-source solutions
- Develop the **SecOPERA framework** with the tools to support the secure development lifecycle
- Validate SecOPERA solution in **two industrial pilots** across several **use cases**
- Provide a **viable**, **open-source** compliant **exploitation**

Work Packages

- **WP1:** Project Management
- **WP2:** Project Dissemination and Outreach Activities
- **WP3:** User and Architecture Requirements
- **WP4:** Design of the SecOPERA Technology/Enablers
- **WP5:** Realization of the SecOPERA services
- **WP6:** Integration, Validation and SecOPERA Outputs

SecOPERA pillars

Decompose: Decomposes open-source solutions in components and classifies them in the SecOPERA layers (device, application, network, cognitive).

Audit/Assess: Performs vulnerability scan on each component and its dependencies and forms a vulnerability graph.

Secure: Consists of several OSS/OSH security modules which aim to harden each component.

Adapt: Adapts security modules in the OS solution

Update/Patch: Formally verifies the final solution and repeats the audit process after each update

SecOPERA functionalities





Decompose

- Open-source solution analysis
- Component dependency graph generation

Audit/Assess

- Known vulnerability analysis based on CVEs/CWEs knowledge bases
- Per layer security auditing and testing
- Penetration testing based vulnerability discovery
- Vulnerability graph generation
- Formal verification of OSS services

Secure

- Design and development of secure pillar modules for mitigating discovered vulnerabilities
- Release a secure module pool for per layer hardening to be used by OSS/OSH community

Adapt

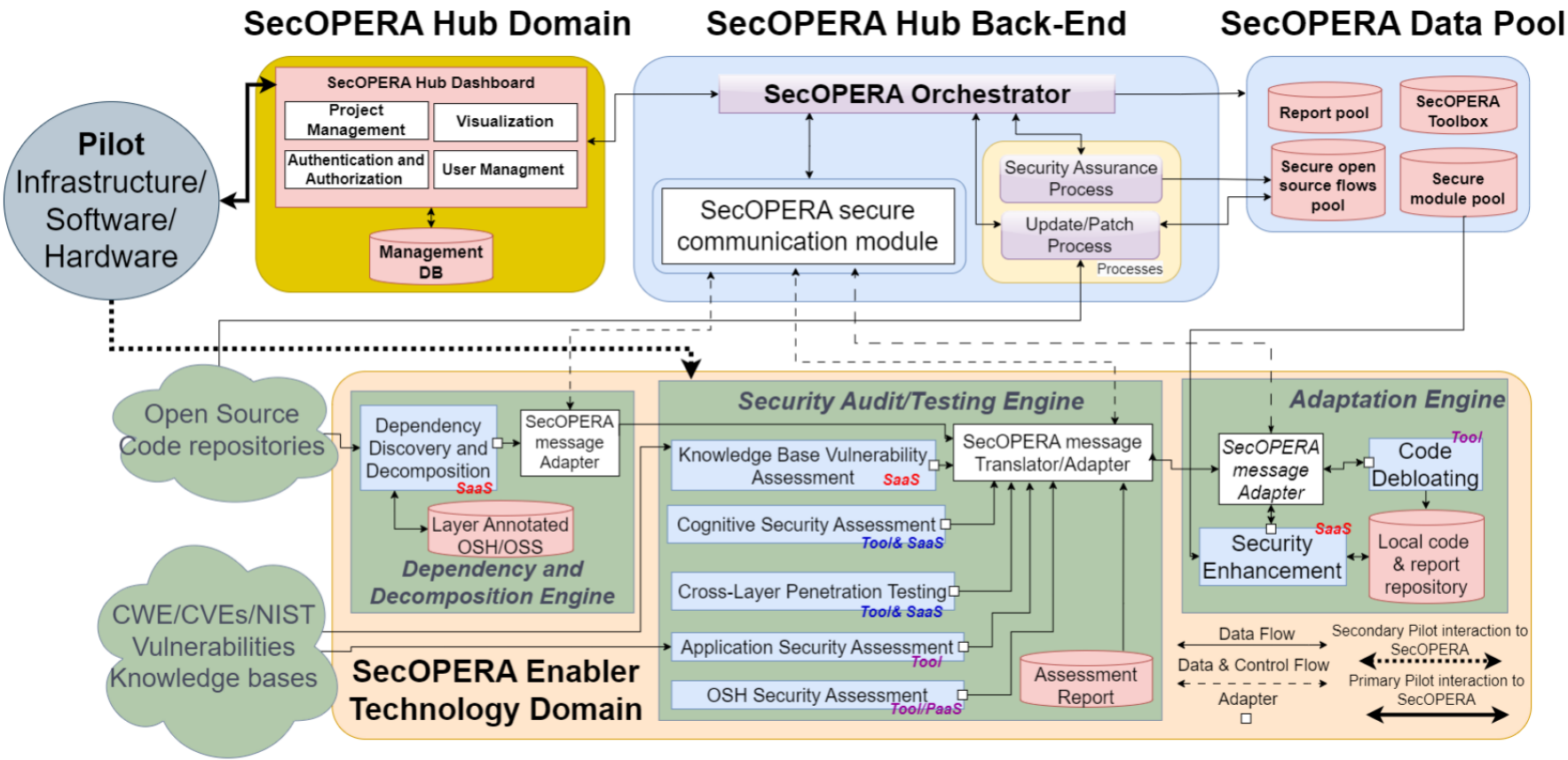
- Code debloating
- Secure module integration for hardening OSS/OSH

Update/Patch

- Monitor OSS/OSH repositories for updates
- Control of Security Audits after each update

Generation of secure flow guarantees for OSS/OSH security assurance

Architecture



Pilot 1
Secure Supply Chain in Automotive Industry

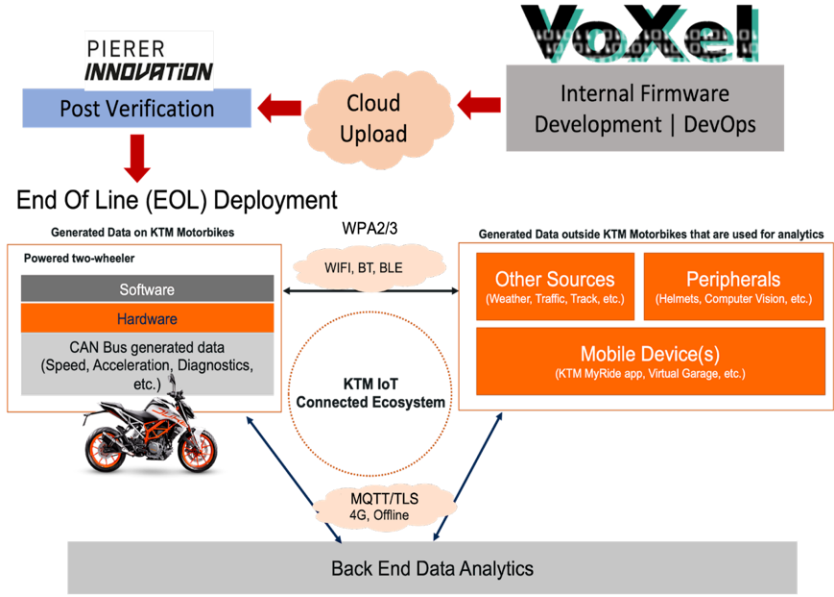
E-bicycle communication unit

Modules:

- Application processor
- RTOS
- Communication processor with LTE
- Various CAN-bus connected sensors

SecOPERA goals:

- Harden each component and the end solution
  - Application debloating
  - Leverage architectural features for security
  - Formally verify the IoT dongle
- Secure communications and data sharing



Pilot 2
Water Management IoT Critical Infrastructure

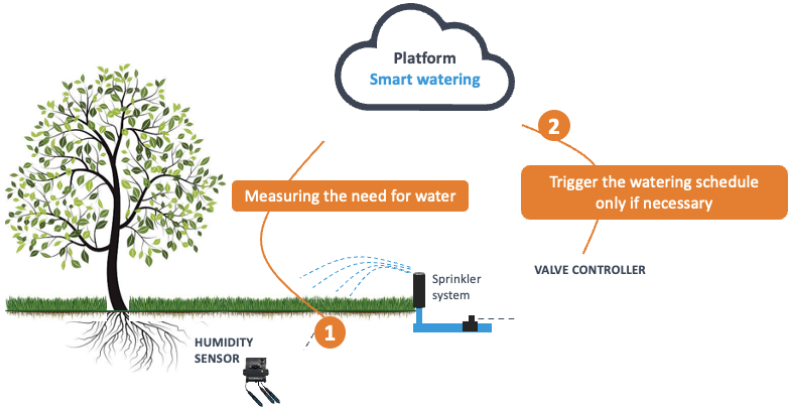
IoT solutions for water infrastructure

Ecosystem:

- IoT solutions for sewer, drinking irrigation
- Open-source
- Applied in smart cities

SecOPERA goals:

- Guarantee secure authentication of ecosystem administrators
  - E.g. Gardeners to start irrigation
- Secure OTA firmware updates
- Secure communication between infrastructure server and IoT devices
- Security hardened IoT components
- Deploy in real-world scenarios



Integrated tools

- IP Core Side Channel Assessment platform
- Static Threat Profile
- Dynamic vulnerability assessment
- Pentest toolkit
- Static C Source Code Analyser
- ML Evasion Assessment toolbox
- Membership Inference Assessment
- Model Inversion Assessment
- Model Extraction Tool

Available Secure Modules

SecOPERA

- PostQuantum CryptoPrimitive HW IP Core Library
- Side Channel Attack Resistance Toolbox Library
- Shadow Stack and Landing Pads- enabled RISC-V soft core
- Trust-based Intrusion Detection and Prevention solution
- Quantum-resistant Network Security Stack
- Dynamically reconfigurable Trusted Execution Environment primitives
- Code Debloating tools (C and Python)
- Membership Inference Hardening
- Model Inversion Hardening
- FastMLH
- ML Evasion Hardening

CEA Contribution

- Dedicated reports from Frama-C/Eva
- New Debloating plug-in
- Integration within SecOPERA eco-system
- Available on SecOPERA's GitHub group

Secopera-report Plug-in

- https://github.com/EU-SecOPERA/Static_analysis_subengine
- Proposes a classification of alarms emitted by Frama-C (mainly Eva) according to CWE nomenclature
- JSON report conforming to SecOPERA's schemas
- Options for describing where the code stands within the SecOPERA platform
- Dockerised version readily usable from the plaform

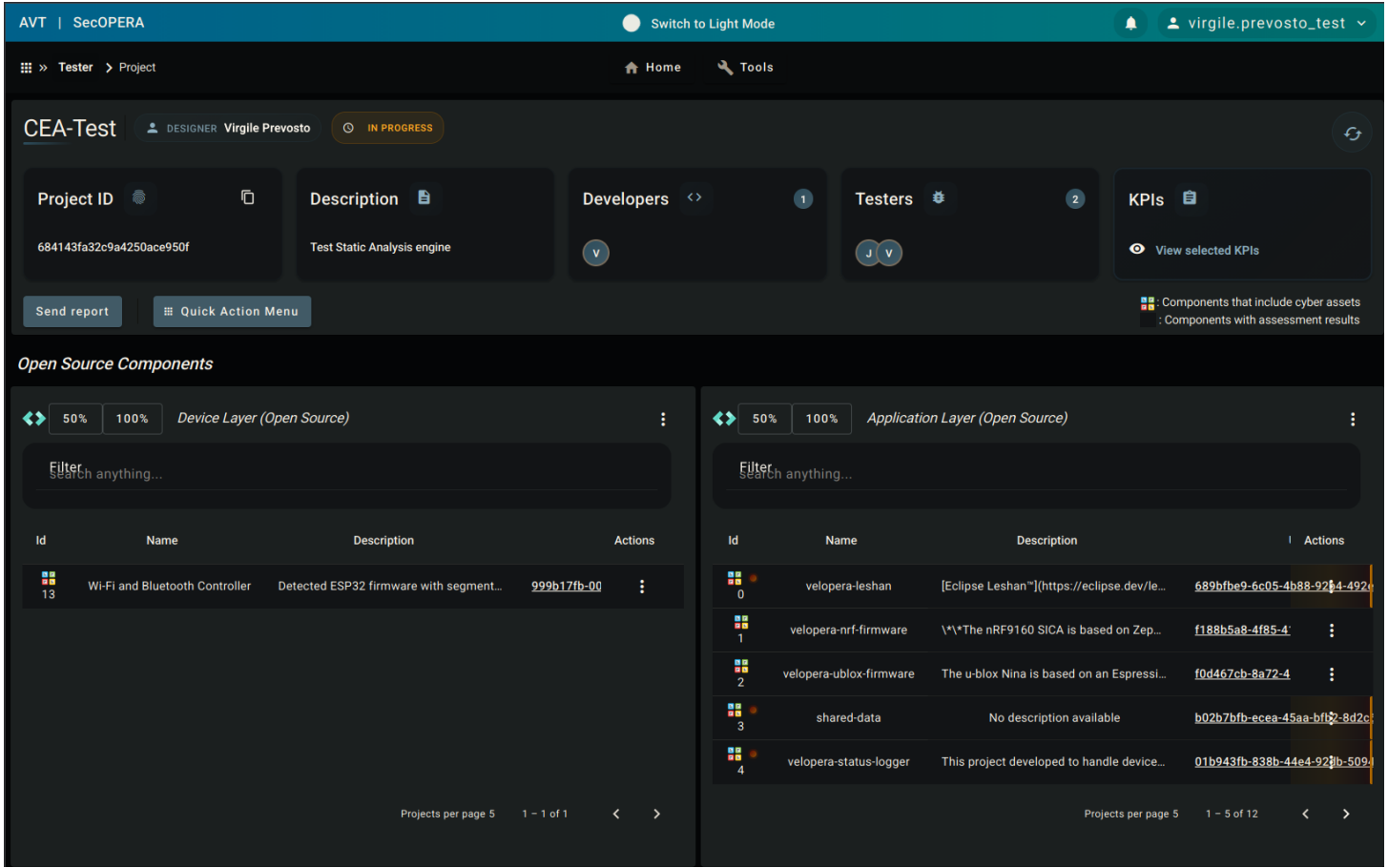
Debloating Plug-in

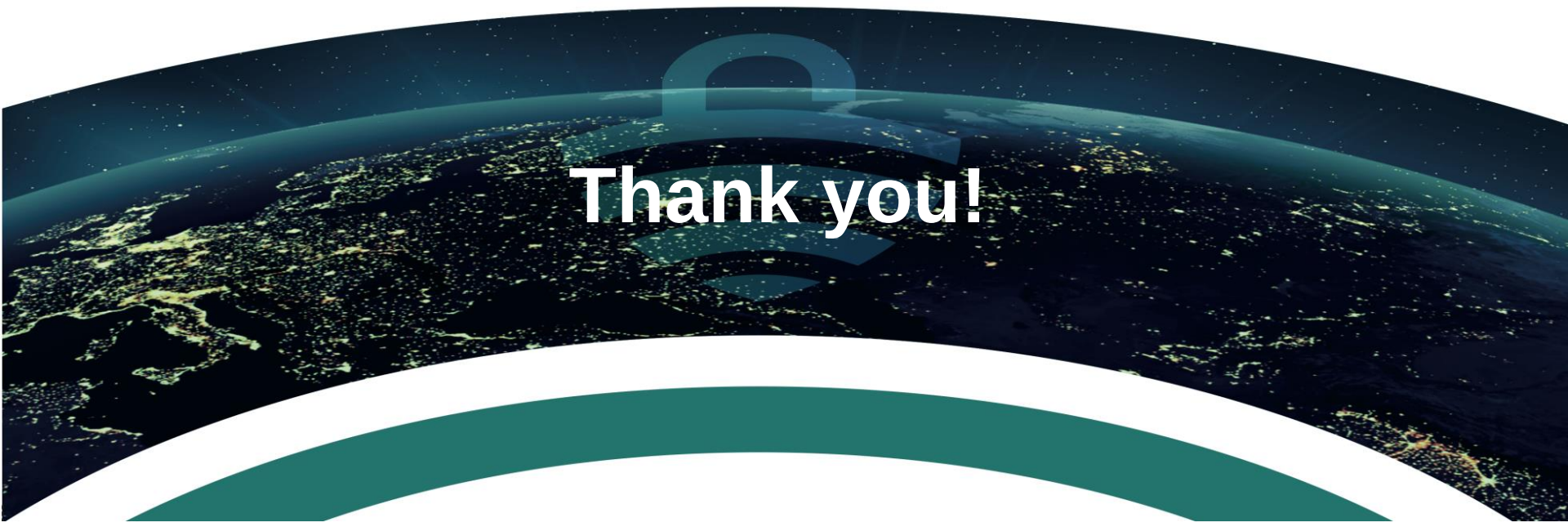
- https://github.com/EU-SecOPERA/Debloating_engine
- Lightweight alternative to SpareCode: removes statements that do not contribute to the final state of the program
- Based on the (new) Alias plug-in
- Still very experimental, testers welcome

Analysis Scripts for SecOPERA

- Part of Static Analysis Sub-engine repo (and documented in README)
- Facilitate setting up a suitable analysis environment for a SecOPERA component:
  - Create Docker image
  - Create Makefile template to drive Eva analysis
  - Create machdep if required
  - Launch main analysis
  - Create report and upload it through SecOPERA's REST API

Demo Time


AVT | SecOPERA
Switch to Light Mode
virgile.prevosto_test
Tester > Project
Home
Tools
CEA-Test
DESIGNER Virgile Prevosto
IN PROGRESS
Project ID
684143fa32c9a4250ace950f
Description
Test Static Analysis engine
Developers
1
Testers
2
KPIs
View selected KPIs
Send report
Quick Action Menu
: Components that include cyber assets
: Components with assessment results
Open Source Components
50%
100%
Device Layer (Open Source)
Filter
Search anything...
Id
Name
Description
Actions
13
Wi-Fi and Bluetooth Controller
Detected ESP32 firmware with segment...
999b17fb-00
Projects per page 5
1 – 1 of 1
50%
100%
Application Layer (Open Source)
Filter
Search anything...
Id
Name
Description
Actions
0
velopera-leshan
[Eclipse Leshan™](https://eclipse.dev/le...
1
velopera-nrf-firmware
**The nRF9160 SICA is based on Zep...
f188b5a8-4f85-4
2
velopera-ublox-firmware
The u-blox Nina is based on an Espressi...
f0d467cb-8a72-4
3
shared-data
No description available
4
velopera-status-logger
This project developed to handle device...
Projects per page 5
1 – 5 of 12



Thank you!

Learn more

https://secopera.eu/

info@secopera.eu

Follow us

company/SecOPERA

@SecoperaP

SecOPERA Project

zenodo /communities/secopera

This project has received funding from the European Union's Horizon Europe Research and Innovation program under grant agreement No 101070599.