



Efficient, portable And Secure orchesTration for reliable servICes

ELASTIC Project Results 1st Reporting Period

M1 [March 2024] - M18 [August 2025]



Co-funded by
the European Union





Efficient, portable And Secure orchesTration for reliable servICes

Project Overview

Project Identity Card



Project Consortium: 13 partners



Project Type:
Research & Innovation Action



Duration: 36 Months



Start Date: 1 March 2024



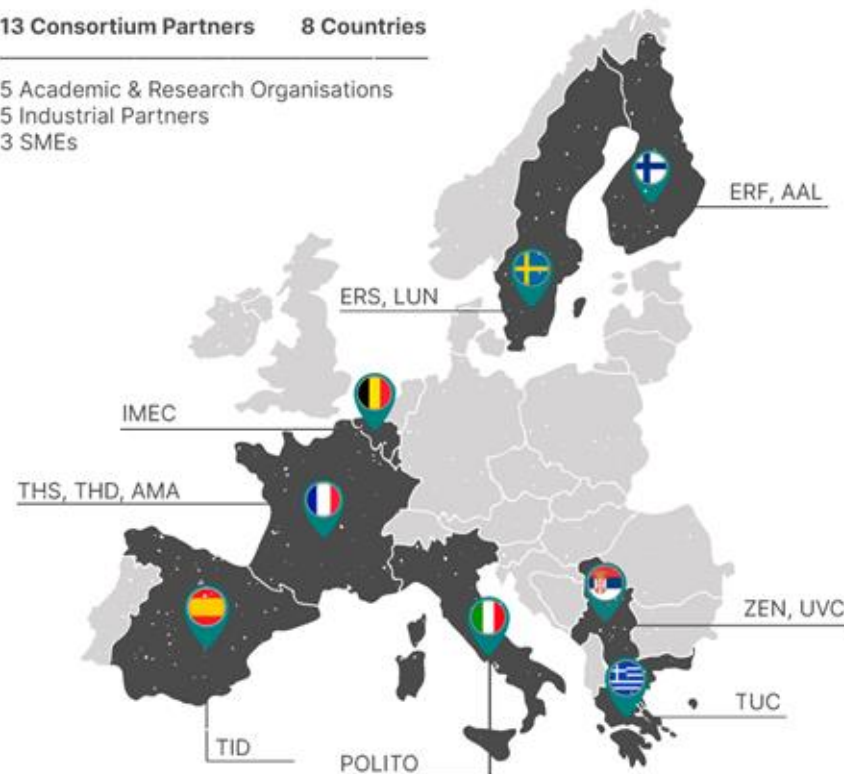
Total Budget: €3,999,990

ELASTIC Consortium

1. POLYTECHNEIO KRITIS (**TUC**)
2. ERICSSON AB (**ERS**)
3. OY L M ERICSSON AB (**ERF**)
4. TELEFONICA INVESTIGACION Y DESARROLLO SA (**TID**)
5. THALES SIX GTS FRANCE SAS (**THS**)
6. THALES DIS FRANCE SAS (**THD**)
7. INTERUNIVERSITAIR MICRO-ELECTRONICA CENTRUM (**IMEC**)
8. ULTRAVIOLET CONSULT DOO (**UVC**)
9. AALTO KORKEAKOULUSAATIO SR (**AAL**)
10. LUNDS UNIVERSITET (**LUN**)
11. ABSTRACT MACHINES SAS (**AMA**)
12. PRIVREDNO DRUSTVO ZENTRIX LAB DRUSTVO SA OGRAN (**ZEN**)
13. POLITECNICO DI TORINO (**POLITO**)

13 Consortium Partners 8 Countries

5 Academic & Research Organisations
5 Industrial Partners
3 SMEs



Motivation



6G communication networks

Important to **ensure efficient and effective orchestration** of its broad range of services and resources



Edge cloud computing

Increasingly important as the data volumes rise with the number of the connected devices



Security in 6G

Critical issue in 6G services due to privacy and confidentiality of sensitive data

Challenges

1

Security of lightweight and portable executable isolation

- Secure portable and lightweight workloads
- Improve orchestration monitoring latencies

3

Privacy-preserving multi-party confidential computing

- HW CPU extensions for creating secure enclaves

2

Efficient and secure serverless orchestration over a heterogeneous continuum

- Fast and secure orchestration services

4

Portable and secure workload distribution and execution over constrained far-edge IoT devices

- Efficient process orchestration and execution over 6G networks

Our mission

ELASTIC aims to enhance the **efficiency and security of service orchestration** within the highly distributed and heterogeneous context of **cloud-fog-edge continuum** technologies.

ELASTIC focuses on **combining** impactful **key technologies** from modern **cloud-native ecosystems** to enhance **service orchestration** and **security** over **6G networks**.

Objectives



Analyse **executable isolation techniques**, and **improve efficiency, portability, and security** for secure **in-network cloud and edge** computing across the entire lifecycle



Implement a **secure, privacy-preserving, architecture-agnostic execution environment** utilising confidential computing and privacy-enhancing technologies to ensure secure services on a programmable platform for multi-stakeholders



Facilitate **6G standardisation, exploitation, and dissemination** of developed technologies, aligning with **EU supply capabilities** for efficient, secure, and privacy-preserving service deployment

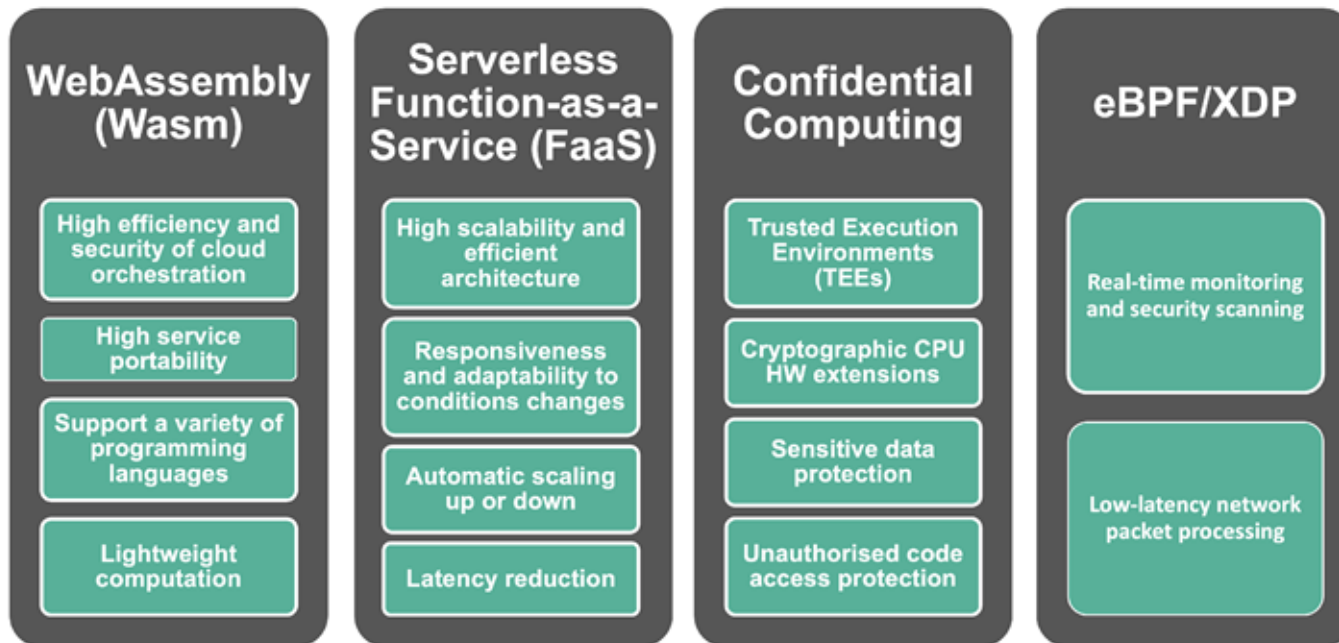


Research and design **secure, architecture-agnostic serverless FaaS orchestration** for diverse artifacts and workloads. Ensure **data authenticity** and **trusted digital interactions** in dynamic service environments



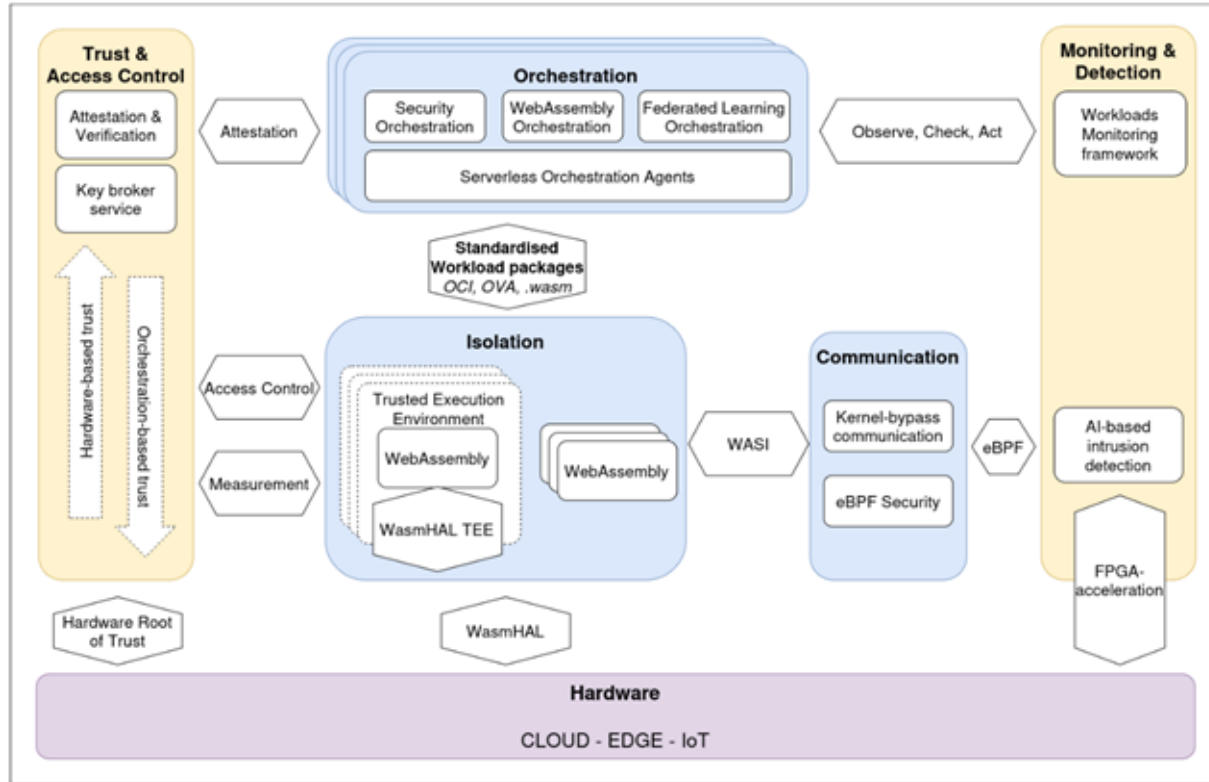
Design and implement **efficient, secure edge and far-edge (IoT) workload orchestration** for critical **6G infrastructure**, ensuring **reliability, trust, and resilience** in a globally connected continuum of heterogeneous environments facilitated by network and IT system convergence for future digital services

Key Technologies & Innovations



Framework that combines all the above tools across cluster-based

ELASTIC Architecture



Innovations

- ✓ Orchestration mechanisms for deploying **Wasm workloads across Cloud-Edge**
- ✓ Running **Kubernetes operators in Wasm** for portability
- ✓ **Secure resource migration protocol** for distributed workloads
- ✓ **Light-weight Security Orchestrator** for zero-trust edge
- ✓ **Secure Federated Learning orchestration** (Wasm + Confidential Computing)

Propeller Orchestrator

Wasm-operator

Light-weight Security orchestrator for Edge devices

Confidential AI Orchestration

TEE Software Management Agent

Reliable Enclave Migration Protocols

Federated AI Orchestration

Impact

- ✓ Bridges **high-performance cloud** with **resource-constrained edge**
- ✓ **Improves scalability & performance**, especially at the edge
- ✓ Ensures **reliable & secure** operation of distributed systems
- ✓ **Continuous compliance and cyber resilience** at edge devices
- ✓ Enables **scalable AI deployment** in IoT networks

Innovations

- ✓ **Flexible cross-platform CC layer**
(WasmHAL-Trust)

- ✓ **Secure HW interaction via IoT protocols** (USB, I2C, GPIO) – WasmHAL Hardware

- ✓ **Standardized security policies for Wasm** (WASI Security)

- ✓ **TEE-based data protection at rest** on the edge

Data protection at-rest at the edge with TEE solution

WasmHAL-Trust

WASI Security

Automatic MAC profiles for Wasm runtime containers

WasmHAL Hardware

Static eBPF code security Analyzer

Impact

- ✓ Enables **portable & secure workload execution** with CC

- ✓ **Secure interface with HW** in edge environments

- ✓ **Improved Security Management**

- ✓ **Robust data protection** stored & processed at the edge

Innovations

- ✓ **Accelerated microservice interconnection** using eBPF & RDMA
- ✓ **High-speed data exchange** with shared memory
- ✓ **Optimized distributed state sharing** for cluster consensus

Static analysis of interaction between Wasm modules

Accelerated microservices interconnection

eBPF distributed state synchronization

Hardware-based cryptography module

Impact

- ✓ **Fast & scalable FaaS orchestration**
- ✓ **Low-latency, reliable synchronization** across distributed components
- ✓ **Improved data consistency & operational continuity**

Innovations

- ✓ **Remote Attestation Platform** for trust verification across distributed environments
- ✓ **Cross-Platform Attestation:** unified attestation for heterogeneous systems using the Wasm component model
- ✓ **Standardized Lightweight Access Control:** fine-grained authorization for Wasm containers at the edge

Remote
Attestation
Platforms

Key Broker
Service

Multi-
platform
attestation
component

Lightweight
ABAC solution

WASI
flexibly-
defined
capabilities

Impact

- ✓ **Confidential workload assurance** across cloud-edge environments
- ✓ **Resilient edge security** with trusted execution & controlled access

Innovations

- ✓ **Real-time network stack analysis** using eBPF for low-overhead trace capture

- ✓ **AI-driven intrusion detection** with hardware acceleration model

- ✓ **eBPF-based observability for Wasm workloads** in Kubernetes environments

NETTO

AI Intrusion
Detection
System

Mobility
attack robust
IoT resource
allocation
model

Observability
framework for
serverless
workloads

Impact

- ✓ **Low-overhead continuous network monitoring**

- ✓ **Scalable & intelligent threat protection**

- ✓ **Enhanced observability for edge workloads** with near real-time visibility & control



Efficient, portable And Secure orchesTration for reliable servICes

WP1: Efficient, Portable and Secure Executable Isolation

Leader: AAL

Contributors: ERF, ERS, IMEC, LUN, POLITO, THD, THS, TUC, UVC, ZEN

Objective 1: **Analyse the landscape of executable isolation** techniques and **enhance efficiency, portability, and security**, with a focus on host-neutral infrastructure for secure in-network cloud and edge computing across the entire lifecycle from development, deployment, operation, and decommissioning.

01.1

To research and determine the **current landscape** of novel Wasm and eBPF networking, development, and deployment technologies for modern cloud-edge continuum.

01.2

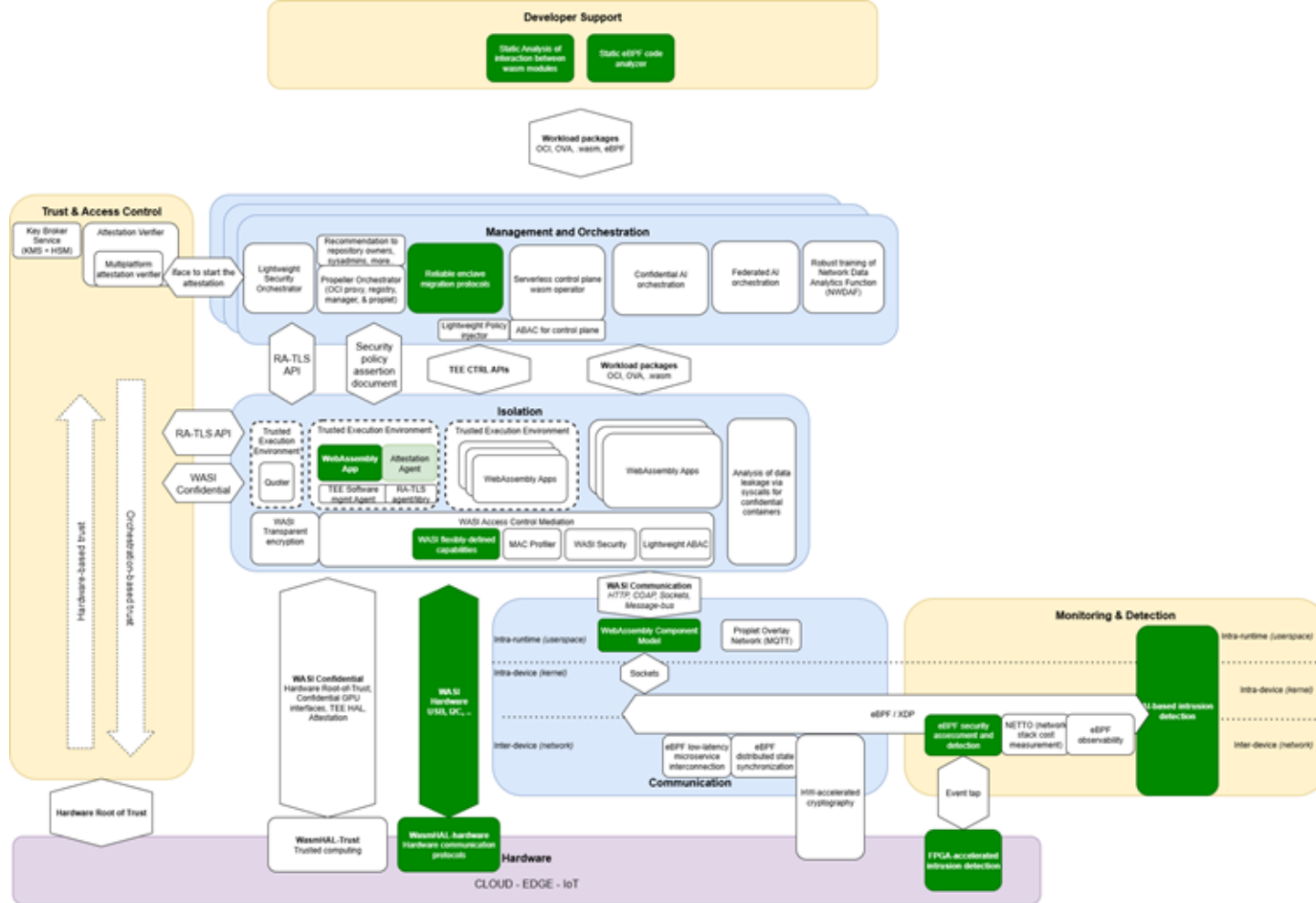
To research **security aspects of Wasm isolation**, and usage of it as a lightweight replacement for containers and VMs in **orchestration** strategies

01.3

To research the **security of eBPF** and its **usage in low-latency** real-time applications with XDP.

01.4

To examine the capabilities of Wasm and eBPF technologies to be **extended, with component-based architecture**, and support of these components for networking and orchestration, as well as the **support of modern languages** to produce this kind of components.



Task 1.1

Wasm & eBPF landscape

Wasm Landscape Report

D1.1: Wasm and eBPF Landscape

- **Motivating** our technology focus based on our “6G data fabric” vision
- **State of the Art** in WebAssembly, eBPF and their security
- **Open challenges** and research questions to be addressed in WP1
- **Wasm Runtime performance** comparison
- **eBPF CVE** analysis using National Vulnerability Database (NVD)

D1.1



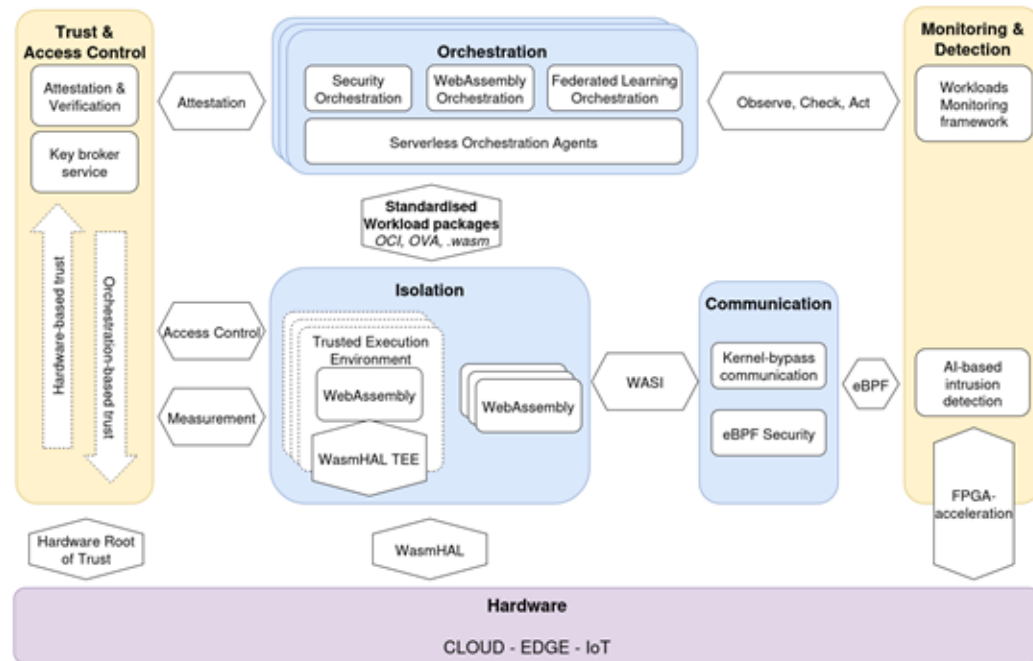
ELASTIC Architecture

Three architectural diagrams

- Conceptual overview
- Simplified overview
- TEE HAL layered architecture

Component descriptions

- For 28 ELASTIC components
- Mapping to demonstrators
- Interfaces and interactions



D1.1

Task 1.2

Security of Wasm isolation

Stack Smashing Protection for Wasm

D1.1

D1.2

Key innovation!

elastic

Previous studies have highlighted the importance of Stack Smashing Protection (SSP) for protecting Wasm binaries against memory corruption.

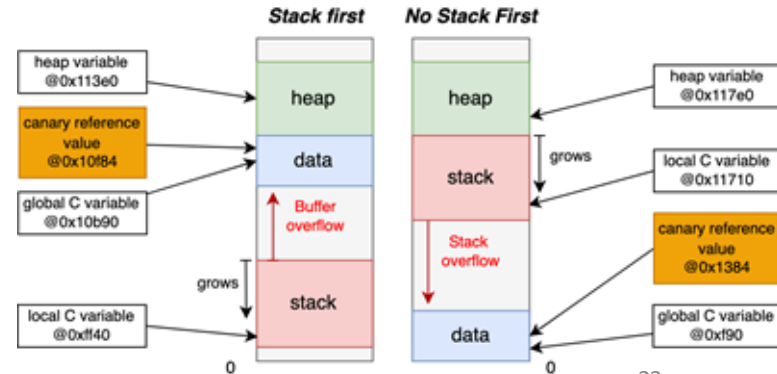
- SSP is a mechanism able to detect a buffer overflow in memory
- In case of detection, the program is immediately killed to prevent exploitation

A systematic evaluation of the existing SSP implementation for Wasm was conducted

- SSP implementation for native binaries is vulnerable in Wasm because of the platform difference
- Two vulnerabilities were uncovered in the existing implementation

ELASTIC's hardened implementation of SSP

- Findings were published in a peer-reviewed conference
- An hardened implementation made open source
- Discussion with the WASI WG community to upstream it



Wasm isolation & side channels



Side channels are a major threat to Trusted Execution Environments (TEEs)

- Bypass most software- and hardware-enforced access control
- Difficult to comprehensively eliminate: new attacks every year

Previous study showed Wasm increased susceptibility to side channel attacks

- Code extracted from Wasm runtime in Intel SGX enclave

Ongoing work to assess vulnerability of VM-based TEE (AMD's SEV-SNP)

- More challenging attack: SEV-SNP gives less control to attacker than SGX
- Initial results: instruction-by-instruction latency measurement

Reliable enclave migration protocols

D1.1

D1.2

Key innovation!

elastic

Allow parties *S* and *D* to transfer responsibility for "something" between systems

- Workloads, keys, abstract responsibility
- If *S* stops executing a workload, then *D* will eventually start
- If *D* starts executing a workload, then *S* will definitely stop

Use fair-exchange protocols to exchange non-repudiable migration certificates

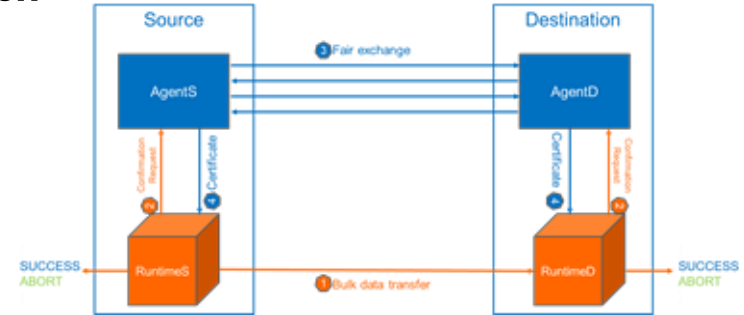
- *S* gets proof that they are no longer responsible for a task
- *D* gets proof that they are authorised to take over from *S*

No orchestrator assistance needed in normal-case operation

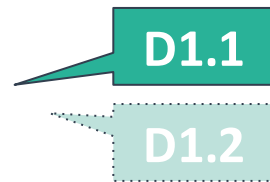
- Provides abort certificates in the event of failure

Developed agent implementing migration protocol

- To be integrated with Propeller in Demonstrator 2



WASI flexibly-defined capabilities



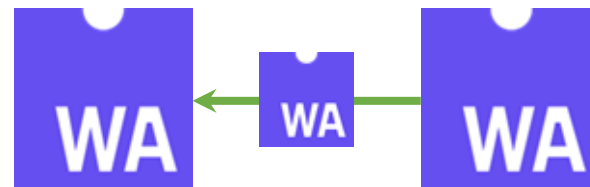
Wasm components' well-defined internal interfaces allow easy insertion of shims

- Components linked together using the WAC composition language
- Defines which components are instantiated and how they are linked together

New tool **wacky** modifies inserts shims into WAC compositions

Shims can provide any functionality that can be implemented in Wasm

- Access control
- Transformations (see this demo)
- Data capture (see Demonstrator 2 MVP)



Task 1.3

Security of eBPF In-kernel Plugins
and Low-latency with eBPF/XDP

Accurate Investigation of the Security of eBPF

Several investigations aimed at identifying risks and attack surfaces:

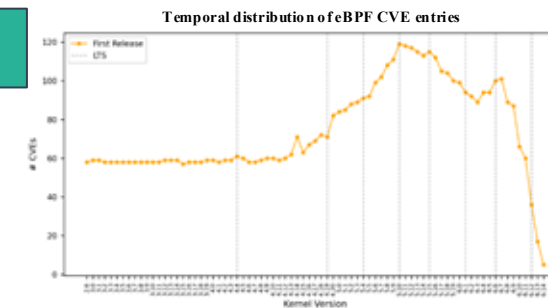
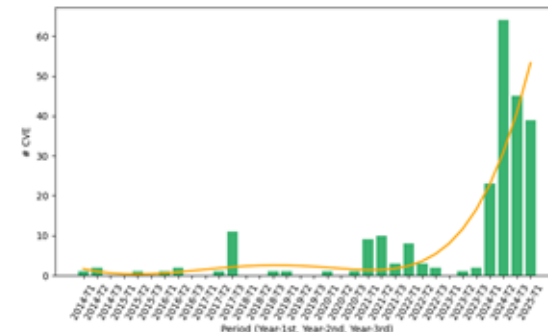
- Systematic scientific literature review (45 relevant papers identified and analysed)
- Analysis of the eBPF-related CVEs and rootkits (249 CVEs and 4 rootkits identified and analysed)

=> The main attack surfaces and security risks implied by running eBPF plugins have been identified

The analysis will be completed in RP2 with additional in-progress experiments aiming at studying the impact of exploits and the effectiveness of protections

D1.1

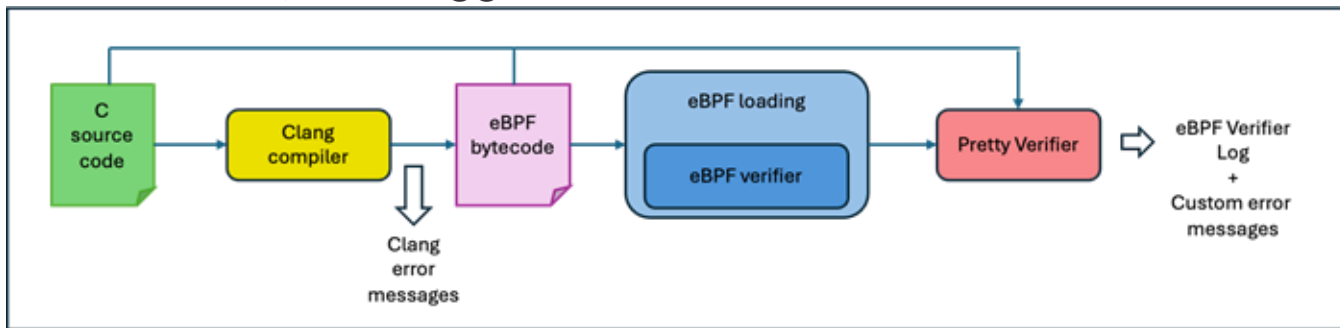
D1.2



Static eBPF Code Security Analyser

Static eBPF C code security analyser

- generates precise and easy-to-understand messages to explain the meaning of the verifier errors, and suggestions to fix them



Paper at
IEEE CSR

- Tests are in progress to measure the error coverage

D1.1

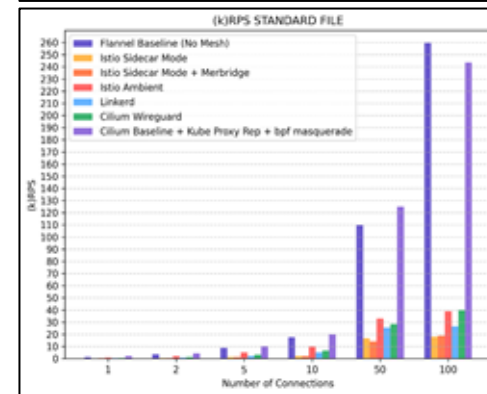
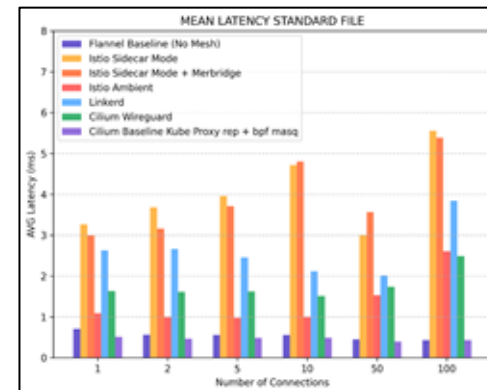
D1.2

Service Mesh Performance Assessment

Tested the performance of Service Mesh deployments, and compared solutions based on their internal technology.

Results show that eBPF-based architectures do not seem to meaningfully improve throughput or latency compared to traditional meshes.

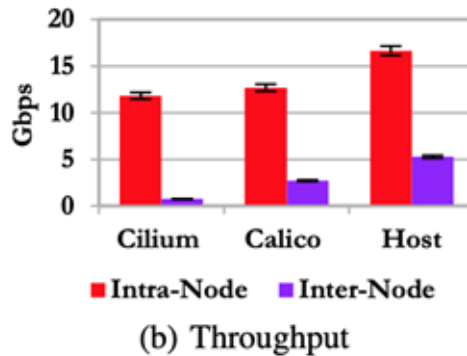
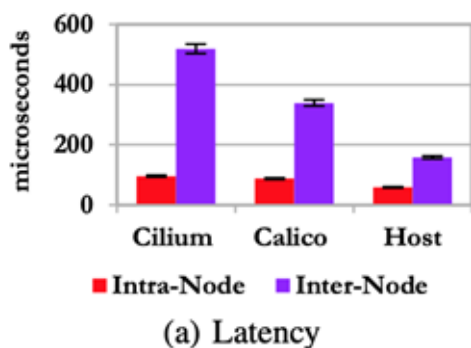
D1.1



Performance Evaluation of eBPF/XDP Deployment Scenarios

Literature review to analyse the performance of different eBPF/XDP deployment scenarios, (e.g. containerised vs bare-metal)

- Deployment performance overheads are becoming no longer negligible, but comparable to the performance gains



D1.1

eBPF-based traffic capture

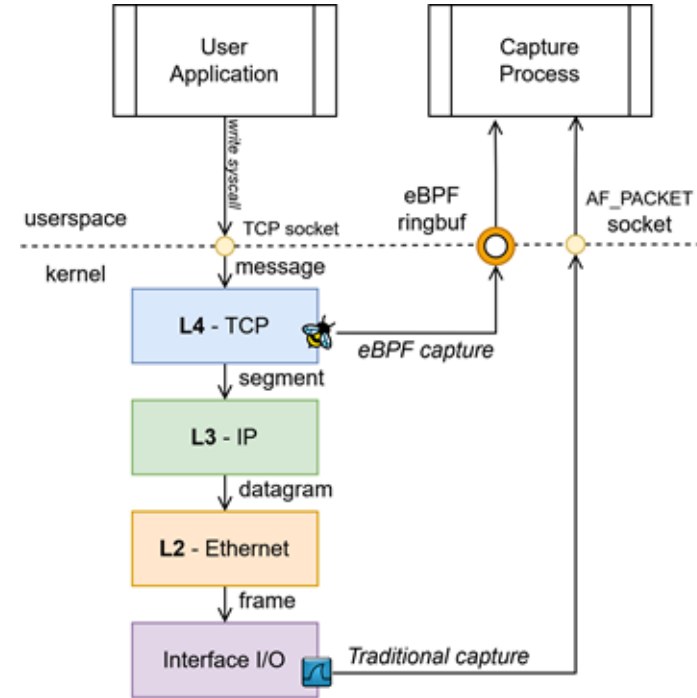
D1.1

D1.2

Traditional packet capture operates at the MAC layer. It is thus not suitable for scenarios that incorporate most Service Mesh deployments, because the mesh redirection function takes place at L4.

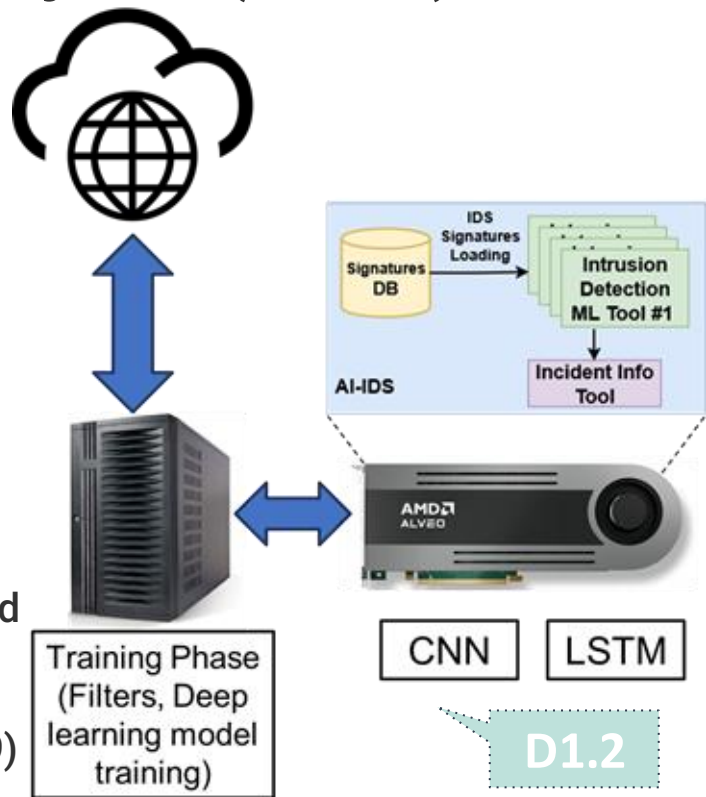
New traffic capture library that uses eBPF probes to anticipate the traffic capture to L4, bypassing this problem.

elastic



Hardware-based AI-Intrusion Detection System (AI-IDS) elastic

- AI-based Framework
 - Statistical filtering: Median, Standard Deviation
 - Deep learning: CNN, LSTM
- Key Characteristics
 - **High detection accuracy**
 - **High performance complexity**
- Tools
 - AI-IDS
 - Xilinx Alveo U200 FPGA
 - High performance system
 - Fully integration into ELASTIC framework and Demos
 - AI-IDS (TUC) and eBPF-based tool (PoLiTo)
 - 6G networks security vulnerabilities (EO-KPI-9)

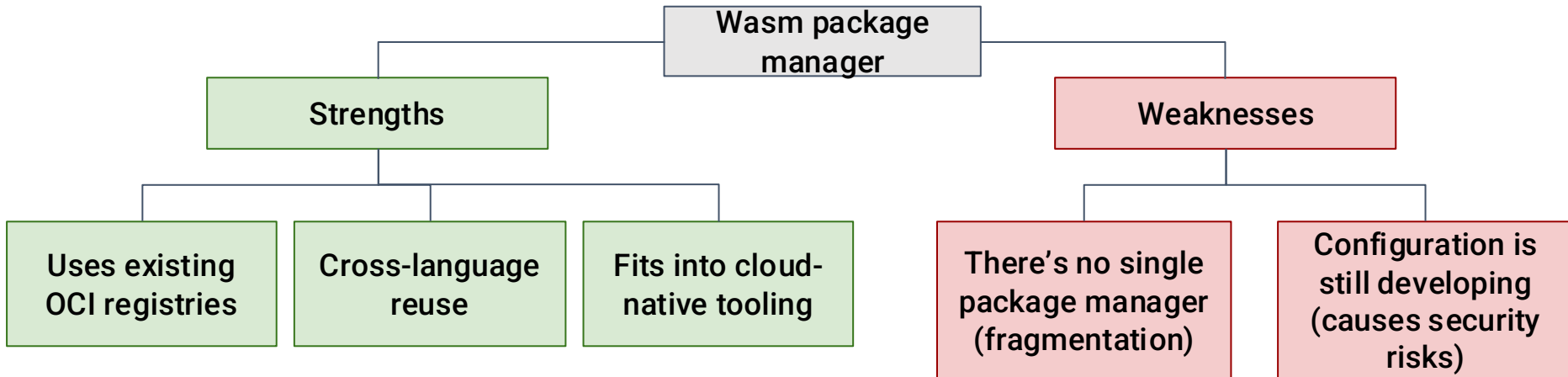


Task 1.4

eBPF and Wasm/WASI Language
Support and Extensibility via
Component Architecture

Strengths and weaknesses of Wasm package management

Literature reviewed on WebAssembly package managers with wadm, npm, wkg, browser add-ons. The study is focused on the benefits and drawbacks.



WASI support for constrained IoT devices

Development of W3C WebAssembly System Interface (WASI) SPI standard

- Allows Wasm applications to communicate with sensors over SPI.
- First iteration of API available
 - <https://github.com/idlab-discover/masters-jarno-vanruymbeke/blob/main/SPI/wit/spi.wit>
- Created (template) standards proposal repo
 - <https://github.com/WebAssembly/wasi-spi/>

Next steps

- Prototype runtime implementation
- Complete standards proposal
- Move standard to Phase 2

D1.4

Deployment-independent measurement

D1.3

D1.2

elastic

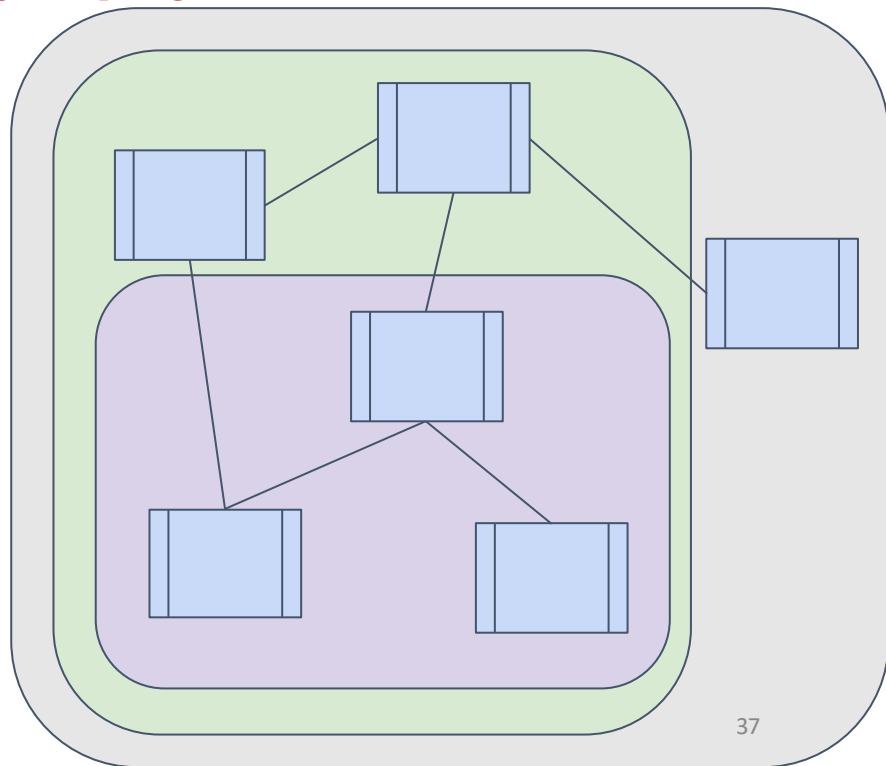
Wasm component structure can vary by deployment

- Compute node scheduling
- Static vs dynamic linking

Inconsistent component hashes

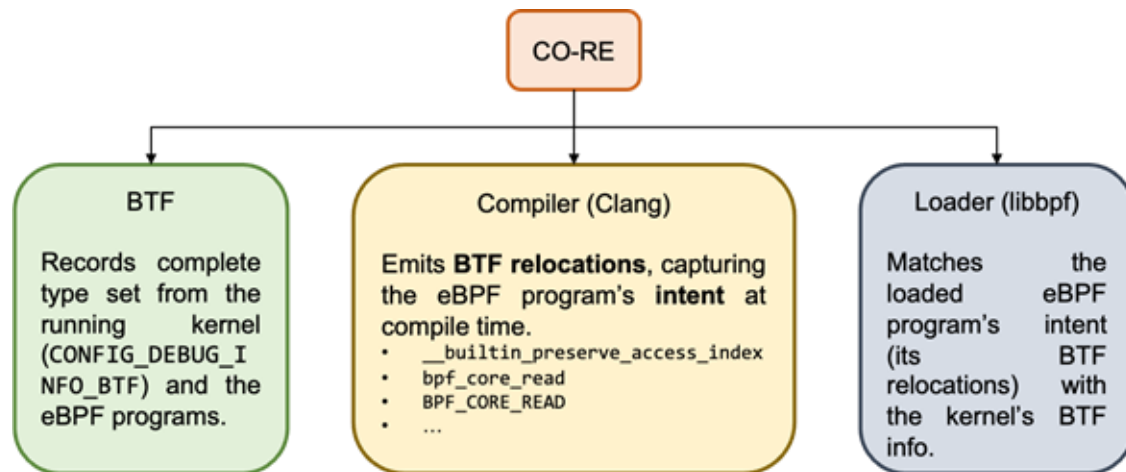
Observation: code+links are **invariant**

- Compare graph with reference component graph
- Can compare **partial graphs**
e.g. for attestation of libraries



Analysis of BTF and eBPF CO-RE technologies

Review of literature and available open-source documentation on the topic, and compiled a preliminary analysis.



Both features are meant to allow developers to build portable eBPF programs, that would run correctly across heterogeneous kernel versions and configurations.

BTF is the format of the kernel's debug information, which is used to match the eBPF *intent* with the running kernel.

D1.3

WP1 Publications & Community Contributions

- Q Michaud, Y. Piperau, O. Levillain, D. Ayed, Robust Stack Smashing Protection for WebAssembly **IEEE FNWF 2024**
- Q Michaud, Y. Piperau, O. Levillain, D. Ayed, Stack Smashing Protection in WebAssembly Applications **PLAS 2024**
 - *Published patches for LLVM compiler infrastructure and associated projects*
- R Rizza, R Sisto, F Valenza, Design and implementation of a tool to improve error reporting for eBPF code **IEEE CSR 2025**
- G Shenavar, Attestation of Distributed Applications, **Masters thesis**
- J van Ruymbeke, WASI-SPI, proposed interface, now in Phase 1.

Next Steps



Selected future work

Immediate future: analyses and memory safety research for D1.2

Continued development

- Expansion of *wacky* tool to broader component model (goal: WASI)
- WASI-SPI implementation
- Incorporate migration protocols into other components

Modular applications in Wasm and eBPF

Joint whitepaper with T6.3 on Wasm/eBPF standardisation

- Recommendations based on gaps in existing standards



Efficient, portable And Secure orchesTration for reliable servICes

WP2: Serverless FaaS Orchestration with Architecture-agnostic In-network Execution

Leader: IMEC

Contributors: AMA, ERF, POLITO, THS, TID, TUC



WP2 Objectives

Objective 2: Research and design secure **serverless FaaS orchestration** with architecture-agnostic in-network execution, suitable for a broader range of deployable artifacts and workloads with new characteristics, while ensuring data authenticity and **trusted digital interactions** in dynamically composed service environments with abstraction mechanisms for the network compute fabric to support function delegation in the **time-sensitive** and **low power** scenarios.

02.1

To implement **lightweight and robust orchestrating mechanisms**, specifically examining and improving supervision and scheduling schemes, focusing on serverless FaaS.

02.2

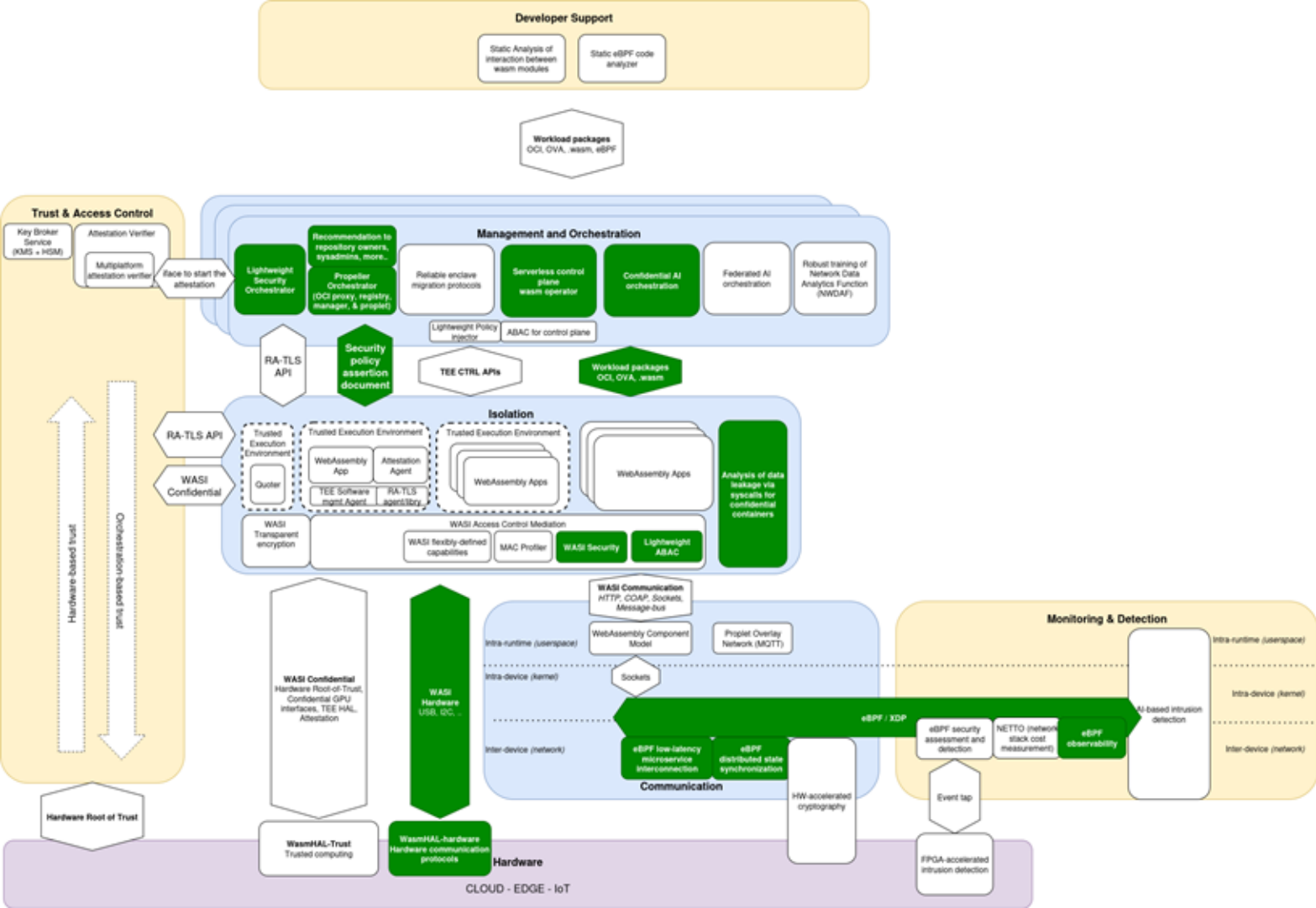
To inspect the capability, portability, and usability of the serverless execution of lightweight **Wasm-based containers** in the **FaaS** context.

02.3

To achieve and improve **low-latency** serverless FaaS orchestration mesh and **monitoring** procedures by leveraging eBPF and XDP technologies.

02.4

To increase the security of lightweight serverless FaaS orchestrating mechanisms by applying robust **access control** and **capability schemes**.



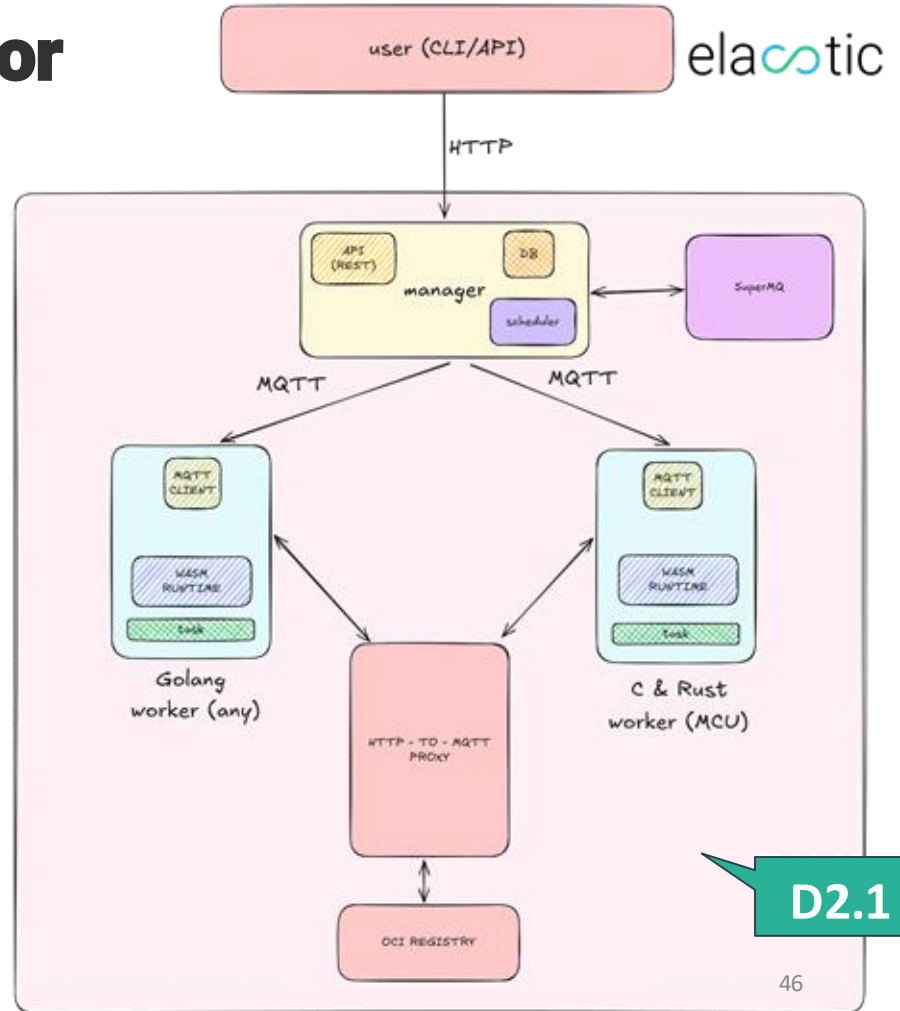
Task 2.1

Lightweight and Robust
Orchestrating Supervision and
Scheduling Mechanisms

Result: Propeller orchestrator

Unified and adaptable orchestration framework for managing and deploying Wasm workloads.

- Unified across **Cloud, Edge and IoT**
 - MQTT for communication
 - C & Rust workers for Microcontrollers
 - RTOS Support with WAMR
- **Compatibility with existing ecosystem**
 - OCI container & registry support
 - HTTP-over-MQTT
 - WAMR Support



Result: CoCoS Confidential AI platform

CoCoS AI: Open-Source Framework for Confidential ML

- **Collaborative AI on private data**
 - For mutually-untrusted parties
 - Combining data in a confidential environment
- **Key Components**
 - **Confidential Virtual Machine (CVM) Manager**
 - **In-Enclave Agent** for secure execution
 - **Command Line Interface (CLI)** for secure enclave communication
- **Ensuring Confidentiality & Integrity**
 - ML models run within TEEs
 - **Remote attestation** safeguards data integrity
 - High security guarantees with Rust and WebAssembly

-> Forms basis for WP3 TEE Agent

D2.1

Result: Cyber-Physical WASI interfaces

W3C standards + open source implementations & SDK support

- I2C WASI proposal: Phase 2
 - Proposal: <https://github.com/WebAssembly/wasi-i2c>
 - Implementation: <https://github.com/idlab-discover/i2c-wasm-components>
 - Collaboration with Siemens
- USB WASI proposal: Phase 1
 - Proposal: <https://github.com/WebAssembly/wasi-usb>
 - Implementation:
 - <https://github.com/idlab-discover/usb-wasm>
- GPIO WASI proposal: Phase 1
 - Proposal: <https://github.com/idlab-discover/masters-jarno-vanruymbeke/blob/main/GPIO/gpio.wit>
 - Implementation: <https://github.com/idlab-discover/masters-jarno-vanruymbeke/tree/main/GPIO/impl>
 - (Currently processing feedback from Embedded-SIG and broader WASI community)
- SPI WASI proposal: Phase 1
 - Proposal: <https://github.com/WebAssembly/wasi-spi>



D2.1



D4.1

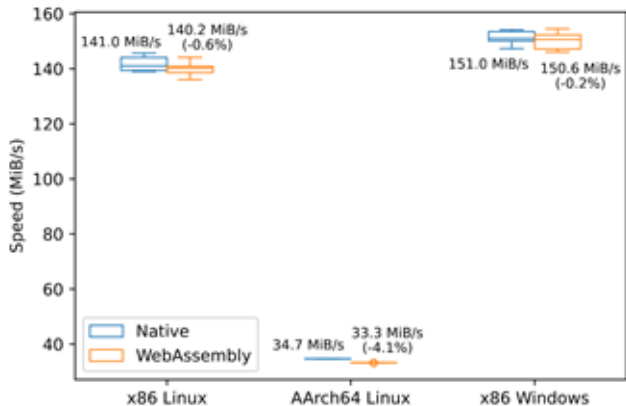


D1.3

Result: Cyber-Physical WASI interfaces

Xbox controller driver in wasm demo

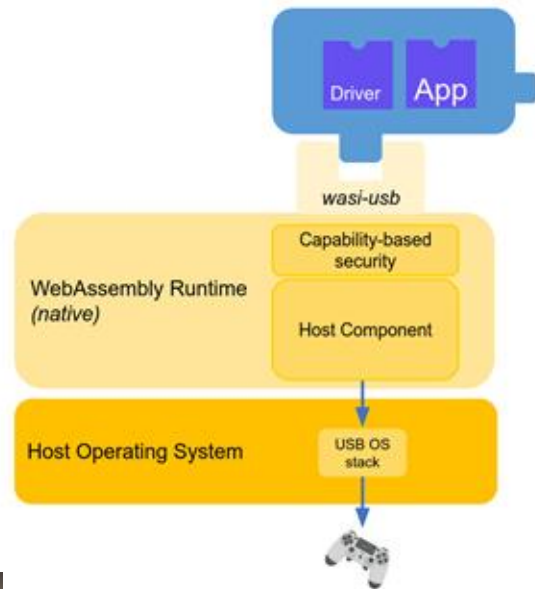
USB round-trip time latency



Cyber-physical WebAssembly: Secure Hardware Interfaces and Pluggable Drivers

Van Kerkhove, Mihail*, Sander, Blažević*, Vandenberghen, Ploessche*, Duzatli, Wane*, Hensen, Wouter*, Vajda, Amir*, Sabharwal, Manoj*, Goshal, Tanu*, De Tonic, Filip*, Veldhans, Bruno*

The rapid expansion of Internet of Things (IoT), edge, and embedded devices in the past decade has introduced numerous challenges in terms of security and configuration management. Simultaneously, advances in cloud-native development practices have greatly enhanced the development experience and facilitated quicker updates, thereby enhancing application security. However, applying these advances to IoT, edge, and embedded devices remains a complex task, primarily due to the heterogeneous environments and the need to support devices with extended lifespans. WebAssembly and the WebAssembly System Interface (WASI) has emerged as a promising technology to bridge this gap. As WebAssembly becomes more popular on IoT, edge, and embedded devices, there is a growing demand for hardware interface support in WebAssembly programs. This work presents WASI proposals and proof-of-concept implementations to enable hardware interaction with I/O and USB, which are two commonly used protocols in IoT, directly from WebAssembly applications. This is achieved by running the device drivers written WebAssembly as well. A thorough evaluation of the proof-of-concept shows that WASI USB introduces a minimal overhead of at most 4%, compared to native operating system USB APIs. However, the results show that further optimization overhead can be significant in low-latency applications.

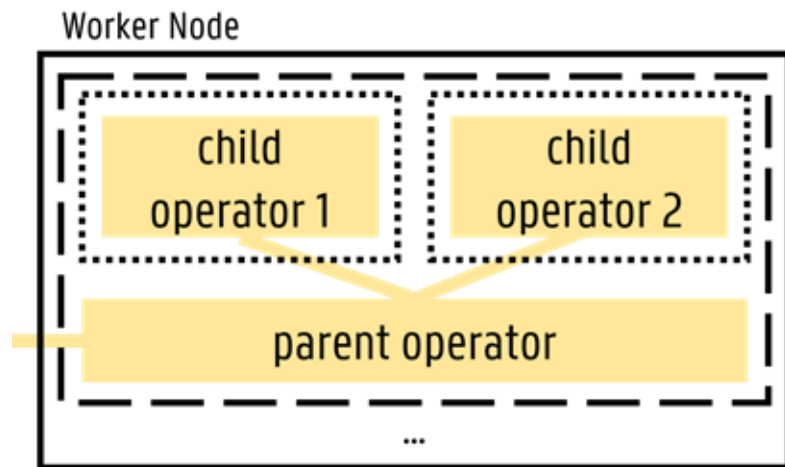


D2.1

Result: Wasm-operator

Framework for running Kubernetes Operators as event-based serverless functions, using WebAssembly.

- Suspends operators to disk when inactive
- Wakes operators when changes require reconciliation
- Predictive unloading
- Supports kube-rs operators (Rust) and Golang
- Wasm Component model support
- Kube-rs enhancements
 - To reduce needless wakes



Task 2.2

Serverless Execution of Lightweight
Polyglot Architecture-agnostic
Isolated Workloads

Result: Serverless repository security

Analyzed 2,758 serverless components in public serverless repositories

- AWS | Docker Hub | GitHub | Red Hat Quay | Serverless Framework.

Five major security risks identified

1. **Vulnerable dependencies:** Using outdated packages with known security vulnerabilities.
2. **Malicious components:** Leveraging public repositories to distribute malicious serverless components at scale.
3. **Sensitive parameters in 'docker run' commands:** Docker run options enabling adversaries to perform attacks.
4. **Risky parameters in IaC templates:** Misconfiguration errors allowing attacks.
5. **Typosquatting attacks:** Names resembling popular legitimate images.

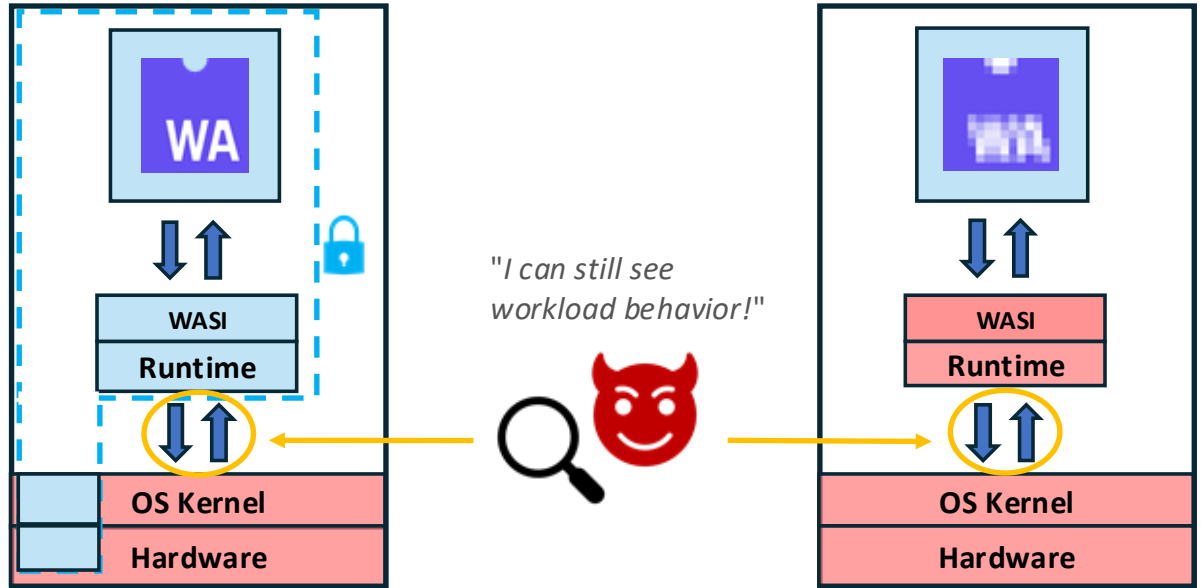
D2.2

This work has been accepted to ESORICS 2025 and was presented on September 24 in Toulouse.

Fingerprinting WebAssembly apps

Two confidentiality scenarios:

1. Wasm modules are **obfuscated** by binary obfuscation tools (WASMixer)
2. Wasm modules are run by a **TEE-backed runtime** (WAMR with Intel SGX and Intel Protected File System)



Identification **accuracies of 85% and 92%** using respectively **43% and 66%** of the **test syscall traces**, highlighting attack stealthiness and practicality.

D2.2

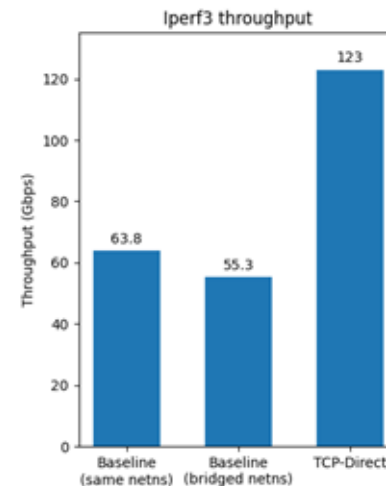
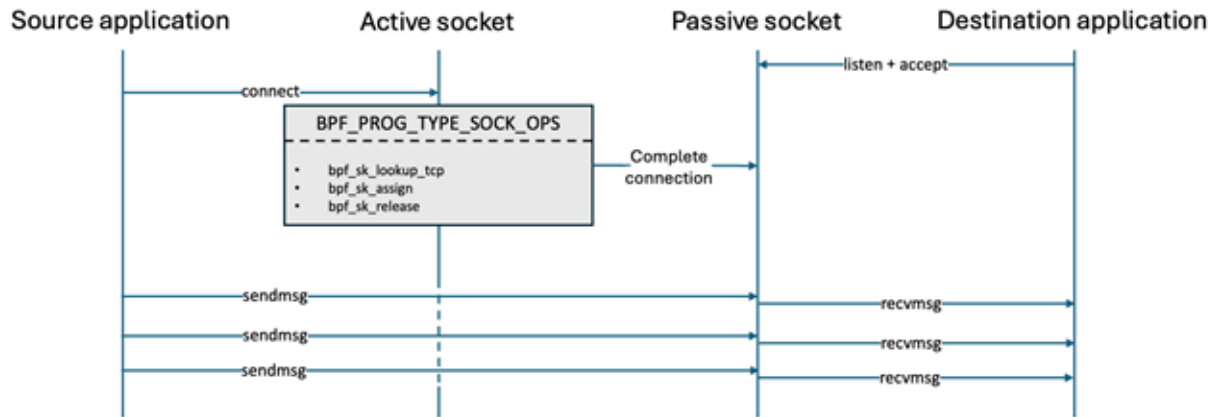
Task 2.3

Low-latency Serverless FaaS
Orchestration Mesh and Monitoring
with eBPF and XDP

Accelerated microservices interconnection

Intra-node communication

- eBPF-accelerated TCP communication **between processes**
- **Doubles throughput and lowers latency** compared to native TCP
 - and Unix Domain Sockets.



D2.3

Accelerated microservices interconnection

Inter-node communication

Communication **between nodes** accelerated using Remote Direct Memory Access (RDMA) with **TCP-over-RDMA proxy**.

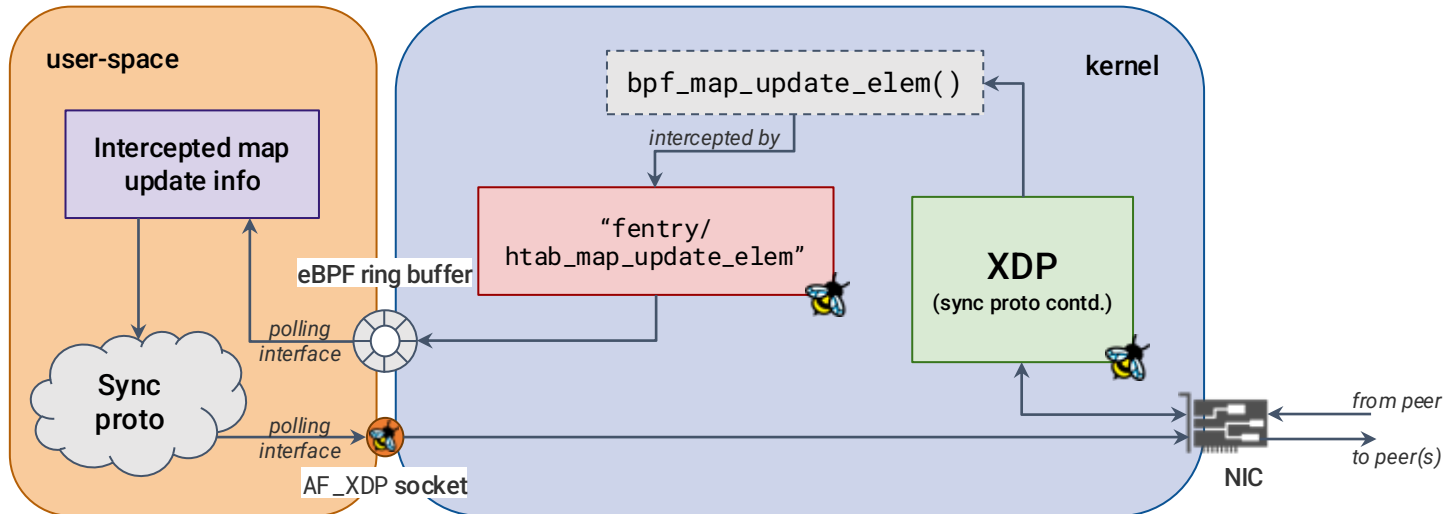
- ✓ **Redirect traffic locally** from the workload to the proxy
- ✓ **Transport over RDMA** between proxies on each node
- ✓ **Multiplex TCP flows** to workaround hardware RDMA Queue Pair Limits
- ✓ **Application-level transparency** by retaining the socket API

10-100% speedup

D2.3

eBPF state synchronization

- Synchronizing eBPF map data across nodes.
- Polling-based architecture with baseline delay of $\sim 25\mu\text{s}$.



D2.3

- Observing WebAssembly functions in **Spinkube** (Kubernetes)
 - **Non-intrusive tracing** of HTTP traffic using eBPF
 - Optional intrusive solution for more **granular tracing** inside of Wasm
 - Observability for Wasm workloads is realized
 - Via workarounds of uprobing the Wasm Runtime instead of the Wasm bytecode
- **Goal 1: Minimal overhead**
 - In worst case scenario (all errors), we have measured
 - **8%**: maximum CPU overhead (no sampling, could be optimized)
 - **17.9%**: HTTP response time overhead
- **Goal 2: No modifications required to apps by default**
 - Modification needed only when ID of specific serverless functions needed

WP2 Publications & Community Contributions

Academic Publications & Presentations

The Hidden Dangers of Public Serverless Repositories: An Empirical Security Assessment.

Eduard Marin et al., European Symposium on Research in Computer Security (ESORICS) 2025

Cyber-Physical WebAssembly: Secure Hardware Interfaces and Pluggable Drivers

Michiel Van Kenhove et al., IEEE NOMS 2025

Industry Presentation

WebAssembly for IoT Devices Interfacing with USB and I2C Hardware

Wasmcon 2024

Standards

W3C **wasi-i2c**, phase 2

Proposal: <https://github.com/WebAssembly/wasi-i2c>, implementation: <https://github.com/idlab-discover/i2c-wasm-components>

(Collaboration with Siemens)

W3C **wasi-usb**, phase 1

Proposal: <https://github.com/WebAssembly/wasi-usb>, implementation: <https://github.com/idlab-discover/usb-wasm>

Open Source Software

Propeller orchestrator

Code: <https://github.com/absmach/propeller>, docs: <https://docs.propeller.abstractmachines.fr/>

Next steps



Selected Future work

- Propeller: integration with **K8s**, Zephyr **RTOS**
- **Paper** on confidential wasm workload unmasking
- **eBPF** state synchronization
- **Observability** of serverless Wasm workloads
- **Security** orchestration & Lightweight ABAC

WP3: Privacy-preserving, Portable and Efficient Execution Using Confidential Computing

Lead: THD

Contributors: LUN, AAL, UVC, ERF, THS

WP3 Objectives

(O3) Objective 3: Implement privacy-preserving architecture-agnostic, efficient and secure execution environment using confidential computing and privacy-enhancing technologies, ensuring secure and trustworthy services in the context of a programmable platform accessed by multiple stakeholders and tenants including vertical industries as users, and a **secure host-neutral infrastructure** where multiple infrastructure providers are involved in the deployment, hosting and orchestration of the network service.

03.1

Determine and specify a **Hardware Abstraction Layer (HAL)** for secure enclaves that is lightweight ensuring the Trusted Compute Base (TCB) is low.

03.2

Implement a **WebAssembly (Wasm) runtime inside secure enclaves (TEEs)** which is portable and architecture agnostic for the operation of high-level applications.

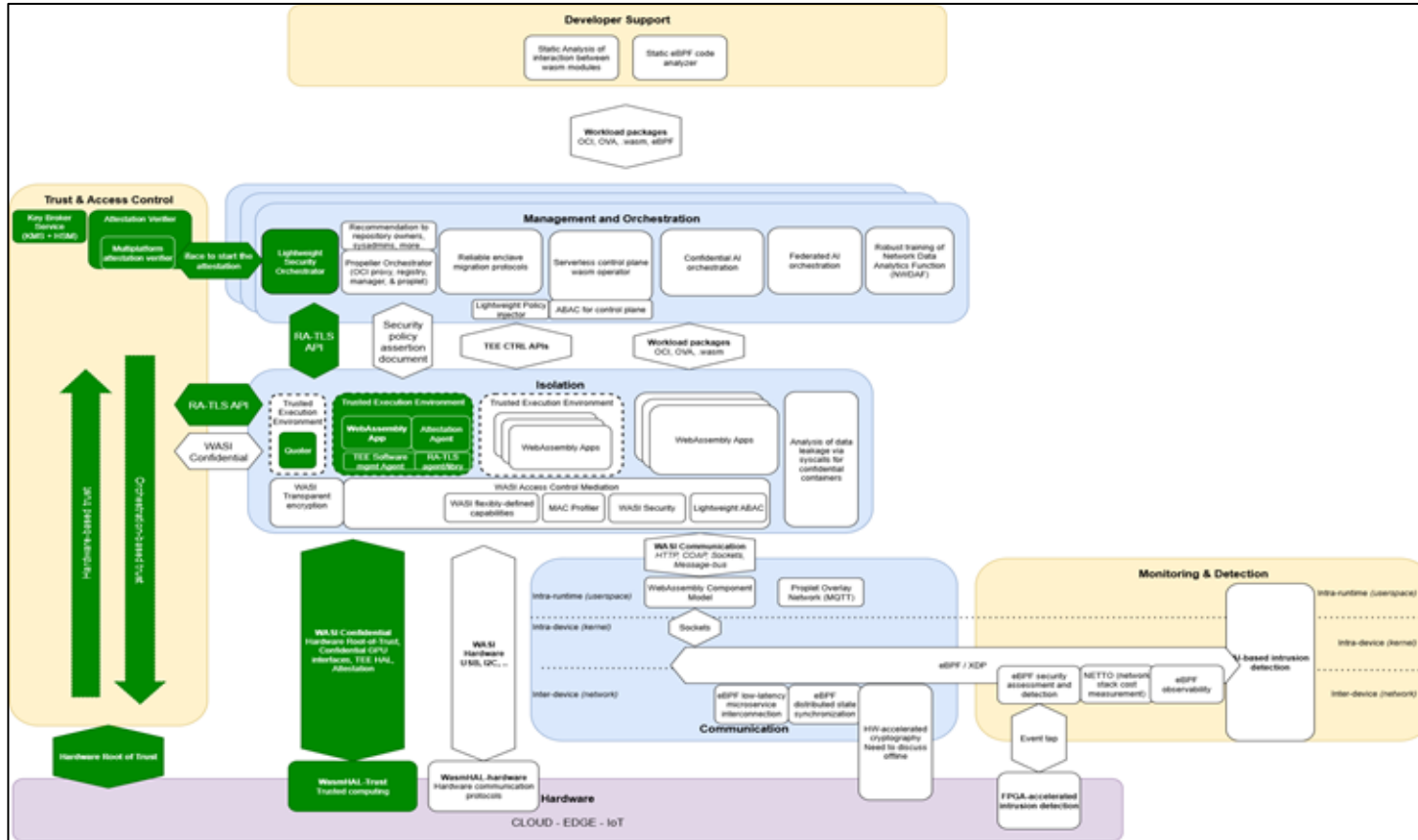
03.3

Analyze and implement cryptographically secured, hardware-supported **Remote Attestations** for Trusted Execution Environments (TEEs).

03.4

Specify and implement an **Orchestration Agent inside the secure enclave (OS.2)** which is capable of orchestrating workloads for Confidential Computing (HW-assisted TEEs).

ELASTIC Architecture WP3 Component Mappings

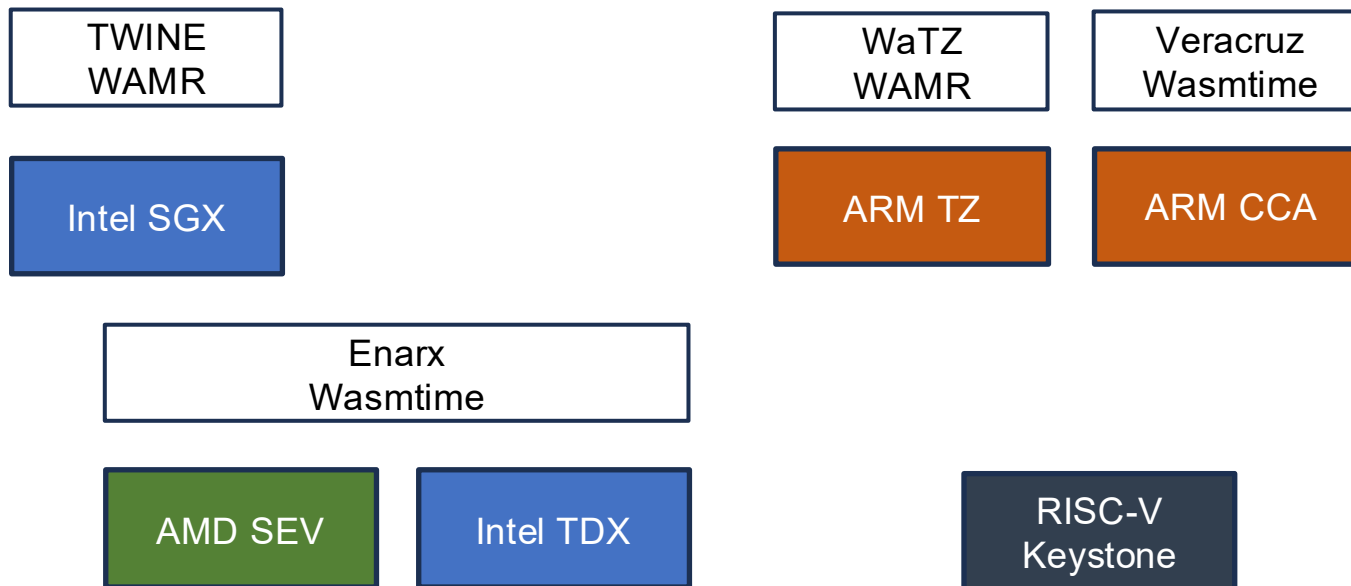


T3.1

TEE Hardware and Abstraction Layer, Enclave Deployment and Monitoring

WASM on TEE Study

A WASM on technology overview with a focus on the five dominating trusted execution technologies (RISC-V excluded but is currently under consideration)



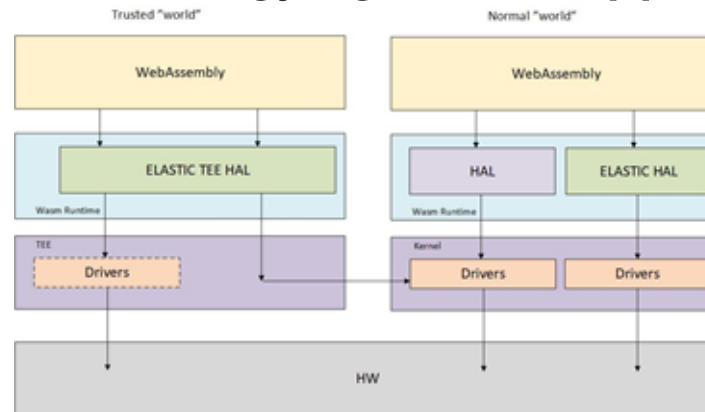
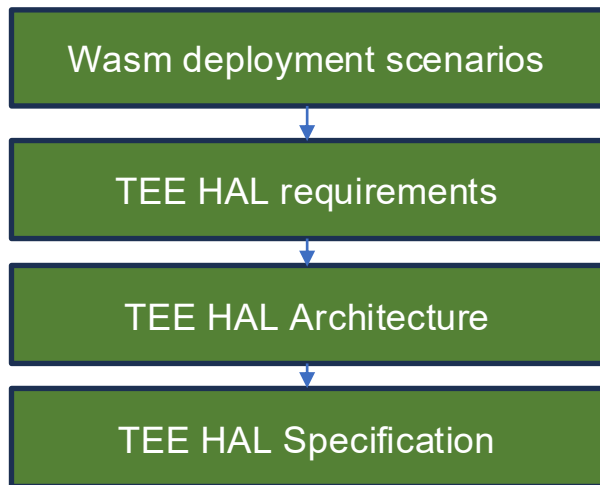
WASM on TEE study – main conclusions

- The TWINE framework gives important insights, but the Intel SGX focus makes it too limited for ELASTIC.
- The Enarx framework is appropriate to build upon but not maintained anymore. **Wasmtime is a widely used and suitable runtime for VM-based containers.**
 - ELASTIC will build on Wasmtime
 - Adopted Wasmtime for Linux -> T3.2
- **WAMR is a suitable runtime for constrained platforms.**
- **WaTZ suits the WP4 needs**
- The WASI standard is suitable for TEEs but causes some security challenges in the increased trusted computing base and limitations in supported data types

ELASTIC TEE HAL – WASI based

- The main goal is to provide TEE technology agnostic support for WebAssembly workloads

- Methodology



TEE HAL Function Classes

Clock	Random	Object storage
Sockets	Cryptography	GPU
Resource alloc.	Event handl.	Internal comm.

Status and Next Steps

Achievements

- A literature study on the status of running Wasm on five dominating TEE platforms
- A performance comparison between different Wasm runtimes and Enarx on AMD SEV
- ELASTIC TEE HAL specification and reference implementation on AMD SEV

Next Steps

- A TEE HAL reference implementation on Intel TDX (Task 3.2)
- Complete the TEE ELASTIC Wasm framework (Task 3.2)

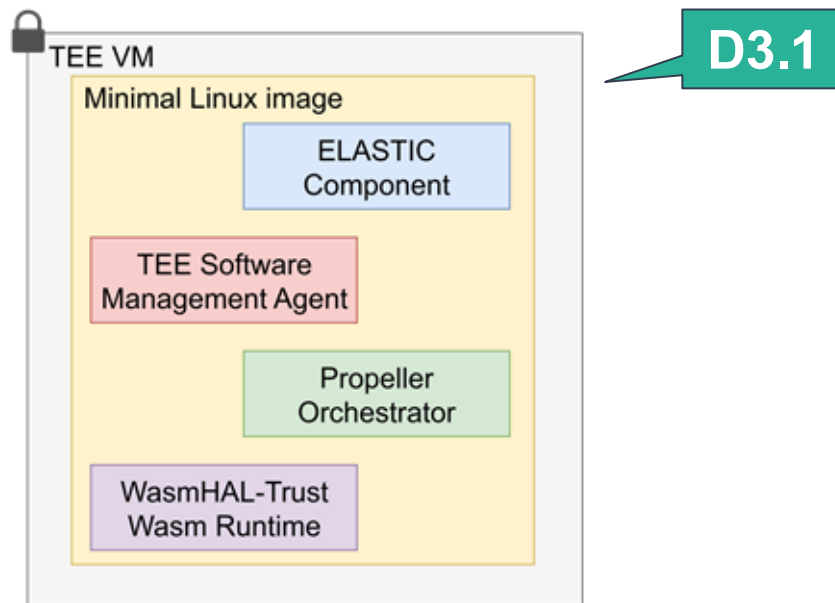
T3.2

WASM Runtime Inside TEE

Wasm Runtime Inside TEE

Develop a secure and portable Wasm framework that operates within a Trusted Execution Environment

- Bare-metal access, syscalls
- Strong isolation
- Trust through attestation procedures
- Seamless workload migration



Key Achievements

D3.1

elastic

- ✓ Research on different approaches to **minimizing TCB**
- ✓ **Wasm framework syscalls approach analyzed**
- ✓ **Build minimal Linux image with Wasm Runtime support**
- ✓ **Integrate ELASTIC components into minimal Linux image**
 - TEE Software Management Agent
 - WasmHAL-Trust (Wasm runtime)
 - Propeller Orchestrator
- ✓ **Attestation mechanisms of minimal Linux image with Wasm runtime**



Next Steps

D3.2

D3.3

- ⚙️ Carry on the work on CoCoS (TEE Agent) from the T2.1
- ⚙️ Use **Confidential Containers** to run HAL components
- ⚙️ Run HAL components in **public clouds** (Azure, GCP)
 - Integrate **attestations support** to Wasm Runtime
 - Add support for **Keystone TEE (RISC V)**

T3.3

Remote Attestation



The Big Picture

HW = Intel Xeon
OS = ELASTIC Platform
App = BRT App



Attester:

- Implemented **Attester service** (enclave / TEE evidence generation)
- Abstracted platform-specific details behind **Unified HAL**
- Develop a WASI-like interface to access the underlying H/W attestation functionality directly.

Verifier:

- Implemented **Verifier-side functionality** (evidence parsing & validation)
- Encapsulated verification into portable components with platform-agnostic interfaces

Attested serverless platform

- Implemented protocol to attested components across many physical TEEs

Multi-platform Attester

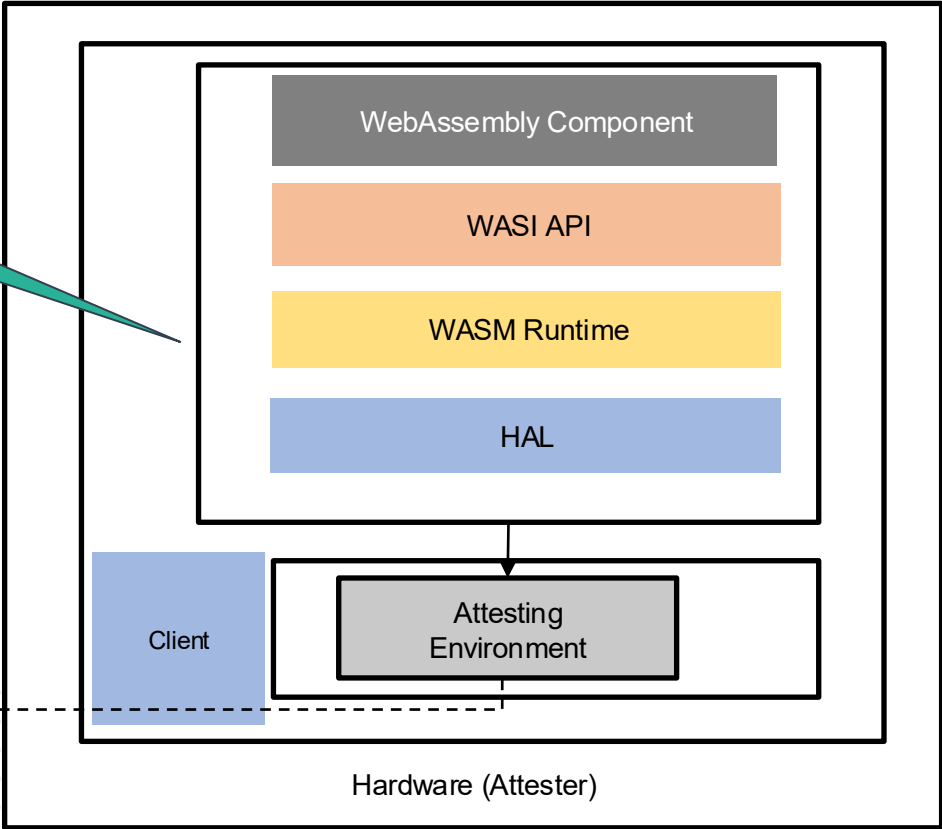
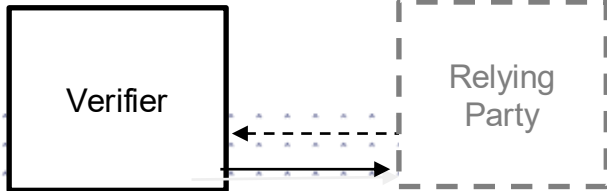
Problem: Wasm runs everywhere, attestation works differently everywhere

Solution: Wasm-focused API and HAL for attestation

Platforms:

- ARM TrustZone
- Intel TDX (in progress)
- AMD SEV-SNP (planned)

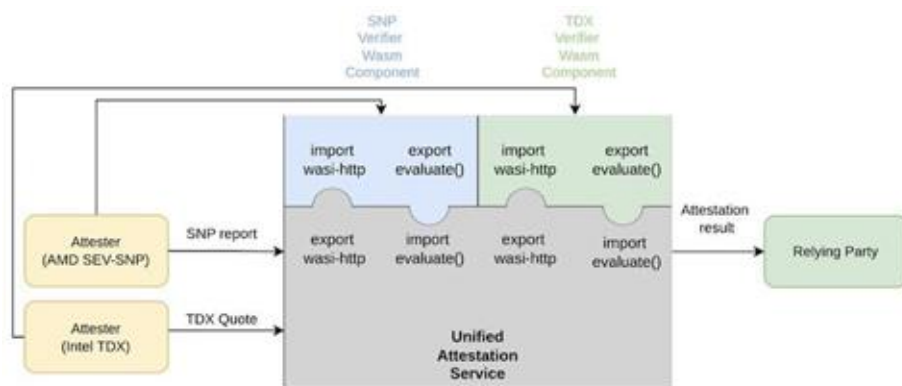
D3.1



Multi-platform Verifier

Problem: Verifier needs to understand evidence from newest versions of every supported platform

Solution: Implement verification functionality within Wasm components



- Verifier can download component on demand when it encounters a new TEE
- Portable, signed components with a common platform-agnostic interface
- No hard-coded platform-specific logic in verifier
- Components use WASI to directly obtain keys, revocation lists, etc.

D3.1

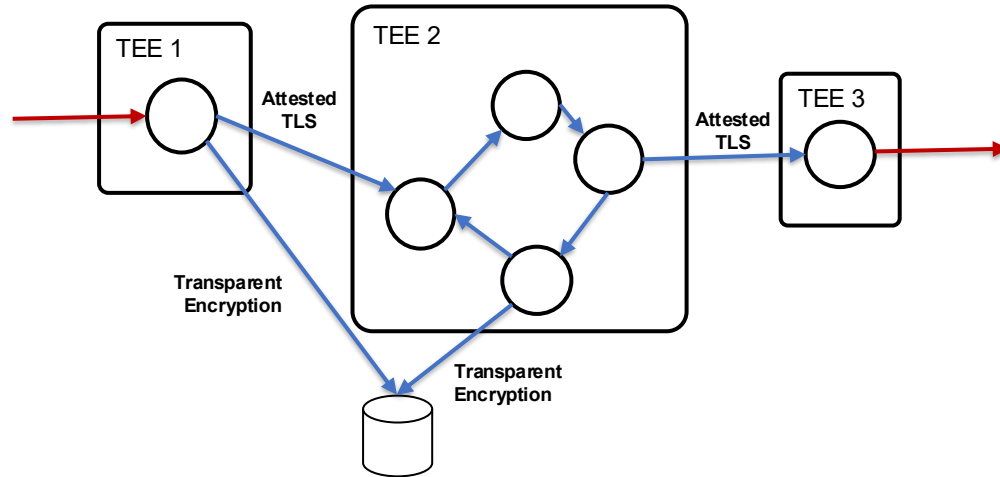
Platforms:

- AMD SEV-SNP
- Intel TDX
- ELASTIC edge platform (TBD)

Attestation of serverless applications

Problem: Serverless applications can be spread across many devices

- Attestation challenge: with many TEEs, no attestation covers the whole app



Solution: Consensus protocol to agree on attested component public keys

- Agreement on components + agreement on links = agreement on application

D3.1

Remote Attestation – Next Steps

- Extend **multi platform Verifier / Attester** for at least three TEEs
- Develop **Key Broker** functionality
- Research new attestation primitives for the Wasm component model

WP3 Conclusion & Highlights

WP3 is enabling secure, trusted, platform-independent interoperable execution for multi-user, multi-tenant applications on the Cloud, Edge and Far-Edge

Components

- WasmHAL-Trust
- Multiplatform attestation verifier
- Lightweight Security Orchestrator
- Cross-TEE attestation for serverless applications

Standards

- IETF RATS
- OCI
- PKCS #11
- WASI

Highlights

- TEE HAL for Wasm
- Platform-agnostic attestation
- TEEs for serverless orchestration

WP4: Efficient, Portable and Secure Edge Workload Orchestration

Leader: TID

Contributors: All partners

WP4 Objectives

Objective 4: Design and implement **efficient, portable and secure edge and far edge (IoT) workload orchestration** with the level of **reliability, trust and resilience** that applies to critical infrastructure like **6G**, based on a globally connected continuum of **heterogeneous environments** supported by the convergence of networks and IT systems to enable future digital services

04.1

Analyse and develop **support** for **Wasm, eBPF and TEE** technologies for **edge** and **constrained IoT nodes**

04.2

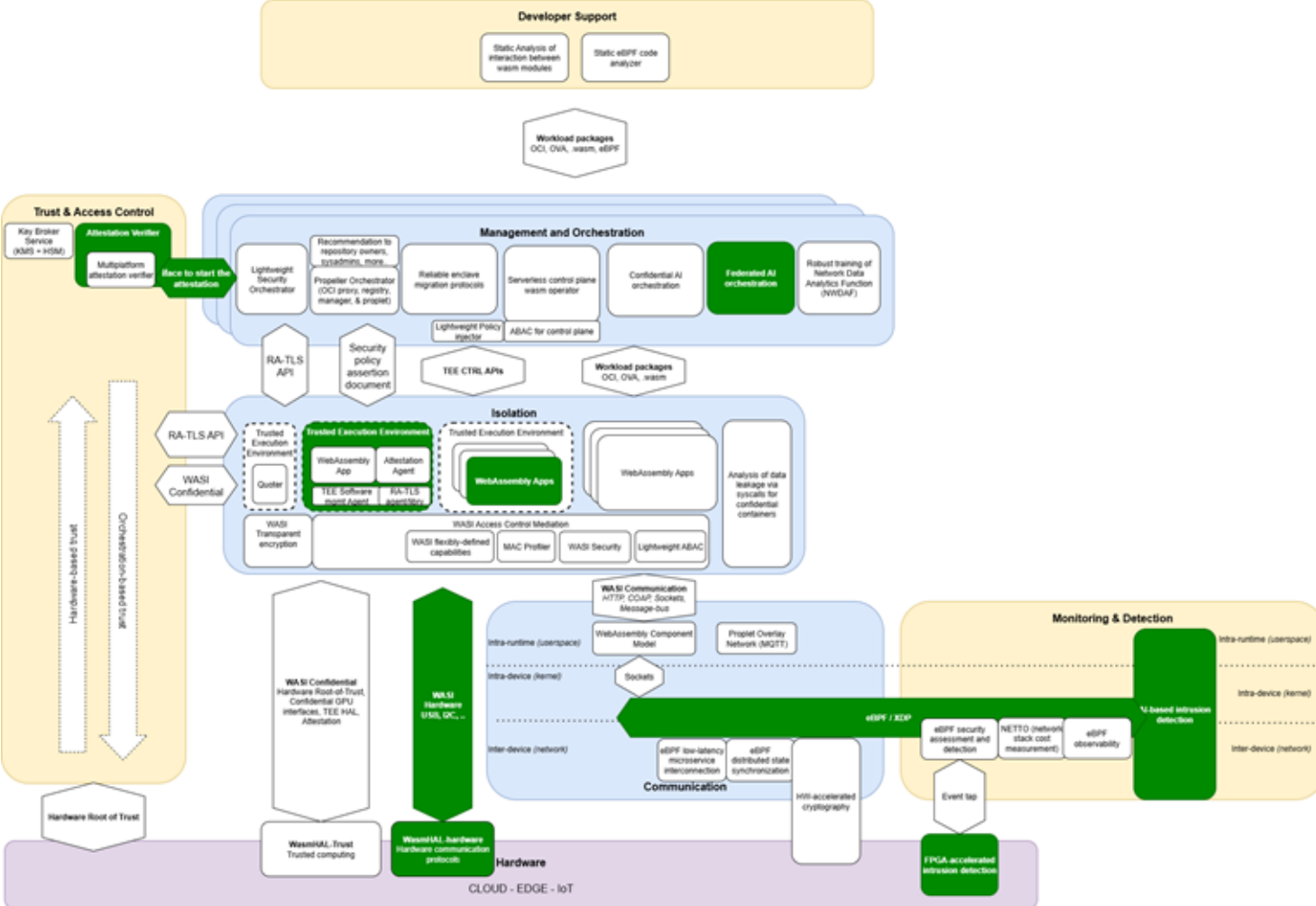
Analyse **HW & SW support** for **ML on the edge** (e.g., lightweight Wasm workloads) while maintaining a high level of **security** (e.g., TEE-enabled GPUs, FPGA-based solutions)

04.3

Analyse **federated ML** orchestration suitable for **distributed** edge and **privacy-preserving security** requirements

04.4

Develop **authorization and authentication schemes** for the **edge** that support new orchestration technologies

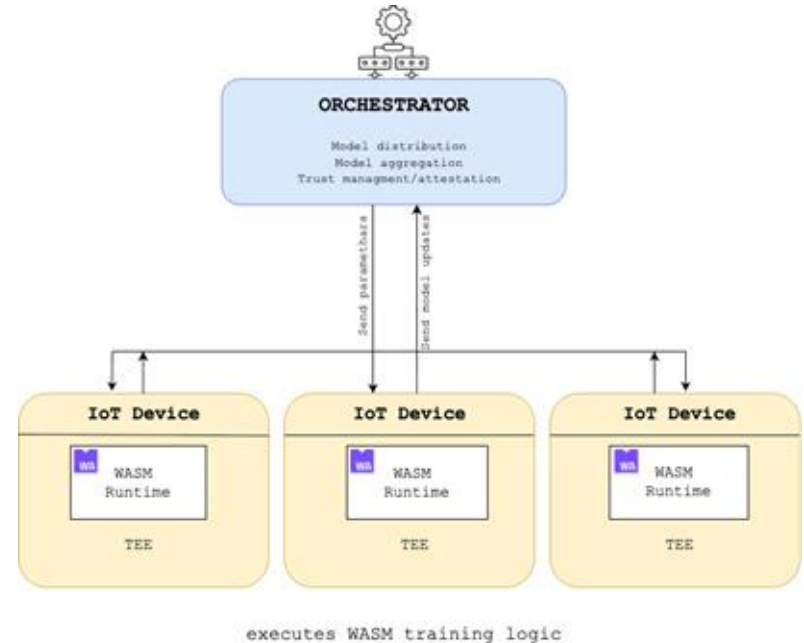


Task 4.1

Support for Wasm, eBPF and TEEs
on IoT Edge Nodes

Wasm, AI, and Federated Learning on IoT Devices elastic

- Studied efficiency (link to D1.1), challenges, and optimisation of Wasm for IoT devices
- Presented how Wasm can be used to bring intelligence to data processing pipelines
- Analysed Federated Learning for IoT and defined **Wasm+TEE-aware FL architecture** for heterogeneous edge environments



Android as an Edge device

Android devices do not let normal applications run code in TEE

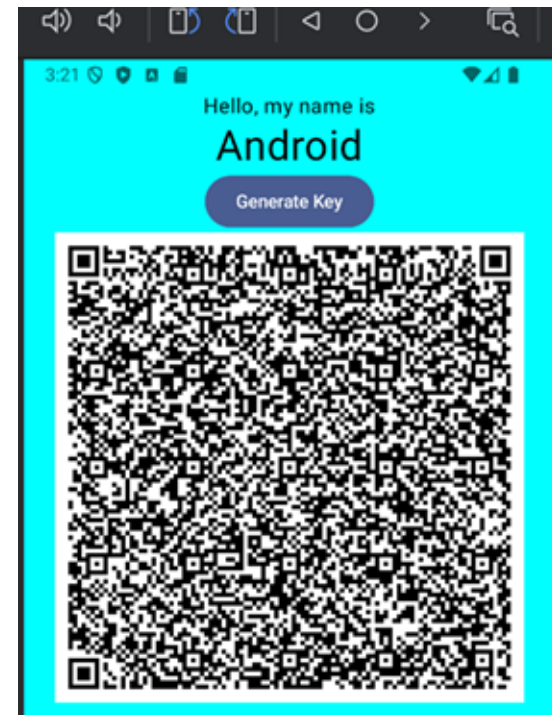
- But can attest the protection **keys**
- Keystore provides certificate chain for a key

Certificate lists applications with access to key

- Initial validation of concept
- Use as a “TEE-lite” to attest data provenance?

Example applications:

- Certify that a photo is original
- Proof of inputs to Federated Learning



Secure Elements for Hardware-Based Attestation and Remote Attestation

Investigated advantages of a secure element in the context of attestation needs in IoT, like:

- Availability of primary cryptographic services and Root of Trust

- High security level guarantees



- Existence of secure elements standards in relation to attestation



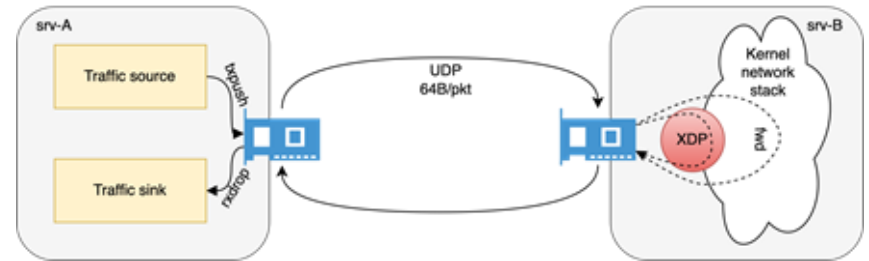
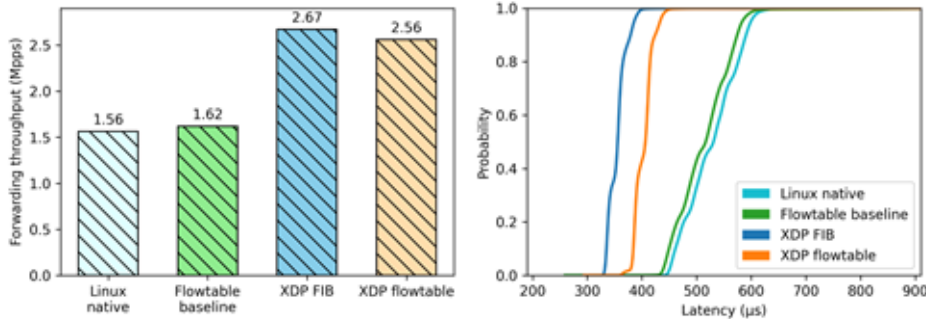
Trusted Platform Services (TPS) Committee

eBPF-Accelerated Network Forwarding

Performance analysis of available forwarding techniques in Linux, including:

- Native ip forward
- Custom XDP network function
- Nftables flow table (with and without XDP offload)

XDP-accelerated flow table fwd provides the best balance between speed and compatibility



AI-IDS + eBPF Deployment on Edge Node

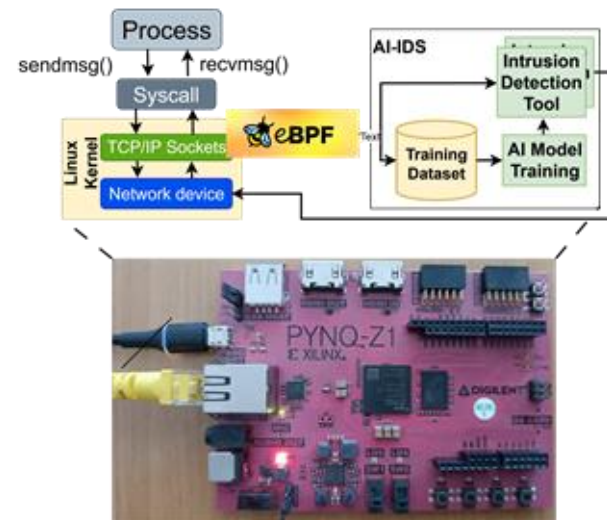
Task 1.3

eBPF + AI-IDS on highly-performant device (Xilinx Alveo U200 FPGA)



Task 4.1

eBPF + AI-IDS on resource-constrained IoT device (Pynq-Z1 prototype)

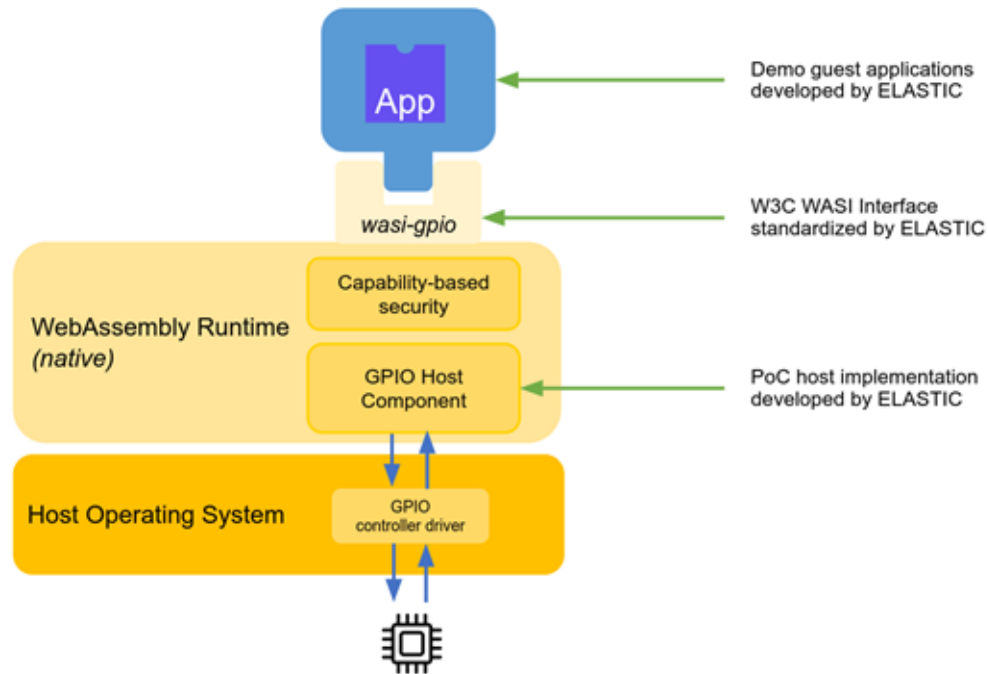


D4.1

W3C WASI Standard Proposal for GPIO

Enable WebAssembly applications to communicate with external sensors and actuators using General Purpose IO Pins (GPIO)

- Supports digital and analog pins
- Reading, writing, configuring pins
- Custom board-specific mapping between application pins and physical hardware



Implementation of Wasm-capable IoT Node

Created PCB with ESP32 and RISC-V architecture

- Runs **WAMR** (Wasm Micro Runtime) & ZephyrRTOS
- Integrated node and runtime with **Propeller** orchestrator (can deploy Wasm workloads on node)
- **ESP32 C6 TEE support enabled and tested**



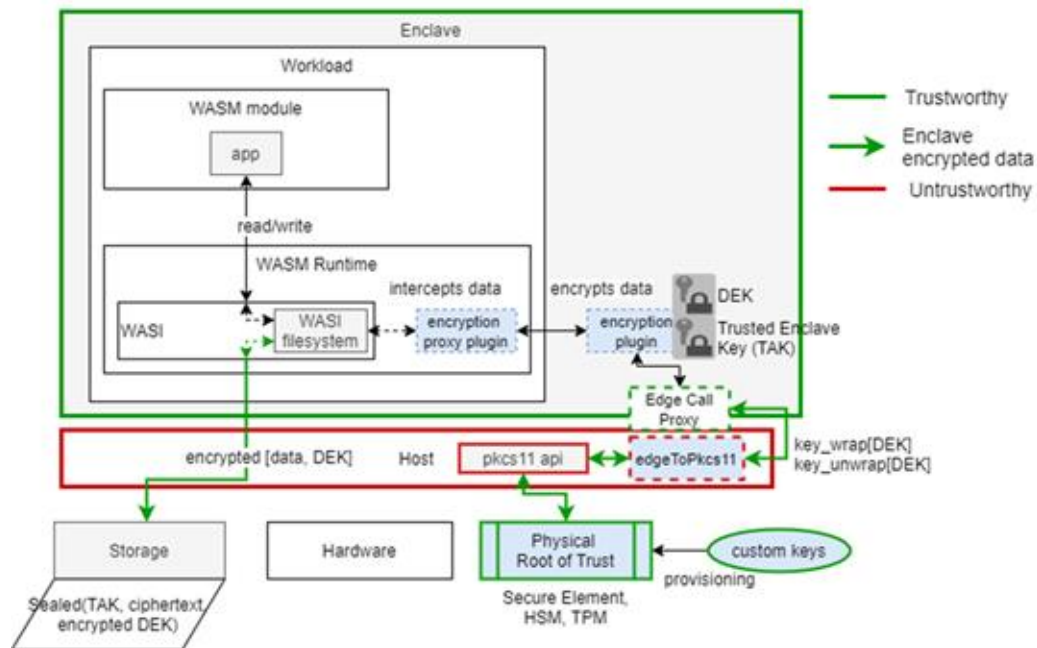
Task 4.4

Security of Embedded Devices
Using Wasm, eBPF and TEEs

Data Protection At-Rest at the Edge with TEE

Goal: encrypt data-at rest from a Wasm workload transparently by addressing a **secret key** protected within an embedded **Secure Element**

Keystone case



Next Steps

Next Steps for WP4

Task 4.2

ML on the edge with Wasm and hardware acceleration

- Lightweight ML models
- Improve performance with TEE-enabled GPUs or FPGA-based components
- TEEs to secure models + data

Task 4.3

Federated and Split Learning with heterogeneous IoT devices

- Wasm workloads
- Secure training via TEEs
- Optimize orchestration

Task 4.4

Security at IoT nodes via Wasm, eBPF, and TEEs

- Remote Attestation
- Secure elements to support Wasm + TEE for sensitive data and storing cryptographic keys
- Enhance AI-IDS + eBPF edge node integration

WP4 Publications & Community Contributions

Contribution Type	Description
Standardisation	wasi-gpio standard: https://github.com/WebAssembly/wasi-gpio/blob/main/wit/gpio.wit
Standardisation	wasi-gpio prototype: https://github.com/idlab-discover/wasi-gpio-implementations/
Publication & Presentation	AutoML in the Face of Adversity: Securing Mobility Predictions in NWDAF (FMEC 2024)
Publication & Presentation	Parameterized Complexity of Caching in Networks (AAAI 2025)
Publication & Presentation	The Computational Complexity of Positive Non-Clashing Teaching in Graphs (ICLR 2025)
Publication	Resilient Automatic Model Selection for Mobility Prediction (Cluster Computing)
Publication	Demystifying Privacy in 5G Stand Alone Networks (MobiCom 2024)
Publication	Metric Dimension and Geodetic Set Parameterized by Vertex Cover (STACS 2025)
Publication	SoK: Evaluating 5G-Advanced Protocols Against Legacy and Emerging Privacy and Security Attacks (WiSec 2025)
Publication	On Using Secure Aggregation in Differentially Private Federated Learning with Multiple Local Steps (TMLR)



Efficient, portable And Secure orchesTration for reliable servICes

WP5: ELASTIC Demonstrators

Leader: UVC

Contributors: TUC, ERF, THD, THS, ERS, IMEC, UVC, ZEN

WP5 Objectives

05.1

Specification of the ELASTIC use cases, and technical requirements for validation of the ELASTIC technology in the demonstrators secure serverless FaaS orchestration and Confidential Computing with Wasm

05.2

To **setup infrastructure and deploy cloud computing testbed** including both private and public cloud resources for the deployment and prototyping of the demonstrators in healthcare

05.3

Extend the demonstrators with security services in order to showcase how these services **improve the security and usability** of the demonstrator applications

05.4

To perform **evaluation and analyse results of the scalability, usability, performance and hardware implications** of the secure privacy-preserving serverless FaaS orchestration and Wasm-enabled TEE-enhanced collaborative AI

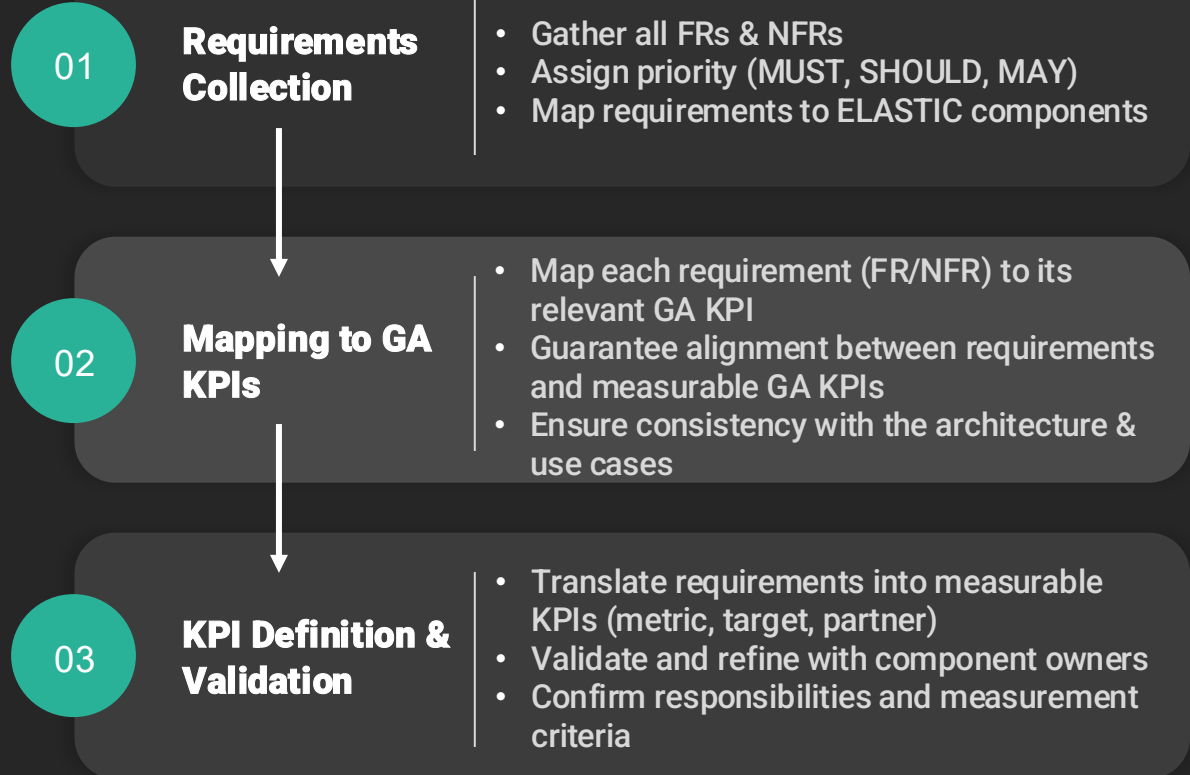
Task 5.1

Specification of the demonstrators
for testing and validation

- **Identify and structure Demonstrator workflows**
 - Defined pilot integration for each technology block (Wasm, eBPF/XDP, TEEs, orchestration)
 - Connected other WP outputs with industrial scenarios
- **Define requirements and evaluation criteria**
 - Collected Functional (FR) and Non-Functional Requirements (NFR)
 - Established evaluation metrics and success criteria
 - Ensured coverage of performance, security, portability, and scalability aspects
- **Map ELASTIC components**
 - Linked each ELASTIC architecture component to the demonstrator(s)
- **Extract and align KPIs**
 - Derived demonstrator-specific KPIs from requirements and project-level goals in the GA
 - Ensured full traceability from GA KPIs → Requirements → Demonstrator KPIs
- **Develop validation methodology and plan**
 - Defined measurement processes, test procedures, and responsibilities

Derivation of Demonstrators KPIs

The process ensures demonstrator KPIs are measurable and meaningful, traceable from GA high-level KPIs through the requirements to the final indicators, while aligning architecture, implementation, and validation.



Performance Goals

- Improving **resource utilisation**
 - Reduce attack **detection and analysis time**
 - Improve **network workload** processing
 - Efficient **serverless security** mechanisms
- } D1
- Improve efficiency of VMs **deployment**
 - Improve efficiency of the **remote attestations**
 - Keep **compatibility** with existing CC infrastructure
- } D2

WP5 Demonstrator KPIs Example

KPI ID	Name	Req. ID	Metric	Relevance	Target
D1.1.1	Local Processing Rate	D1-FR7	% of sensitive data processed locally	High	100%
D1.1.2	FL Model Convergence	D1-FR15	# of rounds to convergence	High	≤ 100
D1.1.3	Sovereign Data Retention	D1-NFR4	% of sensitive data kept in zone	High	100%
D1.2.1	Monitoring Latency	D1-FR10	Data-to-dashboard delay	Medium	≤ 2 s
D2.1.2	Migration Security	D2-FR1	% of migrations with no security issues	High	100%
D2.1.3	Migration Reliability	D2-FR7	% of migrations without interruption or data loss	Medium	$\geq 99\%$
D2.1.4	CC Scalability Efficiency	D2- NFR1	Max concurrent workloads supported	High	≥ 100

Task 5.2

Setup Orchestration Infrastructure
and Confidential Computing Testbed

Setup Orchestration Infrastructure and Confidential Computing Testbed

D5.1

elastic

- Established a **cloud computing testbeds** for ELASTIC demonstrators
- Integrated resources on **edge** and far edge, **private and public cloud**
- Ensured support for **demonstrator-specific requirements**
- Provisioned **hardware, software, and network** resources
 - Provided devices and HW support
 - Installed software and deployed tools
 - Ensured networking operations
- Deployed **orchestration environment** for demonstrators
- Ensured **secure access to testbed**



Demonstrators testbeds Hardware Requirements

D5.1

elastic

Demonstrator 1

Edge Layer:

- MCU devices (ESP32-C6, ≥ 128 –500 MHz, ≥ 512 KB RAM)
- TEE-enabled edge devices
- Raspberry Pi 3+ or Arduino Nano
- Secure Element / RISC-V with disk storage
- FPGA boards for crypto & AI IDS

Fog Layer:

- Linux servers ≥ 2 cores, ≥ 1 GB RAM
- Hosts with RDMA NICs
- FPGA acceleration for AI IDS
- Linux hosts supporting kernel 6.8+

Cloud Layer:

- Kubernetes-capable servers (≥ 1 controller + 1 worker).
- AMD SEV-SNP or Intel TDX TEEs.
- Linux servers with RDMA NICs.

Demonstrator 2

Fog Layer:

- **Remote Attestation Platform:** x86-64 CPU (4+ cores), virtualization support, ≥ 6 GB RAM, ~ 1 TB disk, TPM 2.0 optional
- **WASI Capabilities:** Generic Linux servers receiving TEE inputs (SEV-SNP, TDX)

Cloud Layer:

- **TEE SMA:** CPUs with AMD SEV-SNP or Intel TDX support
- **Propeller Orchestrator:** Edge MCU (ESP32-C6), ≥ 512 KB RAM; Manager/Proxy requires Linux server (≥ 2 cores, ≥ 1 GB RAM)
- **AI-IDS:** FPGA-based reconfigurable platform
- **Key Broker Service:** x86-64 server, ≥ 4 GB RAM, HSM-secured key storage

Demonstrators testbeds

Software Requirements

D5.1

elastic

Demonstrator 1

Edge Layer:

- Wasm runtime
- Keystone enclaves, Secure Element PKCS#11 API
- ML/crypto libraries for federated learning

Fog Layer:

- SuperMQ broker for messaging
- Prometheus / OpenTelemetry
- Linux Kernel ≥ 6.8 for eBPF
- Static analysis + attestation frameworks

Cloud Layer:

- Kubernetes (latest 3 minor releases)
- TEE mgmt agent for AMD/Intel TEEs
- Wasm-operator, observability frameworks, ABAC policy tools

Demonstrator 2

Edge Layer:

- **TEE Mgmt Agent:** Linux kernel with SEV-SNP or Intel TDX support
- **WasmHAL-Trust:** Runs on SEV-SNP/TDX
- **AI-IDS:** Python framework/traffic forwarding tools

Fog Layer:

- **Propeller Orchestrator:** Standalone or with CI/CD, requires SuperMQ, supports Prometheus/OpenTelemetry, OCI registries
- **Remote Attestation Platform:** Linux (Ubuntu 22.04+), GCC/Clang, OpenSSL 3+, Intel TDX/SGX SDK, OP-TEE client, WAMR/Wasmtime, Docker

Cloud Layer:

- **Key Broker Service:** Linux OS, JSON/CBOR parsing, TLS 1.3, gRPC/REST APIs, CMake/Python/Go builds
- **WASI Capabilities:** WebAssembly runtime in verification framework on Linux
- **Verifier:** Delivered as HTTP API service



Efficient, portable And Secure orchesTration for reliable servICes

Demonstrator #1

Smart Connected Factory of the future

(WP5 – T5.3 - An IoT Data Fabric as a native 6G capability)

Ericsson Research, Finland (ERF)



Co-funded by
the European Union



Partner Introduction – Ericsson Research

Ericsson Research globally



750+ researchers
50+% Ph.D.

14 countries
4 continents



2G, 3G, 4G, 5G, ...6G

it's all invented here

>50%

involvement in all of Ericsson patents

Global networking

cooperating in a world-wide network of leaders

Competence and
people

Leading research in
our industry's
technologies

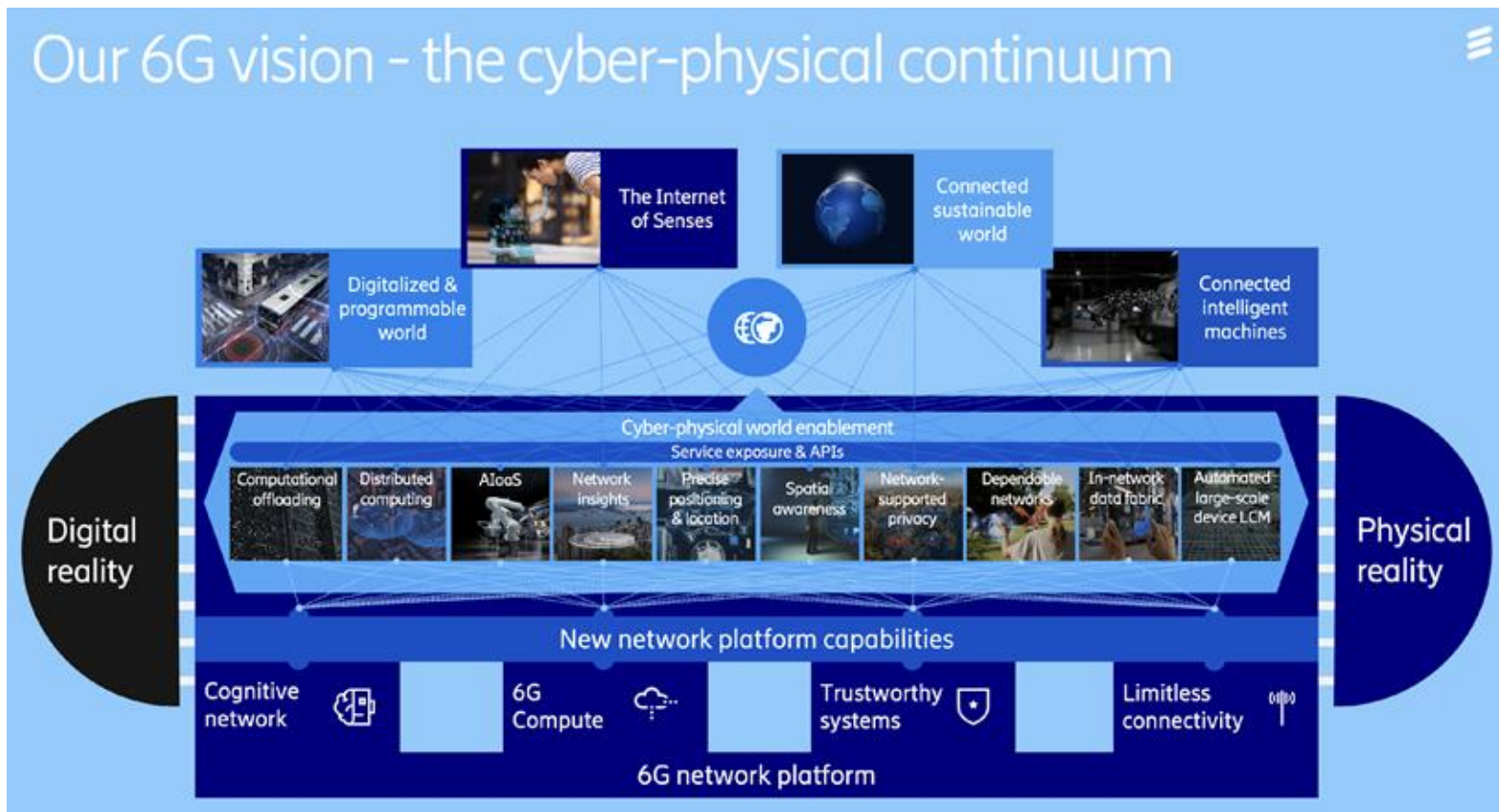
Collaboration with
leading universities
and industries

Ericsson participation in ELASTIC includes:

1. Ericsson Research Finland (ERF)
2. Ericsson Research Sweden (ERS)

From Cyber-physical systems
research and Cloud research teams

Our 6G vision - the cyber-physical continuum



Ericsson expectations from ELASTIC

Further the research on advanced capabilities of 6G

- Bring new insights into opportunities for more secure and efficient operations
- Help guide future product roadmaps on relevant capabilities
- ELASTIC work is related to multiple areas of interest
 - Focus on Distributed Computing, Trustworthy Systems, Network Insights, **In-network Data Fabric**, Automated large-scale LCM aspects

Demonstrator-1: **In-network Data Fabric**

- Drive consumption of advanced 6G capabilities

Smart Connected Factory of the Future

IoT data fabric solution for hyper-scale data processing in a 6G timeframe

Tools:

- eBPF for security vulnerabilities
- WebAssembly and FaaS security frameworks
- Hardware-based, embedded low-power modules for security issues detection

ELASTIC goals & scenarios:

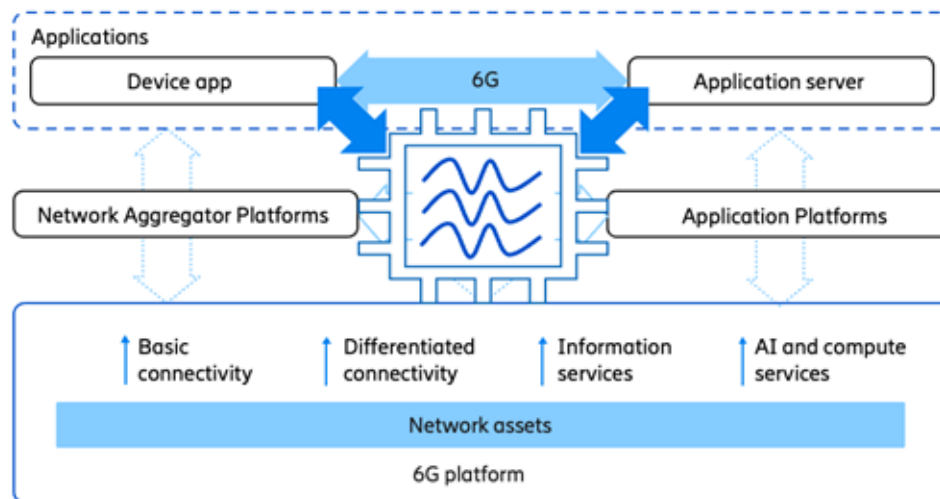
- In-transit **IoT data processing using FaaS**
- Use **lightweight virtualisation** to minimise processing **latency** and **resource utilisation**
- Deploy ELASTIC **stateless and minimal-state** processing on **resource-constrained device clusters**
- Deploy **privacy-aware mechanisms** for sharing threat information among distinct ELASTIC instances



In-network Application Data Fabric Placement

In-network Application Data Fabric

Data-oriented enablers provided by the network platform.
Service to applications. Integrated with network assets.



Value and Trust



- Useful abstractions
 - Infrastructure with observability
 - Transfer efficiency
 - Usable security
 - Network features
- Strong channel and data security
 - Isolated processing
 - Trusted infrastructure
 - Baseline security and Zero Trust

In-network Application Data Fabric

Enablers



Transfer



Discovery, brokering,
transfer enhancements

Interoperability & integration



Transformations,
metadata, data ops

Primary ELASTIC Scope

Observability



Troubleshooting,
performance, compliance

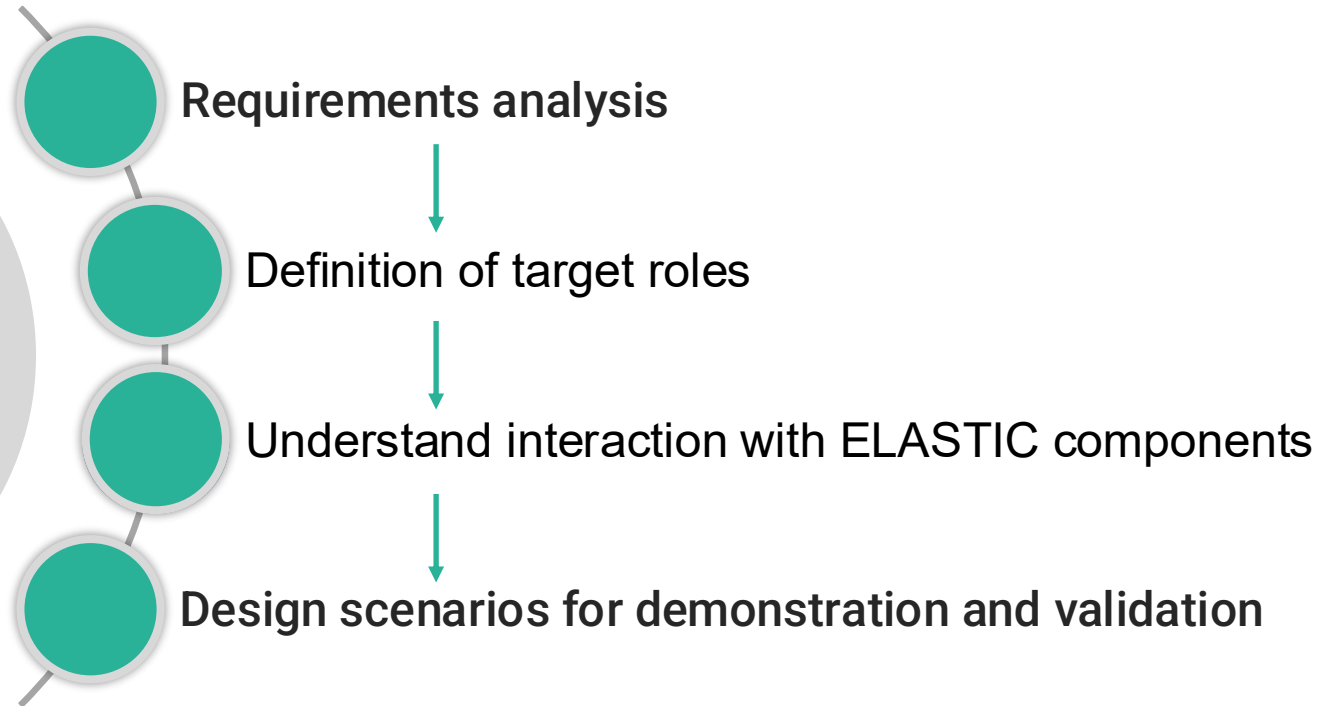
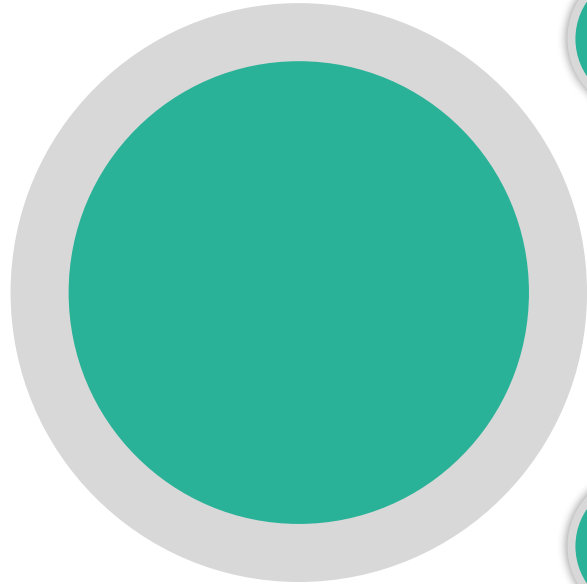
Security



Secure data, provenance,
authentication & access

Use cases, target roles, and ELASTIC components

Approach



What are key industry technical goals manufacturers strive for?



Quality	Sustainability	Flexibility	Productivity	Mobility	Utilization	Safety
Quality rates the degree to which the output of the production process meets the requirements.	Sustainability describes the level to which the creation of manufactured products is fulfilled by processes that are nonpolluting, conserve energy and natural resources.	Flexibility describes the ability to process many different parts within the manufacturing system with minimum engineering effort and changeover time.	Productivity is a measure of manufacturing system or process output per unit of input, over a specific period of time, used as a metric of the production and the	Mobility describes the ability of moving and replacing objects on the factory shopfloor.	Utilization describes the ratio of actual time the machine is used compared to the theoretically available time.	Safety describes the ability of a system to protect the operator from harm or accidents.



Hexa-X-II Use Case Families

Cooperating Mobile Robots

Autonomous Embodied Agents
Within Flexible Manufacturing

Network Assisted Mobility

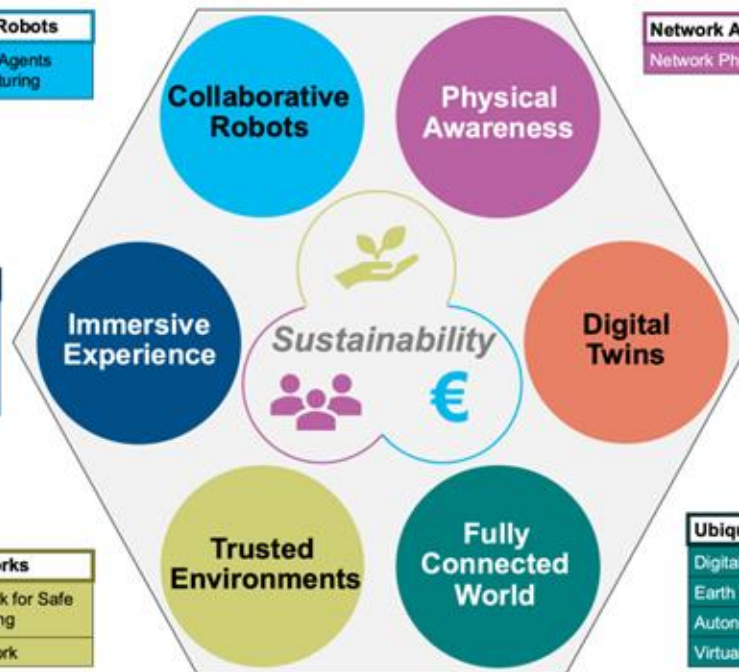
Network Physical Data Exposure

Seamless Immersive Reality

Immersive Education
Immersive Gaming
Live and Interactive Immersive
Content Creation

Human-Centric Networks

Industrial Sensors Network for Safe
Production & Manufacturing
Wireless In-Vehicle Network



Realtime Digital Twins

Cloud Continuum
Smart Maintenance
Digital Twins (Building Model)

Ubiquitous Network

Digital Sobriety and Enhanced Awareness
Earth Monitor, Sustainable Food Production
Autonomous Supply Chain
Virtualization of Device Functionalities

Hexa-X-II Use Cases with **Highlighted** Representative Use Cases

Technical roles



Industrial environment specific stakeholders

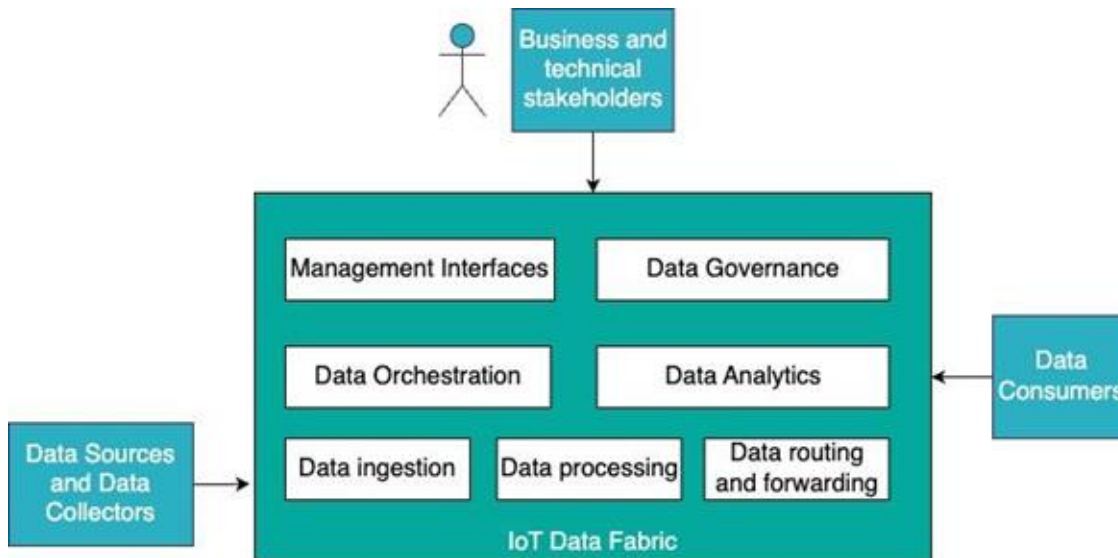
- Concerned with the overall objectives of operating the factory
- E.g., Factory Manager, Maintenance Engineer, Production Planner, Compliance Officer



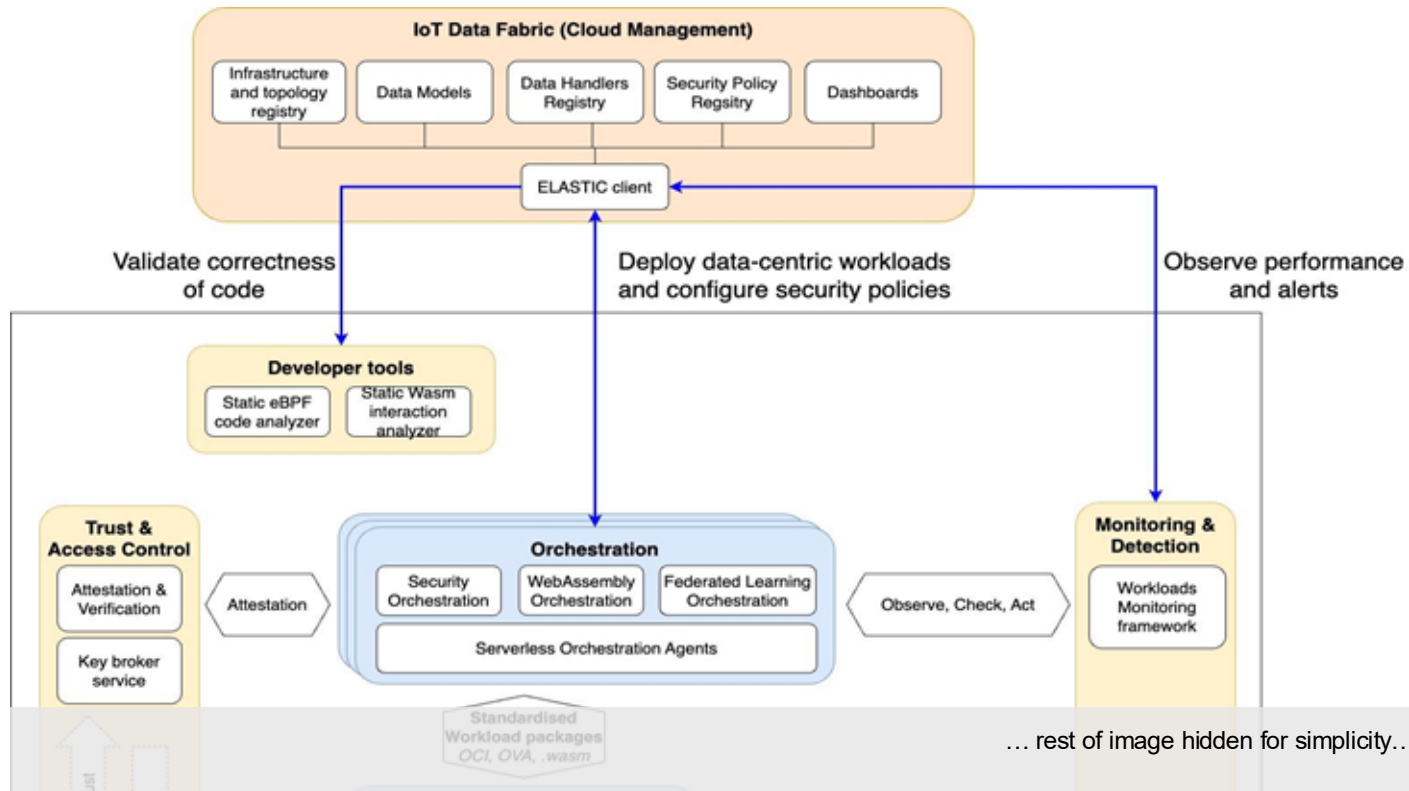
Cross-cutting technical stakeholders

- General roles which apply to the "Smart Connected Factory" but also beyond
- E.g.: Security specialist, data scientist, DevOps engineer, Robotics engineer

High-level Demonstrator System Context



How Demonstrator uses ELASTIC (Conceptual view)



Demonstrator Scenarios

Demonstrator Scenario #1

Predictive Maintenance

Description and purpose

- Enable secure, near real-time analysis of machine sensor data while maintaining data sovereignty
- Process equipment health indicators locally through WebAssembly-based functions and TEEs
- Allow maintenance teams to identify potential failures before they occur without exposing sensitive operational data

Target roles

- Maintenance Engineer
- Plant Operator
- Security Specialist
- Data Scientist
- Platform Engineer
- DevOps Engineer

Key components

- WasmHAL Hardware
- Wasm-operator
- Propeller Orchestrator
- TEE Software Management Agent
- AI Intrusion Detection
- eBPF Observability Framework
- Multi-platform Attestation
- NETTO

Demonstrator Scenario #2

Cross-factory data sharing

Description and purpose

- Enable controlled sharing of equipment and business metrics through federated computation
- Maintain strict data sovereignty through attribute-based access control policies
- Facilitate policy-driven collaborative analytics between autonomous manufacturing facilities

Target roles

- Factory Manager
- Data Integration Specialist
- Compliance Officer
- Production Planner

Key components

- Federated Learning Toolbox
- Lightweight security orchestrator for Edge
- Light-weight ABAC Solution
- Data Protection at-rest with TEE + Hardware-based Cryptography
- Multi-platform Attestation

Demonstrator Scenario #3

#Real time robot control

Description and purpose

- Demonstrate deterministic processing capabilities with comprehensive safety validation
- Leverage eBPF-based network optimizations to minimize communication latency
- Use secure WebAssembly runtime management and formal verification for safe, reliable robot control

Target roles

- Robotics Engineer
- Security Specialist
- Control Systems Specialist

Key components

- WASI Security
- Accelerated Microservice
- eBPF Distributed State Sync
- Static Wasm Analysis
- Static eBPF code analyser
- Reliable Enclave Migration
- NETTO

MVP Demo

Scenario 1 – Predictive Maintenance

ELASTIC Components in Demo

Component Name / Function	Architecture Block	Key roles
Static eBPF code analyser (POLITO)	Developer tools	DevOps Engineer
Security policy configuration (ERF)	Demonstrator	Security specialist
Multi-platform Attestation (ERF)	Trust and Access Control	Security specialist, DevOps Engineer
Data collection, data processing, data consumption (ERF)	Demonstrator (Isolation - Wasm workloads)	Data Scientist, Data Integration Specialist Maintenance engineer
Propeller Orchestrator (AMA)	Orchestration, Communication	DevOps Engineer, Platform Engineer
eBPF Observability Framework (ERF)	Monitoring and Detection (Orchestration - Serverless, Isolation - Wasm workloads)	Platform Engineer
NETTO (POLITO)	Monitoring and Detection	Platform Engineer
AI Intrusion Detection (TUC)	Monitoring and Detection	Security specialist

Demo journey


DevOps
Engineer

Setup infrastructure and
CI/CD pipelines

1


Data Scientist, Data
Integration Specialist
(Robotics Engineer)

2

Develop eBPF and
Wasm code


Security
specialist

3

Configure trust policies

Enable secure
data handling

4

4


5

Enable data
collection

6

Configure / deploy
data processing


7


Maintenance engineer
(Production Planner)

Consume data

8

Monitor system - alerts,
warnings, recommendations


Plant Operator, Platform Engineer
(Factory Manager, Production
Planner, Compliance Officer)

Demo journey


DevOps
Engineer

Setup infrastructure and
CI/CD pipelines

1

(1)
Preparation step (pre-requisite)

Data Scientist, Data
Integrat
(Robo

Develop eBPF and
Wasm code

Configure trust policies

6

Configure / deploy
data processing

5

Enable data
collection

Monitor system - alerts,
warnings, recommendations

7

Consume data

8

Plant Operator, Platform Engineer
(Factory Manager, Production
Planner, Compliance Officer)

Maintenance engineer
(Production Planner)

Demo journey

DevOps Engineer

Setup infrastructure and CI/CD pipelines

1

Data Scientist, Data Integration Specialist (Robotics Engineer)



2

Develop eBPF and Wasm code

(2)

Static eBPF code analyser (POLITO)
Developer tools

Configure trust policies (ABAC)

6

Configure / deploy data processing

5

Enable data collection

Monitor system - alerts, warnings, recommendations

7

Consume data

8

Plant Operator, Platform Engineer (Factory Manager, Production Planner, Compliance Officer)

Maintenance engineer (Production Planner)

Demo journey

DevOps Engineer

Setup infrastructure and CI/CD pipelines

1

Data Scientist, Data Integration Specialist (Robotics Engineer)



2

Develop eBPF and Wasm code

Security specialist

3

Configure trust policies

Enable secure data handling

4

4

6

Configure / deploy data processing

(3)

Demonstrator (ERF) currently

Future work : ELASTIC components in Orchestration and Isolation

7

Maintenance engineer (Production Planner)

Consume data

Plant Operator, Platform Engineer (Factory Manager, Production Planner, Compliance Officer)

Demo journey

DevOps Engineer

Setup infrastructure and CI/CD pipelines

1

Data Scientist, Data Integration Specialist (Robotics Engineer)



Security specialist

3

Enable secure data handling

4

4

Develop eBPF and Open Policy Agent policies

(4)
Multi-platform Attestation (ERF)
Trust and Access Control

5

Enable data collection

Monitor system - alerts, warnings, recommendations

8

Maintenance engineer (Production Planner)

Consume data

Plant Operator, Platform Engineer (Factory Manager, Production Planner, Compliance Officer)

Demo journey

DevOps Engineer

Setup infrastructure and CI/CD pipelines

1

Data Scientist, Data Integration Specialist (Robotics Engineer)



Security specialist



Enable secure data handling

2

Develop eBPF and Wasm code

3

Configure trust policies

4

4

(5, 6, 7)

Demonstrator (ERF) Isolation (Wasm)

Propeller Orchestrator (AMA) Orchestration, Communication

6

Configure / deploy data processing

5

Enable data collection

7

Consume data

8

Monitor system - alerts, warnings, recommendations

Maintenance engineer (Production Planner)



Plant Operator, Platform Engineer (Factory Manager, Production Planner, Compliance Officer)

Demo journey

DevOps Engineer

Setup infrastructure and CI/CD pipelines

1

Data Scientist, Data Integration Specialist

Security Specialist

Enable secure data handling

(8)

eBPF Observability Framework (ERF)
Monitoring and Detection
(Orchestration, Isolation)

NETTO (POLITO)
Monitoring and Detection

AI Intrusion Detection (TUC)
Monitoring and Detection

4

5

Enable data collection

Monitor system - alerts, warnings, recommendations

8

Maintenance engineer (Production Planner)
Consume data

Plant Operator, Platform Engineer
(Factory Manager, Production Planner, Compliance Officer)

Future work & Challenges

- Continue the integration of the various scenarios and components into Demonstrator #1
- Start gathering qualitative feedback from Ericsson factory stakeholders based on MVP

Scenario #1 - Systemize MVP and integrate remaining components



Scenario #2 – Focus on data sets



Scenario #3 – Start constructing detailed flows on the demonstration scenario



Challenges / Risks

Scenario #2 – Security orchestration integration

Scenario #3 – Realtime requirements may prove to be challenging



Efficient, portable And Secure orchesTration for reliable servICes

Demonstrator-2

*IT/OT - Privacy-preserving confidential computing platform
to migrate on-premise sensitive IT services to the cloud*

Thales DIS France SAS (THD)

Demo#2 use case overview

Migration of a sensitive IT service from on-premise to public cloud

Badge Request Tool (BRT)

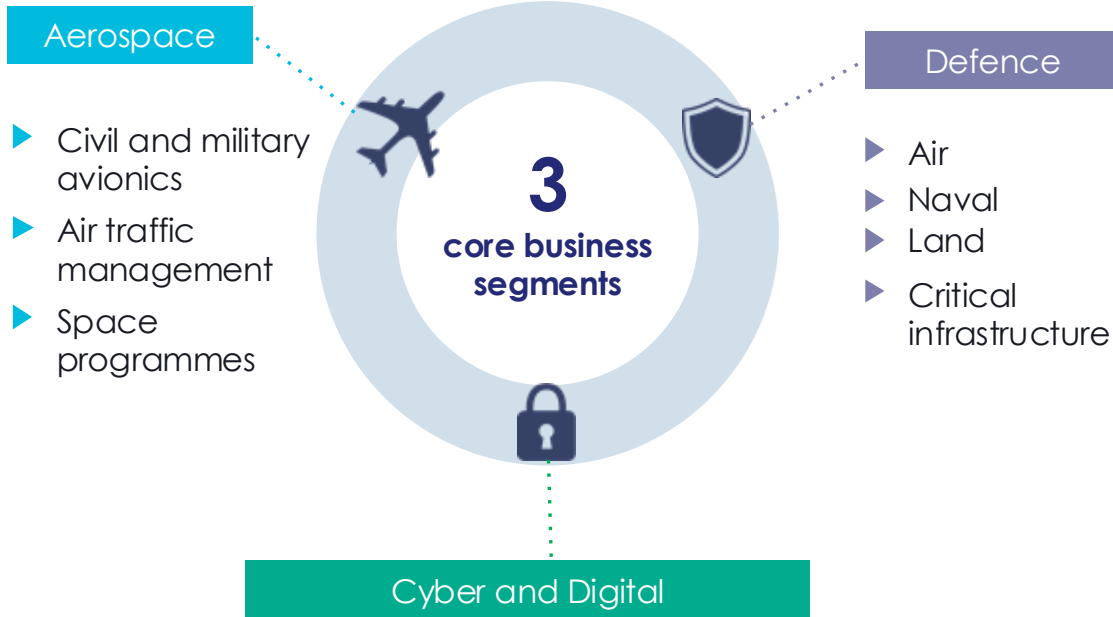
Typical on-premise service difficult to move to the Cloud

Include Personal Data of all employees

Cornerstone of Company Access Control



Thales: Building a future we can all trust



Cyber and Digital

- Cyber risk evaluation and threat protection
- Identity and access management
- Training, consulting & simulation
- Integration services
- Data security
- Threat detection & response
- Application security
- Managed security services

**SECURING THE MOST CRITICAL ASSETS:
PEOPLE'S AND OBJECTS' IDENTITIES,
DATA AND APPLICATIONS THEY RELY ON**

Move to Cloud: Many unresolved challenges

Moving more and more workloads to the Public Cloud is quite appealing



Many benefits

- Better scalability
- Performance Optimization
- Cost efficiency



Difficult to achieve with sensitive application

- Intellectual Property
- Know-How
- Regulations constraints



TEE-based solutions still maturing

- Lack of interoperability
- Proprietary implementation

How ELASTIC will help

By providing many innovative components as part of the ELASTIC Technology Stack

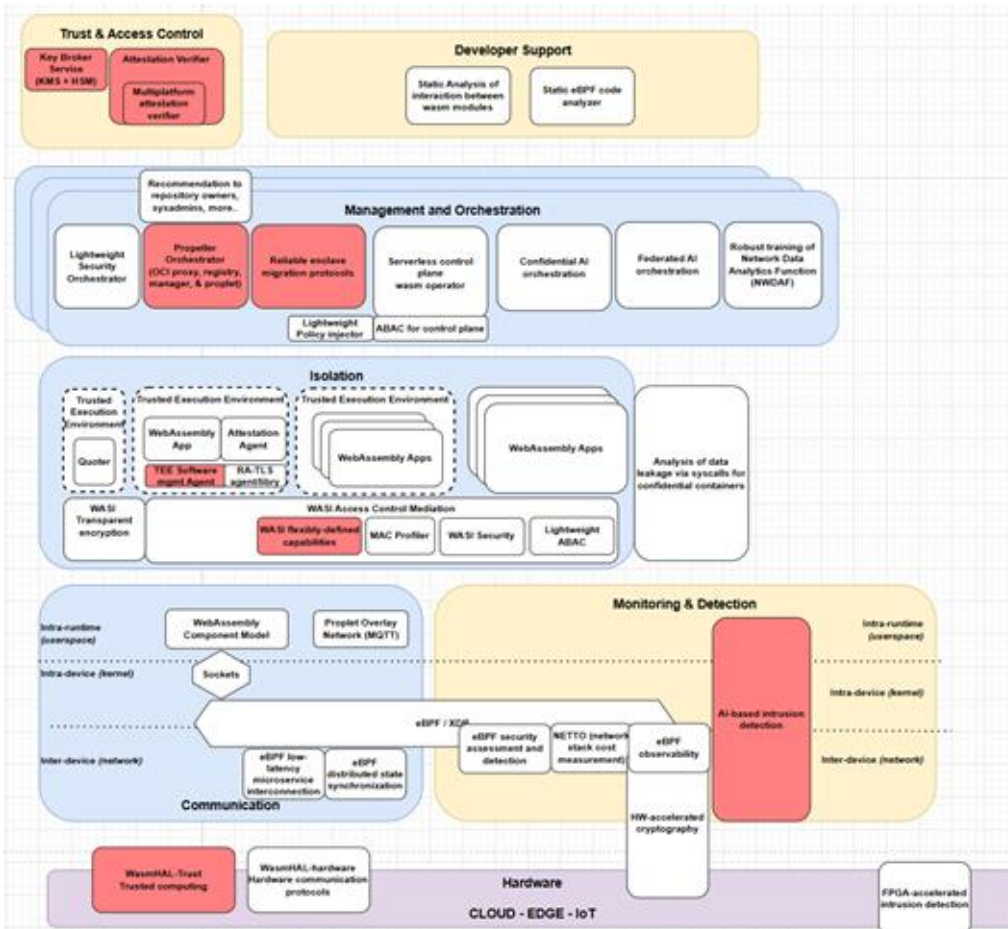
- TEE Software Management Agent
- Propeller Orchestrator
- WASI flexibly-defined capabilities
- AI-based Intrusion Detection System
- Remote Attestation Platform (RAP)
- Key Broker Service (KBS)
- WasmHAL-Trust
- Reliable Enclave Migration Protocol



ELASTIC Vision

Secure, portable and efficient orchestration of services across heterogenous infrastructure leveraging TEEs HW and Wasm Runtime

ELASTIC architecture for Demo#2



THD and ELASTIC vision alignment

Validate ELASTIC vision

using an actual use case

with no satisfactory solution

having strong regulation

and security constraints

Improve SOTA

using a technology stack

working with any TEE technology

any Cloud Service Provider

offering secure and reliable migration

Thales DIS



elastic



Thales DIS

A phased development

1 A MVP for the Mid-term project review

Objective: Showcase the current progress in the development of the different components and their integration.

What:

- Deployment of BRT application within an attested-TEE
- Demoing some early component integration

How:

- A subset of already available components

Where:

- In staging infrastructure

2 Full final Demo#2 use case at Final project review

Objective: Showcase the use of the ELASTIC Technology stack in the context of a real scenario

What:

- Full migration Flow from on-premise to Cloud

How:

- Using all ELASTIC components identified

Where:

- In staging infrastructure
- In THD infrastructure

Two deployment environments

Staging Infrastructure (UVC)

Open to all partners for components development and integration

Support full migration flow

Actionable and reusable artifacts

Cloud Infrastructure (THD)

ELASTIC stack validation in a production-grade environment

Support full migration

Demonstrate multi-TEE support

Envisioned impact on Industry

01

Acceleration of move to cloud for sensitive payloads

By making it easier while ensuring strong security properties
By helping with regulation constraints
By improving business agility

02

Improvement of Sovereignty

By using an open stack working with several TEE technology
By reducing dependencies with Cloud Provider's implementation

03

Increase of Wasm maturity

By contributing to W3C WASI
By improving stickiness of Wasm with existing ecosystem



Efficient, portable And Secure orchesTration for reliable servICes

WP6: Dissemination, Standardisation, and Exploitation

Leader: ZEN

Contributors: ALL

WP6 Contribution to Project Objectives

WP6 contributes directly to **Project Objective 5 (O5): Dissemination, standardisation, and exploitation of orchestration technologies.**

Communication and dissemination activities maximise visibility across communities.



Ecosystem engagement and stakeholder mapping expand adoption pathways.

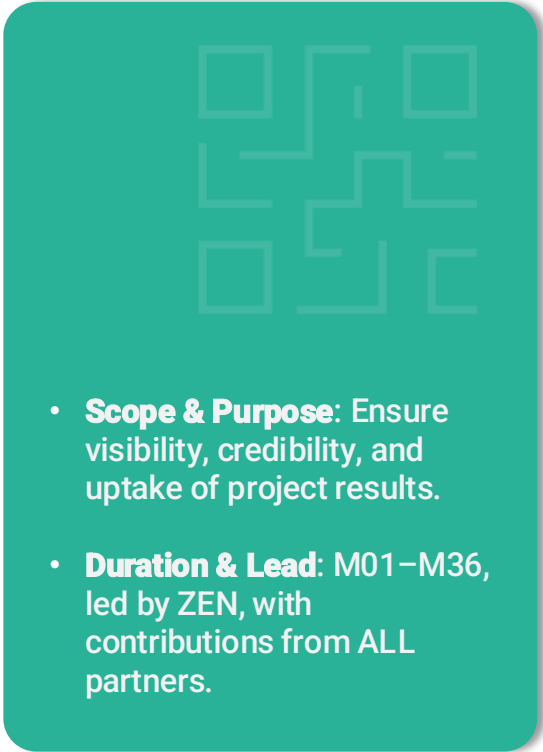


Scientific dissemination and standardisation boost credibility and speed uptake.



Exploitation activities (KERs, IPR) prepare long-term sustainability.



- 
- A teal-colored rounded rectangle containing a faint QR code in the upper half and a bulleted list in the lower half.
- **Scope & Purpose:** Ensure visibility, credibility, and uptake of project results.
 - **Duration & Lead:** M01–M36, led by ZEN, with contributions from ALL partners.

Task 6.1

Communication & Dissemination Plan, Assets, Materials and Activities

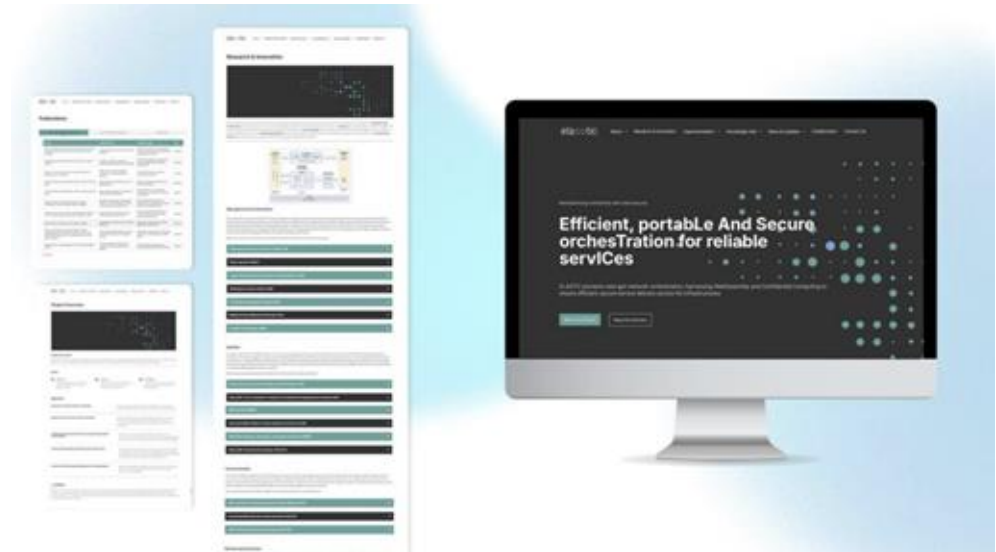
Lead: ZEN

Participants: all partners

ELASTIC Website

Key results achieved

- ✓ Serves as the **primary access point** for stakeholders (research, industry, policy)
- ✓ 2.2K unique visitors, 4.6K visits
- ✓ 53 posts published
- ✓ Hosts **newsletters, press releases, brochures, flyers, posters, and videos**
- ✓ Integrates with social media channels for consistent outreach
- ✓ **Supports analytics tracking** to monitor visitors and engagement
- ✓ Fully **GDPR compliant** and **SEO optimised**



Key results achieved

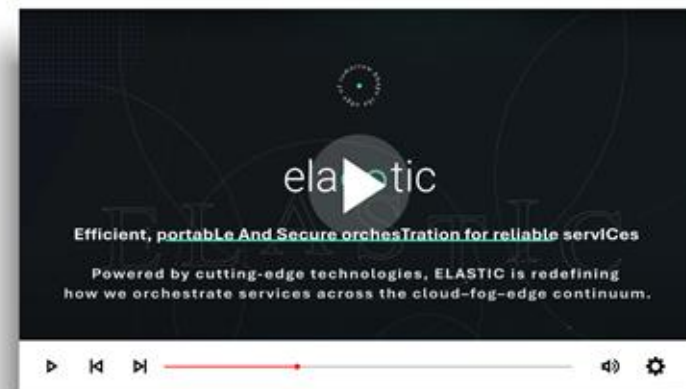
- ✓ **Regular posts and updates** across all platforms, covering project news, activities, and campaigns.
- ✓ Growth in followers and engagement across channels during the first reporting period.
- ✓ **Strong visibility** for project outputs through multimedia content (images, videos, infographics).
- ✓ Cross-promotion with project partners and SNS JU accounts to **boost reach**.
- ✓ Supports **analytics monitoring** for post performance and audience engagement.

Channel	Followers	No of Impressions	No of posts
LinkedIn	427	37,400	48
X	68	4,837	39
Instagram	33	926 reach	29
Bluesky	27	N/A	8
YouTube	37	114 views	1 video

ELASTIC Project Video

Key results achieved

- ✓ Provides a clear and engaging **introduction to the project.**
- ✓ Serves as a **reusable asset** for presentations, events, and online promotion.
- ✓ Published on the ELASTIC website, YouTube, and promoted via social media channels.
- ✓ Supports **outreach** to wider audiences beyond the research community.



[CLICK HERE TO WATCH](#)

ELASTIC Project Newsletters & Press Releases

Key results achieved

- ✓ **3 newsletters** published – covering consortium news, technical updates, events, and partner activities. Distributed through **mailing lists** and project channels, available on the **ELASTIC website** for open access and long-term visibility.
- ✓ **2 press releases** issued – focused on **project launch** and early achievements. Disseminated via the website, social media, and partner networks, reaching **media, policymakers, and wider 6G audiences**.

ELASTIC Project Campaigns

Key results achieved

- ✓ **Meet the Partners** – introduced consortium members and their roles, increasing recognition of partner expertise.
- ✓ **Project Spotlights** – showcased milestones, activities, and technical progress across WPs.
- ✓ **Women in STEAM** – promoted the role of women in science, technology, engineering, arts, and mathematics, fostering diversity and inclusivity.
- ✓ **Did You Know?** – shared engaging facts and insights about 6G, security, and edge-cloud orchestration.
- ✓ **Publications Promotion** – highlighted and disseminated ELASTIC's scientific papers through posts, newsletters, and Zenodo for open access.

ELASTIC Project Campaigns

Technical University of Crete elastic

“ Technical University of Crete plays a pivotal role as the Project Coordinator for ELASTIC, a project that aims to redefine service orchestration within 6G networks. By integrating cutting-edge technologies such as WebAssembly and Confidential Computing, ELASTIC seeks to enhance network functionality and bolster security across diverse infrastructures. ”

Prof. Sotiris Ioannidis
Project Coordinator

Despina Katsani
Project Manager

Dr. Gregory Christos
Functional Researcher

BSNS

elastic

Jasmina Vesic

Marketing & Communications, Zenitix Lab

“The way we communicate ideas shapes how they are understood and embraced. Marketing and creativity bridge the gap between technology and people, making innovation more accessible and impactful. When diverse perspectives influence this process, we open the door to fresh ideas, stronger connections, and meaningful change.”

BSNS

elastic

Jasmina Vesic

Marketing & Communications, Zenitix Lab

“The way we communicate ideas shapes how they are understood and embraced. Marketing and creativity bridge the gap between technology and people, making innovation more accessible and impactful. When diverse perspectives influence this process, we open the door to fresh ideas, stronger connections, and meaningful change.”

BSNS

“Meet the Partners” Campaign

“Women in STEAM” Campaign

elastic

Did You Know?

The ELASTIC project is improving 6G networks by using technologies like WebAssembly and Confidential Computing.

It's focused on making networks more efficient and secure, ensuring data protection while meeting the needs of modern connectivity.

BSNS

elastic

Securing Stack Smashing Protection in WebAssembly Applications

BSNS

elastic

Exploring Crisis-Driven Social Media Patterns: A Twitter Dataset of Usage During the Russia-Ukraine War

BSNS

“Did you know” Campaign

Publication promotion

Promotional and Printed Materials

Key results achieved

- ✓ **Digital materials:** brochure, flyer, poster, roll-up banner, project video, all aligned with the ELASTIC visual identity and published on the website and Zenodo.
- ✓ **Printed and distributed:** 100 flyers, 100 brochures, 25 notebooks, 250 pens, 75 t-shirts, 200 luggage tags, 50 business cards, 1 roll-up banner, 1 poster.
- ✓ **Total:** 802 printed items distributed
- ✓ **Digital downloads:** 928 (posters, brochures, roll-up) via Zenodo.
- ✓ Materials actively used at consortium meetings and major events, such as **EuCNC & 6G Summit 2025**.

Promotional and Printed Materials

elastic

ELASTIC Consortium

Project Description
Your future services. Today's complexity of IT environments.

Start in ELASTIC
Participating Organizations
Learn more
Follow Us

ELASTIC - Efficient, portable And Secure orchestration for reliable services

ELASTIC pioneers next-gen network orchestration, harnessing heterogeneity and Composable Orchestration to ensure efficient, secure service delivery across 5G architectures.

Why ELASTIC?

ELASTIC aims to enhance the efficiency and versatility of service orchestration of the highly distributed and heterogeneous nature of 5G edge networks, enabling consistent QoS in a wide range of scenarios, including edge computing and security services, across a variety of service environments and security use cases.

ELASTIC Benefits

- Optimize resource systems for secure, efficient, and portable in-network cloud and edge computing.
- Design a secure, architecture-agnostic, fault-tolerant framework for managing artifacts and ensuring trusted interactions.
- Implement efficient, secure orchestration for 5G and edge workloads within 5G architectures.
- Process 4G/5G applications and distributed 4G/5G edge-based service scenarios.

ELASTIC impact

- Enables efficient and secure orchestration for 5G architectures, enabling Composable Orchestration and efficient, portable, and secure service delivery across 5G architectures.
- Enables efficient and secure orchestration for 5G architectures, enabling Composable Orchestration and efficient, portable, and secure service delivery across 5G architectures.
- Enables efficient and secure orchestration for 5G architectures, enabling Composable Orchestration and efficient, portable, and secure service delivery across 5G architectures.

ELASTIC Functionalities

- High efficiency and security of cloud orchestration
- High service portability
- Support a variety of programming languages
- Lightweight computation

ELASTIC Plans

- Smart Connected Factory of the Future
- Privacy-Preserving IT Service Migration

ELASTIC Benefits

- Design a secure, architecture-agnostic, fault-tolerant framework for managing artifacts and ensuring trusted interactions.
- Optimize resource systems for secure, efficient, and portable in-network cloud and edge computing.
- Develop privacy-preserving orchestration environments with composable orchestration and 5G.

ELASTIC Functionalities

- High efficiency and security of cloud orchestration
- High service portability
- Support a variety of programming languages
- Lightweight computation

ELASTIC Demonstrators

- Smart Connected Factory of the Future
- Privacy-Preserving IT Service Migration

The ELASTIC framework combines these functionalities across a cluster-based environment.

ELASTIC Consortium

Stay Updated

ELASTIC Consortium

Stay Updated

ELASTIC Benefits

- Design a secure, architecture-agnostic, fault-tolerant framework for managing artifacts and ensuring trusted interactions.
- Optimize resource systems for secure, efficient, and portable in-network cloud and edge computing.
- Develop privacy-preserving orchestration environments with composable orchestration and 5G.

ELASTIC Functionalities

- High efficiency and security of cloud orchestration
- High service portability
- Support a variety of programming languages
- Lightweight computation

ELASTIC Demonstrators

- Smart Connected Factory of the Future
- Privacy-Preserving IT Service Migration

ELASTIC Consortium

Stay Updated

ELASTIC Consortium

Stay Updated

ELASTIC Benefits

- Design a secure, architecture-agnostic, fault-tolerant framework for managing artifacts and ensuring trusted interactions.
- Optimize resource systems for secure, efficient, and portable in-network cloud and edge computing.
- Develop privacy-preserving orchestration environments with composable orchestration and 5G.

ELASTIC Functionalities

- High efficiency and security of cloud orchestration
- High service portability
- Support a variety of programming languages
- Lightweight computation

ELASTIC Demonstrators

- Smart Connected Factory of the Future
- Privacy-Preserving IT Service Migration

ELASTIC Consortium

Stay Updated

ELASTIC Consortium

Stay Updated

ELASTIC brochure

ELASTIC poster

ELASTIC rollup

ELASTIC flyer

Promotional and Printed Materials



Notebooks & brochures



Luggage tags



T-shirts



Brochures and pens

ELASTIC Visual Identity

Key results achieved

- ✓ Project **logo** and **color palette** defined and applied across all materials.
- ✓ **Templates** for deliverables, presentations, posters, and reports created and shared.
- ✓ **Guidelines** established to harmonise the look and feel of the website, social media posts, and printed materials.
- ✓ Visual identity ensured a **coherent and professional image** for ELASTIC in all channels.



ELASTIC logo – different variations

Task 6.2

Ecosystem Bootstrap and Expansion

Lead: ZEN

Participants: all partners

Stakeholder Mapping

Key results achieved



Stakeholders grouped into categories: **research and academia, industry and SMEs, policymakers and standardization bodies, end-user communities, and innovation ecosystems.**



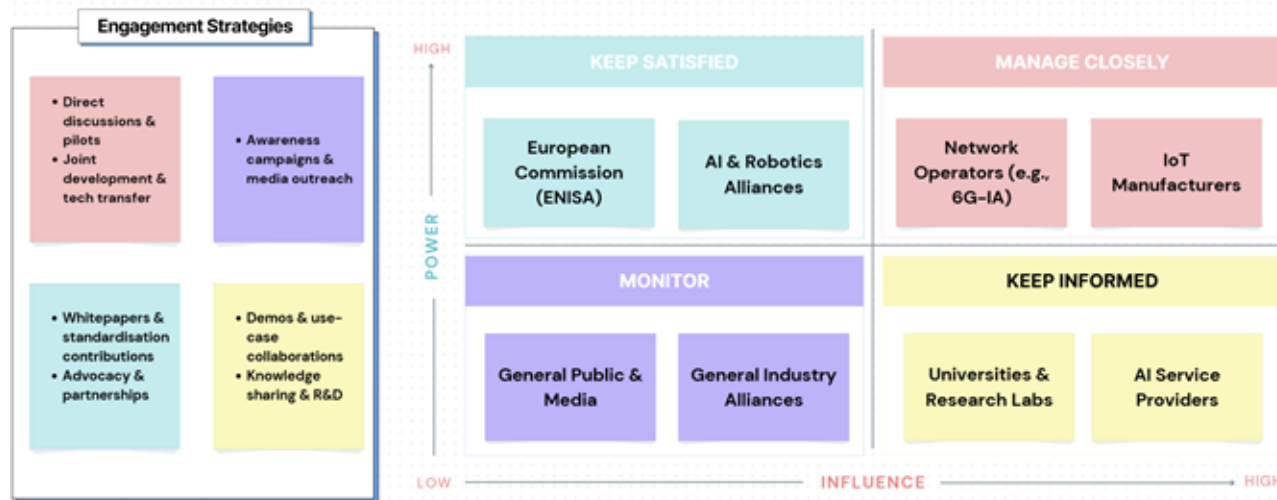
Database created with entries covering **contact points**, relevance to ELASTIC, and potential engagement opportunities.



Mapping serves as a **reference framework** for targeted communication, ecosystem-building, and clustering activities.

Stakeholder Mapping Canvas

Stakeholder Mapping



- **Manage Closely:** high-power stakeholders like network operators and IoT manufacturers, prioritized for intensive collaboration.
- **Keep Satisfied:** policy actors (EC, ENISA) and alliances with strong influence, requiring regular updates and proof of impact.
- **Keep Informed:** universities, research labs, and AI providers, important for validation and early uptake, need consistent engagement.
- **Monitor:** general public, media, and broad alliances, with an indirect role in awareness and trust-building.

ELASTIC Stakeholder Mapping

ELASTIC External Expert Advisory Board

Key results achieved

- ✓ **First meeting** held virtually with experts from academia, industry, and cybersecurity.
- ✓ **Reviewed** architecture and security requirements.

Key insights:

- Improve modularity in architecture.
- Align cybersecurity with industry best practices.
- Explore standardisation pathways.
- Prioritise use cases and pilots

Name	Affiliation	Expertise
Mike Bursell	Director, P2P Consulting & Development Ltd	Cybersecurity, Confidential Computing
Vera Stavroulaki	Co-Owner & Technology Developer, WINGS ICT Solutions (Greece)	ICT Solutions, Innovation
Antonio Escobar	Senior R&D Engineer, Infineon Technologies (Germany)	Hardware Security, Semiconductors
Stefano Salsano	Professor, University of Rome Tor Vergata (Italy)	Networks, Architecture Design

ELASTIC Zenodo Community

The ELASTIC Zenodo Community was established as the central hub for open-access results. The repository ensures compliance with open science principles and provides full traceability of outputs, with TUC responsible for its maintenance and coordination of partner contributions.

Metric	Count	Notes
Uploads	29	Deliverables, publications, promotional materials, presentations
Downloads	2,875+	Includes deliverables, brochures, posters, publications...
Views	616+	Accessed by researchers, policymakers, and industry stakeholders

Collaboration with EU Projects & SNS JU Participation

Key results achieved



Representation in **SNS JU clusters** on Security, Architecture, Orchestration, and Edge Computing.



Collaboration with related EU projects on dissemination and ecosystem-building activities.



Contribution to **joint SNS JU workshops and clustering events**, showcasing ELASTIC use cases and approaches.



Exchange of best practices with **partners from across the 6G community**, strengthening visibility and sustainability.

ELASTIC Participation in SNS JU & 6G-IA Working Groups

Boards	Focus Area	ELASTIC Contribution / Role	Partner(s)
SNS JU Steering Board	Programme governance	Strategic input at high-level discussions	TUC
SNS JU Technical Board	Technical priorities for SNS	Input on technical directions	THS
SNS JU Communication Task Force	Joint communication & outreach	Coordinated dissemination across projects	ZEN
Working Group	Focus Area	ELASTIC Contribution / Role	Partner(s)
6G-IA Security WG	Security challenges in 6G	WG leadership (Dr. Dhouha Ayed)	THS
6G-IA Architecture WG	Architectural frameworks	Contributions to 6G architecture	THS, TUC
6G-IA Hardware Technologies WG	Hardware enablers for 6G	Input on hardware needs	AMA, TUC
6G-IA TMV WG	Test, Measurement, Validation	Focus on data reusability	TUC
6G-IA Pre-Standardisation WG	Early standards alignment	Standardisation contributions	AAL
6G-IA WiTaR WG	White Papers, Trials, Recommendations	Input to trials and recommendations	TUC
6G-IA SNWG (AI/ML)	Software networking, AI/ML	Contributions on orchestration & AI	ZEN

AI & SECURITY Webinar

- **AI & Security Webinar** attracted **125+ participants** from academia, industry, and policy.
- Featured talks on **secure orchestration, AI-driven resilience**, and **privacy-preserving technologies**.
- Organised with **CONFIDENTIAL6G, HARPOCRATES, RIGUROUS, and PREDICT-6G**, with support from **FAITH, CUSTODES, and 6G-Cloud**.
- Strengthened collaboration across the **SNS JU security ecosystem**, boosting ELASTIC's 6G visibility.

ELASTIC contribution:

IMEC's talk *"Resilient Cyber-Physical Devices with WebAssembly Sandboxing"* showed how ELASTIC applies **WebAssembly sandboxing** for secure orchestration and system resilience.



AI & SECURITY Webinar banner

ELASTIC Contribution to AI & SECURITY Webinar

elastic



AI & SECURITY Webinar: Speaker's banner



Registration banner



Online Booklet

Presentation slides from all speakers are available on **Zenodo**.

[Link to slides](#)

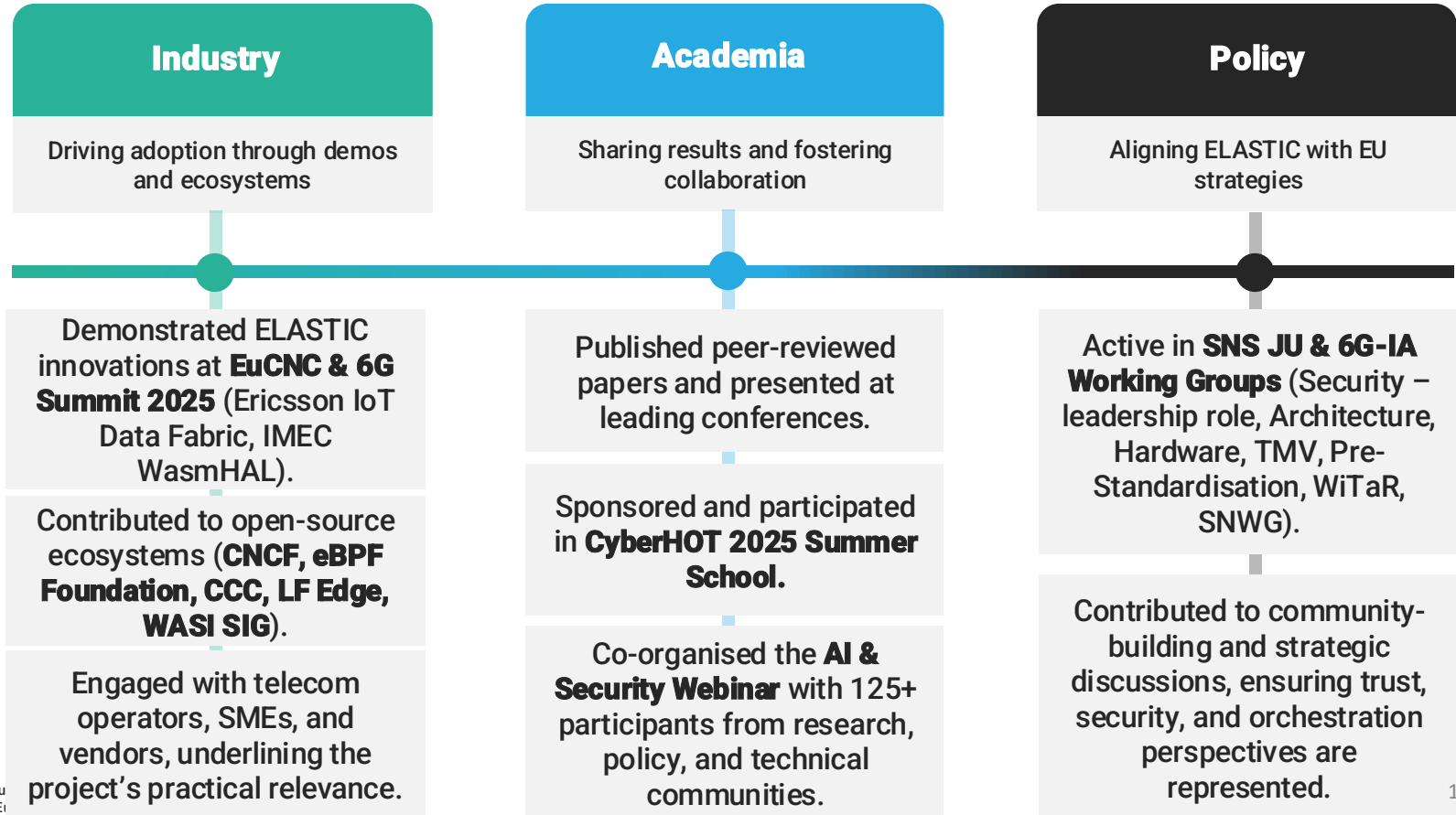
Webinar recordings have been uploaded to the **AI & Security YouTube channel** for open access.

[Webinar recordings](#)

A **dedicated newsletter** was published to promote the webinar.

[Link to newsletter](#)

Engagement with Policymakers, Academia & Industry



Collaboration with Innovation Ecosystems

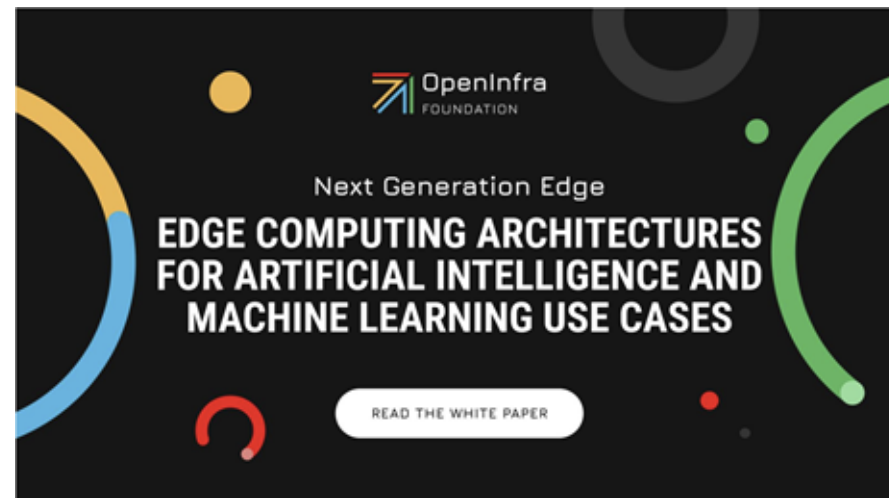
Ecosystem / Group	ELASTIC Contributions	Partners Involved
Confidential Computing Consortium (CCC)	Presented advances in confidential computing (secure workloads); showcased confidential Wasm workload protection at WasmCon 2024	LUN, UVC, AMA
Cloud Native Computing Foundation (CNCF)	Contributed to eBPF observability and Kubernetes SIGs; advanced WebAssembly/WASI at CNCF & CMU WebAssembly Research Center	POLITO, IMEC
eBPF Foundation	Advanced XDP/eBPF research on observability & network security; aligned outputs with standardisation discussions	POLITO
LF Edge & OpenInfra Edge WG (OSF)	Co-authored “Edge Architectures for AI & ML” white paper , aligning ELASTIC orchestration with global edge roadmaps	ZEN, TUC
WebAssembly Communities (WASI SIG, WG)	Promoted cyber-physical WebAssembly security via workshops, meetings, and public presentations	IMEC

White Paper – Edge Architectures for AI & ML

ELASTIC partners **ZEN & TUC** co-authored a white paper within the **LF Edge & OpenInfra Edge WG**, outlining architectural considerations for AI/ML integration at the edge.

Key results achieved

- ✓ Published as part of global **OpenInfra collaboration**.
- ✓ Showcases ELASTIC's expertise in **orchestration and edge computing**.
- ✓ Provides concrete recommendations for **AI-enabled edge orchestration**.
- ✓ Strengthens ELASTIC's role in shaping **global edge computing standards**.



[Link to white paper](#)

Task 6.3

Engaging the Scientific Community and Standardisation

Lead: AAL

Participants: all partners

Standardisation and Open-Source Contributions

Standardisation is central to ELASTIC, ensuring results are aligned with existing frameworks, interoperable across systems, and positioned for long-term sustainability. The consortium builds on three objectives.

1

Build on Partner Activities

Leverage existing partner activities in SDOs for continuity and visibility.

2

Coordinate Joint Contributions

Coordinate joint contributions with cross-partner relevance.

3

Expand SDO Engagement

Expand engagement with additional SDOs for stronger influence and impact.

Partner Contributions to Standards Developing Organisations

SDO (WG)	Contribution	Partner(s)	Relevance to ELASTIC
W3C (WASI)	WASI-USB (Phase 1), WASI-I2C (Phase 2), WASI-GPIO (linked to WasmHAL)	IMEC	Secure hardware integration for WebAssembly & cyber-physical systems
OASIS	Revision of CACAO v2.1 (cybersecurity playbooks)	TUC	Automation & orchestration of incident response
FIRST.org (Automation SIG)	Restarted SIG, 3 meetings on incident response automation best practices	TUC	Strengthening global practices in operational security automation
ENISA (Ad-hoc WG on SOCs)	Report on Playbooks & Automation	TUC	European standardisation of SOC automation
ETSI (NFV Security WG)	Engagement on attestation architectures & lightweight security orchestration	THD	Remote/distributed attestation; security orchestration alignment
IETF / IRTF (ASDF, CoRE, T2TRG)	Contributions on protocols & data models	ERF	Scalable in-network data processing for ELASTIC use cases
3GPP (SA1, SA2, SA3, CT6)	Contributions on network security, authentication, service architecture	ERS, THD	Secure orchestration for 6G networks

Cyber-Physical WASI interface contributions

WASI-USB for Wasm USB drivers

✓ Now in Phase 1

WASI-I2C for accessing I2C busses (e.g. sensors, TPMs)

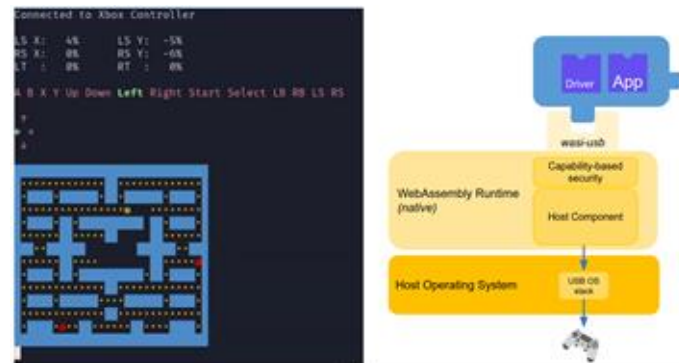
✓ Now in Phase 2

WASI-SPI for accessing SPI devices (e.g. ADCs, DACs)

✓ Now in Phase 1

WASI-GPIO for controlling GPIO pins (for nonstandard interfaces)

✓ Now in Phase 1



Xbox controller driver in wasm demo

Different areas between services and infrastructure for telecom network virtualization

- Non-functional areas of security and reliability are also covered with respect to the different functional areas.

ELASTIC members active in the Security (SEC) sub-working group of ETSI ISG NFV

- ✓ ETSI GS NFV-SEC 020 (in progress)
Identity Management and Security
- ✓ ETSI GS NFV-SEC 025 (in progress, rapporteur)
Secure E2E Virtual Network Function and Network Service management
- ✓ ETSI GS NFV-SEC 026 (recently published)
Isolation and trust domain specification

ELASTIC Open-Source Contributions (M18)

Project / Ecosystem	Contribution	Partner(s)	Impact / Relevance
Propeller Orchestrator	Lightweight Wasm orchestrator (Apache 2.0 licence)	AMA	Enables edge orchestration experimentation and feedback loop to ELASTIC
LLVM Compiler Infrastructure	Runtime safety features, Wasm optimisation flag (merged upstream), prototype Stack Smashing Protection implementation	THS	Improves Wasm security & memory safety; supports IoT workloads
Wasm Ecosystem Tools	wasm-operator (K8s operator), kube-rs patch, WASI APIs (I2C, USB, SPI, GPIO, wasi-embedded-hal)	IMEC	Extends WebAssembly usability for cyber-physical and IoT systems
TEE Hardware Abstraction Layer (wasmhal)	Open-source TEE abstraction for secure workload execution	LUN	Portable, secure execution across heterogeneous hardware
Confidential Computing Consortium (CCC)	Participation in Remote Attestation SIG, attestation practices	THD, AAL	Aligns ELASTIC results with global confidential computing practices
WasmCloud Community	Early engagement on multi-platform verification and Wasm orchestration	AAL	Embeds ELASTIC innovations in future Wasm orchestration models

Developing ELASTIC standardization activities

Workshops to help share standardization knowledge and know-how

- What does each SDO do, how do they operate, how best to contribute?
- Ongoing mentoring by more experienced contributors
- First workshop planned on ETSI (focused on NFV)
 - *Presentation of ELASTIC to ETSI NFV WG and vice-versa*
 - *Discussion of future areas of collaboration*

White-paper on Wasm & eBPF standardization (jointly with T1.4)

- What are the gaps in standardization?
- How can these gaps be filled, both by ELASTIC and post-project?

Strategy

Scientific publications are a cornerstone of ELASTIC's dissemination, ensuring visibility in academic and technical communities, fostering collaboration, and supporting development of secure and efficient 6G orchestration solutions.

Results (M18)

- ✓ **14 conference papers, 2 journal articles and 1 thesis** produced, covering TEEs, secure edge orchestration, Linux networking, and WebAssembly for cyber-physical systems.
- ✓ Additional manuscripts in preparation for high-impact journals.
- ✓ Contributions reflect **all partners' expertise**.

Impact

Publications showcase early technical results, strengthen credibility, and align ELASTIC with global research discussions.

Scientific Publications

Author(s)	Title	Venue
Stavros Eleftherakis, Timothy Otim, Giuseppe Santaromita, Almudena Diaz Zayas, Domenico Giustiniano, Nicolas Kourtellis	Demystifying Privacy in 5G Stand Alone Networks	(ACM MobiCom 2024)
Syafiq al Atiiq, Christian Gehrmann, Yacha Yuan, Jacob Sternby	AutoML in the Face of Adversity: Securing Mobility Predictions in NWDAF	(FMEC 2024)
Federico Parola, Shixiong Qi, Anvaya B. Narappa, K. K. Ramakrishnan, Fulvio Riso	SURE: Secure Unikernels Make Serverless Computing Rapid and Efficient	(SoCC'24)
Quentin Michaud, Yohan Pipereau, Olivier Levillain, Dhouha Ayed	Robust Stack Smashing Protection for WebAssembly	(FNWF 2024)
Quentin Michaud, Yohan Pipereau, Olivier Levillain, Dhouha Ayed	Securing Stack Smashing Protection in WebAssembly Applications	(PLAS 2024)
Ioannis Lamprou, Alexander Shevtsov, Despoina Antonakaki, Polyvios Pratikakis, Sotiris Ioannidis	Exploring Crisis-Driven Social Media Patterns: A Twitter Dataset of Usage During the Russo-Ukrainian War	(ASONAM 2024)
Florent Foucaud, Esther Galby, Liana Khazaliya, Shaohua Li, Fionn Mc Inerney, Roohani Sharma, Prafullkumar Tale	Metric Dimension and Geodetic Set Parameterized by Vertex Cover	(STACS 2025)

Scientific Publications

Author(s)	Title	Venue
Robert Ganian, Fionn Mc Inerney, Dimitra Tsigkari	Parameterized Complexity of Caching in Networks	(AAAI 2025)
Michiel Van Kenhove, Maximilian Seidler, Friedrich Vandenberghe, Warre Dujardin, Wouter Hennen, Arne Vogel, Merlijn Sebrechts, Tom Goethals, Filip De Turck, Bruno Volckaert	Cyber-physical WebAssembly: Secure Hardware Interfaces and Pluggable Drivers	(NOMS 2025)
Robert Ganian, Liana Khazaliya, Fionn Mc Inerney, Mathis Rocton	The Computational Complexity of Positive Non-Clashing Teaching in Graphs	(ICLR 2025)
Rosario Rizza, Riccardo Sisto, Fulvio Valenza	Design and implementation of a tool to improve error reporting for eBPF code	(CSR 2025)
Eduard Marin, Jinwoo Kim, Alessio Pavoni, Mauro Conti, Roberto Di Pietro	The Hidden Dangers of Public Serverless Repositories: An Empirical Security Assessment	(ESORICS 2025)
Syafiq Al Atiiq, Christian Gehrman, Karim Khalil, Jakob Sternby, Yachao Yuan	Resilient Automatic Model Selection for Mobility Prediction	Cluster Computing, 2025

Scientific Publications

Author(s)	Title	Venue
Stavros Eleftherakis, Domenico Giustiniano, and Nicolas Kourtellis	SoK: Evaluating 5G-Advanced Protocols Against Legacy and Emerging Privacy and Security Attack	(WiSec 2025)
Rosario Rizza, Riccardo Sisto and Fulvio Valenza	Analysis of the eBPF Vulnerabilities in the Linux Kernel	(CRISIS 2025)
Mikko A. Heikkilä	On Using Secure Aggregation in Differentially Private Federated Learning with Multiple Local Steps	Transactions on Machine Learning Research (TMLR)
Rosario Rizza, Riccardo Sisto, Fulvio Valenza	Design and implementation of a tool to improve error reporting for eBPF code	(CSR 2025)
Ghazal Shanavar	Attestation of Distributed Applications	Thesis (Aalto University)

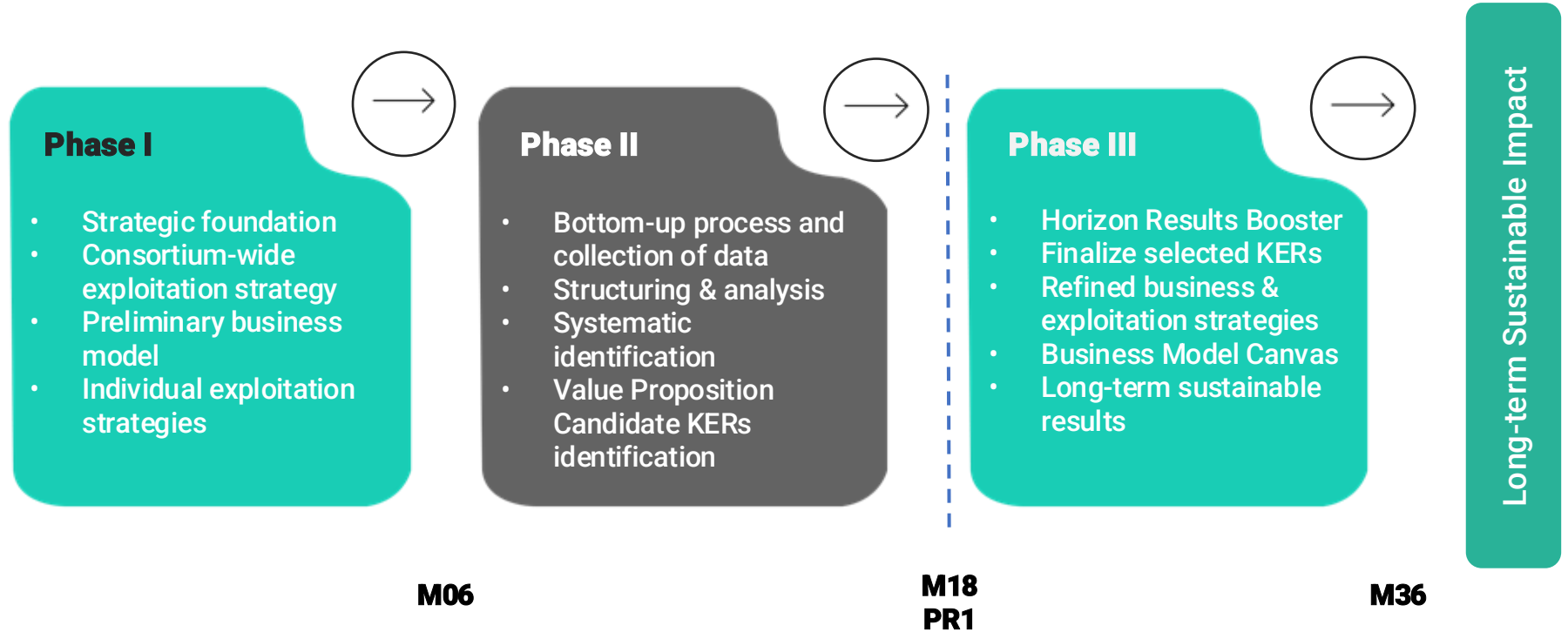
Task 6.4

Innovation Management, IPR Handling and Future Exploitation

Lead: ERS

Participants: all partners

Exploitation plan and methodology

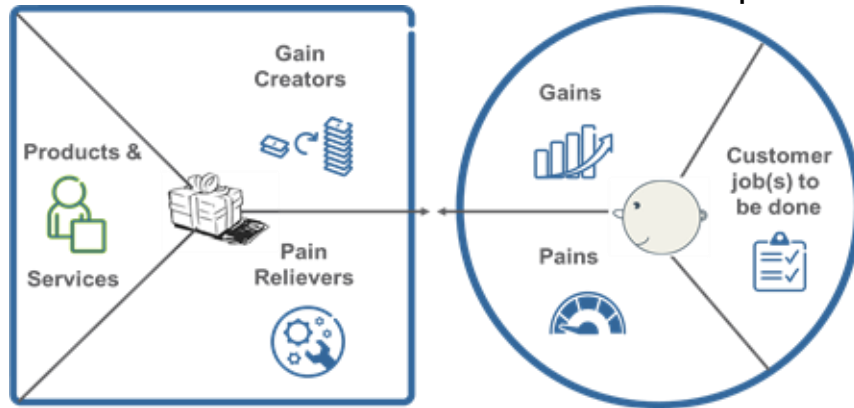


Collected information per component

Simplified view based on HRB with ELASTIC specific extensions, 26 components in total

Exploitable component data	Intellectual Property	Business	Risks & challenges
Name of result	Background IP	Customers/users	Market positioning
Partner	Protection potential	Pains of customers/users	Deployment barriers
WP and demonstrator relation	IPR protection method	Gains/benefits for customers/users	Other challenges
Current -> expected TRL	Exploitation use	Target audience	Mitigation measures
What it does		Exploitation channels	Other similar solutions, competitive landscape

Value proposition canvas



Gains: are positive outcomes customers look for or wanted experiences from a solution

JTBD:

- What is the user segment trying to get done?
- What are they trying to perform?
- What problem are they trying to solve? What needs are they trying to satisfy?

Pains: are negative effects or characteristics customers want to avoid or undesirable situations that might arise

The **Value Proposition Canvas** is the central tool when creating a value proposition and consists of two parts – the Value Map and the Customer Profile.

NB! Pains and gains are typically related, but they do not necessarily come in pairs

Value proposition – identified pains and gains

Gains and user benefits

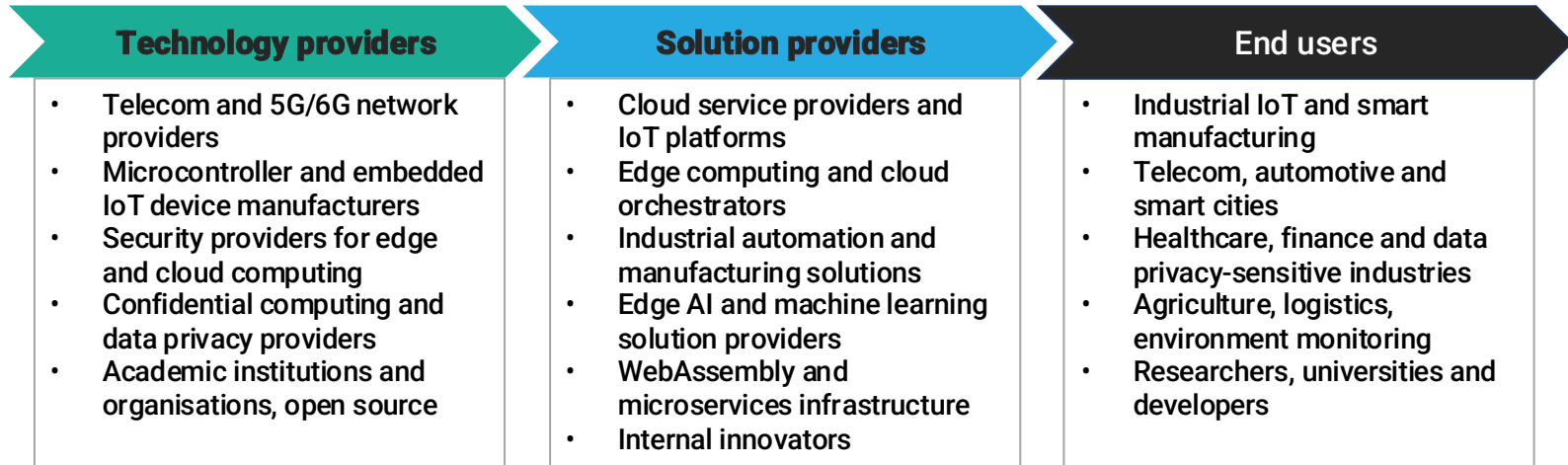
- ✓ Improved security and confidential computing
- ✓ Orchestration across edge-to-cloud continuum and improved resource efficiency
- ✓ Enhanced network, eBPF and observability
- ✓ Improved intrusion detection and threat management
- ✓ Improved WASM capabilities
- ✓ Enhanced authorization and access control
- ✓ Evolved federation learning and edge ML
- ✓ Mobility, prediction and AutoML

Pain points, limitations

- Trust and protection gaps in security and confidential computing
- Modern orchestration frameworks are too heavy for resource-constrained IoT devices
- Cloud and edge systems have network bottlenecks and lack of fine-grained visibility. eBPF faces debugging complexity and scaling across nodes
- WASM at edge has platform and hardware integration limitations
- FL & Edge ML is hindered by lack of lightweight and secure frameworks
- Modern access and authorization control models (e.g. ABAC) is challenging on edge devices

Identified ELASTIC target users

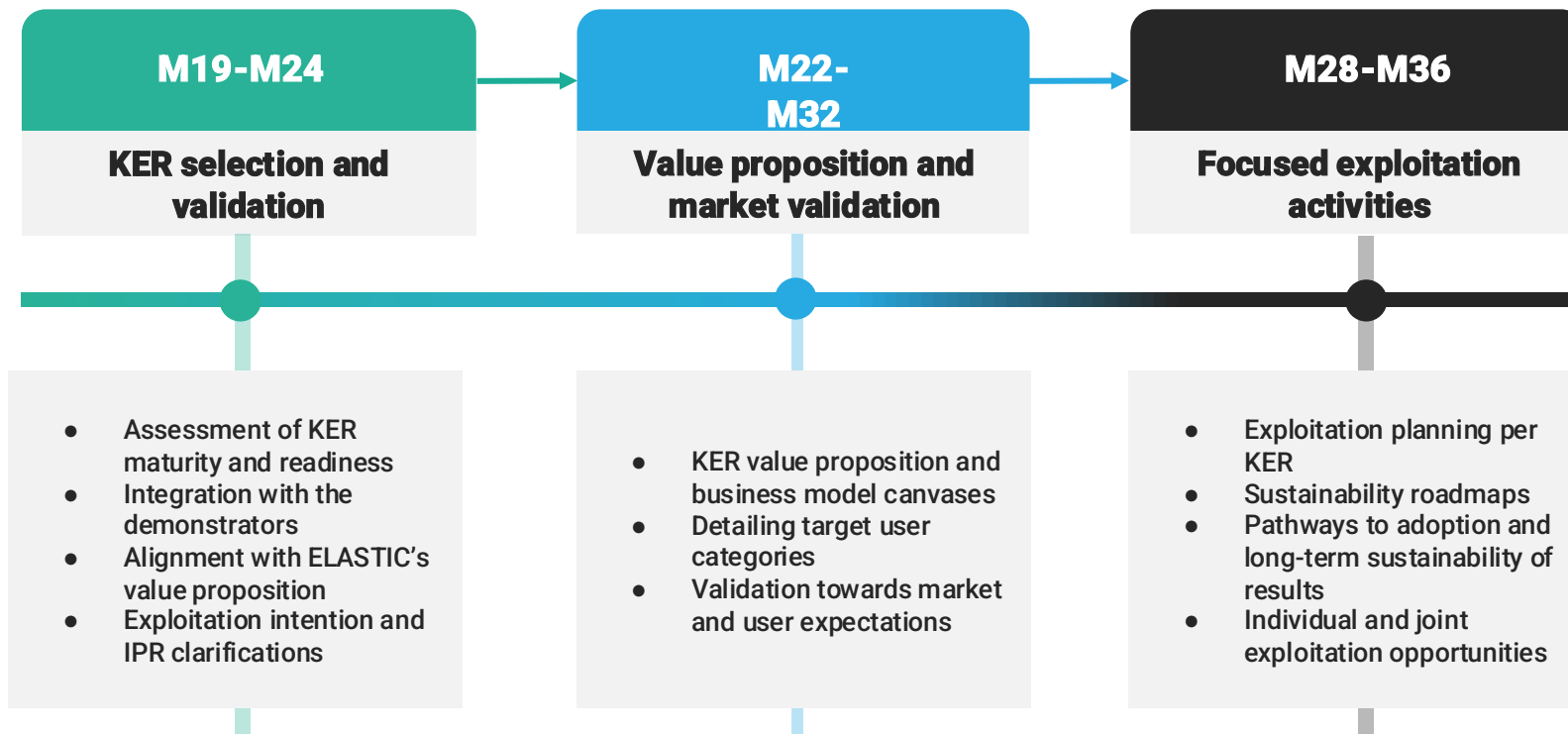
- ELASTIC results target **three main user categories** across the value chain
- A set of **common user groups** have been identified per user category
- **Focused exploitation activities and business development** will follow based on this value chain structure



ELASTIC candidate Key Exploitable Results

KER#	Title	Scope	Contributors
KER1	6G-embedded IoT data fabric	Integration of ELASTIC components into a cohesive platform – orchestrating secure, real-time data processing and analytics at the edge – supporting massive IoT scenarios.	ERF, UVC, IMEC, THS, ZEN, AMA, POLITO, AAL, TUC
KER2	Privacy-preserving and secure on-premise to public cloud migration	End-to-end solution – enabling secure workload migration using confidential computing, attestation, and secure key handling across the cloud–edge continuum.	THD, AAL, UVC, LUN, TUC
KER3	Wasm-native cloud-to-edge workload orchestrator (Propeller Orchestrator)	A highly portable and extensible orchestrator by AMA – enabling dynamic deployment of Wasm-based workloads.	AMA
KER4	WebAssembly Platform for Distributed Trusted Systems	A full-stack Wasm runtime foundation – combining runtime optimisation, platform integration, hardware-level access, secure communication, and enforcement tooling.	IMEC, AMA, POLITO, AAL
KER5	Confidential Computing, Security & Privacy Toolkit	Set of interoperable security components – supporting TEE lifecycle management, attestation, encryption, and policy enforcement.	THD, THS, ERF, UVC, AAL, LUN

Future exploitation pathways – Phase III



Next Steps & Conclusion

Next Steps & Conclusions

Expand webinars/workshops (≥ 4), sustain newsletters/press releases/videos, grow website traffic & social media through partner cross-posting.



Deepen clustering with SNS JU, and engage operators/SMEs for demonstrator feedback



Convert RP1 outputs into ≥ 2 journal articles; sustain conference pipeline aligned with 6G/security venues.



Progress WASI contributions, deliver inputs to ETSI NFV-SEC 020/025, and publish a joint Wasm/eBPF white paper



Mature Phase-II KERs with value proposition canvases, adopter interviews, and mini-pilots; integrate with demonstrators



Prepare per-KER exploitation plans, refine business models, and develop sustainability roadmaps by M36







Thank you for your attention!

 <https://elasticproject.eu/>  <https://www.linkedin.com/company/elastic-project/>

 https://www.instagram.com/elastic_project/  https://twitter.com/ElasticProject_

 <https://www.youtube.com/@ELASTIC-ProjectEU>  <https://github.com/elasticproject-eu>

 <https://bsky.app/profile/elastic-project.bsky.social>  <https://zenodo.org/communities/elastic/records>