ROBUST-6G

SNS JU Call-2 Projects Introduction Webinar

Güneş Kesik
Ericsson Research Türkiye

Project Details

Project Title: Smart, Automated, and Reliable Security Service Platform for 6G

Call: STREAM-B-01-04: Reliable Services and Smart Security

Start Date: 01.01.2024 , **End Date:** 30.06.2026, **Duration:** 30 Months
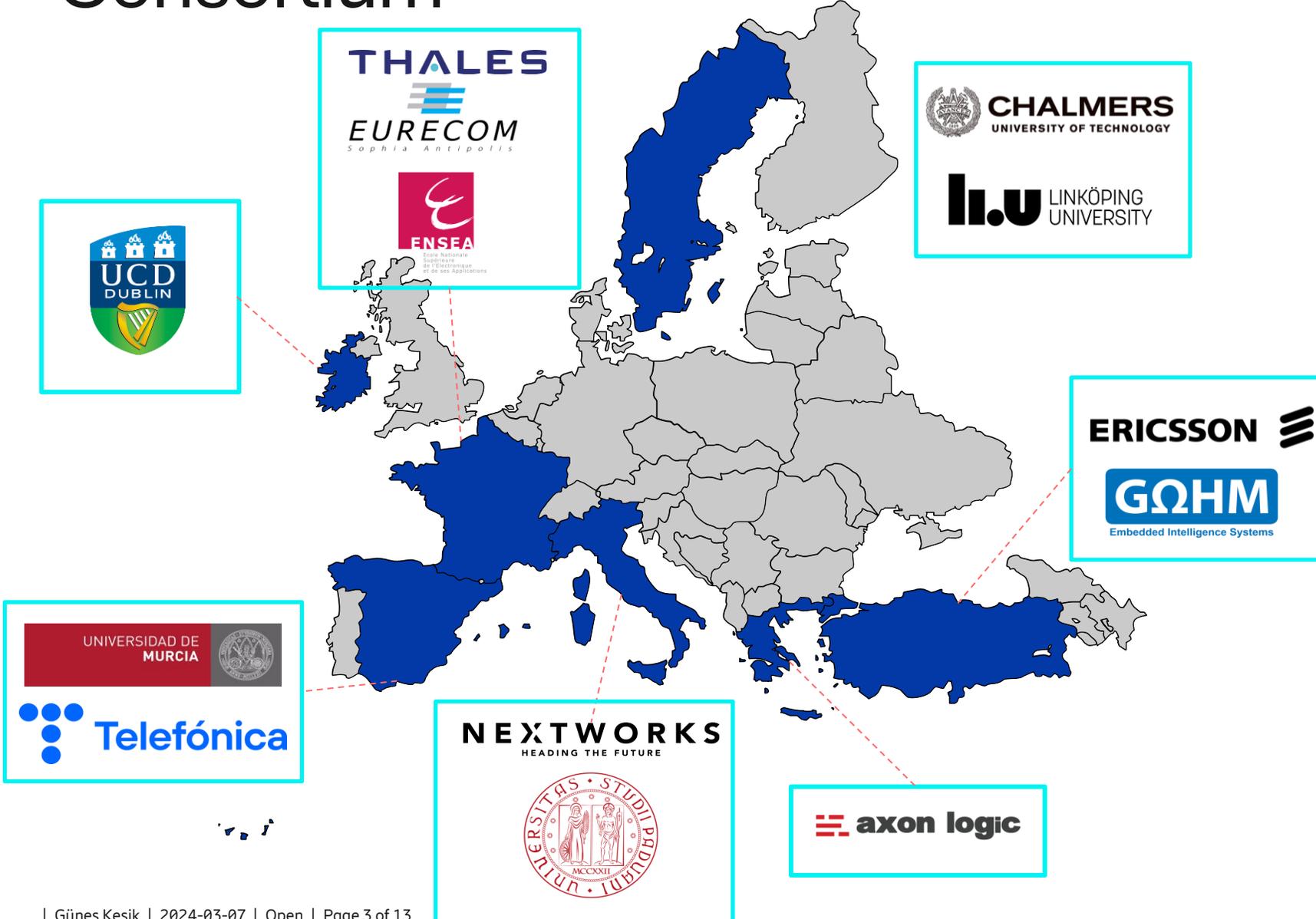
Project Number: 101139068

Total Budget: 4 201 741.25 EUR

EU Contribution: 3 999 956.50 EUR
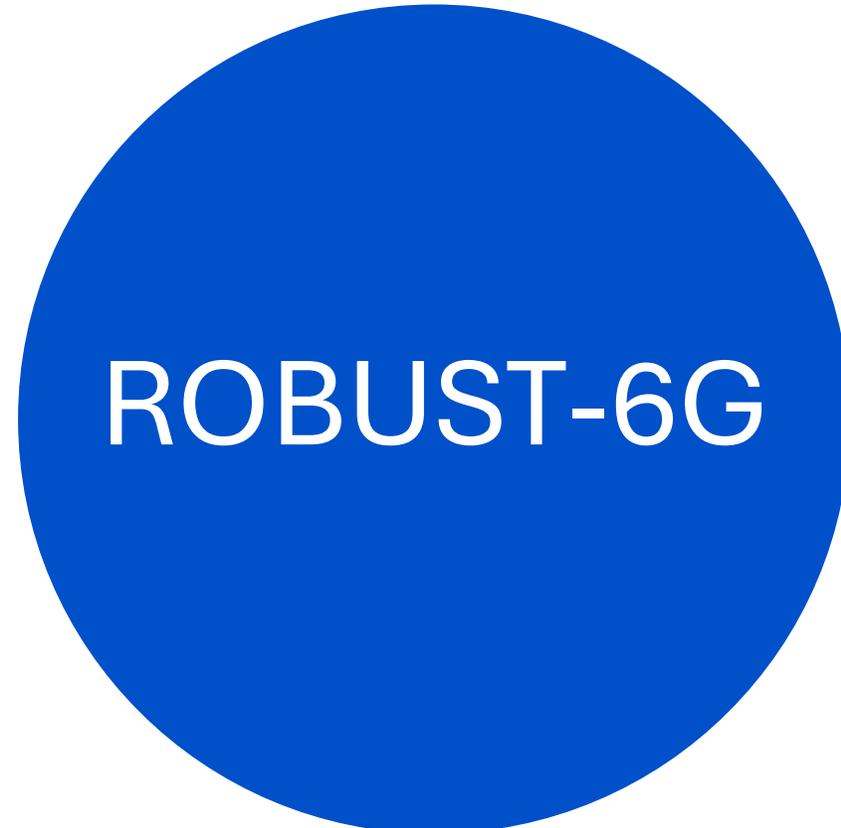
Project Coordinator: Güneş Kesik

Technical Management Committee: Madhusanka Liyanage, Arsenia Chorti, Manuel Gil Perez

Consortium

	#
Universities	6
Research Institutes	1
Large Enterprises	3
SMEs	3
6G-IA Members	8

Project Scope

ROBUST-6G

data-driven, AI/ML based security solutions

the security and robustness of distributed intelligence

privacy enhancements, and transparency by elaborating the explainability in AI/ML.

green and sustainable AI methodologies to optimize the computation requirements

zero-touch network and service management (ZSM)

fully automated end-to-end smart network and service security management framework

advanced AI/ML methodologies for physical layer

trustworthiness and resilience of 6G Radio with PLS

Project Objectives

Objective 1: Analysis of anticipated 6G architecture and scenarios, identification, and characterization of the threat landscape in an AI-driven 6G Network based on globally connected heterogeneous environments – Linked to **WP2**

Objective 2: To develop a holistic E2E 6G security architecture with inherent AI functionalities that will seamlessly integrate different functions in an heterogenous network environment, enabling 6G scenarios with high security requirements. – Linked to **WP2, WP3, WP4 and WP5**

Objective 3: To develop methodologies for ensuring that AI-driven security functionalities are robust, sustainable (in terms of energy efficiency), explainable, effective (in terms of performance) and preserving privacy in all aspects. – Linked to **WP3**

Objective 4: Automatic, zero-touch, security, and resource management for trusted and certified services among multiple stakeholders in distributed dynamic scenarios – Linked to **WP4**

Objective 5: AI/ML-enabled smart techniques to detect and mitigate physical layer attacks on network and user devices and to propose novel physical layer security schemes for demanding scenarios (low latency, low energy consumption, and low complexity), taking into account new radio technologies for 6G – Linked to **WP5**
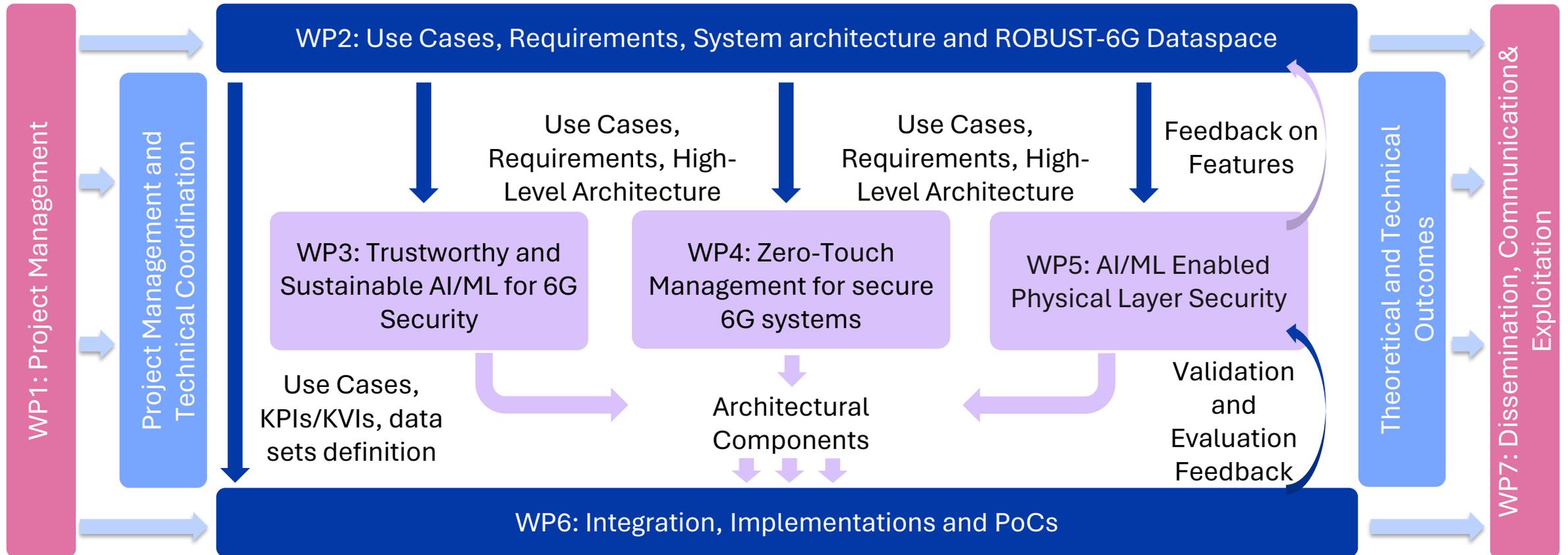
Objective 6: Showcase and validate the ROBUST-6G innovations by means of Proof of Concept (PoC) demonstrations through the use case scenarios. – Linked to **WP6**
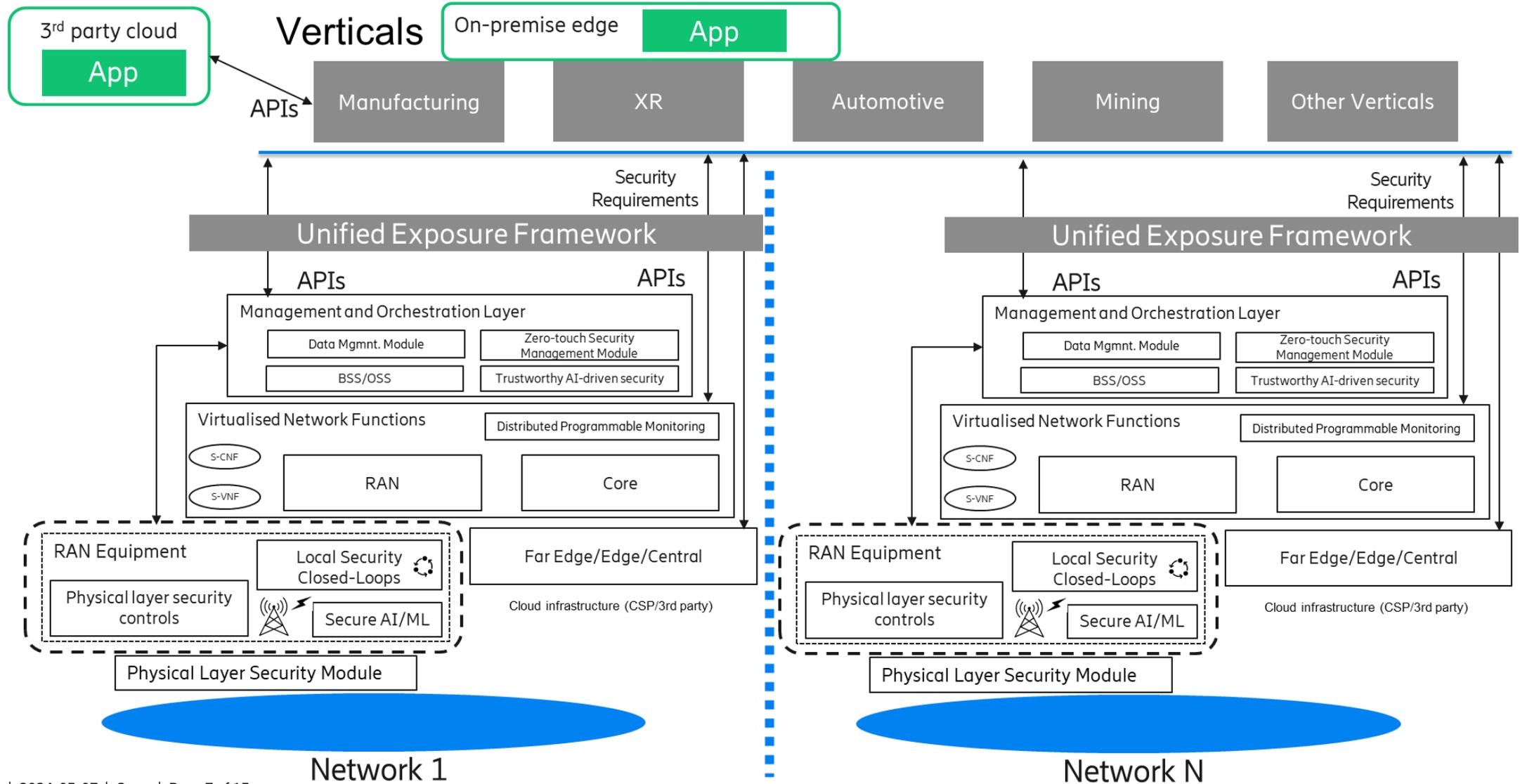
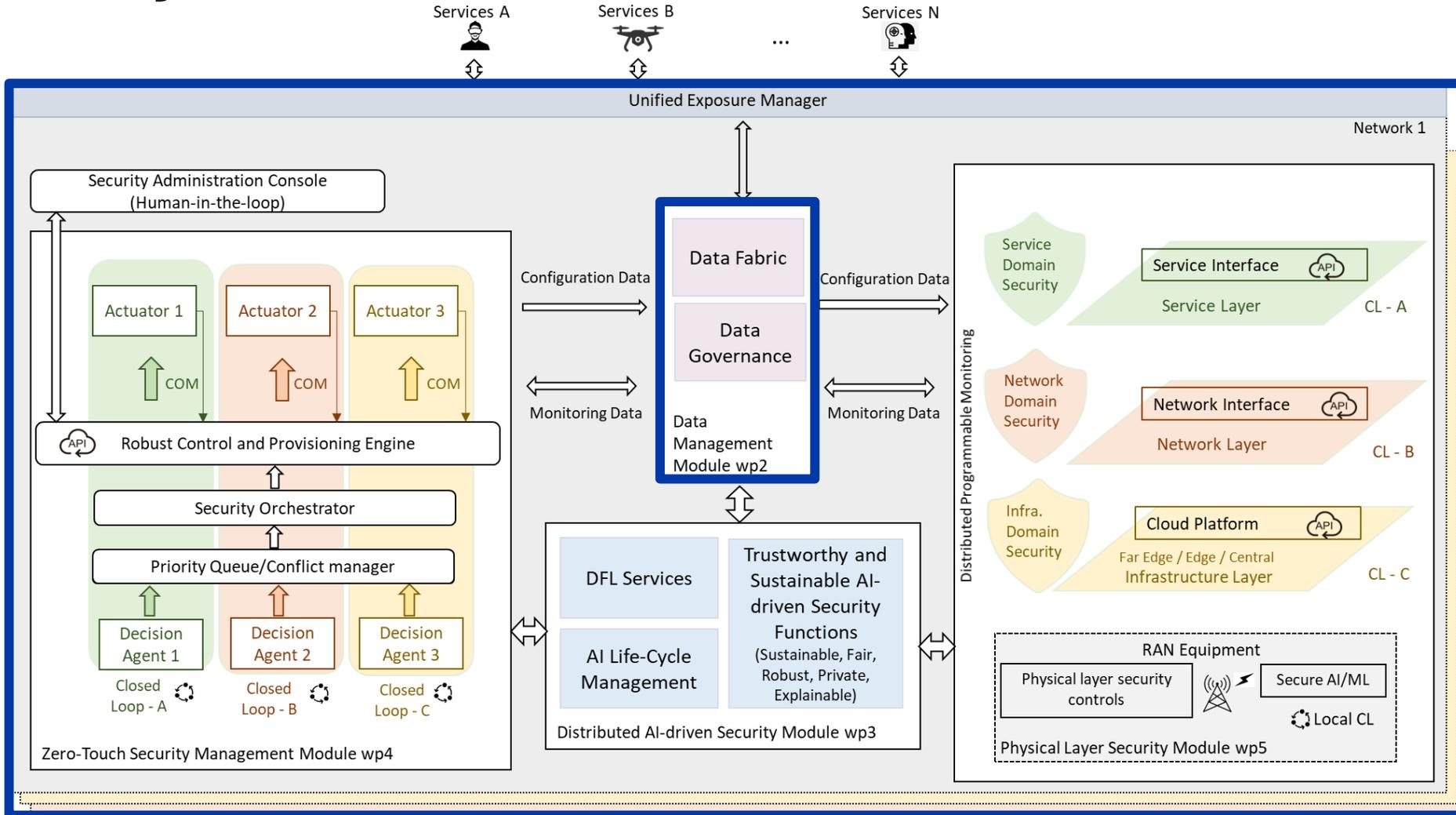**Objective 7:** Carry out extensive dissemination, standardisation, and exploitation activities – Linked to **WP7**
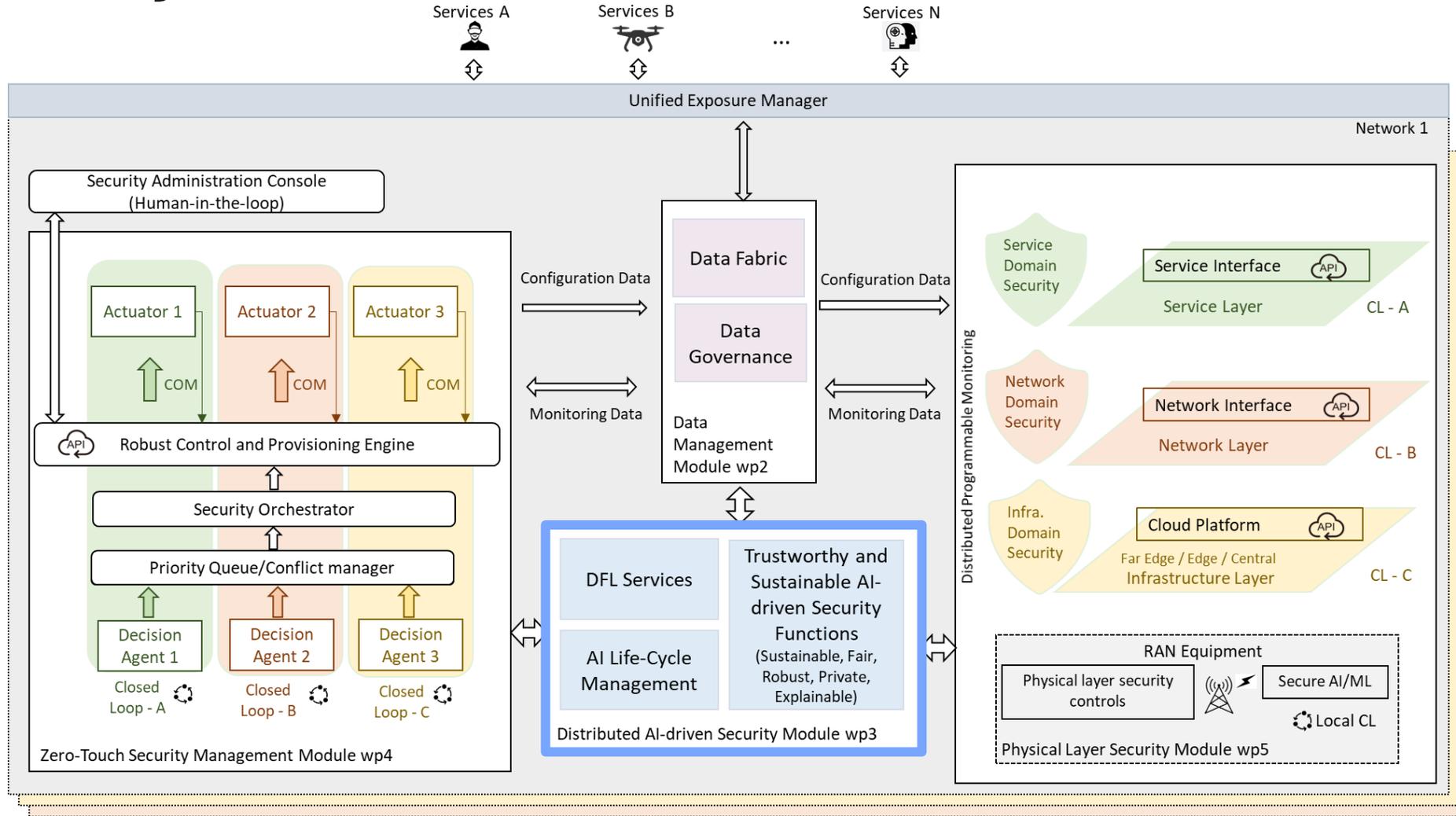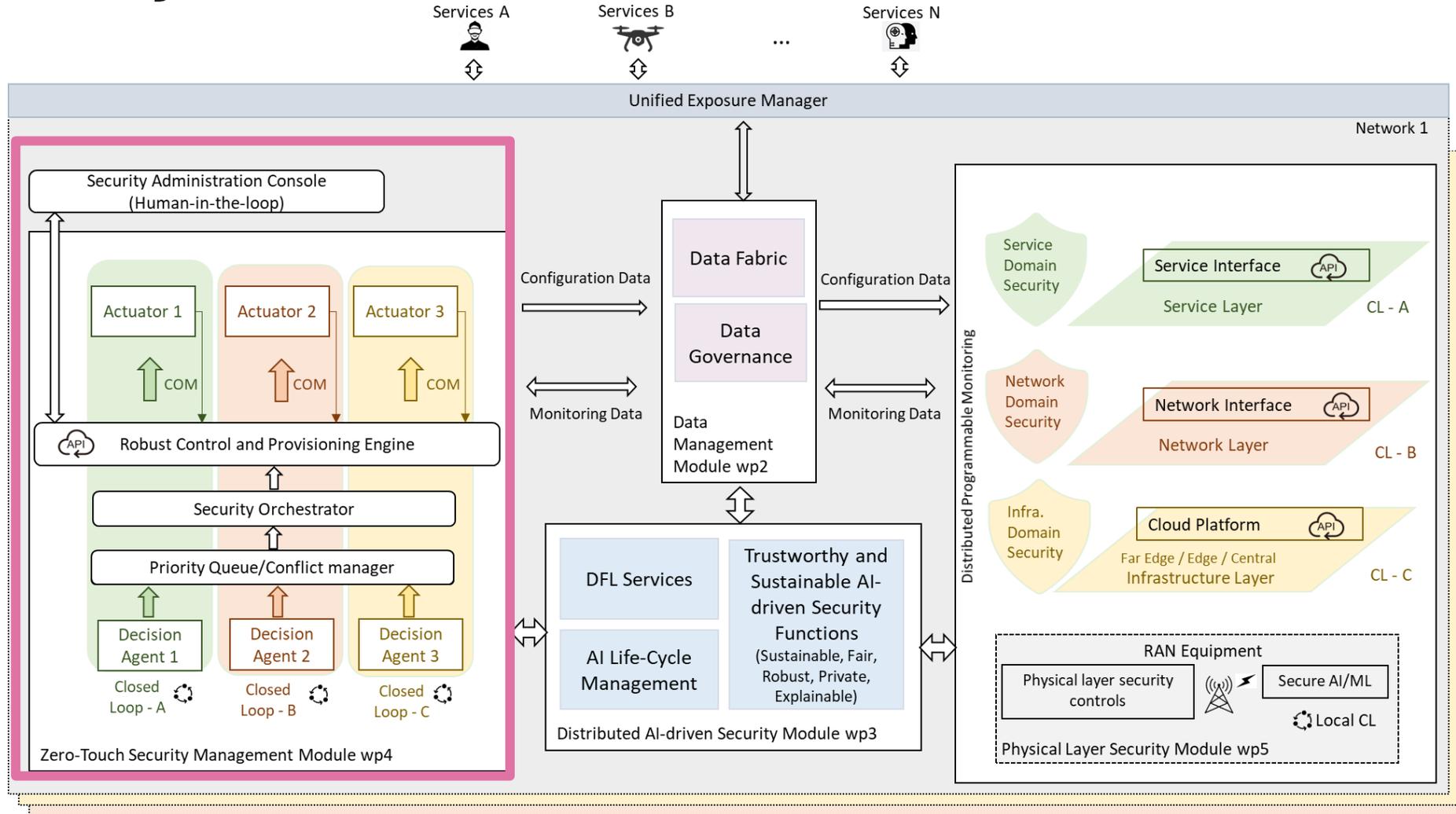
Work Package Structure

WP1: Project Management

Project Management and Technical Coordination

WP2: Use Cases, Requirements, System architecture and ROBUST-6G Dataspace

Use Cases, Requirements, High-Level Architecture

Use Cases, Requirements, High-Level Architecture

Feedback on Features

WP3: Trustworthy and Sustainable AI/ML for 6G Security

WP4: Zero-Touch Management for secure 6G systems

WP5: AI/ML Enabled Physical Layer Security

Use Cases, KPIs/KVIs, data sets definition

Architectural Components

Validation and Evaluation Feedback

WP6: Integration, Implementations and PoCs

Theoretical and Technical Outcomes

WP7: Dissemination, Communication& Exploitation

ROBUST-6G Architecture

Key Innovations

Key Innovations
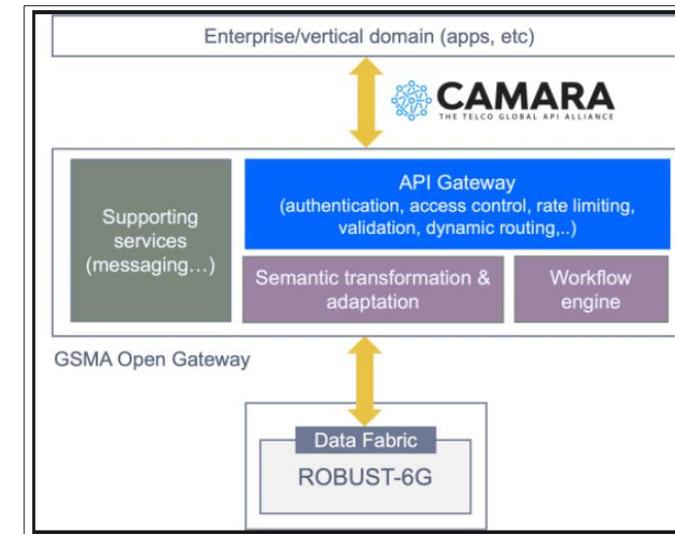
Key Innovations

Key Innovations

ROBUST-6G Demonstrators

Use case 1: AI Model Trustworthiness Evaluation in 6G Distributed Scenarios
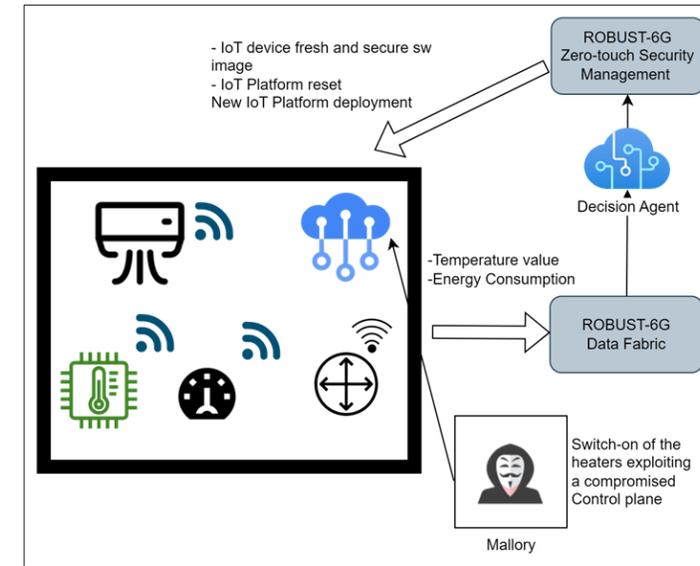
Use case 2: Automatic Threat Detection and Mitigation in 6G-Enabled IoT Environments

Use case 3: Security Capability Exposure via NetSecaaS

ROBUST-6G