

◆ **Projet 6 : ROBUST-6G : janvier 2024 – juin 2026**



Dhouha AYED
Cybersecurity Expert, Thales



Louis CAILLIOT
Cybersecurity Architect,
Thales

ROBUST-6G

Smart, Automated, And Reliable Security
Service Platform For 6G

Presenters

Louis Cailliot, Dhouha Ayed (THALES)



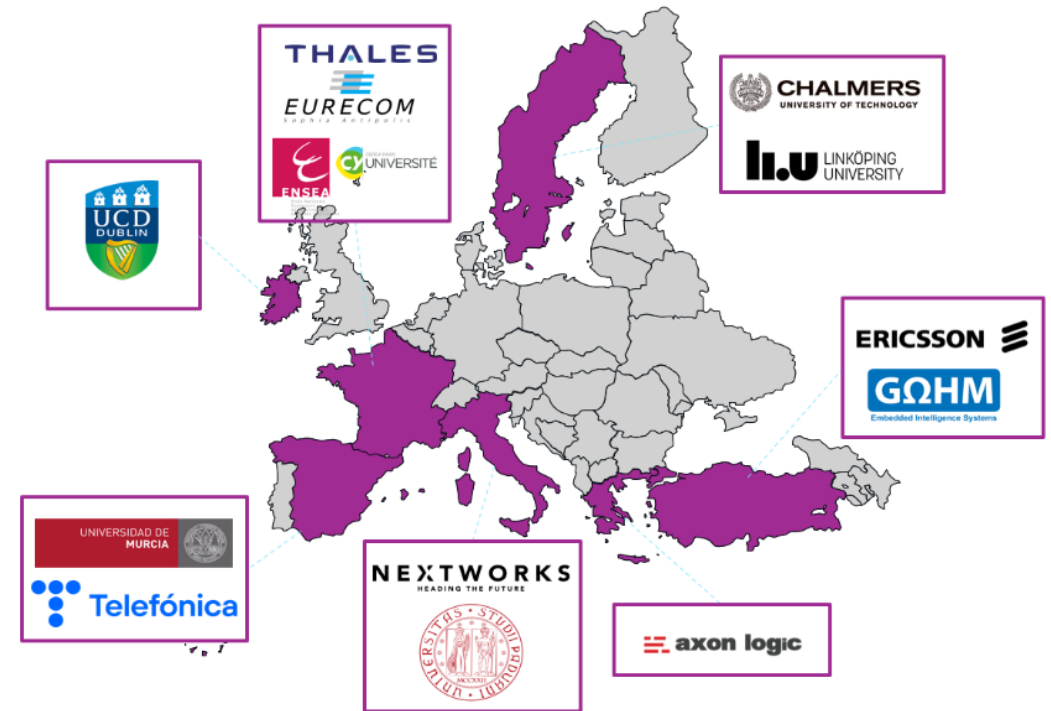
Co-funded by
the European Union

6G SNS

Smart, automated and reliable
security services for 6G

January 2024–June 2026
30 months, seven objectives, three use cases

Project Coordinator, Ericsson Research Türkiye

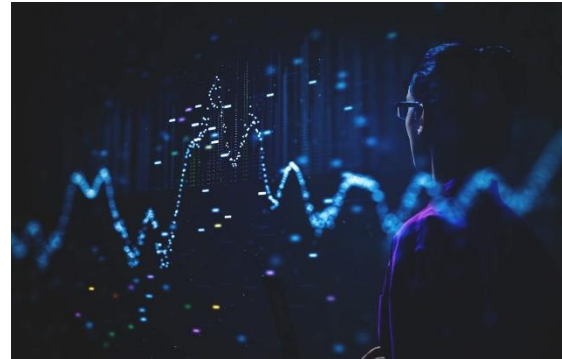


Context



AI/ML Integration

- The native use of AI/ML across the network is crucial for automating decision-making, enhancing performance, achieving zero-touch automation, and ensuring end-to-end security.



Data Management and Privacy

- Efficient data management solutions are necessary to support AI-driven processes.
- Ensuring privacy and security of data, especially in AI systems, is a significant challenge.



Trustworthiness and Robustness

- Trustworthiness in AI solutions is prioritized.
- Policymakers advocate for a human-centric approach focusing on transparency and explainability in AI/ML systems



Energy Efficiency

- Promoting green and sustainable AI methodologies is essential to minimize energy consumption while maintaining performance in AI-driven security functions.

Project ambition and scope

Security for a 6G environment shaped by distributed intelligence.

AI for security



Detect and mitigate threats across network services and the physical layer.
Automate security operations.

Security for AI



Protect learning and model use against attacks and privacy leakage.
Support explainability and efficiency.

Project commitments

Threats and architecture (O1–O2), security capabilities (O3–O5), use-case validation (O6), dissemination and exploitation (O7).

Project Scope and Objectives

data-driven, AI/ML based
security solutions



zero-touch network and
service management (ZSM)



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



ROBUST-6G



the security and
robustness of
distributed intelligence



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

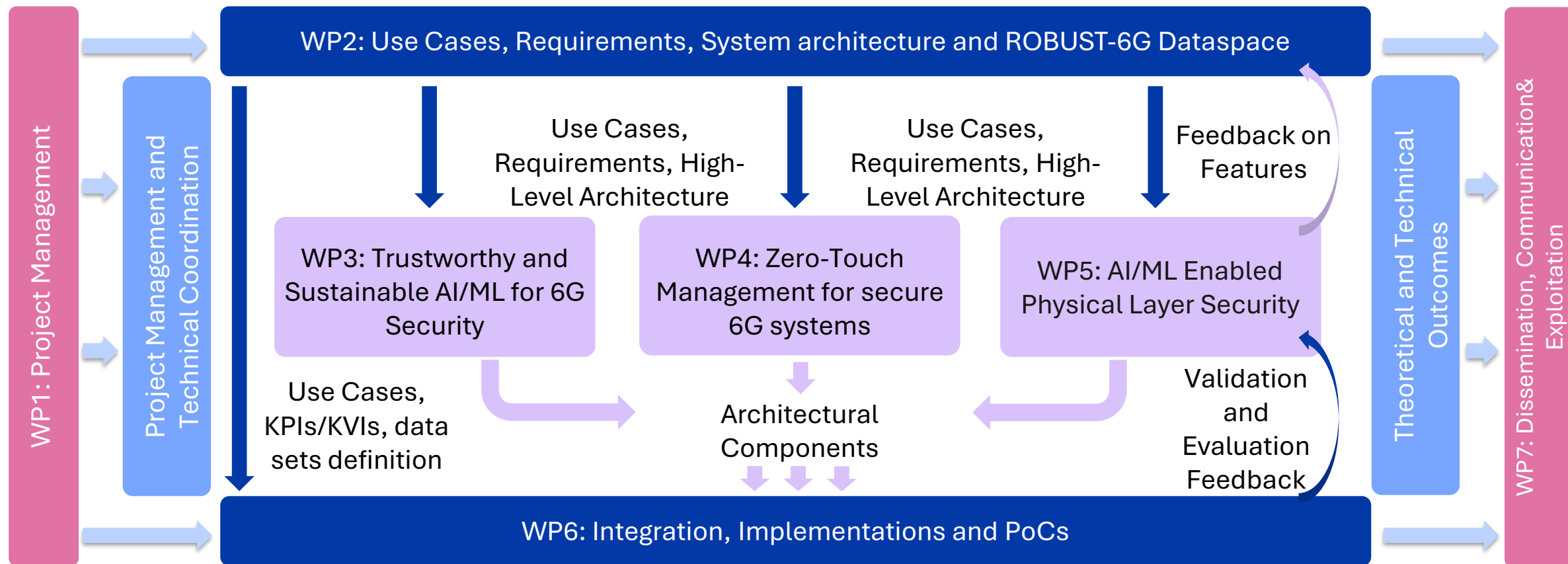


green and **sustainable** AI
methodologies to optimize
the computation
requirements

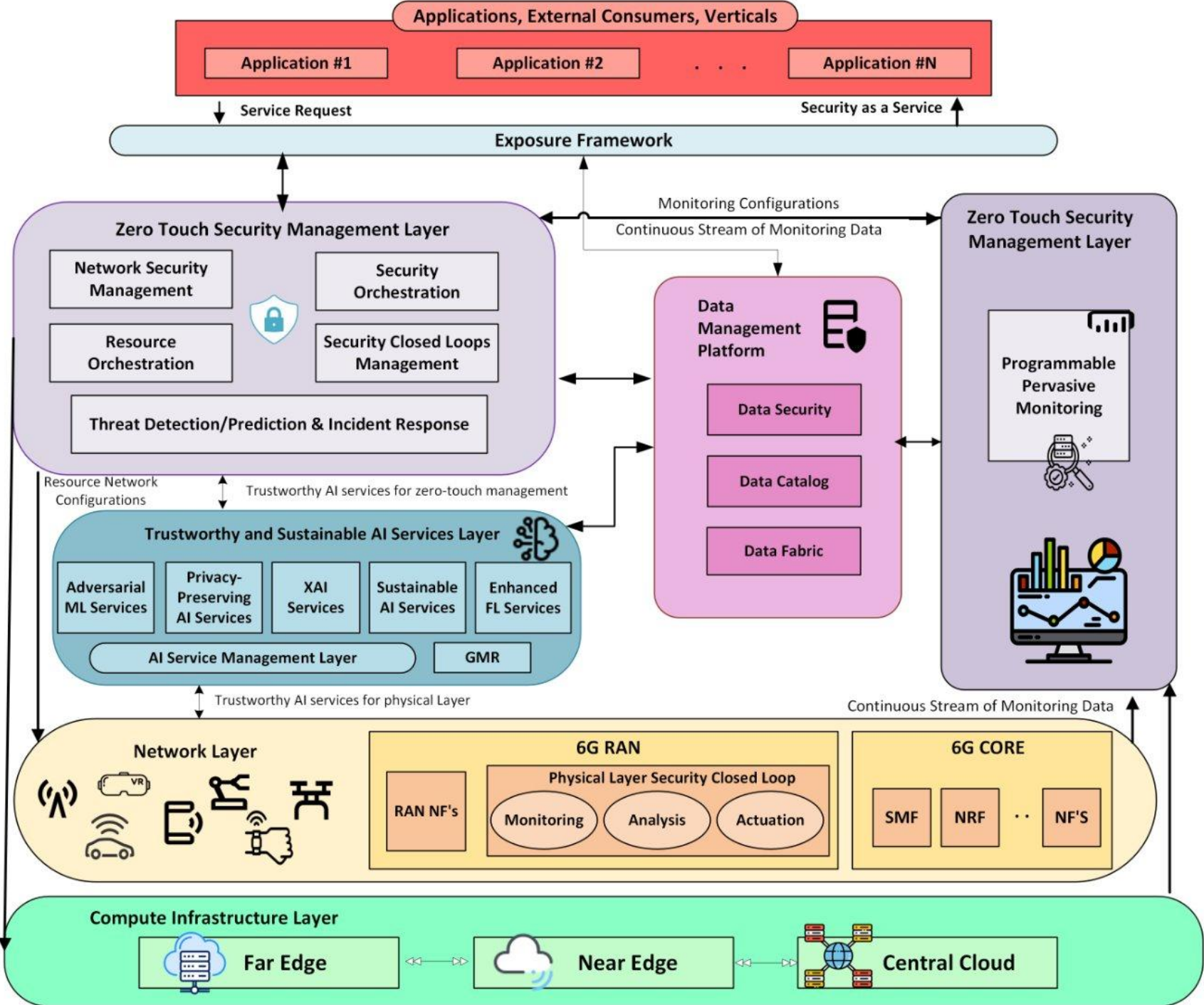


trustworthiness and
resilience of 6G Radio with
PLS

Work Package Structure



Functional Architecture



Three use cases

Each use case validates a different part of the project’s security scope.

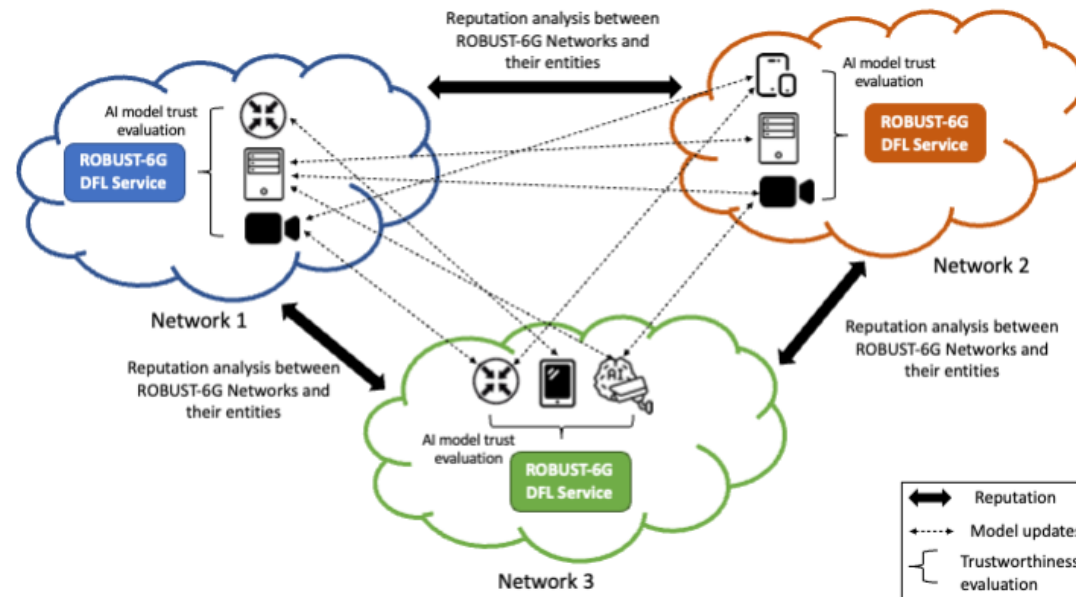


Use case	Validation focus	End-to-end capability
UC1	Trustworthy decentralized AI Physical and sensing-layer trust	Model generation, privacy and reuse Authentication and key generation
UC2	Automatic threat detection and mitigation	Coordinated security closed loops in 6G-enabled IoT environments
UC3	Security capabilities exposure with NetSecaaS	Security discovery, XAI analytics and service requests through APIs

The three use cases yield five prototypes, including one integrated master prototype.

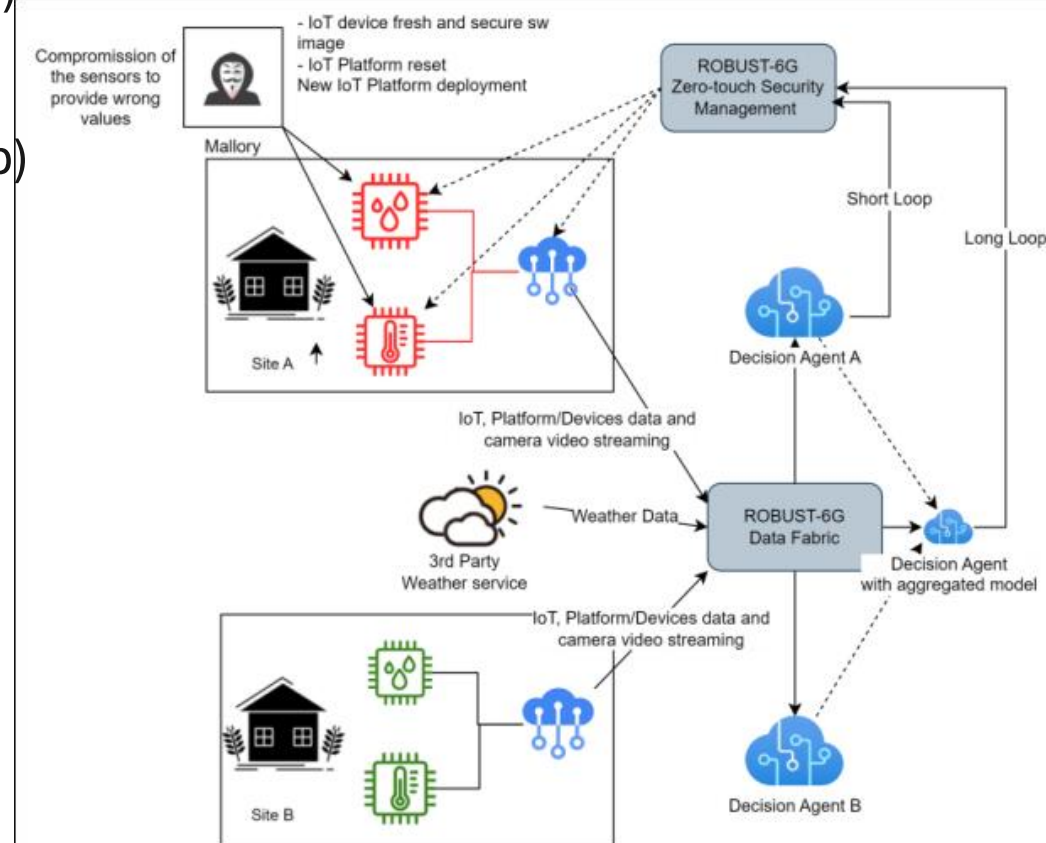
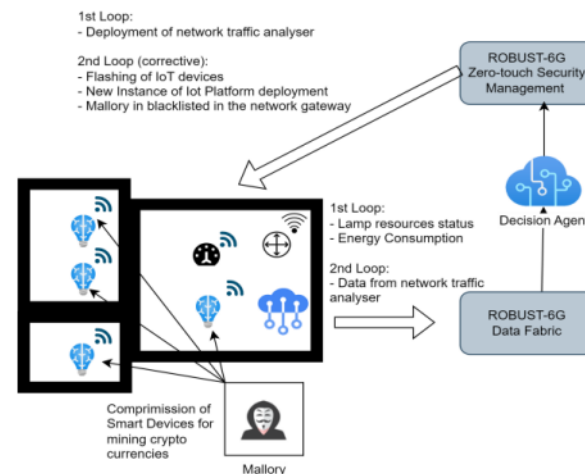
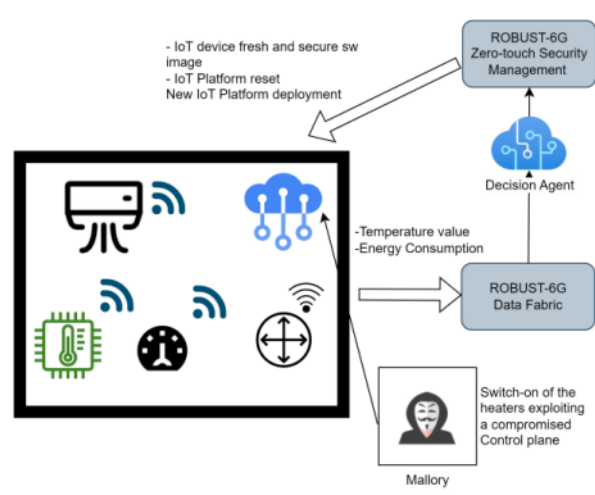
Use case 1 – AI model trustworthiness evaluation for 6G distributed scenarios

- Scenario 1 – Decentralised federated learning for joint privacy-preserving ML/DL model training
- Scenario 2 – Physical and sensing layer trustworthiness and resilience

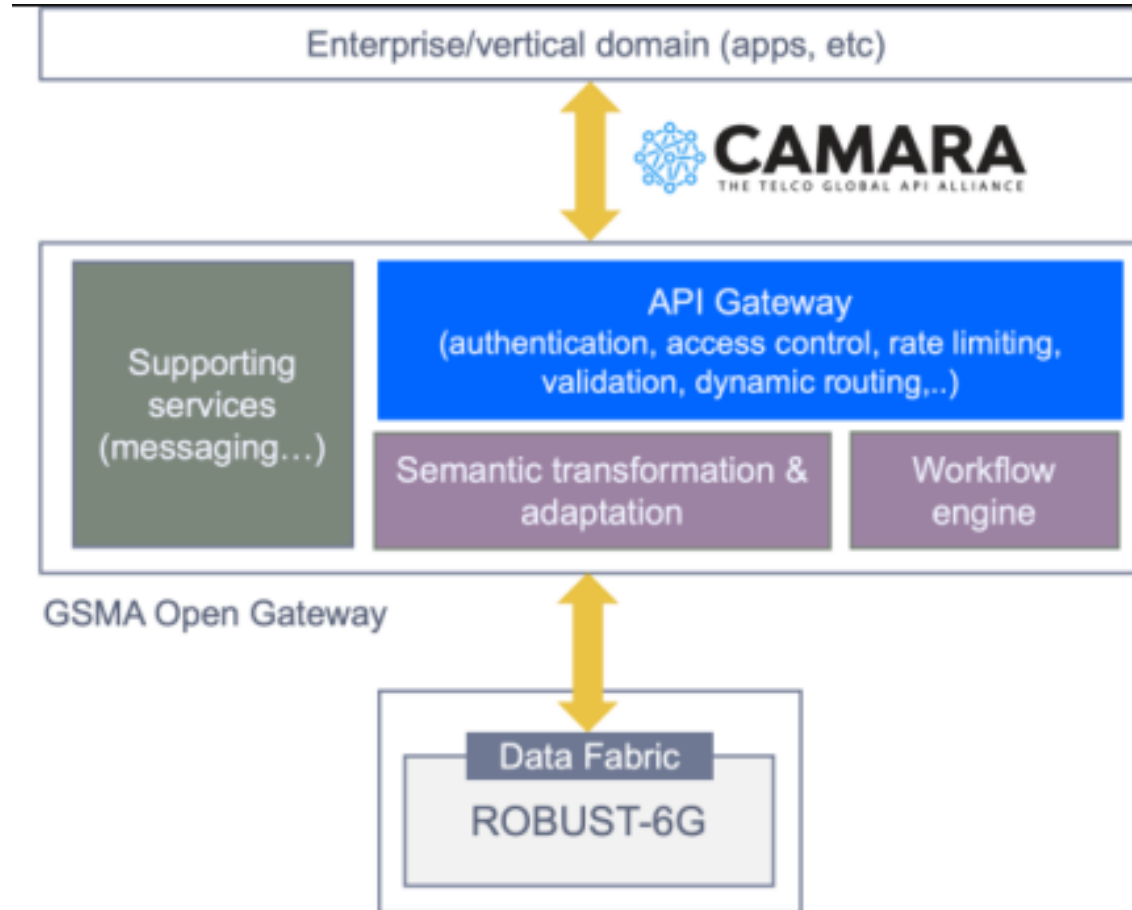


Use case 2 – Automatic threat detection and mitigation in 6G-enabled IoT environments

- Scenario 1 – Device violation to cause an economic harm (a)
- Scenario 2 – Fraudulent usage of device resources
- Scenario 3 – Device violation to cause an economic harm (b)



Use case 3 (TID) – Security Capabilities Exposure with Network-Security-as-a-Service (NetSecaaS).



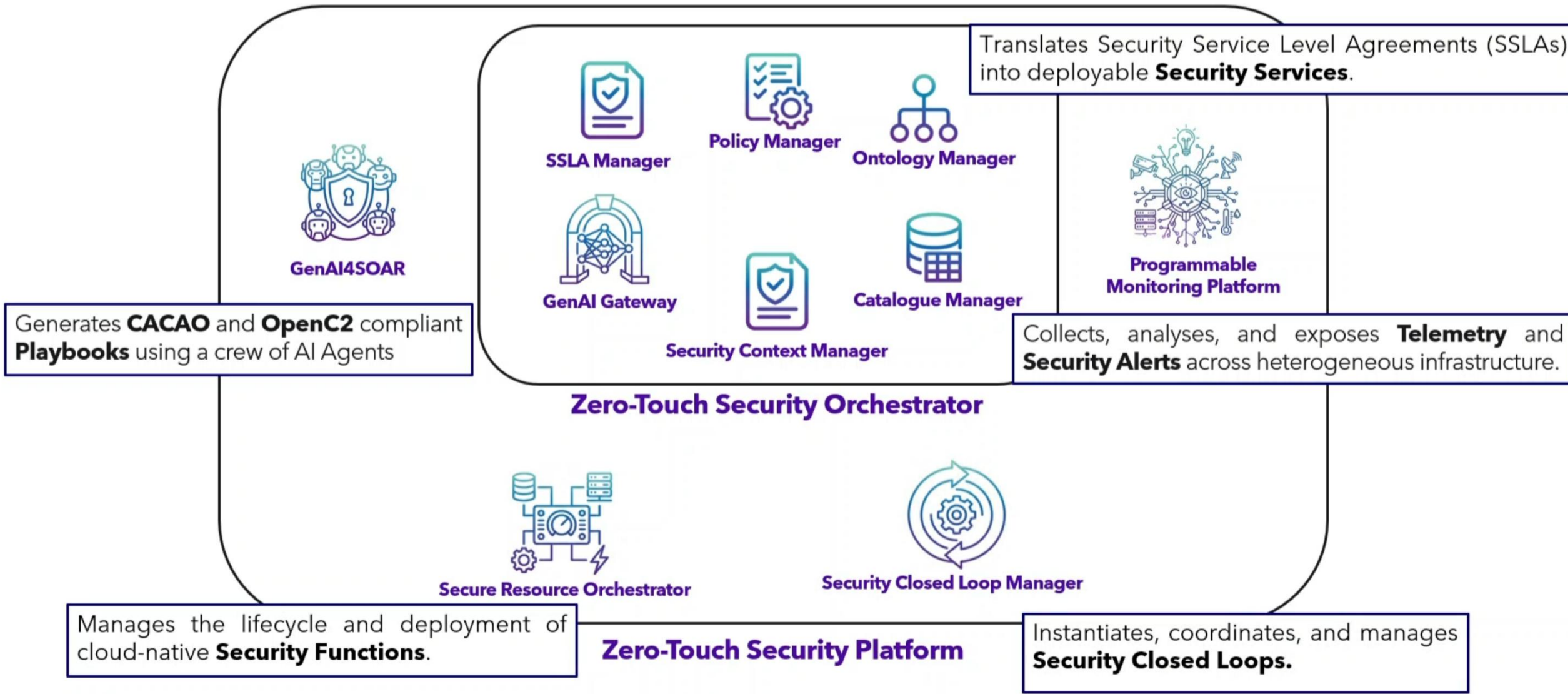
Five prototypes and their combined contribution

Four capability prototypes feed the integrated master prototype.

Prototype	Project contribution	TRL
P1 Trustworthy AI	Model generation, validation and reuse	5
P2 Multi-Layer Zero-Touch Defender	Automated security across IoT and networks	5
P3 NetSecaaS Gateway	Controlled security service exposure	5
P4 Physical and Sensing Layer Trustworthiness	PHY detection, authentication and key generation	4
P5 Master Prototype	Combination of AI, orchestration, PHY services and API exposure	4

Four live demos at EuCNC 2026. The master prototype uses a recorded demonstration.

Zero-Touch Security Platform



Zero-Touch Security Platform NextWorks

THALES



GenAI4SOAR

Generates **CACAO** and **OpenC2** compliant **Playbooks** using a crew of AI Agents



SSLA Manager



Policy Manager



Ontology Manager



GenAI Gateway



Security Context Manager



Catalogue Manager

Translates Security Service Level Agreements (SSLAs) into deployable **Security Services**.



Programmable Monitoring Platform

University of Murcia

Collects, analyses, and exposes **Telemetry** and **Security Alerts** across heterogeneous infrastructure.

Zero-Touch Security Orchestrator

EURECOM



Secure Resource Orchestrator



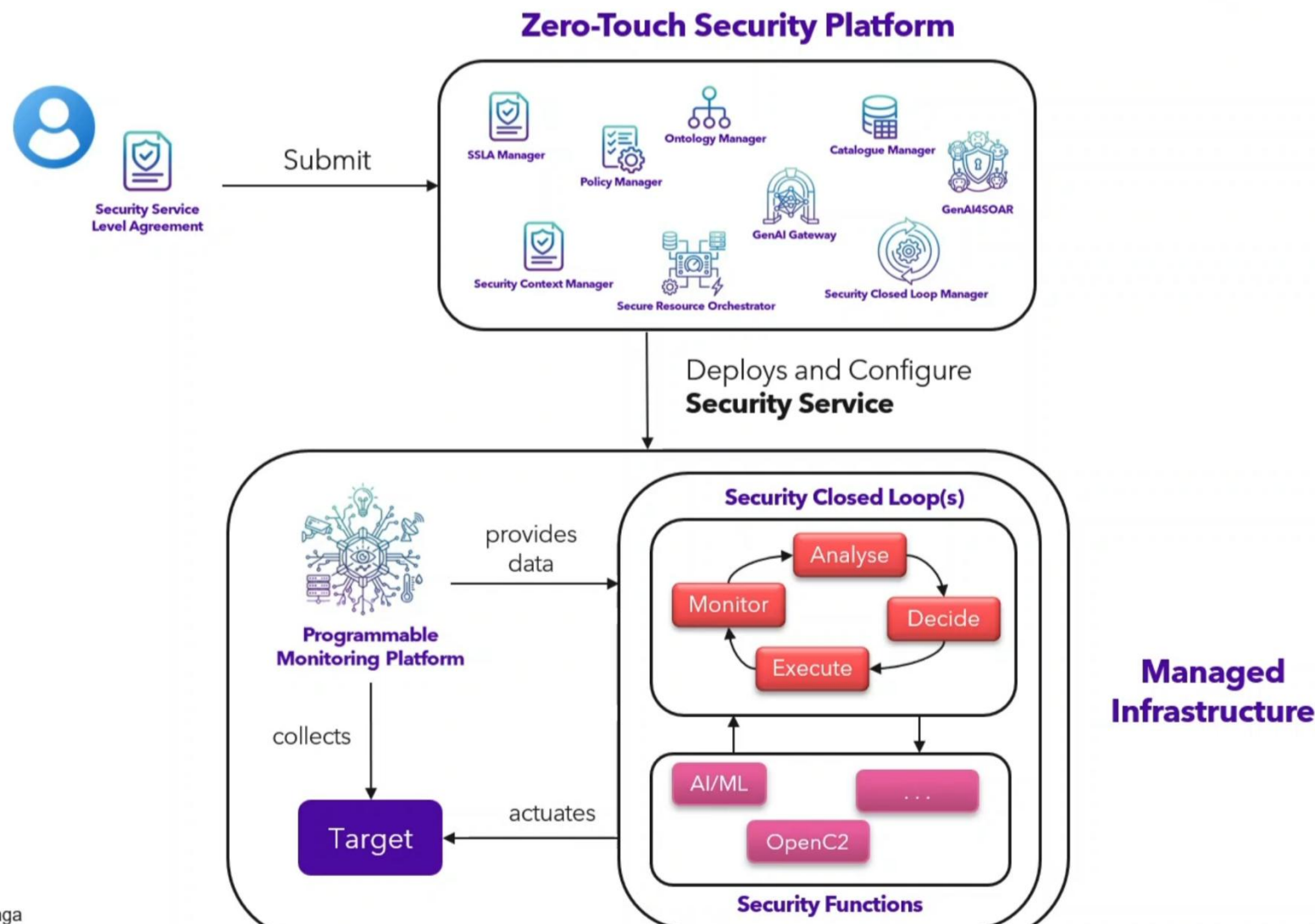
Security Closed Loop Manager

Manages the lifecycle and deployment of cloud-native **Security Functions**.

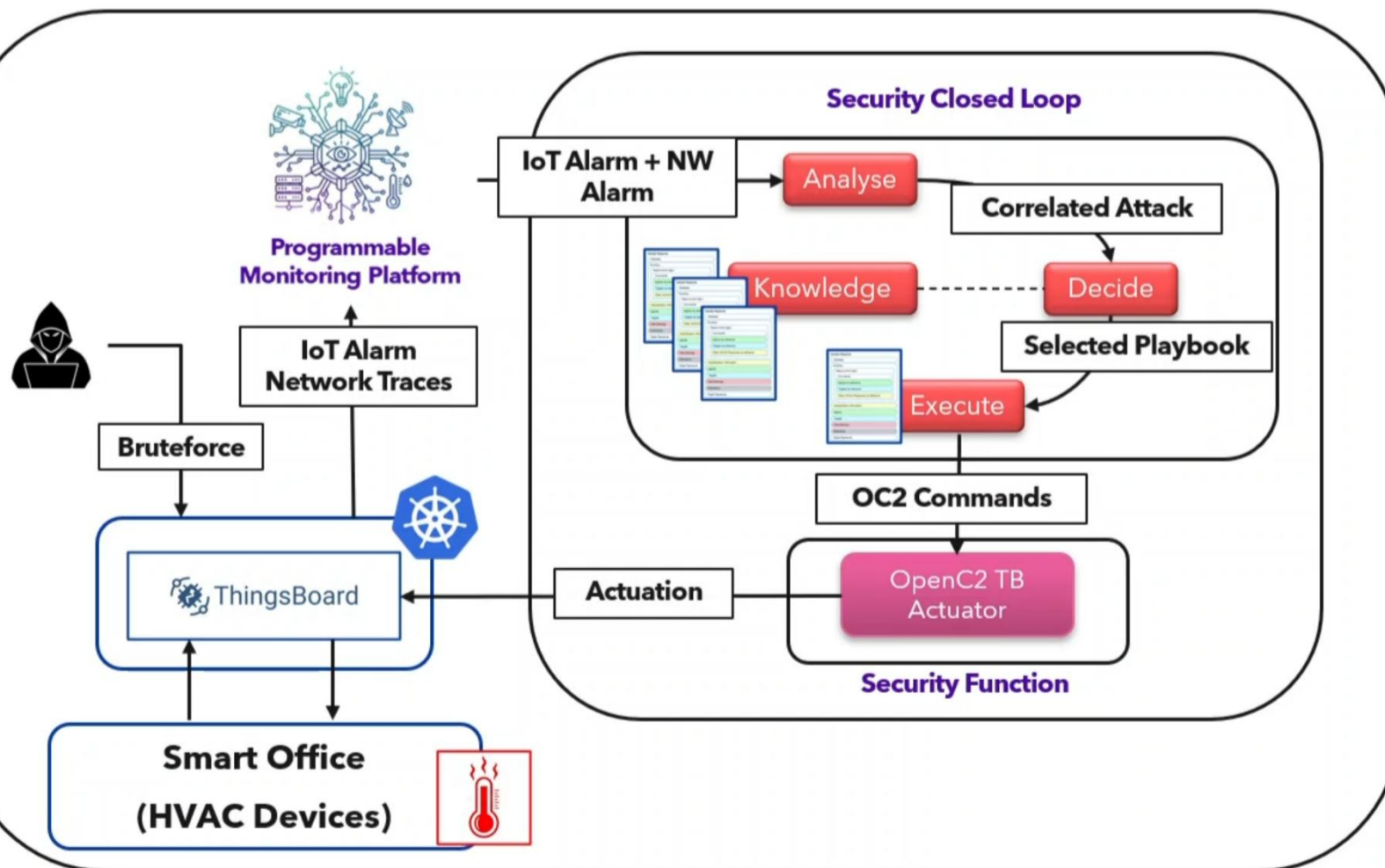
Zero-Touch Security Platform

Instantiates, coordinates, and manages **Security Closed Loops**.

Security Closed-Loops Principles



Attack and remediation scenario



ROBUST-6G UC2 Scenario 1 - Smart Office

- Smart Office with HVAC system managed via Thingsboard (deployed on K8S)
- **(Phase 1)** Security Service for IoT and NW Monitoring with zero-touch remediation is deployed
- **(Phase 2)** Attacker bruteforce the user account (weak credentials) and compromise HVAC logic.
- **(Phase 3)** The security service automatically remediates the attack.

Phase 1

Security Service Provisioning

Standardization Actions

- **More than 100 standardisation actions recorded**

- **IETF**

- YANG data provenance adopted in OPSAWG; COSE signatures draft presented at IETF 122–124 and demonstrated in the hackathon
- Telemetry data manifest; network digital twin architecture in NMRG/NMOP with semantic models and knowledge graphs
- Verifiable geofencing and data residency in RATS
- Capability inventory in IVY
- SKEX BoF on symmetric key establishment: project acting as proponent and convenor

- **3GPP**

- SA3 study on security aspects of CAPIF Phase 3 and Phase 4
- Release 20 activities on security event handling
- 3GPP 6G Workshop: Zero Trust, post-quantum security and an AI intent management layer reflected in the chair's summary

- **ETSI**

- Contributions on data flows for intent expressions and NDT applications
- Evolution of ISG ETI (on encrypted traffic management) towards TC CYBER
- Support to new work item on agent-based networks in ISG ENI
- Leadership of ISG ZSM
 - Address NaaS, anomalies in closed loops, autonomy as a next step beyond automation
 - Alignment with ITU-T and IETF on security enforcement, AI-native networks, and NDT

Conclusion

- **Benefits thanks to AI**

- A significant improvement in threat detection
 - Identify sophisticated attacks and network anomalies more quickly and accurately
 - Automatic and secure orchestration mechanisms, real-time adaptations
- Responsiveness, better predictive and proactive mitigation capabilities for incidents
- French Partner