RIGOUROUS: secu**R**e des**IG**n and depl**O**yment of tr**U**sthwo**R**thy c**O**ntin**U**um computing 6G **S**ervices

Project Introduction

SNS Lunchtime Webinar 3 – Strands B1 & B4

Antonio Skarmeta

University of Murcia – Spain

https://rigourous.eu/

RIGOUROUS has received funding from the European Union's HE Research and Innovation Programme HORIZON-JU-SNS-2022 under Grant Agreement No 101095933

23/02/2023

RIGOUROUS: secuRe desIGn and deplOyment of trUsthwoRthy cOntinUum computing 6G Services

RIGOUROUS

11 partners from 8 countries

Project start January 1st, 2023, for 36 months

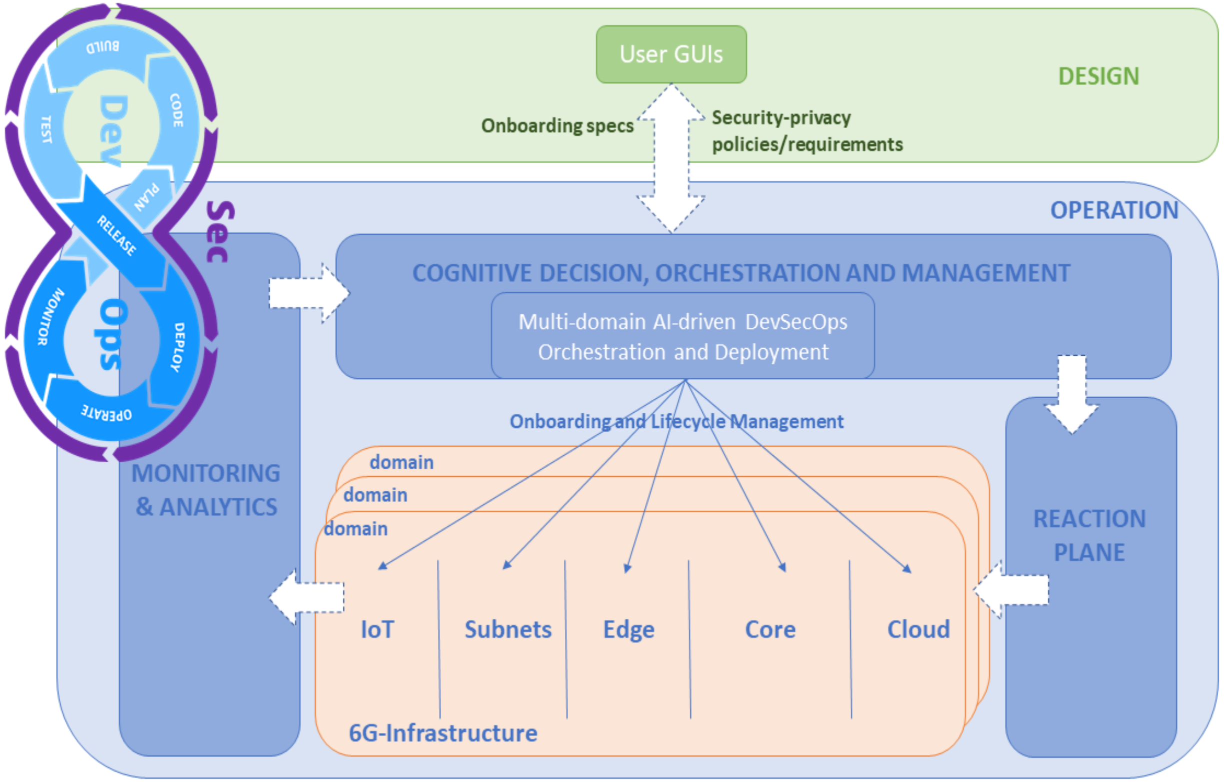
Total Cost 4 860 550€

Work programme topic addressed: STREAM-B-01-04 “Secure Service development and Smart Security”. HORIZON-JU-SNS-2022

1 (Coordinator)	University of Murcia (UNIV)*	UMU	Spain
2	ORANGE Romania*	ORO	Romania
3	LENOVO DEUTSCHLAND GMBH*	LNVO	Germany
4	RHEA System Luxembourg S.A. *	RHEA	Luxembourg
5	EBOS Technologies Ltd (SME)*	EBOS	Cyprus
6	WINGS (SME)*	WINGS	Greece
7	OneSource, Consultoria Informática Lda. (SME)*	ONE	Portugal
8	ICT-FI (SME) * *	ICT-FI	Finland
9	University of Oulu (UNIV)*	OULU	Finland
10	Instituto de Telecomunicações (UNIV)*	ITAV	Portugal
11	University of the West of Scotland (UNIV) *	UWS	UK

Introduction

RIGOUROUS will introduce a new holistic and smart service framework leveraging new machine learning (ML) and AI mechanisms, which can react dynamically to the ever-changing threat surface on all orchestration layers and network functions.



Smart service framework is capable of ensuring a **secure, trusted and privacy-preserving** environment for supporting the next generation of trustworthy continuum computing 6G services along the full **device-edge-cloud-continuum on heterogenous multi-domain networks**. This includes establishing compliance with the design of software (SW), protocols and procedures, as well as AI-governed mechanisms to cope with the security-related requirements in the **full DevOps lifecycle**, from the service onboarding up to the day-2 operations.

Objectives

O1: Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management

- Federated AI-governed zero-touch cognitive and secure management framework able to manage DevSecOps in diverse and heterogeneous cross-domain and cross-network segments in 6G.
- based on AI-governed mechanisms that allow a distributed smart-services lifecycle security management.
- It will strengthen security, trust and privacy in operations through a zero-touch cognitive SOAR (Security Orchestrate Automation response) loops,

O2: Human-Centric DevSecOps

- Open-source user-friendly tools and new open models for the design stage of DevSecOps, security and privacy models, risk management as well as services and devices onboarding specifications.
- Formalized security policies and onboarding specifications for enforcing the required security trust and privacy properties identified during the entire lifecycle, at design state and during operation, and to be enforced either:
- Zero trust identification and security adaptation supporting privacy-preserved and verifiable secure identification of the end-users

Objectives

O3: Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment

- **the policy-based approach within the DevOps lifecycle** will ensure an easy management of the system security.
- Novel IoT bootstrapping mechanisms will be introduced, preventing unauthorized access and privilege escalation.
- Furthermore, Security control Agents and Controllers will be developed to allow the orchestration and enforcement of **End-to-end network slices** expanded across multiple-domains and horizontal inter-network segments. These slices will be used as advance **mitigation mechanisms** against cyber-attacks to demonstrate the feasibility of the security strategy.

O4: Advanced AI-driven Anomaly Detection, Decision and Mitigation Strategies

- Novel privacy-preserving **Cyber-Threat Intelligence (CTI) mechanisms** will be devised to protect exchanged CTI data during the continuous FL process and during incident reporting. Diverse mitigation strategies will be delivered for countering cyberattacks such as Economical Denial of Sustainability (EDoS) attack and Denial of Service (DoS).
- Devise and prototype novel Moving Target Defense (**MTD**) strategies to empower proactive robustness of ML models to adversarial attacks.
- A **SOAR** solution intended to perform the automatic detection of cyber-attacks and join such detection with a complete automation process where autonomous reactions will be performed in the network related to perform distributed mitigation of such cyber-attacks in the different points of the network, without any human intervention.
- Novel **network slicing technology as mitigation mechanisms** to demonstrate the automatic usage of slicing as an effective security mechanism.

Objectives

- O5: Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments

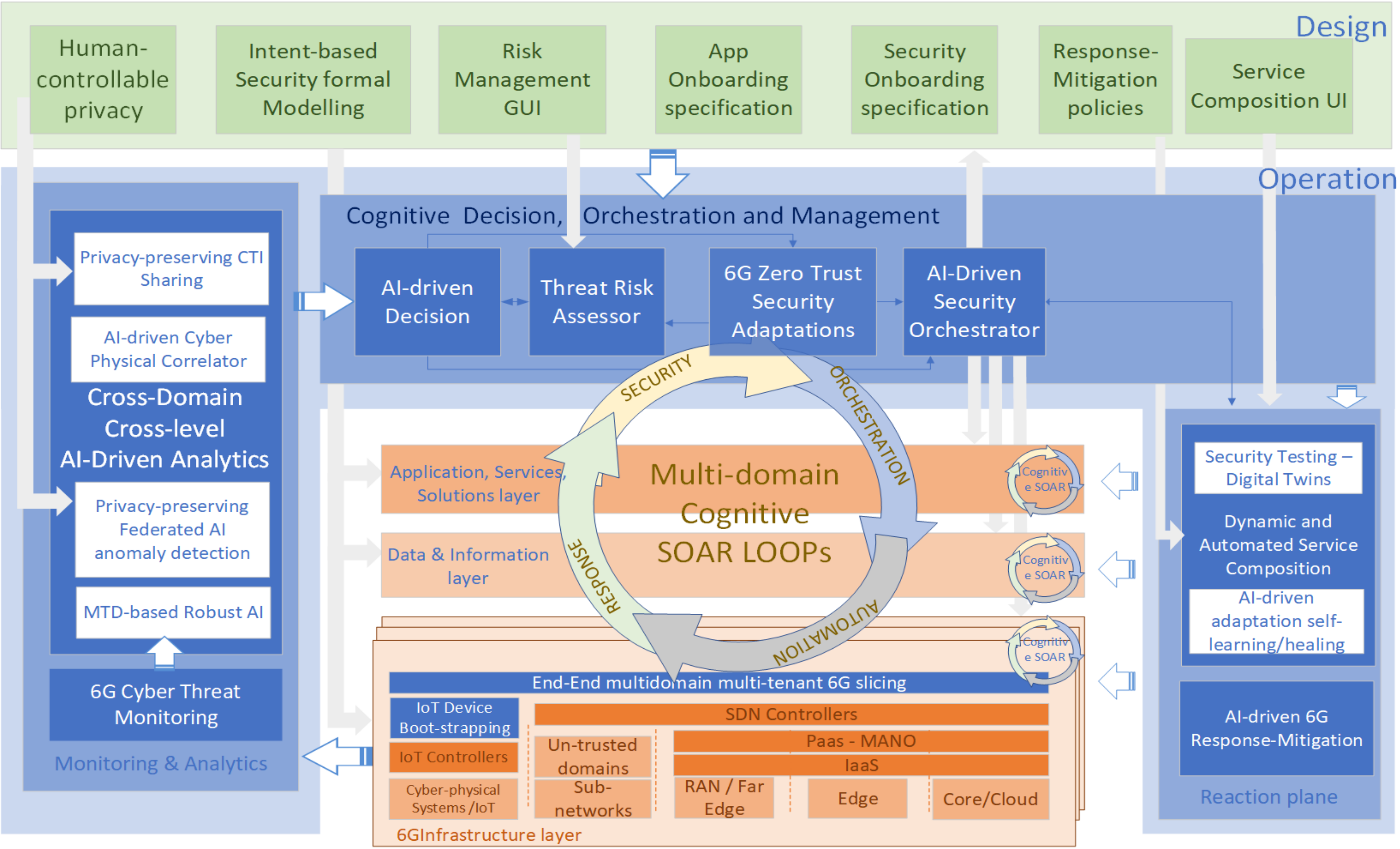
This objective will validate and demonstrate the RIGOUROUS framework in a set of industrially relevant use cases of immersive services in operational environments, showcasing the key innovations provided by RIGOUROUS. Aiming for validation and demonstration of the RIGOUROUS frameworks, these use cases will allow both to assert the robustness of the solutions created, and to foster the discussion regarding future killer applications

UC1 - Protection of 6G-enabled Services against Cyber Threats,
UC2 - Digital City Twining Platform,
UC3 - Utilities Management and security, and
UC4 - PPDR IoT Situational Awareness platform.

Innovations

- Intent-based Security & Privacy Formal Modelling and Onboarding Specification
- AI-based Security Orchestration across Network Segments
- Privacy-preserving AI for Anomaly Detection in B5G
- End-to-End Multidomain 6G Slicing over Zero-touch Security Network Management
- 6G Zero Trust Security Adaptations
- Continuum SOAR Loop Reaction and Mitigation
- IoT Device Bootstrapping and Trusted Application Onboarding
- Intelligent Detection and Mitigation of EDoS Attacks against 6G Network Slicing
- MTD-based Robust Mechanisms for Enabling Trustable Autonomic Security
- End-to-End Threat Risk Assessment
- Dynamic and Automated Software Composition
- Cyber Physical Correlator
- AI-driven Decision-Making Mitigation Framework

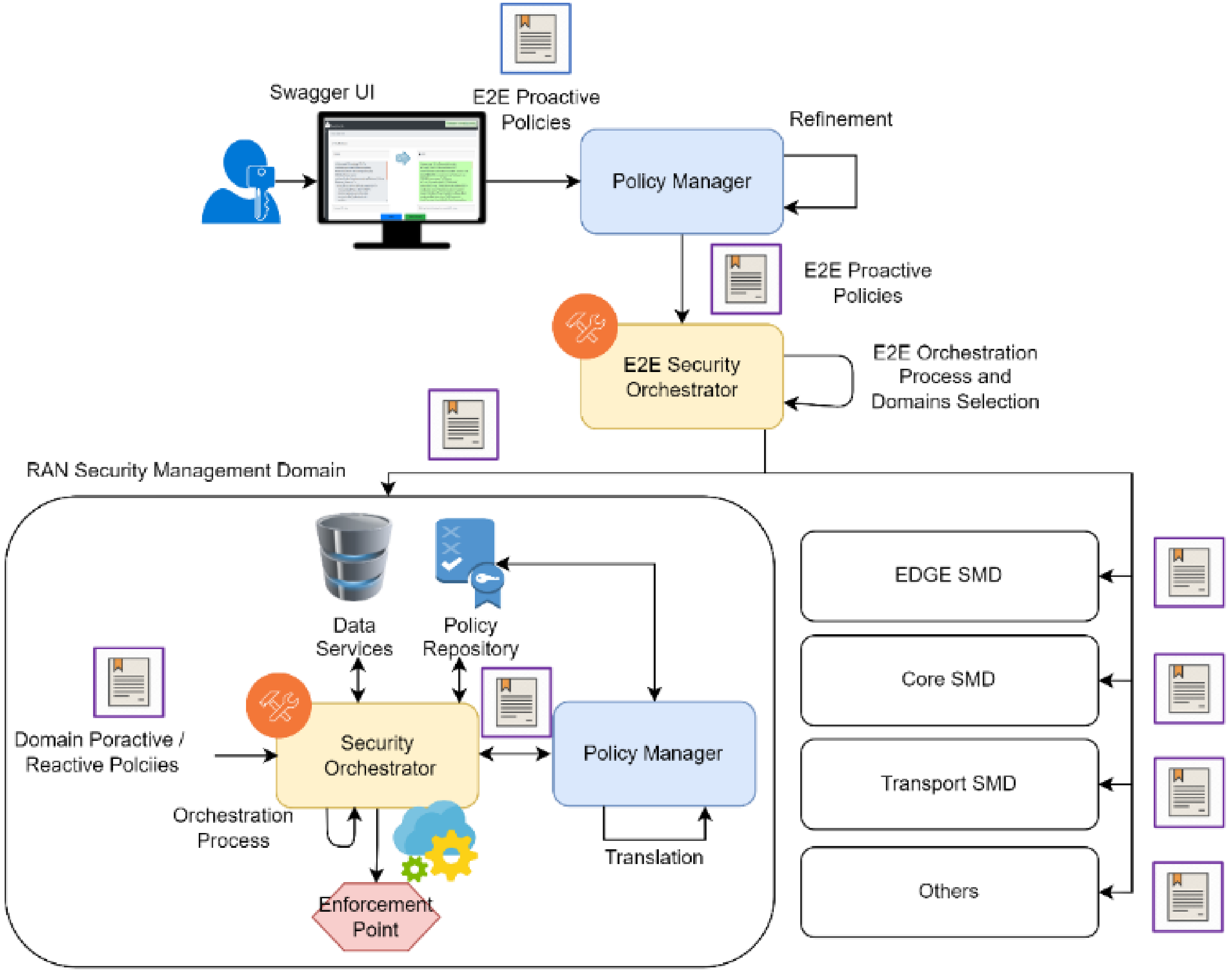
High-level Functional Architecture


Design
Human-controllable privacy
Intent-based Security formal Modelling
Risk Management GUI
App Onboarding specification
Security Onboarding specification
Response-Mitigation policies
Service Composition UI
Operation
Cognitive Decision, Orchestration and Management
AI-driven Decision
Threat Risk Assessor
6G Zero Trust Security Adaptations
AI-Driven Security Orchestrator
Privacy-preserving CTI Sharing
AI-driven Cyber Physical Correlator
Cross-Domain Cross-level AI-Driven Analytics
Privacy-preserving Federated AI anomaly detection
MTD-based Robust AI
6G Cyber Threat Monitoring
Monitoring & Analytics
SECURITY
ORCHESTRATION
AUTOMATION
RESPONSE
Multi-domain Cognitive SOAR LOOPs
Application, Services, Solutions layer
Data & Information layer
Cognitive SOAR
Cognitive SOAR
Cognitive SOAR
End-End multidomain multi-tenant 6G slicing
IoT Device Boot-strapping
IoT Controllers
Cyber-physical Systems /IoT
SDN Controllers
Un-trusted domains
Sub-networks
Paas - MANO
IaaS
RAN / Far Edge
Edge
Core/Cloud
6GInfrastructure layer
Security Testing – Digital Twins
Dynamic and Automated Service Composition
AI-driven adaptation self-learning/healing
AI-driven 6G Response-Mitigation
Reaction plane

Policy-based AI-driven Security orchestration

RIGOUROUS

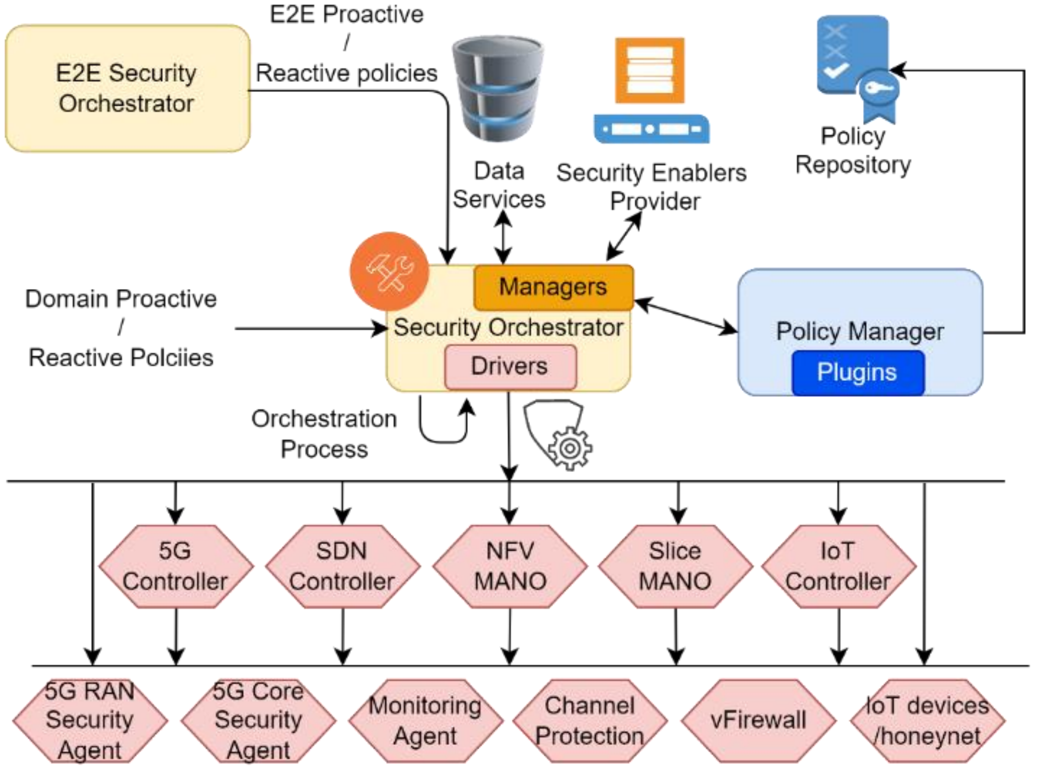
- User intent driven security policy definition
- The orchestrator will be driven by AI to make their chaining and orchestration decision
- Rely on special modules to translate the intents, policies and behavioural profiles coming from the decision into concrete actions
- **Federated Learning (FL)** approach to make orchestration decisions
- Decide best actions for **dynamic** provisioning, deployment, and **reconfiguration** (during operation) of the virtual network security functions and associated intents and policies
- Orchestrator will consider the time- and space-varying parameters of the network, such QoS capacities, actual resources constraints (CPU, RAM, storage), system status, current deployed policies, and threat incidents…



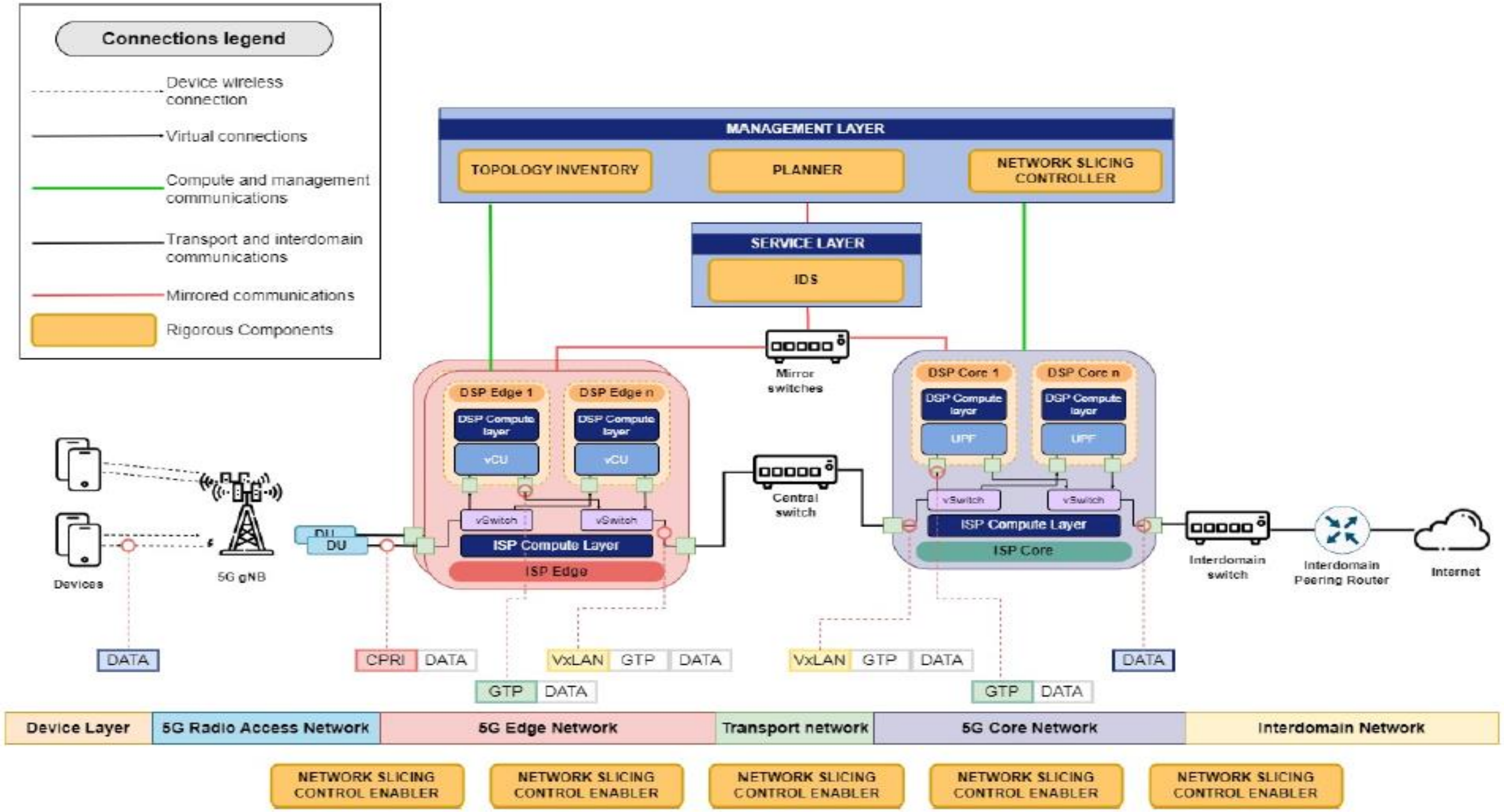
23/02/2023

Security enforcement

- Extensible orchestration enforcement:
  - NFV, SDN, IoT Controllers
- Integration with Security Enabler Providers (to enforce actions) and Trust Managers to make decisions
- ZSM approach



End-to-End multidomain multi-tenant 6G slicing

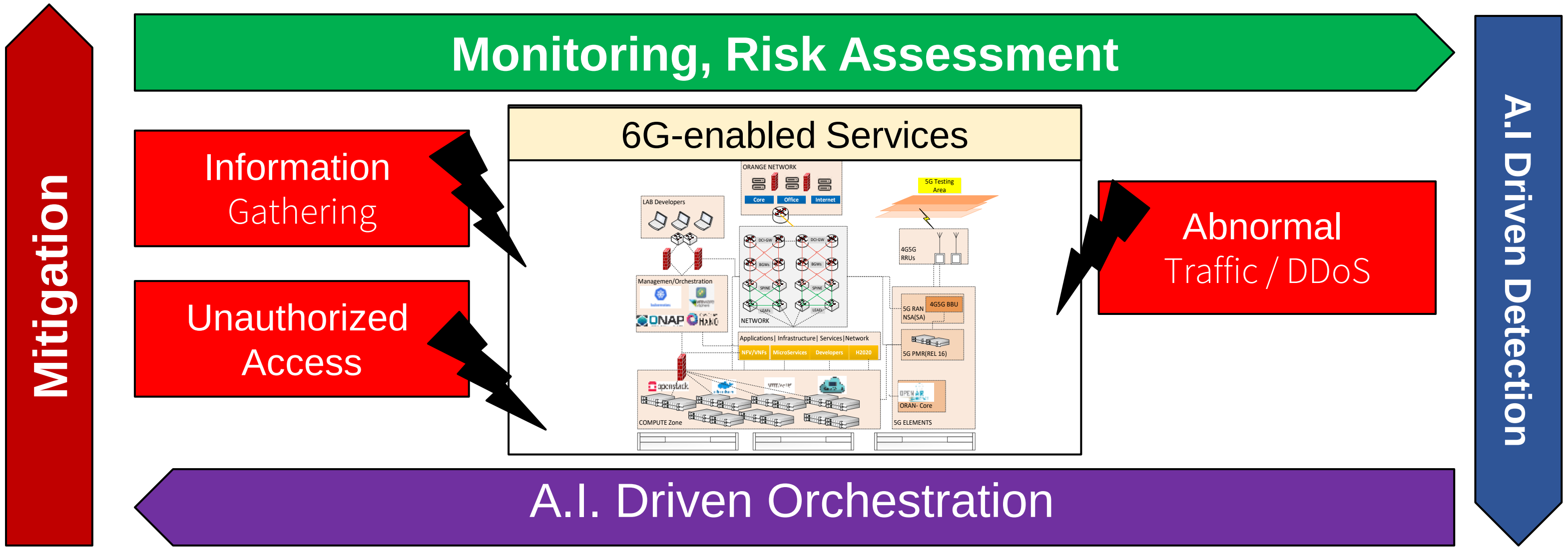


UC#1 description

It will validate the capacity and **capabilities of the platform to increase the resilience of the Telecom infrastructures** by protecting against threats to services offered by Orange Romania.

UC#1 **will run in Orange 5G LAB Bucharest***

- ❑ a complete 5G/6G testing network infra for several use cases (IoT – edge – cyber)
- ❑ suitable to be exposed as a 5G/6G infra running security threats
- ❑ includes the 5G/6G network components and functions



Mitigation

Monitoring, Risk Assessment

6G-enabled Services

Information Gathering

Unauthorized Access

Abnormal Traffic / DDoS

A.I. Driven Orchestration

A.I Driven Detection

* https://5glab.orange.ro/en

Areas of Standardization

- Project activities / technologies that may lead to standardization:
  - LNVO’s Distributed Ledgers and EDGE Services (ETSI PDL / ETSI MEC);
  - prediction of the performance of the physical devices and dynamic task allocation (IEEE P2413);
  - IoT security architecture for trusted IoT devices (AIOTI WG5);
  - Machine Learning applied for 5G/6G Network Management (ITU 5GMLFG)
- Potential targeted standardization bodies / groups:
  - ETSI ISG MEC, ISG ZSM, ISG NFV, PDL
  - IEEE ComSoc IoT Emerging Technologies Subcommittee
  - AIOTI Standardization WG
  - 5G-PPP / 6G-IA
  - 3GPP (CT1 / SA2 / SA3 / SA5 /SA6)
  - ITU 5GML FG

Conclusion

- RIGOUROUS will investigate on
  - End user intent based security policy management and its deployment
  - Zero trust and Smart security management
  - End-to-End multidomain multi-tenant 6G slicing
  - AI-driven Security Evolving, Response and Mitigation
  - AI driven federated cross-domain analytics

- Validation over several use case and 5G testbed

RIGOUROUS: secu**R**e des**IG**n and depl**O**yment of tr**U**sthwo**R**thy c**O**ntin**U**um computing 6G **S**ervices

Thanks

Follow us at https://rigourous.eu/

Antonio Skarmeta skarmeta@um.es

University of Murcia - Spain

23/02/2023

RIGOUROUS has received funding from the European Union’s HE Research and Innovation Programme HORIZON-JU-SNS-2022 under Grant Agreement No 101095933