MAchine learning-based, networking and computing infrastructure ReSource mAnagement of 5G and Beyond inteLligent networks: the MARSAL Vision

Kostas Ramantas

Senior Researcher

kramantas@iquadrat.com

John Vardakas

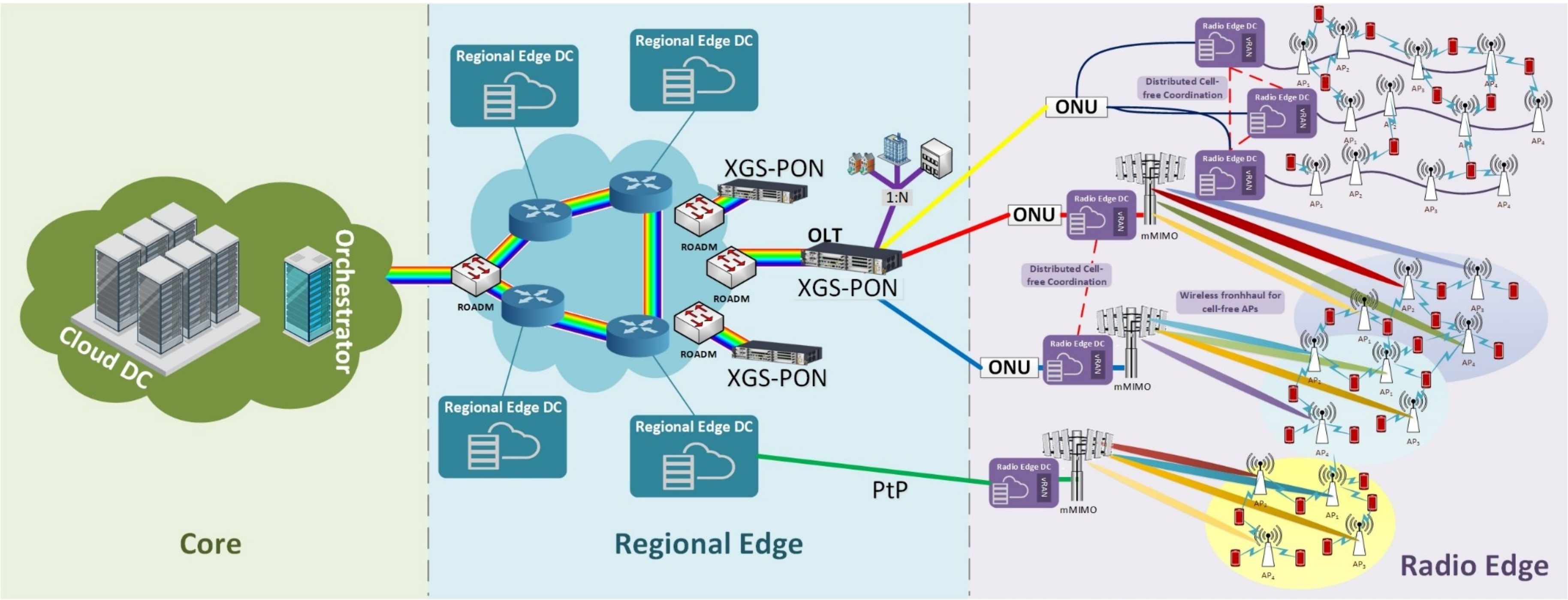
Senior Researcher

jvardakas@iquadrat.com

MARSAL project network architecture

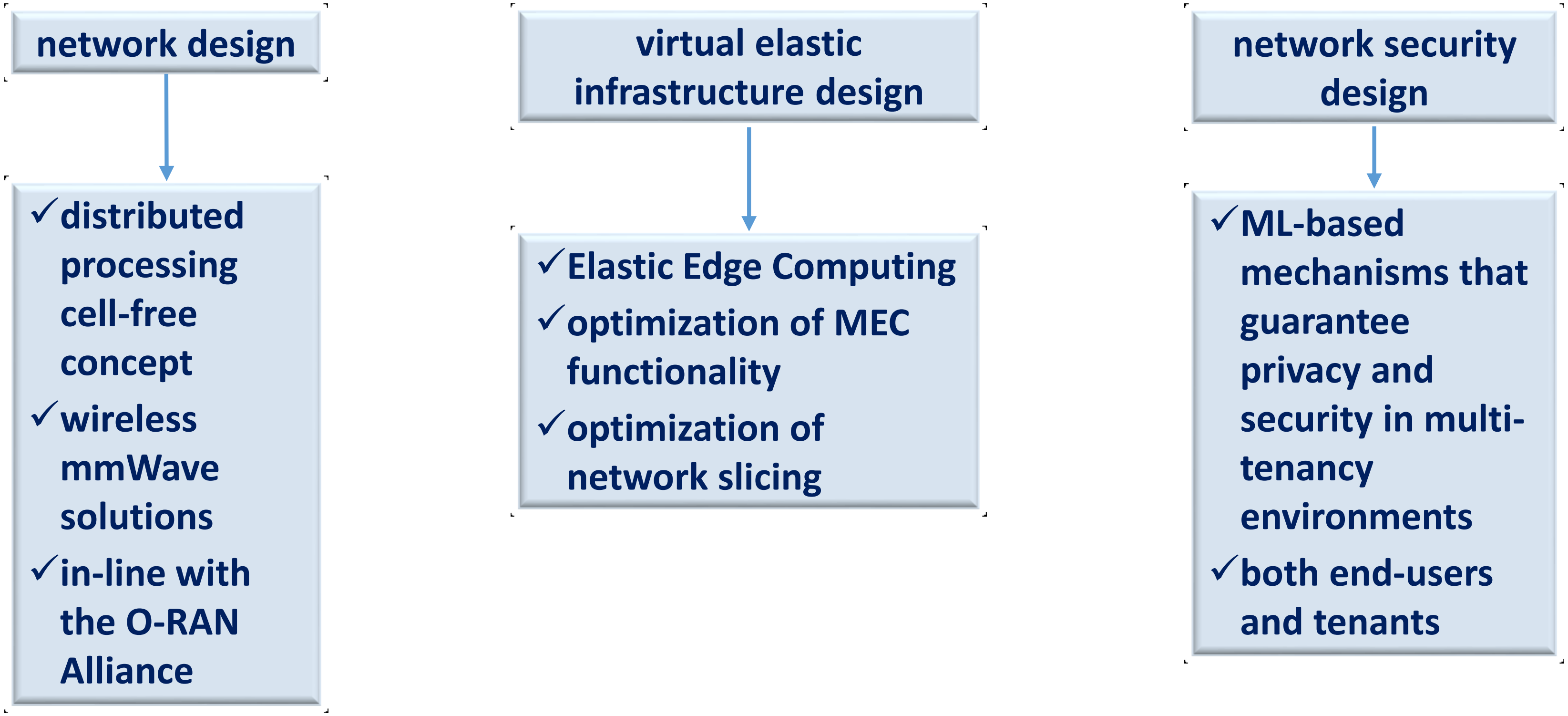
iquadrat

MARSAL



MARSAL project concept

MARSAL focuses on three pillars to enable a new generation of ultra-dense, cost-efficient, flexible and secure networks



network design

- ✓ distributed processing cell-free concept
- ✓ wireless mmWave solutions
- ✓ in-line with the O-RAN Alliance

virtual elastic infrastructure design

- ✓ Elastic Edge Computing
- ✓ optimization of MEC functionality
- ✓ optimization of network slicing

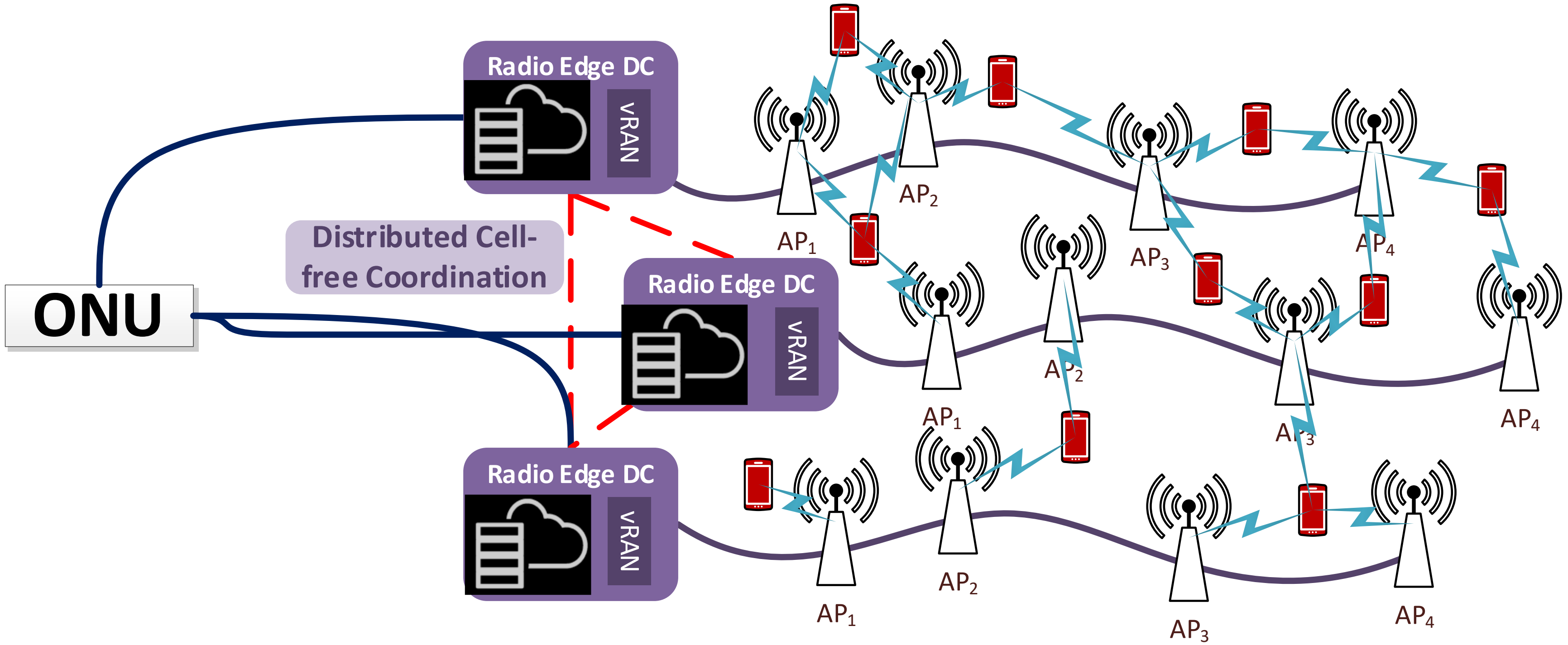
network security design

- ✓ ML-based mechanisms that guarantee privacy and security in multi-tenancy environments
- ✓ both end-users and tenants

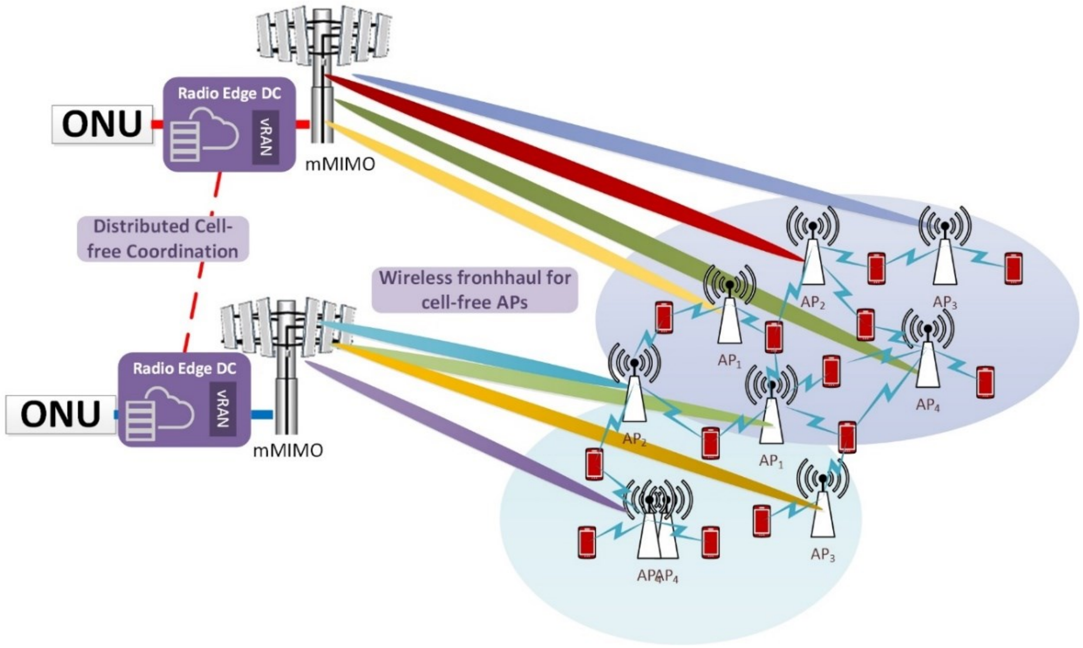
MARSAL: multi-DU CF configuration

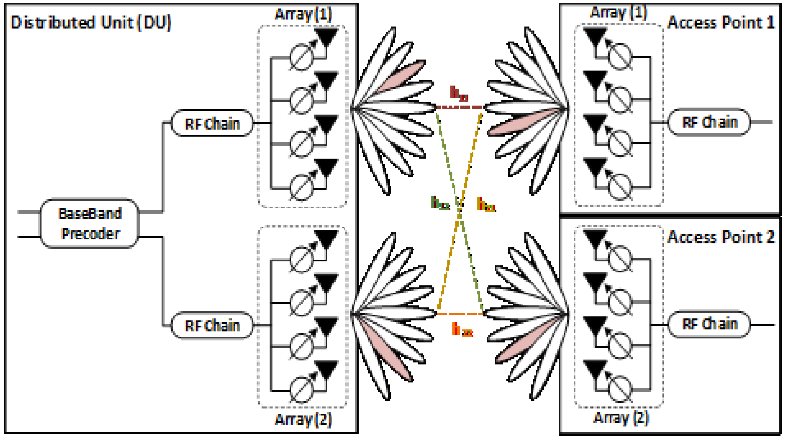
iquadrat

MARSAL



MARSAL: Hybrid MIMO Fronthaul



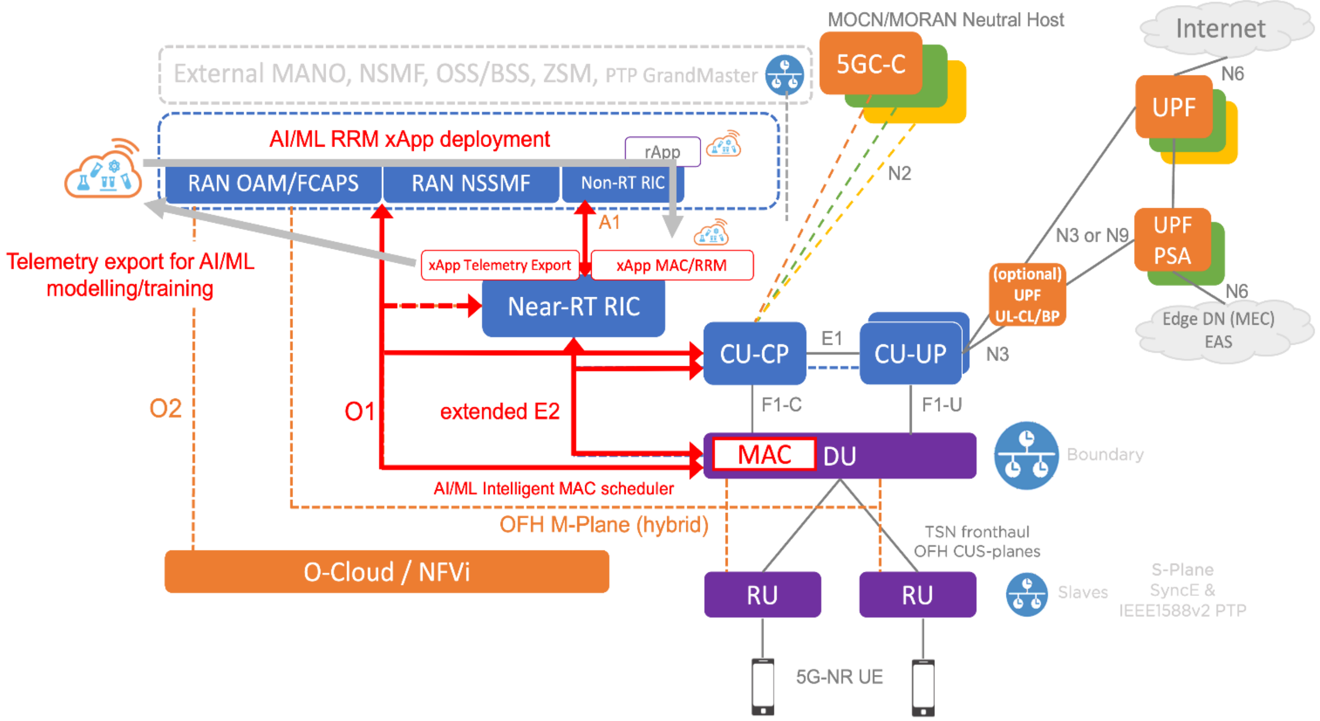


- ➢ An innovative cell-free and Hybrid MIMO combination for the RAN and Fronthaul domains that will unlock the potential of cell-free networking in future B5G networks
- ➢ Optimal AP deployment strategies that fully exploit the capabilities of Hybrid MIMO
- ➢ Dynamic AP clustering
- ➢ Functional splitting

MARSAL:Cell-Free – ORAN alignment

iquadrat

MARSAL

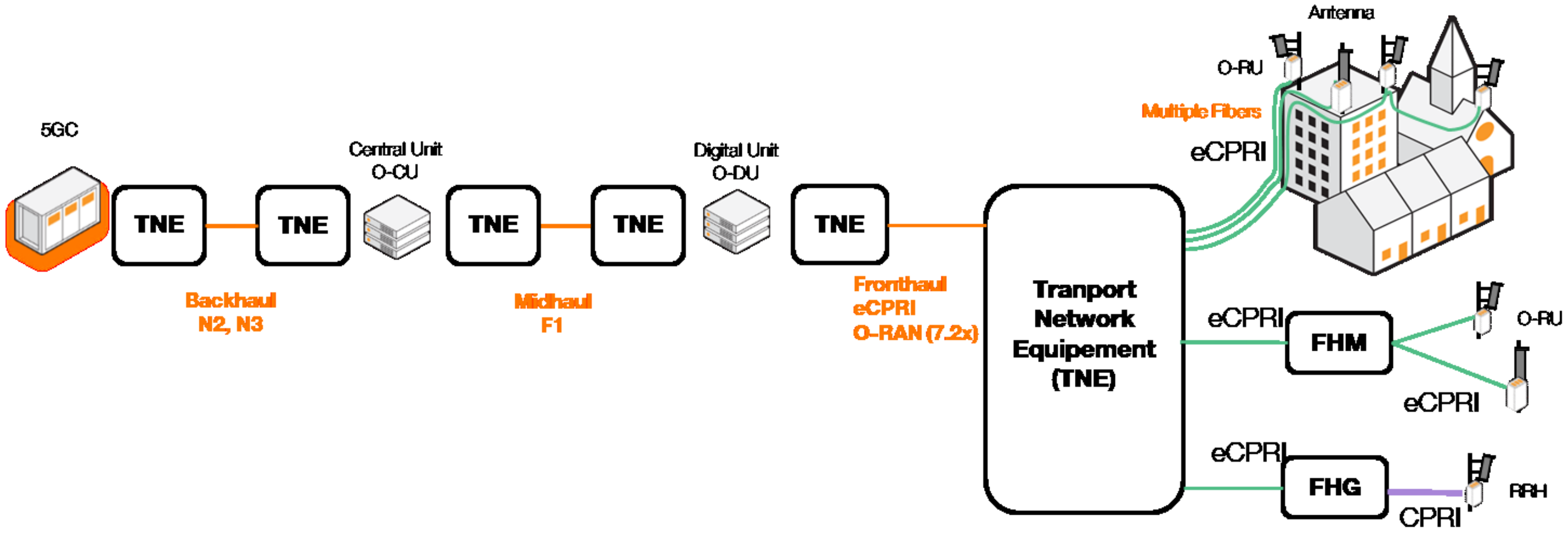


- CU User Plane function and DU deployment at the Radio Edge
- ORAN-compliant CU and DU components in the form of RAN VNFs, and use APs as RUs
- CF support in ORAN’s architecture

Converged optical-wireless fronthaul

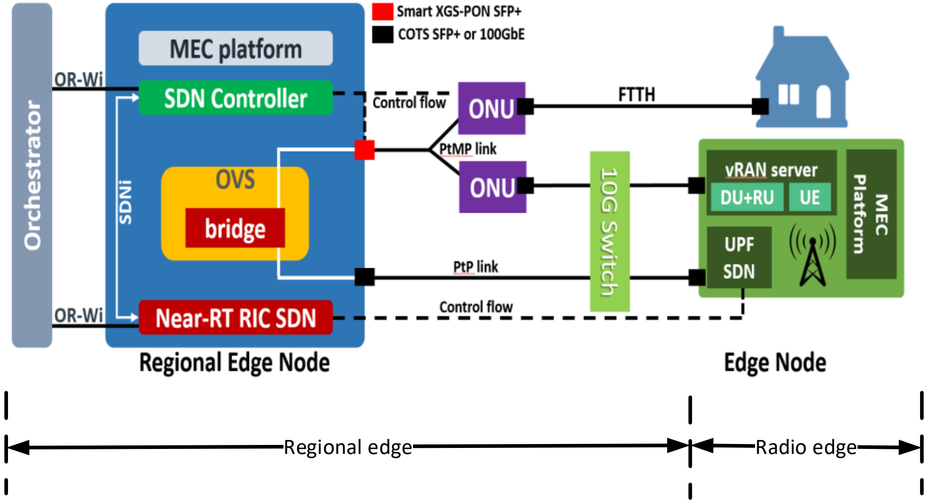
iquadrat

MARSAL



- ➢ A novel Fixed Mobile Convergence (FMC) solution can be supported to facilitate integrated connectivity of mobile and fixed (i.e., FTTH) services, that share the same Midhaul and Edge infrastructure (e.g., MEC hosts) and are both served by the 5G core.
- ➢ FMC is implemented through two transmission approaches seamlessly integrated at the Regional Edge node, including a standard point-to-point (PtP) connection with or without wavelength division multiplexing and a very disruptive point-to-multipoint (PtMP) approach based on XGS-PON modules.

Converged optical-wireless fronthaul

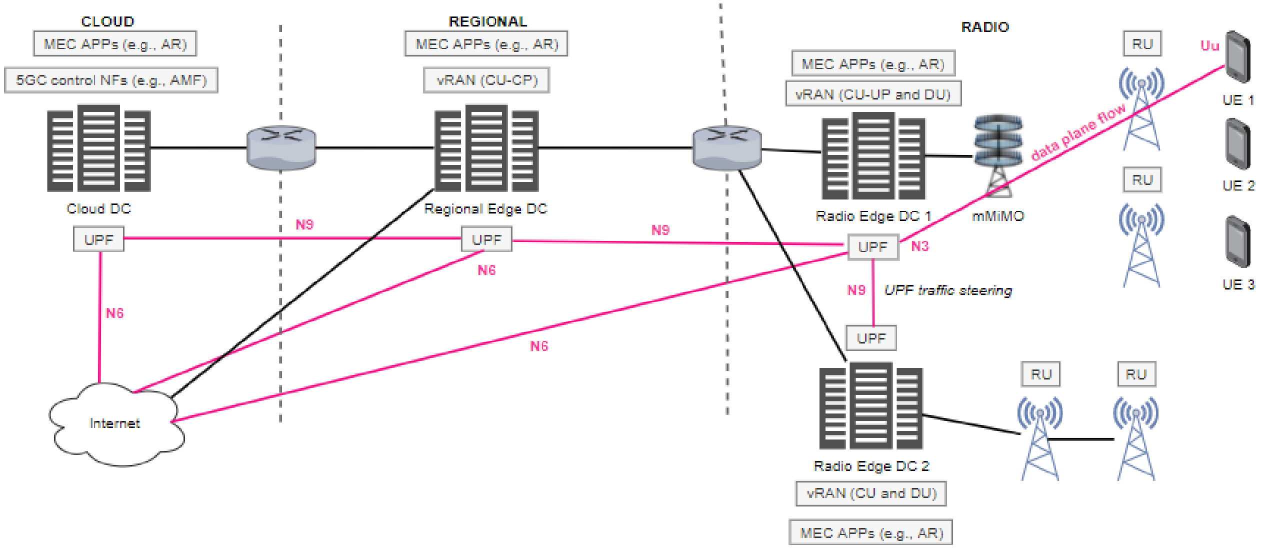


- ➢ Most optical / wireless convergence in C-RAN architectures are centralized, and thus sub-optimal for disaggregated vRAN solutions
- ➢ O-RAN solution is also centralised, since the O-RAN Orchestration and Automation layer is deployed at the Core tier:
- ➢ A novel hierarchical control plane solution, federating the SDN controllers of the fixed segment (i.e., the Midhaul) and mobile segment (i.e., the cell-free RAN) of the network under a common orchestration subsystem.

Converged optical-wireless fronthaul

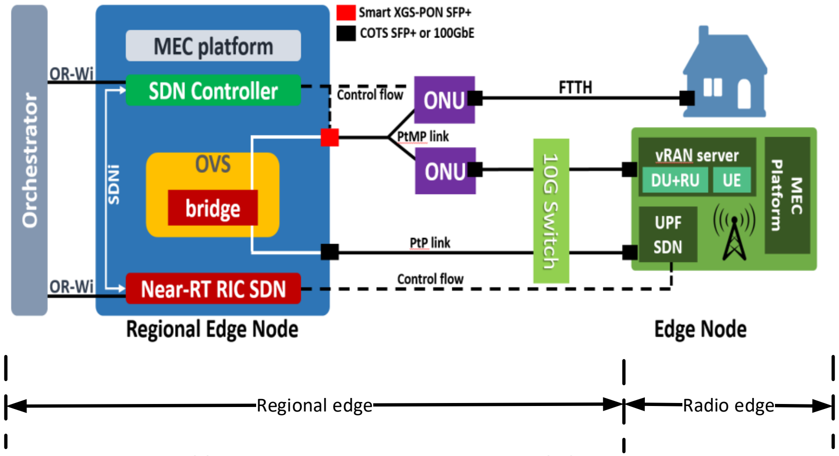
iquadrat

MARSAL



- Disaggregation of the Non-RT SDN Control function into Near-RT SDN functions that will be hosted by the Near-RT RIC at the Regional Edge nodes.
- Deployment of Software-Defined Transport Network Controllers (i.e., SDTNs) at the Regional Edge to control the fixed segment, i.e., the Midhaul (or E2) interfaces, that will be implemented with standard Optical Ethernet technologies. The Core Tier NFVO, based on ETSI OSM will provide **Network Slicing As a Service (NSaaS)** functionality as per 3GPP TR 28.801 specifications via the OR-Wi Southbound SDN interfaces and WIM plugins offered by ETSI OSM,
- Thus, End-to-End slicing with centralized orchestration is supported, while still allowing innovative closed-loop (or ML-driven) control of each individual domain.

Converged optical-wireless fronthaul



- This optical access architecture offers a high degree of flexibility, allowing capacity to be dynamically shared by fixed and mobile clients, leveraging on the aforementioned hierarchical control plane:
- The SDTN controller can flexibly control traffic aggregation at the Regional Edge node and dynamically configure various parameters at the SFP-OLT level
- An energy efficiency scenario can also be considered, with traffic aggregation on a limited set of wavelengths which will allow shutting-down individual SFP+ transceivers.
- Predictive dynamic slicing approaches can also be explored, leveraging an ML-driven control loop to trigger slice reconfiguration proactively, based on Convolutional Neural Networks (CNNs) that predict traffic fluctuations.

Security in MARSAL

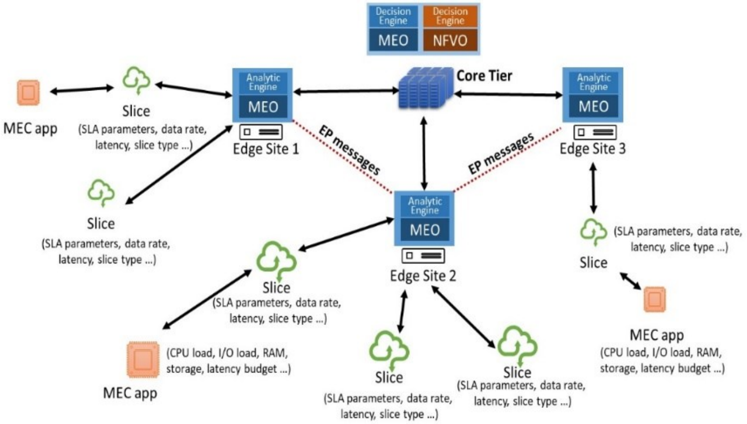
Network security pillar

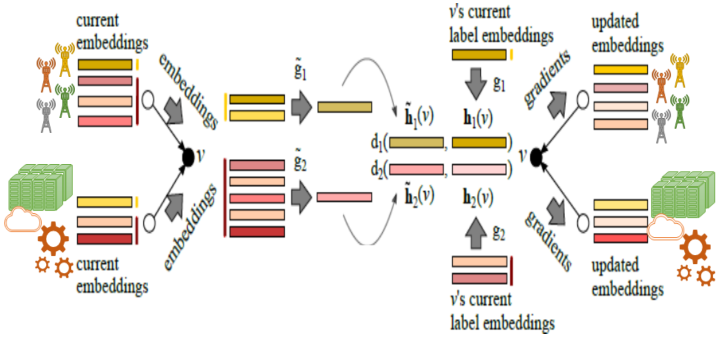
ML and Blockchain technologies for trust-less multi-tenant slicing

Policy-driven data protection and integrity assurance

Hardware Accelerated, ML-based data plane security and malicious traffic detection

1. Delivery of a decentralized, blockchain-based platform that supports Network Slicing transactions via Smart Contracts, integrated with the NSaaS subsystem
2. Implementation new privacy-preserving Context representations, for the exchange of local embeddings
3. Innovative techniques guarantee that embeddings can't be reversed.


Decision Engine
MEO
Decision Engine
NFVO
Core Tier
Analytic Engine
MEO
Edge Site 1
Analytic Engine
MEO
Edge Site 3
Analytic Engine
MEO
Edge Site 2
EP messages
EP messages
MEC app
Slice
(SLA parameters, data rate, latency, slice type ...)
Slice
(SLA parameters, data rate, latency, slice type ...)
Slice
(SLA parameters, data rate, latency, slice type ...)
(SLA parameters, data rate, latency, slice type ...)
Slice
MEC app
(CPU load, I/O load, RAM, storage, latency budget ...)
(CPU load, I/O load, RAM, storage, latency budget ...)
MEC app
Slice
(SLA parameters, data rate, latency, slice type ...)
Slice
(SLA parameters, data rate, latency, slice type ...)



Security in MARSAL

iquadrat

MARSAL

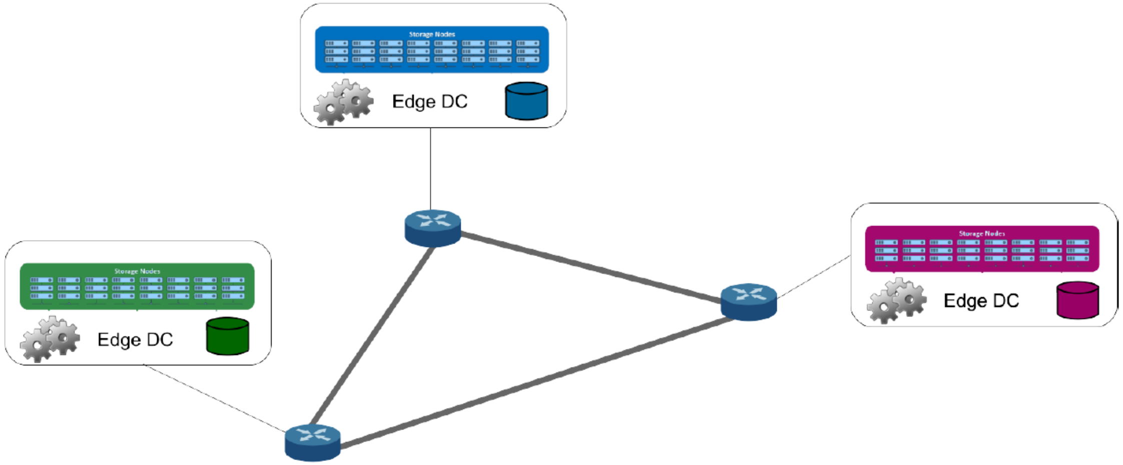
Network security pillar

ML and Blockchain technologies for trust-less multi-tenant slicing

Policy-driven data protection and integrity assurance

Hardware Accelerated, ML-based data plane security and malicious traffic detection

1. Authorizations that each infrastructure owner can define over its data, which support three levels of visibility over data (no visibility, full visibility, and partial visibility over encrypted versions of data
2. Solution to the problem of computing an assignment of the operations in a computation to subjects such that the economic cost associated with the execution of the computation is minimized



Security in MARSAL

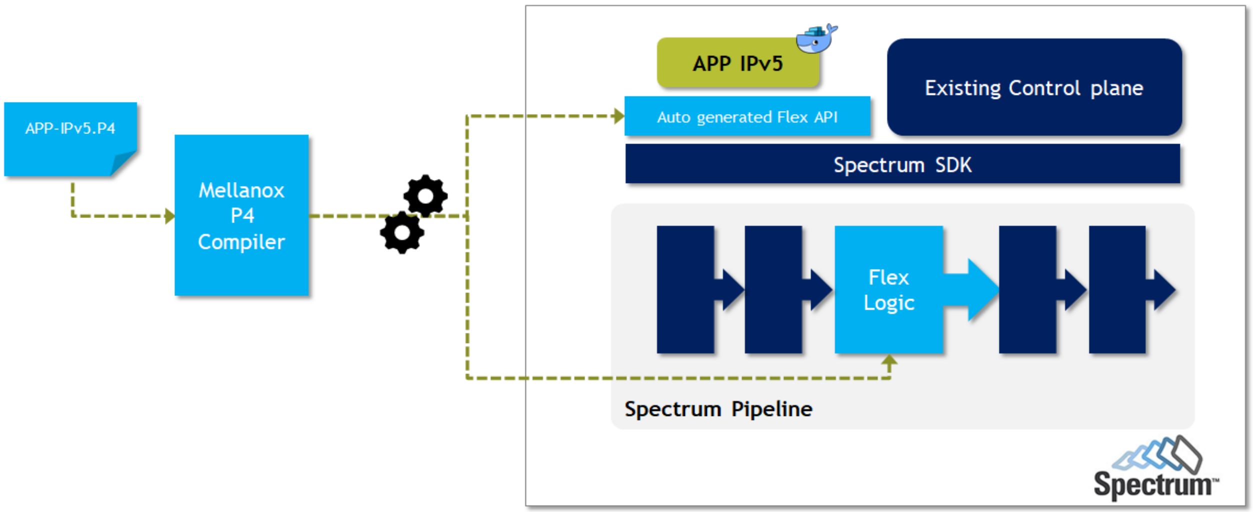
iquadrat

MARSAL

Network security pillar

- ML and Blockchain technologies for trust-less multi-tenant slicing
- Policy-driven data protection and integrity assurance
- Hardware Accelerated, ML-based data plane security and malicious traffic detection

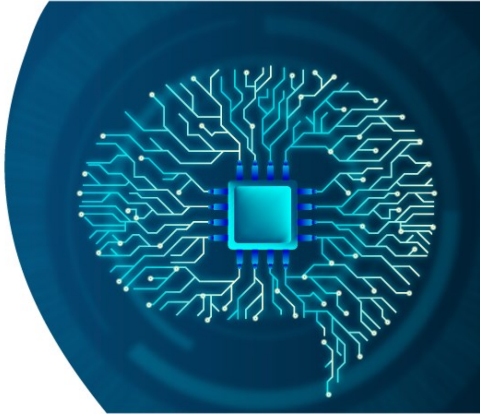
1.provide hardware accelerated solutions for a decentralized Threat Detection Engine and a centralized Threat Analysis Engine
2.leverage the capabilities of a new generation of MELX programmable SDN Switches, that support the new P4 programming language for stateful processing, header inspection, and packet metadata extraction
3.propose a centralized Threat Analysis Engine (TAE), that will operate as an ML Fusion Centre



MARSAL factsheet

MARSAL

iquadrat



✓ **Grant Agreement:** 871780

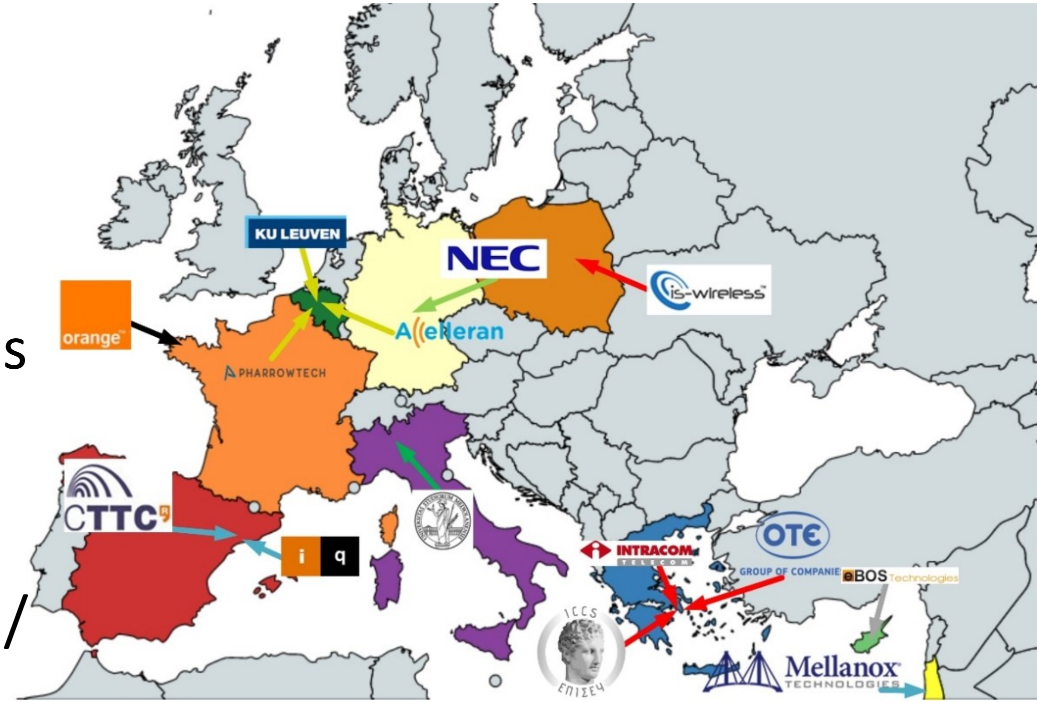
✓ **Duration:** 36 months

✓ **Starting date:** 01/01/2021

✓ **EC funding:** 6,126,683.75 Euros

✓ **Total PMs:** 703.5

✓ **URL:** https://www.marsalproject.eu/



Thank you!

KOSTAS RAMANTAS

SENIOR RESEARCHER

KRAMANTAS@IQUADRAT.COM

JOHN VARDAKAS

SENIOR RESEARCHER

JVARDAKAS@IQUADRAT.COM