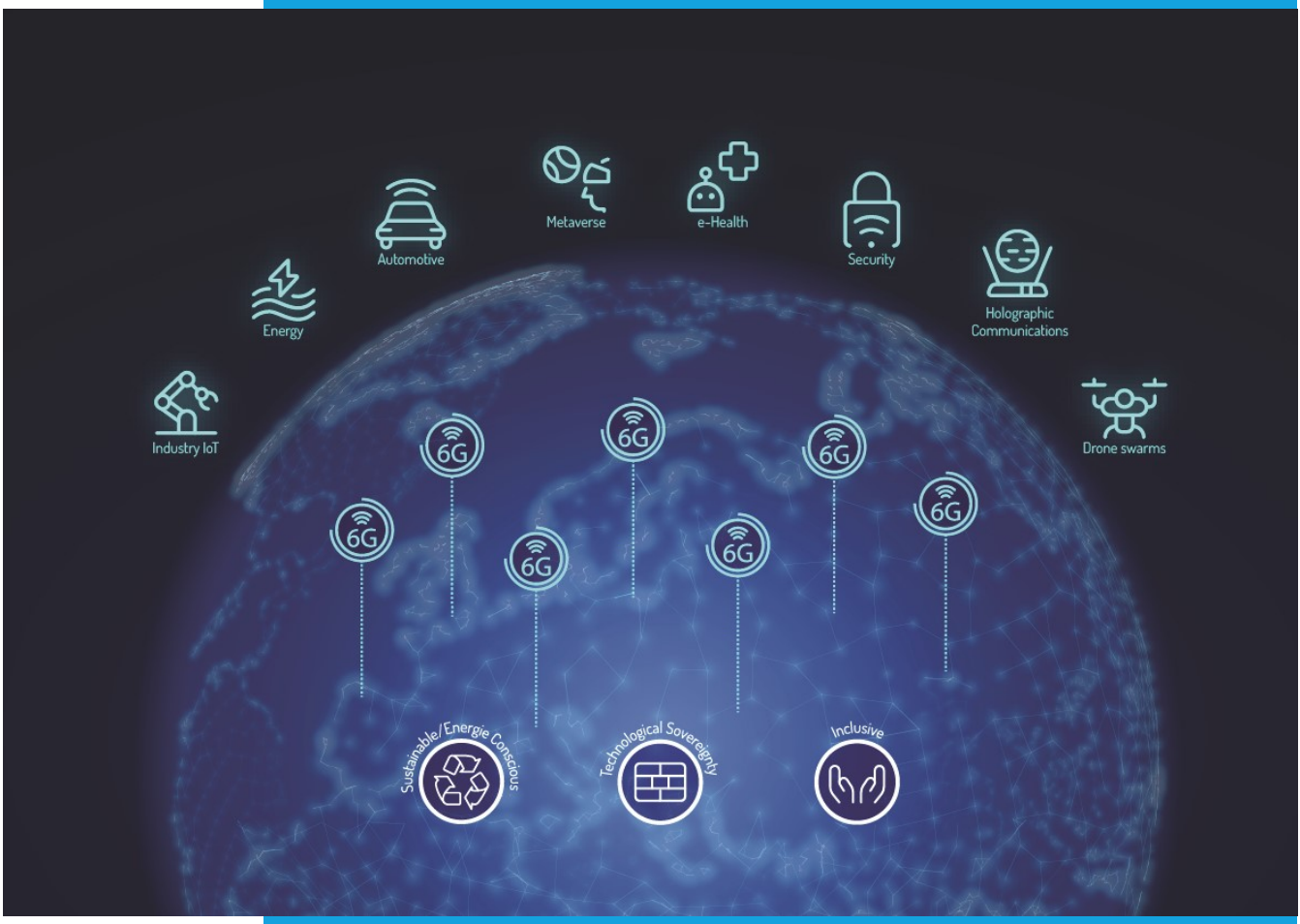
Smart Networks and Services Joint Undertaking (SNS JU)
Reliable Software Networks Working Group (SoftNet WG)



Version 1.0
December 2024

WHITE PAPER

NETWORK AND SERVICE MANAGEMENT ADVANCEMENTS

Key Frameworks and Interfaces towards Open, Intelligent and Reliable 6G networks

DOI: 10.5281/zenodo.14234897
URL: https://doi.org/10.5281/zenodo.14234897

EXECUTIVE SUMMARY

Software has emerged as an essential part of mobile telecommunication networks for the efficient and effective operation of the 5G and 6G systems. This trend is evident in several network processes, among others in network *programmability, management and security*, while it has enabled automation in service and resource management processed with the integration of artificial intelligence (AI) and machine learning (ML) mechanisms.

A key role for enabling programmability in telecommunication is played by Application Programming Interfaces (APIs) and frameworks. Indeed, APIs are considered as the main way to harvest and expose the capabilities of 6G networks. On the one hand, APIs enable standardized, seamless interaction between software components and network services, supporting features like capability exposure, edge computing, AI/ML, and integration of other technology domains like cloud computing, data analytics and Internet of Things. APIs facilitate the integration of complex 6G use cases, enhancing interoperability and supporting dynamic service creation and management. On the other hand, API frameworks provide reusable components that address network programmability, scalability, intelligent operations, and security. They accelerate the development of high-performance use cases for 6G by ensuring consistent and structured solutions. Frameworks are essential for managing the dynamic, scalable nature of 6G networks and driving innovation.

In the network management domain, 6G networks are poised to revolutionize the telecommunications landscape by intelligently supporting a vast number of simultaneous and heterogeneous network slices tailored to various vertical use cases. However, this advancement brings forth challenges related to scalability and sustainability, particularly in the deployment of AI-driven zero-touch Management and Orchestration (MANO) of End-to-End (E2E) slices under stringent Service Level Agreements (SLAs). To address these challenges, next-generation networks will incorporate mechanisms at multiple levels to optimize resource allocation for enhanced service management. Several enablers have been identified that support the challenges.

In the context of security in 6G networks, a wide range of topics is considered, including but not-limited to Secure Onboarding, SOAR (Security Orchestration, Automation, and Response)-enhanced 6G Orchestration, Decentralized Security Analytics, Remote Attestation, Privacy-Aware Orchestration, Cyber Threat Intelligence (CTI) Sharing and Trustworthiness assessment of network components. All These elements collectively contribute to a secure and trustworthy 6G network environment, while safeguarding user privacy and responding effectively to emerging threats.

Software, with APIs, frameworks, enablers, as well as advanced and tailored security, transforms 6G into a dynamic, intelligent, and secure platform capable of meeting the demands of future applications. These elements collectively drive innovation, scalability, and reliability while ensuring that 6G networks remain adaptable and resilient in a rapidly evolving technological landscape.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

Abbreviation	Meaning
3GPP	3rd Generation Partnership Project
5G	5th Generation
5G IA	5G Infrastructure Association
5G PPP	5G Public Private Partnership
6G	6th Generation
6G IA	6G Industry association
ADRF	Analytic Data Repository Function
AEF	API Exposure Function
AI	Artificial Intelligence
AMF	API Management Function
APF	API publishing function
API	Application programming Interface
AUF	Authorisation Function
B5G	Beyond 5G
CAPIF	Common API Framework
CCF	CAPIF Core Function
CDF	Cumulative Distribution Function
CNF	Containerized network function
CSP	Communication Service Provider
CTI	Cyber Threat Intelligence
DLT	Distributed Ledger Technology
DRL	Deep Reinforcement Learning
E2E	End-to-End
eMBB	Enhanced Mobile Broadband
EMF	Electric and Magnetic Fields
ETSI	European Telecommunication Standards Institute
FL	Federated Learning
GSMA	Global System for Mobile Communications Association
HW	Hardware
IBN	Intent Based Network Management
ICT-52	5G-PPP ICT-52-2020
IDO	Intent-Driven Orchestration
IETF	Internet Engineering Task Force
INT	In-band Network Telemetry
ITE	Information Technology Equipment
KPI	Key Performance Indicator
LCM	Life Cycle Management
LMLC	Low mobility large cell
MANO	Management and Orchestration
MAS	Multi-Agent System
MEAO	Mobile Edge Application Orchestrator

MEC	Multi-access Edge Computing
MIMO	Multiple Input Multiple Output
ML	Machine Learning
mMIMO	Massive MIMO
mMTC	Massive Machine Type Communications
MNO	Mobile Network Operator
NDT	Network Digital Twin
NFV	Network Function Virtualization
OAM	Operation Administration and Management
OCF	Open CAPIF
OS	Operating System
OSL	Open Slice
RAN	Radio Access Network
RFC	Request for Comments
RL	Reinforcement Learning
RNAA	Resource owner-aware Northbound API Access
RO	Resource Owner
ROC	Resource Owner Client
SBA	Service Based Architecture
SBI	Service Based Interface
SCP	Service Communication Proxy
SDG	Software Development Groups
SLA	Service Level Agreement
SMO	Service Management and Orchestration
SNS	Smart Networks and Services
SNS JU	Smart Network and Services Joint Undertaking
SOAR	Security Orchestration, Automation, and Response
SW	Software
TAPI	Transport API
TFS	TerraFlow SDN
TLS	Transport Layer Security
UE	User Equipment
VIM	Virtualized Infrastructure Manager
VNF	Virtual network function
VPN	Virtual private network
XAI	Explainable AI
ZSM	Zero-touch Network and Service Management

1. INTRODUCTION

This document presents recent advancements in network and service management, focusing on key frameworks and interfaces towards open, intelligent and reliable 6G networks. The content reflects the work that has been done in various SNS JU projects[1], all of them converging to a key message; there is a need for open software solutions and standardized interfaces that can facilitate the development of the new era in network and service management.

The document is structured in three main sections, namely Section 2, 3 and 4, covering respectively: programmability (exposure services and interfaces), management (end-to-end automated management over a compute continuum) and security (secure orchestration including privacy and trustworthiness considerations) enablers for 6G telecommunication networks and systems.

Section 2 delves into the role of Application Programming Interfaces (APIs) and frameworks in enabling seamless interaction between software components and network services.

Concerning management and orchestration APIs, a wide variety exists, and the following list is not conclusive. APIs for Service and Resource Management and Orchestration are central to managing 6G services and resources, Service Management APIs handle lifecycle management, adapting services to evolving conditions, while Resource Management APIs optimize the allocation of bandwidth, computing capacity, and storage.

Furthermore, Closed-Loop Runtime APIs highlight AI-driven control operations in 6G. These APIs enable real-time network management through monitoring, analytics, decision-making, and execution, supporting closed-loop systems for dynamic network optimization. AI/ML services interact with these APIs, aligning with standards like ETSI Zero-touch Service Management (ZSM).

A further set of APIs address network monitoring and control. APIs for Network Telemetry and Monitoring facilitate efficient data retrieval, essential for network performance optimization. Tools like gRPC, NETCONF, and Apache Kafka enable telemetry data collection from diverse network components, ensuring smooth monitoring and control.

Transport Network Control APIs manage optical and packet/optical devices using data modelling languages like YANG and controllers like ETSI TeraFlowSDN. This framework ensures efficient orchestration of complex transport networks, with the TeraFlowSDN controller playing a key role in network provisioning and telemetry management.

[1] Mainly referring to SNS JU Call 1 projects: https://smart-networks.europa.eu/sns-call-1/

Lastly, a common API framework, called CAPIF, is a central element in Management of API-based Services. CAPIF enables secure, open network access across different network layers. It facilitates API registration, discovery, and authentication, promoting a unified approach to API management, as for example demonstrated by the integration with ETSI MEC (Multi-access Edge Computing) where it ensures real-time service execution at the edge, aligning CAPIF with emerging edge computing needs

Section 3 focuses on service and resource management aspects. At service level, architectures towards a common and intent-based service management and orchestration are provided. At resource level, the compute continuum potential in 6G era is examined. The role of AI/ML for resource management is also highlighted, while the challenges set from heterogeneous infrastructure (like the 3D networks) are provided.

At service management level a common and intent-based approach is envisioned with representative example the Open RAN evolution towards a 6G Common Service Management Orchestrator (SMO). SMO proposes a unified orchestrator for RAN, Core, and Transport domains, with a shift towards distributed, federated architectures. On top of this, Intent-Based Network Management (IBN) can be applied, with the main role to align network operations with business objectives, translating high-level intents into actionable tasks. In addition, Multi-Agent Systems (MAS) for distributed decision-making and knowledge sharing among network entities, can enhance responsiveness and coordination.

At (compute) resource level, an Edge-to-Cloud Compute Continuum is realized. Frameworks like ReproRun/ReproAccel, split computing, COMPSs, TMForum oneAPI, and federated learning to support distributed computing across edge and cloud resources. In this framework Meta-Operating Systems manage the edge-cloud continuum, providing services like federation, data fabric, cybersecurity, trust management, and AI decision support. Integration of Extreme Edge Resources is also under intensive consideration. It focuses on managing resources beyond the RAN, including IoT sensors and mobile devices, through a constrained MEC (cMEC) architecture.

Towards dynamic management of any type of resources services and infrastructures AI/ML is a powerful and widely adopted tool. AI/ML algorithms are used already for local control loops. Reinforcement learning is a good fit for near-real-time resource management, while Federated Learning can be used to ensure SLA compliance and efficient resource utilization.

Section 4 addresses the critical aspects of security and trust in 6G networks, highlighting enhanced security management, privacy considerations, and decentralized security analytics.

Focusing on privacy considerations, emphasizes is given at the integration of Security Orchestration, Automation, and Response (SOAR), Moving Target Defense (MTD), and Privacy-Enhancing Technologies (PETs) to ensure privacy during the onboarding of network applications. Privacy modeling is also a key aspect. Φor this purpose, current approaches use privacy manifests and quantification models, allowing users to assess and compare the privacy levels of different services.

Towards secure orchestration the integration of intelligent processes is fundamental. Deep Reinforcement Learning (DRL) may be used to guide orchestration decisions based on the Level of Trust (LoT) and Privacy Index (PI) metrics. In addition, federated learning, differential privacy techniques, and adversarial training to enhance the robustness and privacy of AI/ML models used in security analytics. Cyber Threat Intelligence (CTI) Sharing is also under study where distributed indexes and proxies are used to facilitate the confidential exchange of threat intelligence among stakeholders.

The establishment of trustworthiness is a key pillar in 6G networks, and as such related frameworks are needed to offer cumulatively: isolation in deployment of network functions, verifiable credentials and regular security audits, as well as network alignment with security replated intents at business level.

Irrefutably, open-source solutions play a fundamental role towards the realization of the approaches and solutions presented in the main sections of the document. The use of and contribution to ETSI Software Development Groups (SDGs) like TeraFlowSDN, OpenSlice, OpenCAPIF, and Open-Source MANO are becoming a trend, facilitating collaboration and innovation in the telecom industry. Given that, in the Annexes of this document the reader can find fundamental information on open-source projects related to 6G, including projects hosted by ETSI, the Linux Foundation, and the TMForum. The catalogue of open-source projects covers the major ones that are currently used and expanded by SNS JU projects.

2. APPLICATION PROGRAMMING INTERFACES

The development of robust Application Programming Interfaces (APIs) and frameworks becomes crucial to harness the full potential of 6G. This section presents APIs and frameworks designed to support the diverse and demanding applications of 6G networks.

APIs will play a key role in the 6G ecosystem by providing standardized interfaces that enable seamless interaction between software components and network services. They facilitate the integration of advanced features such as edge computing and artificial intelligence, thereby creating a cohesive and interoperable environment. With 6G's promise of enhanced capabilities, APIs need to evolve to support more complex and demanding use cases, ensuring that applications can leverage the network's full capabilities efficiently and effectively.

Identifying API frameworks for 6G, on the other hand, we will be able to provide the essential scaffolding for building and deploying applications in the future landscape of 6G networks. These frameworks will offer pre-defined structures and reusable components that will potentially accelerate development processes and ensure consistency across different applications. In the context of 6G, frameworks will be instrumental in addressing challenges related to intelligent operation, orchestration, exposure, network programmability, scalability, security, and resource management, enabling developers to create innovative solutions that can meet the high performance and reliability standards expected of next-generation 6G networks, thus aid in the creation of more efficient and powerful applications but also drive the innovation needed to fully realize the potential of 6G

This section discusses the latest advancements in API design and framework development tailored for 6G technology as performed in SNS research projects. It examines the key features and capabilities that these APIs and frameworks must encompass to support the unique requirements of 6G applications. while providing insights into how APIs and frameworks are shaping the definition of 6G.

2.1. THE ECOSYSTEM OF TELCO APIS

Operators in the 5G era have a significant opportunity to monetise the capabilities of their networks. Moreover, with the existing relationships that operators have with enterprises, their vast local footprint, their ability to support digital sovereignty principles and their competence to provide high-reliability services, the missing piece is the ability to package and expose their networks in a scalable fashion across multiple operators. The Operator

Platform concept, as introduced in GSMA[2], describes the architecture of a generic platform to fill this gap, identifying main functional blocks and interfaces. A Network as a Service (NaaS) approach is proposed for realizing this concept[3]. The NaaS realization follows an agile, "code-first" and crowd-sourcing approach, which eventually opens the source code so that the industry community can adopt it, becoming a de-facto standard solution. Based on the abstract representation of the NaaS architecture (depicted in Figure 1), three main API types are identified.

- The **Service APIs** provide a purpose-specific capability to third parties, including management APIs, allowing the application developer to run certain management functions from within the application. The CAMARA project has been the major contributor for the definition, development, and validation of the Service APIs.
- The **OAM APIs** offer programmable access to Operation, Administration and Management (OAM) capabilities to facilitate the integration of the Open Gateway NaaS Platform with portals, marketplaces and other aggregation platforms.
- The **Technology-specific APIs** refer to operator internal APIs offering programmable access to telco infrastructure and network, service and IT capabilities. These APIs are typically defined in standardization bodies (e.g., 3GPP, IETF, ETSI, TM Forum) and cloud communities (CNCF) and are typically tied to the underlying technology.

Practically, a Communication Service Provider (CSP) shall offer a single entry-point for third parties to gain quick and easy access to Service and OAM APIs. The Operator platform provides all the features that are needed to policy manage the interaction between the CSP and the third-party domains (other operators and third-party aggregators), including API publication & discovery, access control (registration, authentication, authorization), auditing and user consent management, among others.

Given a "code first" NaaS realization approach, already open-source projects have provided mature implementations for related functionality. Representative examples are the ETSI SDGs OpenSlice and OpenCAPIF, presented in the ANNEX A of this document. For instance, considering the OpenCAPIF functionality, any API provider that resides at any layer of the NaaS architecture should publish its APIs through the CAPIF core function (CCF), while any API consumer or invoker shall be onboarded and authenticated by the CAPIF core function to discover and use the published APIs.

[2] https://www.gsma.com/futurenetworks/resources/operator-platform-concept-whitepaper/

[3] https://www.gsma.com/solutions-and-impact/gsma-open-gateway/wp-content/uploads/2023/05/The-Ecosystem-for-Open-Gateway-NaaS-API-development.pdf

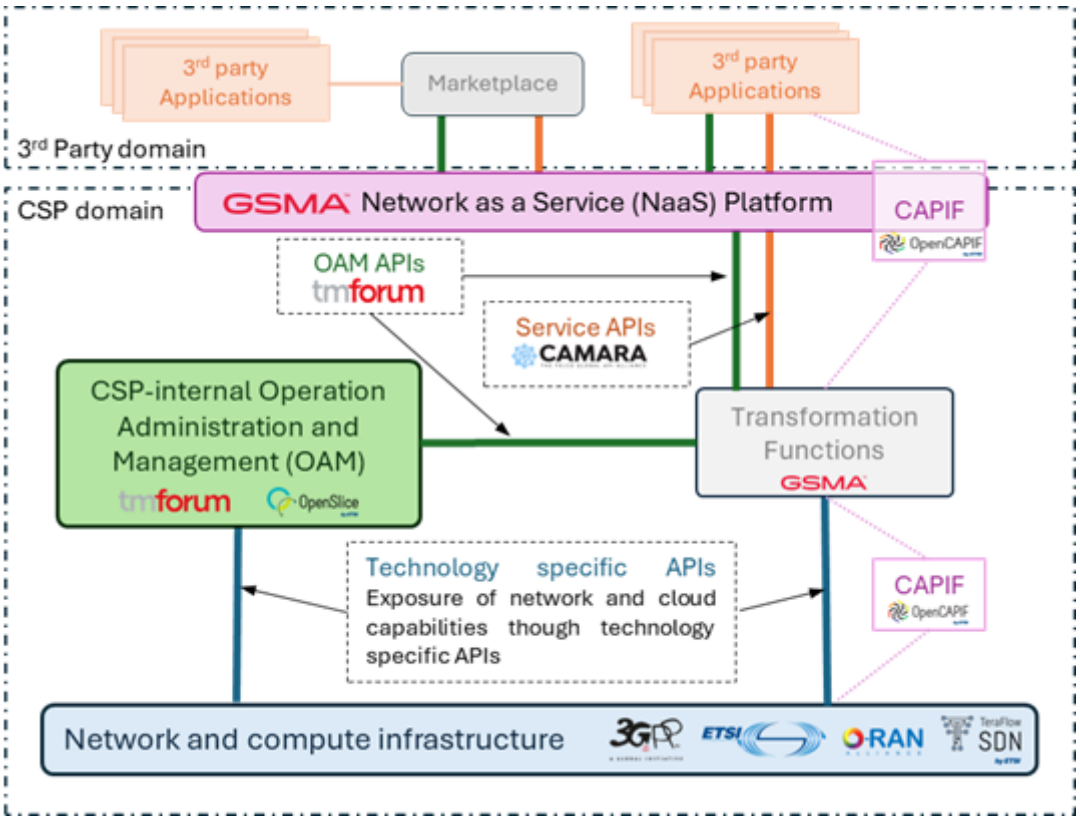


Figure 1: NaaS enables access to operator networks for developers.

To further analyze the APIs that are involved in the Operator Platform, Table 1: API categories and APIs related to the Operator Platform conceptTable 1 provides a comprehensive list of Service categories and related APIs that a telco network and compute infrastructure can offer to third parties.

Table 1: API categories and APIs related to the Operator Platform concept

Category	Related APIs
Service and Network Capability Exposure APIs – Adjust QoS profiles for guaranteed bandwidth, latency, or jitter. – Location Discovery APIs – Authentication APIs – Network Monitoring: Expose network performance metrics to applications for enhanced analytics.	3GPP Network Exposure Function (NEF) 3GPP CAPIF CAMARA APIs GSMA Operator Platform: Requirements and Architecture[4] TMF921 Intent Management API

[4] https://www.gsma.com/solutions-and-impact/technologies/networks/wp-content/uploads/2024/09/OPG.02-v7.0-Operator-Platform-Requirements-and-Architecture.pdf

– Event Notification: Allow applications to subscribe to network events, such as connection changes or mobility updates.	TMF931 Open Gateway Onboarding and Ordering Component Suite TMF633 Service Catalog, TMF634 Resource Catalog, TMF620 Product Catalog
Application Onboarding and Instance Management – APIs to onboard new applications by providing metadata, dependencies, and configuration settings. – APIs to publish onboarded applications to an operator-managed catalog for enterprise and consumer access. – APIs to deploy application instances to specified locations, such as edge nodes or central data centers, scale, upgrade applications and provide analytics	GSMA User-Network Interface API[5] GSMA NBI APIs Realisation in the SBI[6] TMF620 Product Catalog and Product Ordering, TMF702 Resource Activation TMF931 Open Gateway Onboarding and Ordering Component Suite CAMARA APIs
Edge Computing APIs – Application Deployment and Lifecycle Management – Manage application instances on edge nodes and allow deployment, scaling, updates, and removal of applications. – Edge Location Discovery: Identify optimal edge computing resources based on user location, latency requirements, or resource availability.	ETSI MEC API family 3GPP Network Exposure Function (NEF) 3GPP CAPIF TMF633 Service Catalog, TMF634 Resource Catalog, GSMA Operator Platform: Requirements and Architecture[7] CAMARA APIs
Network Slicing APIs – Slice Creation and Management: dynamic allocation of network slices	3GPP Network Exposure Function (NEF) GSMA Operator Platform: Requirements and Architecture

[5] https://www.gsma.com/solutions-and-impact/technologies/networks/wp-content/uploads/2023/03/GSMA-Operator-Platform-Group-User-Network-Interface-APIs-v1.pdf
[6] https://www.gsma.com/solutions-and-impact/technologies/networks/wp-content/uploads/2024/09/OPG.09-V2.0-NBI_SBI-Realisation.pdf
[7] https://www.gsma.com/solutions-and-impact/technologies/networks/wp-content/uploads/2024/09/OPG.02-v7.0-Operator-Platform-Requirements-and-Architecture.pdf

tailored to specific use cases (e.g., IoT, AR/VR, enterprise networks). – Slice Performance Monitoring: APIs provide insights into slice health, latency, throughput, and other KPIs. – QoS Management: Allow applications to request specific Quality of Service levels for their network traffic.	CAMARA APIs TMF909 API Suite Specification for NaaS
Identity and Security APIs – Authentication and Authorization: Facilitate secure user identification using telco infrastructure (e.g., SIM-based authentication). – Data Privacy and Compliance: APIs ensure adherence to data protection regulations by managing user consent and data access.	3GPP Network Exposure Function (NEF) CAMARA APIs OAUTH 2.0
Location and Context APIs – User Location Services: Provide real-time or near-real-time location data for enhanced service delivery. – Context Awareness: Enable applications to adapt based on the user's network environment or device status. – Service Usage Analytics: Provide detailed reports on data usage, user engagement, and service performance. – Predictive Analytics: Leverage AI/ML models for proactive management of applications and services.	3GPP Network Exposure Function (NEF) 3GPP CAPIF ETSI MEC API family CAMARA APIs
East-Westbound Interface APIs – Allow an Operator Platform (OP) to share the edge cloud resources and capabilities securely to other Partner OPs over the East/West Bound Interface	GSMA East-Westbound Interface APIs[8] MEF's Lifecycle Service Orchestration (LSO) APIs TMF Party management APIs, TMF691 Federated ID management

[8] https://www.gsma.com/solutions-and-impact/technologies/networks/wp-content/uploads/2024/09/OPG.04-v5.0-EWBI-APIs.pdf

– Create partner federation: share services and edge network and cloud resources, life-cycle management of apllications and services	
Billing – Usage Tracking:Track application or user consumption of network resources for billing purposes. – Service Monetization: APIs facilitate revenue-sharing models and invoicing. – enable the purchase of third-party digital goods and to request payment against the user's Mobile Operator billing system.	TMF Product APIs, TMF Customer APIs, TMF Business Partner APIs CAMARA APIs 3GPP Network Exposure Function (NEF)

2.2. APIs FOR SERVICE AND RESOURCE MANAGEMENT

Service management APIs focus on the deployment, configuration, and monitoring of network services and are used to manage the lifecycle of services from initial service ordering and instantiation to ongoing updates. These APIs ensure that services are delivered with the initial requirements and can adapt to changing user demands and network conditions. Resource management APIs, on the other hand, are concerned with the efficient allocation and utilization of resources such as bandwidth, compute power, and storage. These APIs play a crucial role in managing resource usage and ensuring that resources are available where and when they are needed. Orchestrators utilize service and resource management APIs, enabling the coordination and automation of network functions across different domains when performing complex workflows that can dynamically adjust to varying conditions and requirements. Orchestrators implement policies and rules that govern the behavior of network functions and resources, and through these APIs ensure that the network operates efficiently and in alignment with business objectives.

The role of an orchestrator is to manage the service lifecycle, which boils down to three main operations described in the following paragraphs. Per case, some of the existing dominant API specifications are detailed.

Service onboarding on service catalog is a process that requires an already packaged service (e.g., as a container) to be associated with a service descriptor that guides an orchestrator on how to incorporate this service into its service catalog. The data models for

the service specification, category, and catalog can follow the TMF633 Service Catalog Management API [1] model schema and may be accessible through standardized API endpoints. Moreover, the Resource catalog accepts well-known industry packages, i.e. NFV artifacts or helm charts, and associates them with a service descriptor that facilitates the orchestrator to deploy them. The applied procedure offers flexibility to the designer, who describes the service to be onboarded with characteristics and intent that can be requested upon service ordering affecting the implementation aspects, e.g. computational flavor, serving area, scalability, etc. The data models employed are based on the TMF634 Resource Catalog Management API model schema and are offered through standardized API endpoints.

Service ordering from a Service catalog is a process that entails the selection of an already onboarded service from the service catalog and the ordering of this service using important runtime information. The data models for the service order can follow the TMF641 Service Ordering API [2][2] model schema and will be accessible through standardized API endpoints.

Service inventory for runtime management once an instance is deployed on a given (set of) domain(s). The data models for the service inventory can follow the TMF638 Service Inventory Management API model [3] schema and be accessible through standardized API endpoints. The inventory is available and comprises the service instances created and maintained from the respective service orders. Each service also provides information about the allocated resources, if present. The data models employed are based on the TMF638 model schema and are offered through standardized API endpoints.

Resource inventory points to the actual network and compute resources that are created from the process of the corresponding service order fulfillment. These resources are utilized by the orchestrator to deploy the end-to-end vertical services. The data models employed are based on the TMF639 Resource Inventory Management model [4] schema and are offered through standardized API endpoints.

The following table presents a list of the most common APIs used for Service and Resource management and Orchestration

Table 2: List of APIs used for Service and Resource Management

API, model, frameworks, Open-Source Solution	Usage and Scope
TMF633 Service Catalog Management API	Service Catalog Management API allows the management of the entire lifecycle of the service catalog elements.

TMF641 Service Ordering API	Create, update & retrieve Service Orders and manages related notifications from the catalogs for orchestration
TMF638 Service Inventory Management API	provide a consistent/standardized mechanism to query and manipulate the Service inventory
TMF634 Resource Catalog Management	Resource Catalog Management API allows the management of the entire lifecycle of the resource catalog elements.
TMF639 Resource Inventory Management	Describe compute and network resources that are created from the process of the corresponding service order fulfillment
TMF657 Service Level Specifications	Service Quality Management REST API Specification
TMF655 Change Management API	Standard integration capabilities between external applications and Change Management Application
TMF645 Service Qualification API	Provide service availability to the customer
TMF640 Activation and Configuration API	Allows the user to retrieve, create, update, delete services and retrieve the monitor resource used to monitor the execution of asynchronous requests on specific resource
TMF702 Resource Activation API	Activate Resources, as in the Resource Inventory
TMF921 Intent Management API	Autonomous Networks Reference Architecture (IG1251)
TMF931 Open Gateway Operate API	a consolidation of multiple TMForum-based APIs into a single endpoint (a component suite)
IETF CFI - IETF I2NSF Consumer Facing Interface	for policy definition from customer side through TeraFlowSDN
IETF NSFFI - IETF I2NSF Yang Data Model	for internal policy management in Secure SLA & Policy databases through TeraFlowSDN
IETF YANG Data Model for Network Topologies	to acquire the network topology from TeraFlowSDN
IETF YANG Data Model for Network Access Control Lists (ACLs)	to configure ACLs in the network devices through TeraFlowSDN
IETF YANG Data Model for the RFC 9543 Network Slice Service	for Network Slice service requests through TeraFlowSDN
GSMA GST template	Used by ACDO to describe Service Specification templates
ETSI GS NFV SOL 005 API	Used by ACDO to access the NFVO
Kubernetes NBI API	Used by ACDO to access the Kubernetes cluster and manage CRDs and CRs

ETSI SDG OSL	OpenSlice is used as the Cross Domain Orchestrator
ETSI SDG TFS	TeraFlowSDN is used as a transport controller

2.3. APIs FOR CLOSED-LOOP RUNTIME FUNCTIONS

The APIs that use closed-loop functions can provide a comprehensive framework for implementing and operating AI-driven Unified & Open Control Operations Framework. Such APIs can facilitate functions like monitoring, analytics, decision-making, and execution:

- Monitoring, closed-loop system, tasked with the collection, aggregation, storage, and exposure of data related to network performance, resource utilization, and application performance
    - Data Collection
    - Data Aggregation
    - Data Exposure
- Analytics function processes the data collected by the monitoring function to generate insights, predictions, and recommendations
    - Data Analysis
    - Predictive Modelling, Model interface trains a predictive model using historical data and a specified model type
        - Prediction interface uses a trained model to make predictions based on new input data
        - Decision Support - interface provides actionable recommendations based on the analysis results to optimize network performance and resource utilization
- Decision-making function uses insights and recommendations from the analytics function to make informed decisions
    - Decision Execution - interface executes a decision by implementing the recommended action within the network
    - Policy Management -interface sets a policy that guides decision-making processes within the network
    - Model Management - interface loads a machine learning or AI model into the decision-making system
    - Execution Function - responsible for carrying out decisions made by the decision-making function
    - Execution Status, interface implements a specified action within the network
    - Resource Management, interface allocates necessary resources to support a specific action or decision

- Configuration Management, interface applies a new configuration to the network or a specific component. This function is crucial for updating network settings
- AI/ML Services - the interfaces to the AI/ML models via APIs
    - ETSI GS NFV-IFA 022 [5]: It outlines the requirements for applying ML in the management and orchestration of Network Function Virtualization (NFV) systems
    - ETSI GR SAI 004 [6]: This provides an overview of how AI can be applied in various ETSI standardization areas, including use cases and potential benefits.

In this context, ETSI ZSM (see Annex A: Open-Source Projects Catalogue) provides an end-to-end operable framework, solutions and core technologies enabling AI-driven zero-touch automation of emerging and future networks and services and Closed-loop governance. The goal of closed-loops and their governance is to achieve complete automation in service and network management via AI-driven service and network operations, efficiently handling the complexities and heterogeneities of 6G network and service operations. We consider two groups of closed loops:

- Composed closed-loops, internal closed-loop functions:
    - monitoring: for data ingestion and processing
    - analytics: for analysis of the incoming data stream, which could include AI/ML inference from the given data
    - decision: for determining and executing an action to achieve a desired state defined in closed-loop policies, which also could include AI/ML elements for assisted decision making
- Beliefs – Desires closed-loops, the AI-driven internal functions:
    - belief: informational state of the system
    - desire: desired state of the system (objectives or situations that the agent would like to accomplish) defined through policies

The concepts of ETSI GS ZSM 009-2 will further be extended in 6G networks to allow full model automation for AI-based closed-loop functions, deploy and oversee a diverse range of closed-loops, including those composed of the closed-loop functions for deployment across the network. The governance then follows the following steps for placement of a closed loop:

- **Closed-loop instance creation,** creates a closed-loop instance, which can be thought of as a compiled closed-loop description, containing all the parameters and settings of the requested closed-loop, including the composite closed-loop functions. This instance is stored in the CL Instance records and can be retrieved via REST API.

- **Retrieve closed-loop function descriptors**, includes monitoring, analytics, decision, or belief, desire, intent blocks. Each of these individual closed-loop functions also have a descriptor associated to them, containing information such as input and output parameters, ml model selection criteria, requirements.
- **Closed-loop functions resource allocation and placement,** the resource allocations for the Closed-loop functions (Closed-loop functions can be deployed in separate physical locations for example). In the case where a closed-loop function uses an AI model, the Closed-loop Governance requests the required AI/ML Service.
- **Closed-loop function instances creation,** creates instances of the closed-loop functions that will then be deployed. In the case of a function that requires a served AI model, the endpoints for the model determined in the previous step, will be embedded in the instance.

2.4. APIs FOR NETWORK TELEMETRY AND MONITORING

To retrieve and exchange telemetry data, API consumers can rely on a combination of gRPC (using either OpenConfig or OpenROADM YANG models) for out-of-band telemetry from optical devices, packet and computing nodes. Legacy protocols like NETCONF, RESTCONF, and SNMP remain possible solutions to also feed telemetry collectors at lower pace. Apache Kafka data streaming is an option to exchange telemetry data as simple text messages, which provides the flexibility to deal with data variety. In addition, Kafka facilitates the integration of different data sources. The following table presents a list of most common APIs used for network telemetry and monitoring

Table 3: List of APIs used for network telemetry

API, model, frameworks, Open-Source Solution	Usage, Scope
Monitoring/Telemetry APIs, like OpenTelemetry	Testbed exposed APIs for telemetry and monitoring data
gRPC (using either OpenConfig or OpenROADM YANG models)	for out-of-band telemetry from optical devices, packet and computing nodes
Legacy protocols like NETCONF, RESTCONF, and SNMP	solutions to also feed telemetry collectors
Telemetry enablers like Prometheus, Apache Kafka	solutions that enable telemetry

Given the available APIs for telemetry, ***In-band Network Telemetry*** (INT) is emerging as a crucial enabler for the next generation of 6G networks, as it allows for real-time monitoring and analysis of network conditions without interrupting data flows. INT embeds telemetry data within the same packets that carry user data, allowing for seamless data collection across network paths. This approach contrasts with traditional methods, where telemetry data is collected out-of-band and often incurs additional overhead and latency. Postcard telemetry, a variant of INT, enables each network node to send "postcard" telemetry reports

directly to a centralized telemetry collector. This collector aggregates and processes these reports, providing a comprehensive view of network performance and allowing for immediate insights into packet loss, latency, jitter, and other critical network parameters. Additional components, such as programmable switches and intelligent network controllers, play a role in making INT adaptable and scalable to the high-performance, ultra-reliable requirements of 6G. Together, these telemetry systems ensure a robust and self-optimizing network infrastructure, laying the groundwork for innovative applications like holographic communication, immersive virtual reality, and autonomous vehicles in 6G.

2.5. APIS ENABLING TRANSPORT NETWORK CONTROL

The transport network management involves the control of optical and packet/optical devices in the underlying data plane. Work focuses on model-driven approach, and this depends on the YANG model adapted by the optical or packet/optical entities. Among the optical domain components, OpenConfig is generally used for transceivers and packet/optical devices while OpenROADM YANG models for ROADMs. However, the scope of the work also considers evaluation of OpenROADM to control pluggable in packet/optical devices. The optical controllers SBI are based on NETCONF/YANG while their NBI interfaces are usually based on RESTCONF (e.g., with ONF Transport API, TAPI data models). Specific subsystems (e.g., Intelligent Pluggable Control) have their own REST-enabled dedicated controller.

TeraFlowSDN (TFS) Controller is an ETSI-hosted open-source cloud-native SDN controller (see the main features in Annex A: Open-Source Projects Catalogue). TFS plays two essential roles: IP/MPLS (packet) controller and Transport Network Orchestrator. TFS's release 4 already has several features, such as Layer 3 VPN service provisioning, L2 VPN, ACL management for security, and inventory information using Netconf/OpenConfig as the Southbound interface. TFS uses conventional L3NM/L2NM protocols in the northbound direction. It can also gather telemetry data from packet devices using gNmi/OpenConfig.

TFS is also used as an IP/multidomain Network Orchestrator. The TAPI (Transport API) SBI driver, which interfaces with the optical controller, is improved to access the increased TAPI context supplied by the MBoSDM optical controller more effectively. This innovation guarantees that the TFS controller and the optical domain communicate and coordinate in real time. In addition, a new SBI driver has to be designed expressly for the PON (Passive Optical Network) domain, including the appropriate access domain abstract representation into the Context module.

2.6. MANAGEMENT OF API-BASED SERVICES

With the convergence of the software engineering and the telecommunication domains, flexible software implementations have emerged, covering almost any aspect of mobile networks' functionality. In this section, we present recent advancements in the concept of network openness through a standardised API framework, called Common API Framework (CAPIF), which is being implemented in the context of ETSI SDG OpenCAPIF (see the main features in Annex A: Open-Source Projects Catalogue). CAPIF includes common aspects applicable to any northbound service API. As such, it is a complete 3GPP API framework that covers functionality related to on-board and off-board API invokers, registering, and releasing APIs that need to be exposed, discovering APIs by third parties, and authorization and authentication.

Considering functionality, any API provider that resides at any layer of the architecture should publish its APIs through the CAPIF core function (CCF), while any API consumer or invoker shall be onboarded and authenticated by the CAPIF core function to discover and use the published APIs. This means that APIs from all the layers of the architecture and from all the planes (user, control, and management) can be included in the framework. For instance, at the network core domain, such APIs can be the ones that network core exposes; at the RAN domain, the RIC APIs for development of xApps/rApps; while at the management level, APIs from the services and resource management tools can be considered

2.6.1. CAPIF IN THE MEC ARCHITECTURE

ETSI MEC (Multi-access Edge Computing) is a standardization initiative launched in 2014 by the European Telecommunications Standards Institute (ETSI). MEC aims to bring cloud computing capabilities closer to the edge of the network, enhancing performance, reducing latency, and improving service quality. This proximity allows applications, such as video streaming, gaming, IoT, and AI, to be executed near the end users, ensuring real-time processing and lower data transfer times.

Since its inception, ETSI MEC has grown to include numerous stakeholders from across the globe, including network operators, infrastructure providers, and application developers. The initiative has produced a series of standards that define the architecture, interfaces, and APIs for deploying and managing edge services in a multi-vendor ecosystem. Some basic capabilities in ETSI MEC include creating an API Catalogue (publication of APIs), API Discovery, Authentication to consume MEC services. Those capabilities are also addressed in 3GPP CAPIF standard, therefore, ETSI MEC and 3GPP SA6 have worked together to align ETSI MEC and 3GPP specifications to converge in a solution described in ETSI 123.958/3GPP TS 23.958: Edge Application Standards in 3GPP and alignment with External Organizations.

The 3GPP CAPIF API registry and the ETSI MEC service management solve the same problem (differently) and offer synergy potential. To align, ETSI MEC has defined a profile of CAPIF, re-using the CAPIF service registration, discovery and announcement functionalities. The commonalities between ETSI MEC and CAPIF are presented in the table below.

Table 4: Commonalities between ETSI MEC and CAPIF

MEC Service Management	CAPIF API Registry
Register Service	Publish Service API
Discover Service	Discover Service API
Notify Service Changes	Events API

There are some differences though, that have been addressed by the definition of a CAPIF profile in ETSI MEC (Table 5).

Table 5: Differentiation aspects between ETSI MEC and CAPIF

MEC Service Management	CAPIF API Registry
REST+JSON + alternative API architectures	REST+JSON only
REST APIs: Endpoint only (resources, methods)	REST APIs: Endpoint and structure
Discovery filters: core set + MEC specific	Discovery filters: core set + CAPIF specific
REST security: MEC profile of OAuth	REST security: TLS-PSK, PKI, 3GPP profile of OAuth

ETSI MEC defined several requirements for extending CAPIF to better support MEC-specific needs. These requirements aimed to ensure that the MEC system could enhance its integration with the CAPIF framework while maintaining compatibility with native CAPIF APIs. The requirements were later included in 3GPP Release 18, which introduced new CAPIF extensibility mechanisms. The key requirements defined by ETSI MEC included:

- The ability for ETSI ISG MEC to extend enumerations, such as data formats, protocols, and security mechanisms, without breaking existing CAPIF API invokers. This ensures smooth updates and interoperability.
- Support for extension containers, allowing the inclusion of additional, MEC-specific information during the service API publication process. This information would be returned as part of the service API discovery results, enabling more tailored and precise service discovery.
- A mechanism for defining additional filtering criteria for service API discovery queries. This allows for more specific and relevant results, enhancing the efficiency of discovering services in a MEC-enabled environment.

These suggestions have been implemented through the CAPIF extensibility mechanisms in 3GPP Release 18, ensuring the framework is more flexible and adaptable to MEC's evolving

requirements. Consequently, ETSI MEC can be deployed using CAPIF as API manager as illustrated in TR 23.958.

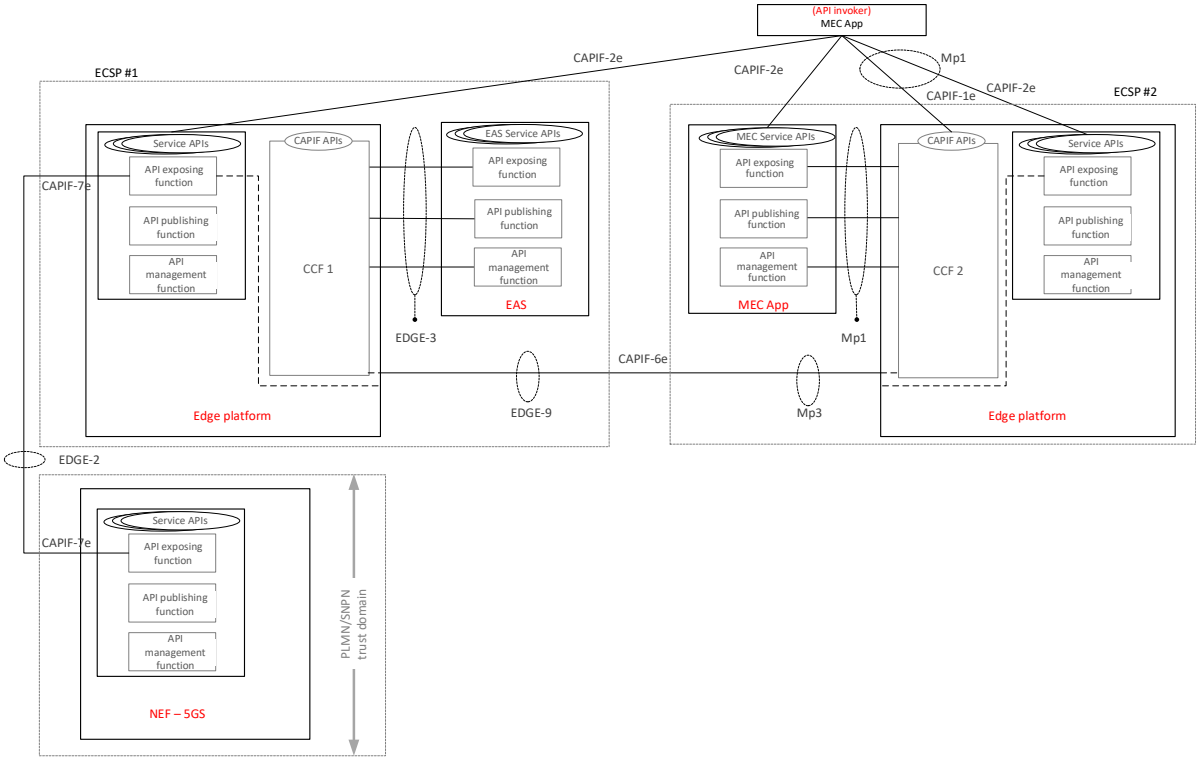


Figure 2: MEC Platform deployed using CAPIF as API Manager

In Figure 2, we can see the following mapping of ETME MEC and CAPIF entities:

- MEC App act as an API Provider (including AMF, APF and AEF) exposing APIs in the MEC platform using CAPIF Core Function (CCF2).
- MEC App can also act as API Invoker consuming MEC APIs but also NEF APIs discovering the APIs in CCF2. (It is assumed that CCF1 and CCF2 publish their APIs between each other using CAPIF-6 interface).

2.6.2. OPENCAPIF IMPLEMENTATION ASPECTS

OpenCAPIF scope is the open-source development of the 3GPP CAPIF, allowing for secure and consistent exposure and use of APIs. SDG OpenCAPIF complements other ETSI software and open-source projects (please refer to Annex A: Open-Source Projects Catalogue), such as Open-Source MANO, TeraFlowSDN and OpenSlice.

In the current release of OpenCAPIF [7], all the API services defined in 3GPP TS 29.222 Rel. 17 have been implemented. Release 18 presents upcoming extensions, referring to the Resource

owner-aware Northbound API Access (RNAA) (TS 23.222 Rel-18) and the alignment of OpenCAPIF with EDGEAPP (TS 23.958 Rel-18). Until Release 17, when service APIs were invoked, the end users (UEs) were neither aware of the API invocation nor had any control over which APIs were executed. RNAA aims to protect end users against such unintended access to their resources. CAPIF implements RNAA concept by introducing the following new functional entities:

- Resource Owner (RO): entity that grants access to a protected resource
- Resource Owner Client (ROC): Connects RO with CCF via CAPIF-8 interface
- Authorization Function (AUF): CCF entity that manages the authorization among RO, API Invoker and API Provider.

In Release 18, CCF, to grant access to API Invoker(s), willing to consume a set of provider APIs, will have to make a complementary check, via the AUF, if the RO allows the invoker(s) to access the resources of the corresponding end users.

3. SERVICE AND RESOURCE MANAGEMENT ENABLERS

6G networks are expected to intelligently support a massive number of simultaneous and heterogeneous slices associated with various vertical use cases. In this respect, challenges of scalability and sustainability might surface in the deployment of AI-driven zero-touch Management and Orchestration (MANO) of the End-to-End (E2E) slices, under stringent Service Level Agreements (SLAs). Next generation network will contain mechanisms at various levels to optimize research allocation needed for better service management. We group the key enablers into three main categories: 1) High-level Service Management components including intent-based approaches; 2) Enablers solving the management problems of cloud-to-edge computing continuum; and 3) Technologies supporting the management of resources in dynamically changing environments including non-terrestrial networks.

3.1. COMMON AND INTENT-BASED SERVICE MANAGEMENT

A cohesive and adaptable service management and orchestration (SMO) framework becomes essential in future 6G networks. This section delves into the key advancements in towards a unified and intent-driven architecture. Subsections explore the evolution proposed from Open RAN towards a common SMO framework covering all network domains; the role of intent-driven architecture in simplifying SMO processes; and the application of multi-agent systems for achieving end-to-end (E2E) SMO capabilities, collectively underscoring the importance of intelligent and adaptive service management in modern networks.

3.1.1. OPEN RAN EVOLUTION TOWARDS A COMMON SMO

From a perspective of architectural evolution of a 5G Open RAN, based on O-RAN Alliance [8] extensions to 3GPP towards 6G, there are several pertinent drivers and evolutions, shown below in Figure 3, especially in the RAN control-plane.

To better explain the evolutions portrayed in Figure 3, these 6G evolutions to 5G Open RAN can be broadly group into:

- “Southbound RAN evolutions”, with changes within the RAN NFs themselves (CU/DU/RU).
- “Northbound RAN evolutions” towards NBI/API integrations of RAN with other domains (Core, transport) and ‘Common SMO’.

Within the control-plane, a lot of the evolution beyond addition of functionality (like ISAC) considers telemetry export and training/deployment frameworks to support advanced AI/ML

intelligence throughout the RAN, from the lower levels (such as embedded AI/ML in PHY) to the higher layers (such as automated zero-touch operation).

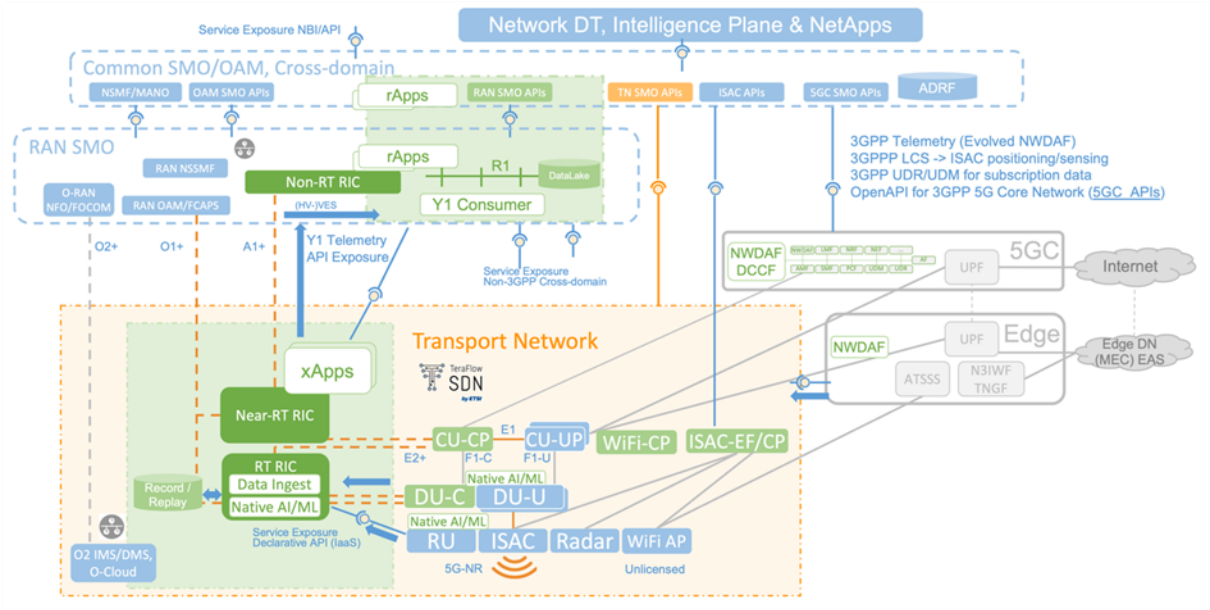


Figure 3: Evolutions of Open RAN (control-plane) towards 6G

Whereas the 5G Open RAN SMO only considers the RAN itself, there is an emerging consensus that and efficient and effective 6G architecture needs to be considered cross-domain (RAN, Core and Transport), so the higher layers (termed SMO by O-RAN) require integration into a '6G Common SMO':

- O-RAN nGRG 'Common SMO'
- 3GPP Hierarchical Management and Orchestration
- 3GPP NWDAF Evolution for Federated Learning, see 3GPP TS 23.288 v18.6.0 [13]

For integration with existing higher-layer frameworks, like ETSI OpenSlice (Annex A OpenSlice) or ETSI ZSM (Annex A Zero-touch Service Management), it is assumed that some or all the cross-domain integration (RAN, Core, Transport) will occur within those frameworks. However, a more integrated standalone O-RAN 'Common SMO' can be considered, where there is a merging of the integration of the RAN & Common SMOs, with the current non-RT RIC and rApps being extended to the cross-domain layers. Providing programmable extensibility has been a key advantage and driver for adoption of the O-RAN Near-RT RIC with xApps, and increasingly to provide intelligence into B5G networks, such as for energy efficiency goals. This cross-domain integration and extensibility of the 'common SMO', with API exposure and non-RT RIC rApps will be a fundamental evolution of the O-RAN 5G SMO, to provide 6G

capabilities such as Native AI/ML, zero-touch automated operation and Network Digital Twins (NDT).

One aspect of integrating AI/ML intelligence throughout a converged SMO is the scalability restrictions of a purely centralised SMO, due to the bottleneck of sending all telemetry to a central SMO layer (e.g. for AI/ML training). It has been demonstrated that a scalable architecture needs to support a distributed federated architecture, as also seen in the evolution of the 3GPP NWDAF Evolution for Federated Learning [9].

3.1.2. INTENT-DRIVEN ARCHITECTURE FOR SMO

Providing multiple services with different performance and functional requirements brings problems such as the complexity of network management and the need to ensure the required performance levels. Network management automation emerges as a viable solution to mitigate this complexity [22]. Concepts such as zero-touch [28] networks and intent-based networking [15] are pivotal in enabling and facilitating this automation, aiming to streamline operations and enhance efficiency.

Intent Based Network Management (IBN, see Figure 4) plays a crucial role in the realm of 6G services, where service complexity will increase significantly. At its core, IBN aligns network operations with business objectives by translating high-level intents into sub layer intents and orchestration. Intent is the formal definition of service expectations, including objectives, goals, and restrictions, for a technical system (Forum, IG1253 Intent in Autonomous Networks (Version 1.3.0), 01-Aug-2022). By focusing operations on intents rather than specific tasks, the recipient system gains significantly more latitude in selecting solution strategies and actions to implement. Embracing a requirement-centric approach is fundamental for achieving a distinct separation of concerns, fostering higher levels of autonomy within the system. IBN introduces a proactive and agile management paradigm, where networks can anticipate and respond to emerging requirements and opportunities dynamically. In the context of 6G, IBN holds a critical architectural position within the Service Management and Orchestrator framework. Positioned as a central component, IBN serves as the cognitive engine that bridges the gap between high-level business intents and the underlying network infrastructure.

In the service layer, IBN interprets and analyses incoming service requests, ensuring they align with existing services or creating new ones as needed. In this study, our focus lies in creating a new service when existing ones cannot fulfil the demand for a new service. Creating a new service is achieved through the following steps.

1. Receive business request (usually in the form of service level agreement – SLA)

2. Translate the SLA to intents
3. Creation of service description and service graph
4. Decompose the service for actual deployment (low level intents and sub service-graphs)

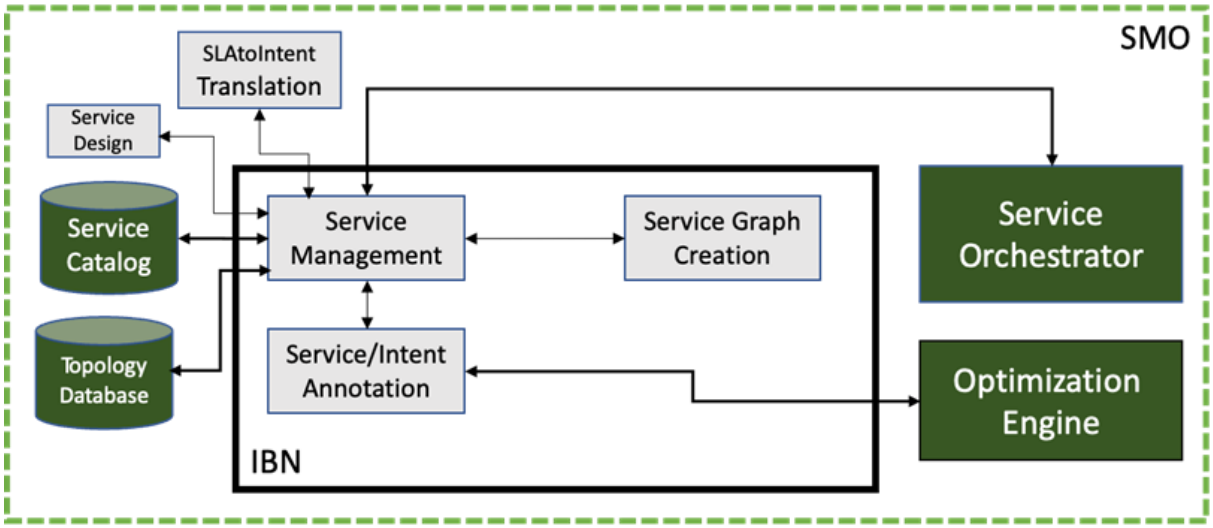


Figure 4: An example for an IBN architecture

3.1.3. MULTI-AGENT-BASED E2E SMO

Multi-agent systems (MAS) have been proposed to distribute knowledge and decision-making among the different entities/segments in the networking infrastructure. MAS is a subfield of AI that deals with the behaviour of the software entities (*agents*) available to solve a given problem. MAS can be defined as a set of individual - mostly AI-based - agents that share knowledge and communicate with each other to solve a problem that is beyond the scope of a single agent. For example, in the future 6G networks network nodes will communicate with each other to exchange control, data, and models to create self-organized systems. Decision-making will be performed by every individual agent with up to sub-second granularity based on its own observed data, as well as on the data and models received from other agents in the same layer. AI/ML techniques like reinforcement learning (RL) and long short-term memory (LSTM) will potentially be used to achieve near real-time responsiveness.

Agents will also share coarser granularity, aggregated observed data and models, together with control commands with the E2E SMO. This is of paramount importance for inter-segment coordination, e.g., between RAN and cloud or RAN and transport, as well as to support global view coordinating activities, e.g., to reallocate services in case of failures, resource optimization (e.g., energy reduction), etc.

MAS agents also require configurations and settings from the SMO. A component as part of the centralized SMO will be responsible for deploying and, if needed, reconfiguring the MAS agents. It will be in charge of creating AI/ML pipelines and relating them to the target service. AI/ML pipelines are associated to network entities and need to be deployed and reconfigured properly according to needs, e.g., flow rerouting of a service requires moving agents (with their performance data and models) among different 6G network domains.

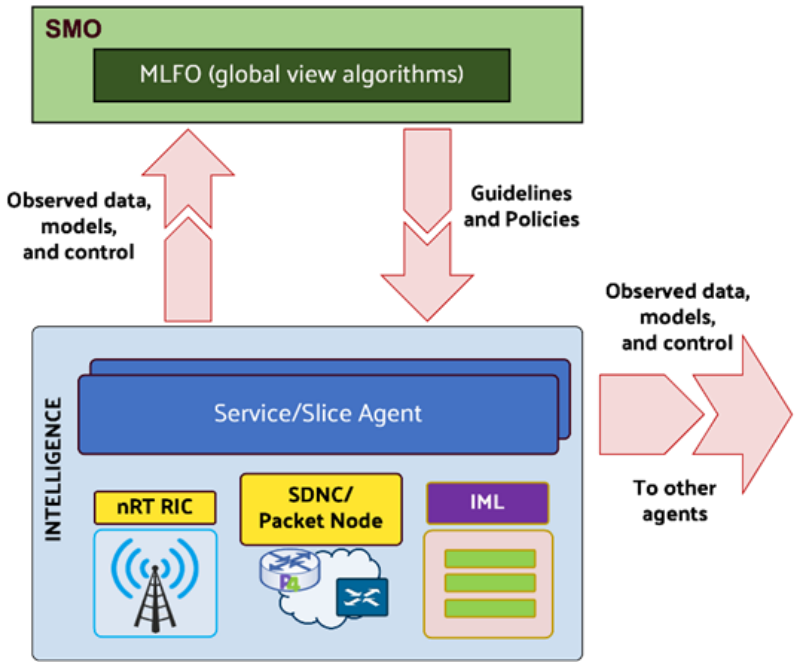


Figure 5: Distributed intelligence architecture

Figure 5 illustrates the roles of agents and the centralized decision-making component of SMO. The As SMO has a global view on the infrastructure, it can execute more complex AI/ML models to optimize the network configuration and deployment. The MAS agents always have a local scope, and their decisions rely on more lightweight AI/ML models, as their execution time requires feedback with low latency.

3.2. EDGE-TO-CLOUD COMPUTE CONTINUUM

The increasing demands for low-latency and high-performance computing have driven the emergence of an edge-to-cloud computing continuum. This architecture seamlessly integrates edge and cloud resources to deliver efficient and responsive services. This section explores the critical components required to build and manage this continuum, which spans from centralized cloud infrastructures to highly distributed edge resources.

3.2.1. PROGRAMMING MODELS FOR EDGE-CLOUD CONTINUUM

This section presents a suite of programming models and frameworks that abstract the underlying infrastructure into an **edge-to-cloud compute continuum**, forming a virtualization

layer that decouples the application logic from the heterogeneous hardware platforms where the applications are actually executed. These programming models and frameworks are employed for the design of application and network workflows that leverage split and distributed computing, advanced learning techniques or intra-node reprogrammability of FPGA-based devices.

- ReproRun [30], a programming framework for FPGA-based SoC devices, which can be employed to provide intelligent reconfiguration capabilities to optimize software and hardware-accelerated disaggregated RAN functions at the Distributed Unit (DU) and Radio Unit (RU) levels, i.e., starting from the Medium Access Control (MAC) and high-physical (PHY) layer all the way through the digital front-end, the power amplifier and the antenna array.
- A split computing framework [31], which will be employed to optimally and dynamically split heavy AI inference workloads, vertically distributing computation between constrained User Equipment (UE) and more powerful edge resources.
- COMP Superscalar (COMPSs) [32], a distributed computation programming model and runtime framework, which will facilitate the development complex AI workflows and their distributed execution over heterogeneous edge computing resources (e.g., CPUs, GPUs, etc.). This framework can be employed in horizontal distribution scenarios within edge resources of the same cluster, without excluding the possibility of exploring edge-to-cloud distribution if needed by the use cases.
- oneAPI [33] (See within Annex A the OpenAPITMForum section), an open, cross-industry, multi-architecture programming model developed by Intel, that aims to simplify development across diverse computing architectures (CPUs, GPUs, FPGAs, etc.) through a unified software interface.
- A federated learning (FL) framework [34] to enable and optimize the execution of FL workflows over heterogeneous edge computing environments, supporting time-triggered aggregation methods that leverage the advantages of both synchronous and asynchronous aggregation approaches.

3.2.2. INTEGRATED EDGE-CLOUD CONTINUUM

This section proposes an open, modular, and distributed architecture to accelerate the evolution of edge computing toward an integrated, next-generation edge-cloud compute continuum. One of the main goals of the proposed design is to create an integrated compute and communication continuum where cloud-native application and network services can be flexibly deployed and orchestrated, fully exploiting the capabilities of heterogeneous

platforms for high computational performance. The proposed design also provides the necessary framework and common interfaces to facilitate the design and the life cycle management (LCM) of AI-powered solutions, handling also the necessary data collection and management processes.

The high flexibility in the deployment of the cloud-native solutions over a heterogeneous edge-to-cloud compute continuum infrastructure and the support for multi-tenancy and distributed execution call for a unified design for the service orchestration, management and control planes. A distributed/hierarchical approach is adopted for this layer, considering both a global multi-site view and a local edge-site perspective, to better deal with the distributed nature of the underlying infrastructure. On the one hand, this design enables the E2E optimization across multiple sites, facilitating functionalities such as service migration, edge federation, mobility support, etc. On the other hand, having a local orchestration layer at each edge-site enhances the flexibility and modularity of the system, enabling localized optimization actions with reduced management overhead, such as intra-node orchestration or single-site interference management.

Figure 6 illustrates the different layers of orchestration, management and control considered in the proposed service management and orchestration architecture, each with a different view (scope) of the overall system. As shown in the figure, some components apply to the orchestration of the cloud-native services and computing resources, whereas others form part of the B5G network orchestration, control and management plane.

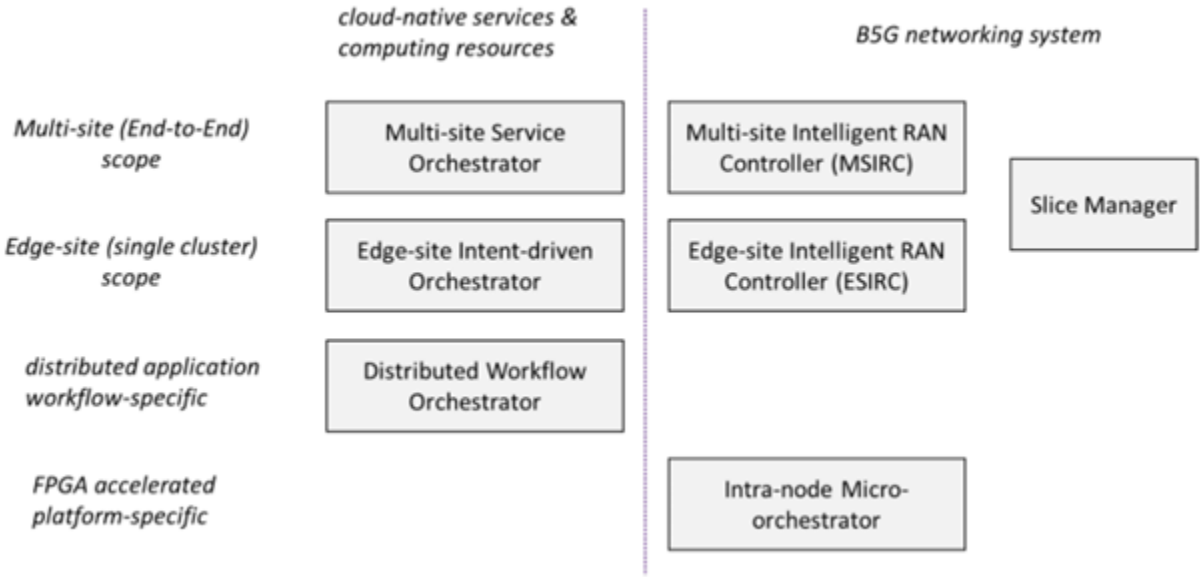


Figure 6: Service orchestration, management and control layer

With respect to Life Cycle Management (LCM) of cloud-native services and computing resources, the relevant components are summarized below:

- Multi-site Service Orchestrator, with an End-to-End (E2E) scope spanning across the edge-to-cloud compute continuum, formed by multiple edge sites, as well as cloud resources. The multi-site orchestrator, leveraging the NearbyOne[1] orchestration solution, manages the life cycle of the applications and services from an E2E perspective. As an example, the multi-site orchestrator decides the edge site where applications/services are deployed (or migrated from/to, if necessary). The multi-site orchestrator also registers the underlying computation targets used to host applications and services (i.e., the edge-site clusters).
- Edge-site Intent-driven Orchestrator, overseeing the LCM of the applications/services and resources on each local edge site or point-of-presence. The edge-site orchestrator will be based on Kubernetes, a widespread open-source solution for container orchestration and will be extended by the Intel open-source Intent-Driven Orchestration (IDO) planner[2]. The rich set of extensible APIs exposed by Kubernetes, are already used in the ecosystem, will greatly facilitate the integration between the edge-site and multi-site orchestration, as well as the lower use-case specific orchestration layers.
- Distributed Workflow Orchestrator, part of the BSC COMPSs framework responsible for handling the distributed execution of complex application workflows across the compute continuum, developed with the BSC COMPSs programming model. The COMPSs distributed framework will manage: i) the deployment of the necessary runtime environment to enable the distributed processing of computing tasks within an edge cluster, and ii) the application workflow orchestration, managing the allocation of tasks to the available computing resources, based on some scheduling policy. Hence, there is a close interaction of the distributed workflow orchestrator with the multi-site orchestrator, for the onboarding the distributed applications to the most appropriate edge location, and the edge-site orchestrator, for providing the available computing infrastructure for the distributed execution. This optional component will be leveraged to support the use case scenarios where distributed computing capabilities are required.

With respect to the B5G networking system, the key components are:

- Multi-site and Edge-site Intelligent RAN Controllers, responsible for the management of the RAN elements. Intelligent RAN control decisions are spatially separated into: i) a multi-site perspective, i.e., making decisions regarding the optimization of multiple

RAN sites, and ii) and edge-site perspective, applying intelligent control decisions with a local RAN site scope. The RAN controllers will be leveraged to implement several intelligent solutions for different scenarios and applications (from relay management to intelligent reconfiguration and scaling of accelerated RAN functions).

- Slice Manager, handling the LCM of end-to-end network slices. Network slicing is a critical concept in B5G, enabling the development of several virtualized and separated network instances on a shared physical infrastructure to satisfy a variety of service requirements. The slice manager design will enable the implementation of intelligent network slicing solutions for the RAN segment provided with the support of the intelligent RAN controllers.

Intra-node Micro-orchestrator for software and accelerated computed resources, enabling the joint micro-orchestration of the radio and computing resources in FPGA-based SoC accelerators. This framework will provide the means for a seamless runtime reconfiguration of the functions across the different processing elements comprising this type of heterogeneous computing devices. Therefore, function reconfiguration, replacement, scaling, or migration (i.e., to another on-chip processing element) will be enabled with the developed micro-orchestration framework. The framework will expose fine grain observability metrics of compute resources in FPGA-based multi-processing SoC devices via an O-RAN compatible or O-RAN-like interface (e.g., O2 interface for the management plane) to the service management and orchestration layer, where policies can be reinforced by employing the multi-site and edge-site RAN controllers.

3.2.3. INTEGRATION & ORCHESTRATION OF EXTREME EDGE RESOURCES

The integration and orchestration of extreme edge resources within the compute continuum defines the necessary interfaces and components for seamless management of compute resources extending beyond the radio access network. The extended cloud continuum comprises centralized cloud resources, distributed edge resources, and heterogeneous extreme edge resources. Integrating these extreme edge resources introduces new challenges, such as decentralized end-to-end orchestration, which differs from the MNO-centric management approaches of 5G.

To integrate the cloud continuum into the common 6G M&O framework, three main enablers have been studied:

- Multi-cluster resource management, providing a unified interface for compute continuum resource management (inventory, provision, operate), enhanced placement mechanisms to distribute network functions and applications in the cloud-

continuum to address resource and proximity constraints, and automated discovery mechanisms for virtualization platforms and extreme edge devices

- Decentralised orchestration, providing a distributed and decentralized orchestration to handle an increased amount of network services and workloads of different shapes and sizes across multiple stakeholders and domains at scale, automated extreme edge devices discovery with distributed registry of infrastructure resources to ease migration of service components across multi-stakeholder volatile extreme edge nodes, and integrated intelligence, with AI/ML algorithms to enable proactive distributed orchestration actions for service assurance.
- Orchestration of the extreme edge providing ETSI MEC enhancements for next-generation hyper-distributed applications, such as edge robotics and smart agriculture, a lightweight constrained version of a MEC platform to be deployed in mobile end terminals or closest location and solutions to address loss of connectivity, near-zero latency requirements, and privacy concerns, while maintaining compatibility with a full-fledged ETSI MEC framework.

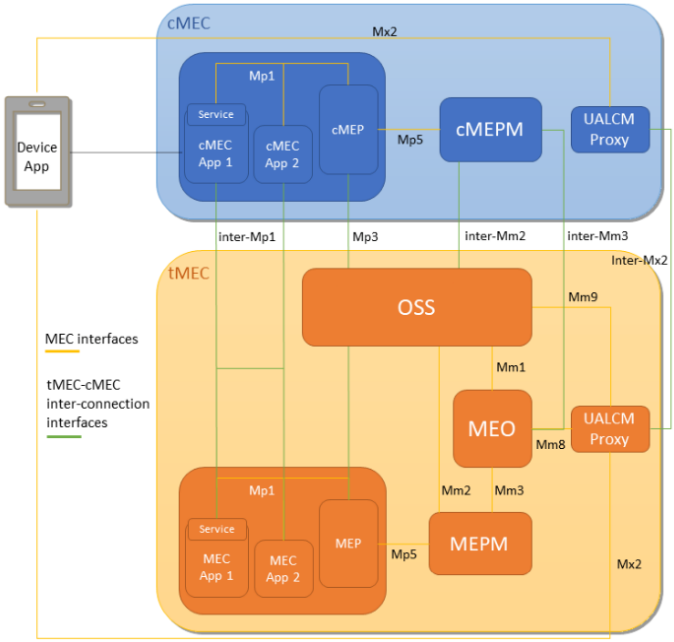


Figure 7: Architectural scheme of constrained MEC together with traditional MEC

On the context of this white paper, we will focus on the later. The architectural modifications required for integrating extreme edge resources involve several key elements. One significant development is the constrained Multi-access Edge Computing (cMEC) [29] architecture (see Figure 7), which extends the traditional MEC framework to include devices beyond the RAN. This architecture addresses the limited computational capabilities of

extreme edge devices, such as IoT sensors and mobile devices, which often rely on battery power and have restricted processing power.

The cMEC architecture introduces efficient features and a layered design that allows it to function as a complete MEC system when resources permit. However, it can also operate with limited MEC functionalities in more constrained environments. This architecture relies on traditional MEC (tMEC) systems for certain functions and introduces new workflows and interfaces to support MEC application development and deployment. The cMEC departs from the tMEC framework and exhibits attributes customized and particular to devices with limitations:

- **Efficient Features:** The cMEC can function as a complete MEC system, encompassing all its elements if the computational resources (e.g., industrial PC) in the extreme edge are powerful enough to handle the complete framework. However, due to the limited resources in extreme edge devices, the cMEC might support only a subset of MEC functionalities. For example, the MEC Orchestrator, with its resource-demanding functions, may be opted out in particularly restrictive circumstances only if a less demanding action is feasible.
- **A Layered design:** given that the tMEC depends on the edge for computational for offloading, content fetching, user authentication, and context, cMEC depends on tMEC for similar functions. This layered strategy necessitates an interconnected relationship between cMEC and tMEC, without involving the implementation of federation concepts that require explicit business agreements and reliance on orchestrators. This conclusion is supported by the research on inter-MEC system connection and federation [27], The MEC Orchestrator (MEO) is regarded as the crucial facilitator for numerous workflows, although cMEC might lack support for it. However, a particular cMEC has option to share various resources with different tMECs by leveraging its orchestrating abilities, or even with peer cMECs. Dependency on a tMEC System: In instances where the cMEC lacks the implementation of a particular MEC function, it must depend on the upper layer tMEC system to provide the lacking functionalities. New workflows, guidelines for MEC application development, and specific interfaces must be established to address the deficiency in functions.
- **End-User Device Co-location and Awareness:** The cMEC system has the flexibility to either operate within the same end-user device as the MEC application or to run on a **constrained device in** its immediate vicinity. The end-user device can engage in the cMEC integration in the following manner:
    1. cMEC-aware: the end-user device and cMEC are either within the same local network or have knowledge of each other's identity (e.g., the cMEC

operates on that specific end-user device). The end-user device has the capability to examine the available cMEC systems and request the deployment of a MEC application, leading to the establishment of a connection between the cMEC and a tMEC.

2. cMEC-unaware: The end-user device lacks awareness of any nearby cMEC and consequently requests the deployment of a MEC application directly to the tMEC. However, upon recognizing the presence of a nearby cMEC deployment, the tMEC opts to instantiate the application on the interconnected cMEC.

The transformation of virtualisation and cloud resources for 6G involves integrating and orchestrating extreme edge resources, addressing architectural challenges, and implementing a flexible, driver-based M&O framework. This approach aims to support the diverse and demanding requirements of 6G applications, ensuring efficient traffic handling, resource management, and service delivery across the extended cloud continuum.

3.2.4. META-OPERATING SYSTEMS TO SUPPORT EDGE-CLOUD CONTINUUM

As the available distributed computing domains and the volume of data continues to increase, mechanisms that help make optimal use of the **edge-cloud computing continuum** at its full extent have become more and more necessary. To cope with the large heterogeneity that such ecosystem entails (in terms of systems' tenancy and underlying processing architecture and capabilities, Operating Systems – OS, networking and virtualization capabilities), solutions based on the "classical" concept of meta-OS are emerging, [10] deployed on top of an existing OS. Thus, future framework may consider a **Meta-Operating System (meta-OS) as an enabler** for managing the underlying edge-cloud computing continuum infrastructure.

Focusing on service orchestration, a meta-OS envisions a clear ***two-level structured orchestrator*** (see Figure 8) to deploy the vertical services, the core network and any software-based supporting service. Once the system receives (via the management portal) a user's intention to deploy a service, this is translated into an "*Intention Blueprint*" (based on TOSCA). This blueprint is sent and processed by the *High-Level Orchestrator* (**HLO**) of one of the domains of the computing continuum, which decides the optimal Infrastructure Element/s (IE) that should deploy the service – based on requirements and AI support. The generated *Implementation Blueprint* is then sent to one *Low-Level Orchestrator* (**LLO**) of the domain, which can deploy the service in the selected IE lies, considering the particularities of the underlying VIMs. While the system can run autonomously (including in the case of self-

detected need for reallocations), an administrator has the last word on the decisions made. Some existing meta-OS are aerOS, ICOS, FluiDOS, NebulOuS, NEMO and NEPHELE [11].

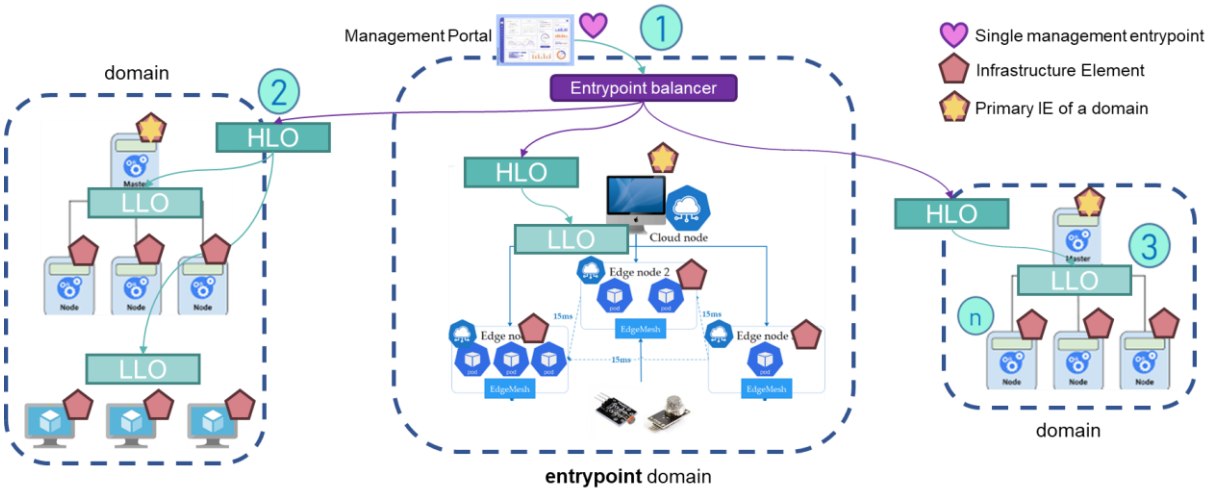


Figure 8: Example of decentralised decision-making of existing meta-operating systems

The meta-OS has to be deployed in the different domains composing the continuum, and leverages the following services to provide its orchestration capabilities:

- *Federation service*, which facilitates the bidirectional exchange of information among different domains of the continuum,
- *Data fabric services*, that enables seamless data integration and accessibility within the domain and across the continuum, supporting advanced data management, semantics and query capabilities,
- *Cybersecurity services*, which enforce authentication, authorization, and access control policies based on roles and identities,
- *Trust management services*, which ensure the integrity and reliability of interactions within the continuum, as well as logging and auditing of key events,
- *AI decision support services* (including Federated Learning (FL) and Machine Learning and Operations (MLOPs)), which leverage data retrieved by the data fabric to recommend optimal workload placements to the orchestrator,
- *Embedded analytic tools*, complementing the previous, providing real-time data analysis and insights within the ecosystem.

All of them work together based on a common continuum ontology [12] and can be consumed by the MNOs to enhance other business-related use cases beyond orchestration. It should be mentioned that further research and integration efforts are needed, as meta-operating systems currently lack some standards and features that are of interest in the 5G and beyond area. For instance, implementation of MANO-compliant interfaces, integration

of *Service Communication Proxy* (SCP) as native load balancer of the system to support the execution of the cellular cores, *Service Function Chaining* (SFC) to enable the creation of chains of connected services (considering Cloud native network functions) and providing support to VNF-based workloads (currently, only CNFs are supported), among others.

3.3. DYNAMIC RESOURCE AND INFRASTRUCTURE MANAGEMENT

As network demands fluctuate and user expectations rise, dynamic resource and infrastructure management has become a cornerstone of modern network design. This section examines cutting-edge techniques for optimizing resources in real time, focusing on adaptive, intelligent, and decentralized approaches that enhance efficiency and performance.

3.3.1. AI/ML FOR RESOURCE MANAGEMENT

To reduce the amount of monitoring/telemetry data being conveyed to a centralized location and reducing decision-making time, AI/ML algorithms should be executed as close as possible to the data plane. IBN enables implementing local control loops, while providing centralized coordination and knowledge sharing [16]. Reinforcement Learning (RL) has been considered for near-real time resource management [17][18]. To reduce the complexity of network management 6G will rely on a re-architected transport network control and a distributed knowledge and decision-making process enabled by the concept of Multi-Agent Systems [19]. Techniques like RL will be used in conjunction with inter-agent communication to achieve faster and coordinated responsiveness. This will bring remarkable advances to optical and packet network control.

Within 3GPP TS 23.288 of Release-18 [13] the evolution of the NWDAF function is increasingly becoming distributed between central consumer and local source analytic functions, to support flexible telemetry collection, federated learning, distributed data processing, etc, to support future 'Native AI/ML' capabilities in the RAN, with ADRF (Analytic Data Repository Function), shown below in Figure 9.

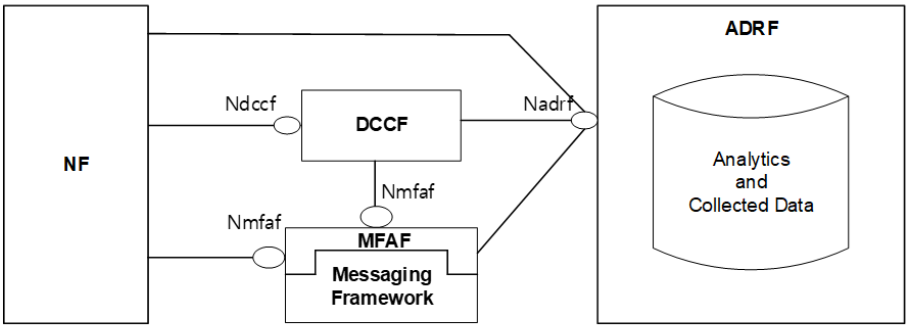


Figure 9: 3GPP Evolved NWDAF with Distributed Analytics *[13]*

To handle the complexity and heterogeneity of the network infrastructures the extension of SMO with an AI-based service deployment optimization module has been proposed. The main objective of this optimization engine is to supervise and coordinate AI/ML operations for the automation of service life-cycle management. For example, during service deployment, it receives network service requests in the form of service graphs or service descriptors, annotated with their respective functional (HW requirements, etc.) and non-functional (E2E latency, availability etc.) requirements. With the use of advanced AI/ML models the component partitions the service graph, decomposes its non-functional requirements and matches its functional requirements in an optimized way, as seen in Figure 10.

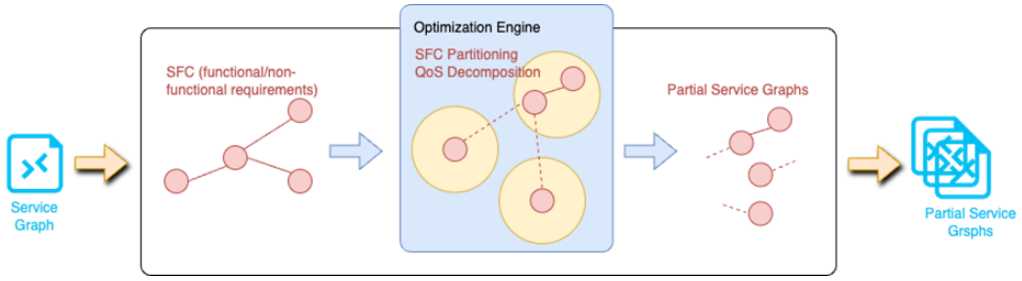


Figure 10: Service partitioning automation example.

3.3.2. FEDERATED LEARNING FOR SLICE AND RESOURCE MANAGEMENT

Key enabler technologies for managing and orchestrating heterogeneous network slice-related computing resources in the RAN-Edge domain include the development of an SLA-driven adaptive learning rate for Federated Learning (FL). This approach addresses several challenges in managing these resources efficiently, particularly in dynamic and resource-constrained telecommunications environments.

Key considerations and solutions include:

- **Heterogeneous Data**: In FL, clients often have diverse datasets. The adaptive learning rate mechanism addresses this by adjusting the learning rate to account for data heterogeneity, ensuring efficient model updates across different clients.
- **Dynamic Conditions**: Telecommunications environments, especially in the 6G RAN-edge domain, are characterized by changing conditions. The learning rate is dynamically adjusted based on real-time client performance, allowing the system to adapt to fluctuations.
- **SLA Compliance**: Service Level Agreements (SLAs) are vital in ensuring performance and reliability standards. The adaptive learning mechanism integrates SLA metrics

such as CPU load into the learning rate adjustment, ensuring FL processes remain compliant with SLAs.

- **Resource Constraints**: Telecommunications environments often have resource limitations. The adaptive learning rate mechanism considers these constraints, contributing to a more efficient FL process.
- **Optimizing Convergence**: The method optimizes the global model's convergence speed by dynamically adjusting the learning rate based on SLA metrics, overcoming the limitations of static learning rates and improving system responsiveness.

The solution is integrated into an AI-driven Management and Orchestration Framework, facilitating slice and resource orchestration in a closed-loop system. This enables zero-touch automation for resource allocation in network slices, particularly in edge computing environments. CPU load, a critical metric in resource utilization, is one of the supervised outputs, and adjustments to the learning rate based on SLA metrics help align predictions with expected resource usage.

Additional features for resource orchestration include managing OTT traffic (traffic generated by over-the-top applications), Channel Quality Indicators (CQI), and Multiple Input Multiple Output (MIMO) technology, which enhances communication by using multiple antennas for transmission and reception.

Key Benefits:

- **Resource Efficiency**: Adaptive learning rates ensure FL client updates align with resource constraints, improving overall efficiency.
- **Reduced Communication Overhead**: By adapting the learning rate, unnecessary communication rounds that could lead to SLA violations are minimized.
- **SLA Compliance**: The FL model training remains aligned with SLA requirements, enhancing system reliability.
- **Adaptability to Dynamic Conditions**: The system is responsive to SLA metric changes and varying operational environments, improving performance and model convergence.
- **Efficient Resource Utilization**: Probabilistic client selection prioritizes clients with favourable SLA metrics, and adaptive learning rates enhance resource allocation.
- **Real-Time SLA Compliance**: The system supports real-time SLA monitoring and adjustment, promptly addressing any violations.

- **Enhanced Convergence Stability**: The combination of adaptive learning rates and client selection ensures stable convergence, reducing the risk of divergence.
- **Balanced Learning and Stability**: The strategy balances the need for fast learning with maintaining stability, ensuring optimal performance across different SLA scenarios.

3.3.3. DYNAMIC INFRASTRUCTURE ORCHESTRATION

The growing demand for ubiquitous connectivity and increasing data traffic challenges the capacity of current terrestrial networks. To meet these demands and deliver next-generation connected experiences, the integration of Non-Terrestrial Networks (NTNs) with terrestrial systems is essential. NTNs, which include satellite constellations, High-Altitude Platforms (HAPs), and unmanned aerial vehicles (UAVs), provide enhanced coverage, resilience, and reduced latency in specific regions. Together with terrestrial networks, they form a "3D Network" composed of ground, aerial, and space stratums, organized into three layers: infrastructure, service, and Management & Orchestration (MANO). This approach addresses the need for seamless service management and orchestration across a heterogeneous and dynamic network environment.

A flexible and dynamic MANO architecture is required to manage services across the static and non-static environments of 3D networks. The architecture builds upon ETSI NFV (Network Functions Virtualization) standards for NFVI management and ETSI MEC (Multi-access Edge Computing) standards for managing edge environments. Additionally, it integrates Software-Defined Networking (SDN) principles for orchestrating various network segments, including the Radio Access Network (RAN), transport, and core networks. However, the unique challenge posed by 3D networks is the management of highly dynamic, non-static infrastructures, such as drones, satellites, and HAPs, which introduce ever-changing topologies.

Challenges in 3D Network Orchestration. Managing and orchestrating infrastructure and network services across static and mobile domains, particularly the non-static components like HAPs, poses several challenges. These include:

- **Mobility of Non-static Infrastructure**: Satellites, drones, and other airborne platforms follow either predictable or random movement patterns, leading to connectivity challenges due to changing network topologies.
- **Connectivity Intermittence**: Limited connectivity due to satellite visibility or HAP movement can impact services that require high availability.

- **Tracking and Coordination**: Real-time tracking of mobile network elements is essential to ensure continuous service availability and to enable dynamic fault recovery or reconfiguration.

To maintain seamless connectivity, unified resource coordination is required to allow proactive and reactive network updates. Hierarchical mobility management models must be applied to orchestrate services across the multiple stratums of ground, aerial, and space domains.

Solutions for Dynamic Infrastructure Orchestration To address these challenges, specific solutions are proposed to manage both static and non-static NFVI resources within 3D networks:

1. **Virtualized Infrastructure Manager (VIM) for Space and Ground**: The VIM manages satellite NFVI, encompassing computing, storage, and network resources, with support for FPGA reconfiguration for hardware adaptability. Using lightweight Kubernetes orchestration (K3s), the system ensures autonomous and scalable resource management between space and ground components, while enabling integration with 5G/6G networks. This facilitates dynamic service provisioning and hybrid network architectures.
2. **Infrastructure Mobility Management Model**: A novel management model is introduced to handle the mobility of non-static infrastructure. It integrates three hierarchical mobility management functions:
    a. **Global Mobility Management Function (GMMF)**: Registers and discovers available domains across the 3D network, facilitating efficient resource allocation and service continuity as physical infrastructures move across different domains.
    b. **Domain Mobility Management Function (DMMF)**: Manages domain-specific mobility and ensures seamless communication between local mobility management functions and the global system.
    c. **Local Mobility Management Function (LMMF)**: Tracks the location and movement patterns of infrastructure components, providing real-time and predictive location updates for optimal resource management.

This mobility management model ensures continuous service delivery and optimal network performance despite the dynamic movement of network elements. Integrating terrestrial and non-terrestrial networks into a cohesive 3D network is key to unlocking next-generation connectivity. By combining innovative orchestration frameworks with real-time infrastructure mobility management, this approach enables efficient, resilient, and scalable service management across heterogeneous and dynamic environments, paving the way for enhanced global connectivity and future communication systems.

4. SECURITY AND TRUST ENABLING SOLUTIONS

In the rapidly evolving landscape of next-generation networks, ensuring robust security and privacy is paramount. This comprehensive approach involves several key enablers: Secure Onboarding items, Security Orchestration, Automation, and Response (SOAR)-enhanced 6G orchestration, privacy considerations enablers, Decentralized Security Analytics, Remote Attestation, Privacy-Aware Orchestration, Cyber Threat Intelligence (CTI) Sharing, and assessing the Level of Trustworthiness. Each of these elements plays a critical role in building a secure and trustworthy network environment, facilitating seamless integration and management of services while safeguarding user privacy and responding effectively to emerging threats. The following sections delve into these enablers, highlighting their significance and contributions to the overall security framework in the 6G ecosystem.

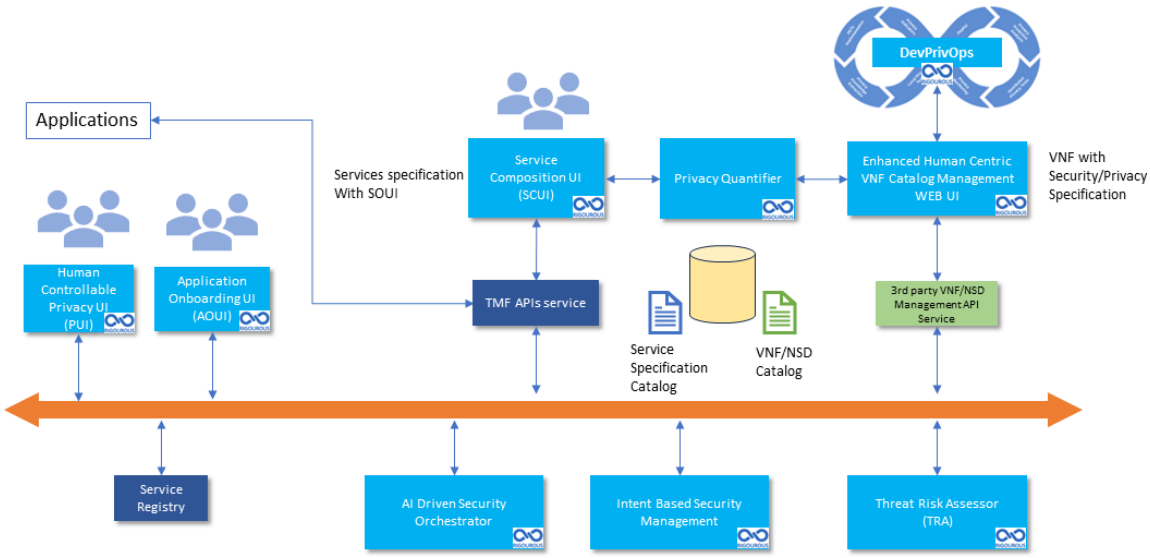


Figure 11: High level approach to security and privacy deployment framework

4.1. ENHANCED SECURITY AND PRIVACY MANAGEMENT

The next generation of network and computing infrastructure is expected to unlock unprecedent levels of connectivity and evolved vertical services by (re-)engineering all its components and characteristics. Nevertheless, these future technologies hold great challenges when it comes to the security, privacy, and trust. In this context, new enablers and new services are being developed to dynamically respond to the ever-changing threat surface on all orchestration layers and network functions. This approach includes 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.

4.1.1. SECURE AND PRIVACY ONBOARDING

In the modern digital landscape, the deployment and management of network applications require advanced technologies to ensure robust security and privacy. The integration of SOAR, Moving Target Defense (MTD), and Privacy-Enhancing Technologies (PETs) is crucial. These technologies collectively enable the secure onboarding of applications, allowing for dynamic adaptation and continuous protection against evolving threats, while maintaining compliance with stringent privacy standards.

In the envisioned deployment of network applications and their subsequent onboarding into a secure infrastructure best practice from DevSecOps, as well as DevPrivOps are essential. Under this, security by design and effective CI/CD pipelines help guarantee that the services are developed with a focus on security and that the resulting applications are privacy aware.

The onboarding process makes the security and privacy aware applications available to customers through a comprehensive catalogue, utilised by solutions such as OpenSlice (Annex A OpenSlice), and orchestrated within a secure orchestration infrastructure. The specifications of the network applications may include security and privacy characteristics, which can facilitate automatic service mutation through MTD, and pluggable PETs, while continued SOAR processes throughout the entire service lifecycle.

The network applications may consist of one or more network services; each service may be composed of multiple VNFs. These artefacts are represented by their descriptors (NSDs and VNFDs, respectively), and they need to be previously onboarded into the NFVO to be instantiated and then orchestrated.

An application can take an already existing service or application and extend it through means of another network service to provide it with additional capabilities, including those about security, such as offering HTTPS connections to legacy systems or increasing the encryption strength of the communication with the application through a proxy; or those related to the privacy of the application and the users, for example, through redaction of logs or anonymization of data, which a sidecar service can offer.

Furthermore, a network application can be enhanced with the capacity to change itself or to be modified by an external orchestration tool to improve its level of security. For instance, the application can update the ports it utilizes periodically or in response to specific threats. Another form of mutation can be exercised by rotating the certificates or cyphers used to connect with a client.

Finally, the catalogue allows the customer to customize to a certain extent the available applications and to receive valuable metrics about the service during runtime. Depending on the user's requirements, the same service may also be offered with different security parameters or privacy profiles.

The SOAR loops ensure that a given application complies with the security and privacy requirements. Moreover, the SOAR processes can react to threats and update the applications accordingly to respect the existing SLAs [20].

4.1.2. ENABLERS TOWARDS PRIVACY CONSIDERATIONS

Regarding privacy considerations, formalizing privacy modelling within data management systems by identifying and quantifying data processing characteristics through a service-specific privacy manifest, appears to be an effective approach. In such case, the core of the system lies in two components: the privacy manifest and the privacy quantification model. The privacy manifest is a formal document outlining the specific service's privacy service definitions. This document is a transparent and clear record of the service's data practices. The privacy quantification model then analyses this manifest using predefined metrics and algorithms to assess the overall privacy level offered by the service, in the scope of an adopted set of policies [21].

The main advantage of such an approach lies in its flexibility. The quantification process can adapt to users' preferences or regulatory standards, following potential privacy impact risk, ensuring applicability in diverse contexts. This quantification offers several benefits. Firstly, it allows users to distinguish between similar services, making informed decisions about which service best suits their privacy needs. Additionally, it provides a benchmark for comparing the privacy performance of different services.

Such an architecture accommodates service updates seamlessly, by maintaining a privacy benchmark even as the service evolves with the establishment of a control version. The privacy quantification component reevaluates the privacy level of the updated service, ensuring the final metric reflects the current practices.

A human-centric approach is emphasized through the Human-Controllable Privacy UI (PUI) which empowers users to assess the privacy levels provided by network services, make informed decisions regarding service usage, and receive suggestions for more privacy-conscious alternatives when necessary. This formalization of privacy quantification empowers users and promotes the development of privacy-conscious services.

4.2. LEVERAGING INTELLIGENCE FOR ORCHESTRATION & SECURITY

6G is currently envisioned as a collection of new technological enablers and thus, it is anticipated to expand the cellular threat landscape through its new elements, e.g., heterogeneous radio, RAN softwarization, multi-stakeholders' deployments, and AI-driven network management. As a result, this vision requires even more stringent and advanced security measures. Addressing these challenges of security and privacy foreseen in 6G networks involves leveraging Decentralized Security Analytics, Remote-Attestation, Privacy-Aware Orchestration and Cyber Threat Intelligence (CTI) Sharing. In the light of the above, a White Paper focusing on Security and Privacy KPIs/KVIs for 6G to assess the performance of the emerging technologies envisioned to be part of the 6G architecture, has been already published [22]. The paragraphs below explore elements related to Decentralized Security Analytics, Remote-Attestation, Privacy-Aware Orchestration and Cyber Threat Intelligence Sharing.

4.2.1. SOAR ENHANCED 6G ORCHESTRATION

The SOAR reflects an architecture aiming to improve the Security Orchestrator (SO) components designed and developed initially for 5G, updating them to the needs of 6G and its new services/use cases, integrating these components with the service orchestration layer with continued feedback to power the DevSecOps paradigm. Central to this architecture is the fusion of cognitive decision-making, operations, and management, ensuring that service development, security, and continued operation are fused seamlessly into a human-centric loop that enforces the expected security requirements for that service. Moreover, this type of fusion informs the human in the loop about the relevant metrics, potential operation issues, identified threats, how the incident response will be carried out (fully automatically or with human intervention/authorization within given parameters). Key components such as Security Analytics Engine (SAE), Threat Assessor, and Decision framework are crucial to bringing into 6G services the best cybersecurity solutions and practices. Intent-based Security management can enable the use of AI without sacrificing the informational needs of the human-in-the-loop to make the decisions that achieve the intended aim (decision making).

Further features/technologies, such as Zero-Trust Identity management and a Cross-Domain Integration Fabric, can further enhance the capabilities of a DevSecOps approach. These features can address the multidomain needs of service owners and Telecom operators, allowing to tackle the latest challenges in Industrial IoT and other more consumer-oriented IoT offerings, enabling cross-border service consistency and further considerations that would fall outside the scope of a typical DevSecOps loop.

4.2.2. DECENTRALISED SECURITY ANALYTICS

A Security Analytics pipeline shall include a rich workflow of modules focusing on sensitive data anonymization, trustworthy and privacy-preserving AI models leveraging Federated Network Data Analytics Function (NWDAF) for anomaly detection, adversarial hardening for enhancing model robustness, and potentially FPGA accelerators for AI models optimization. The enhancement of the underlying AI/ML models of the NWDAF with Explainability (XAI) capabilities can be augmented with Adversarial Training methods to protect the models from data tampering attacks. Data anonymization protocols can also be implemented to protect the subscribers' privacy-sensitive data from deliberate or unauthorized leakage considering the pervasive nature of foreseen 6G use cases. Security Analytics can identify unusual patterns coming from connected UEs (e.g., being misused due to malware) and the wider network infrastructure. Federated learning, coupled with differential privacy techniques, helps maintain data privacy while adversarial training techniques based on generative neural networks strengthen models against privacy-extraction attacks. , while adversarial training techniques based on generative neural networks can strengthen the AI/ML models against attacks that target the extraction of private data [23].

The above-mentioned technologies can be reflected through a Zero Trust concept, requiring continuous verification of entities, including virtualized environments, FPGA edge accelerators and the AI/ML models running on the accelerators. In such case, AI/ML models are attested during bootup using cloud-based FPGAs and Trusted Components (TCs) to establish a Root of Trust (RoT), utilizing unique device identification keys. Real-time verification of virtualized environments ensures configuration integrity through local attestation and key restriction policies, utilizing zero-knowledge techniques to protect privacy. Additionally, integrating Verifiable Credentials (VCs), that constitute digital credentials about data subjects, containing relevant information allows for utilising information attributes associated with a person (such as name/surname) or a device (e.g., ID of the device). The VCs are generated by an entity - the Issuer - and are provided to the users that want to authenticate to a network and get access to provided services. All the attestation information and the VCs are registered on a Distributed Ledger to ensure transparent and auditable information exchange [24].

4.2.3. PRIVACY AWARE ORCHESTRATION

An efficient approach towards the Privacy-Aware Orchestrator involves leveraging the concept of Trust Assessment and Deep Reinforcement Learning. To identify the Level of Trust (LoT) inputs from different components to assess the trust of a deployed E2E service are required. This LoT assessment process takes information stored in the Distributed Ledger Technology (DLT) by an Attestation service, a Proof of Trust (PoT) controller – which attests

Network Paths in order to verify that the traffic follows the defined route- Service Level Agreements (SLAs) verification process and Privacy Index estimation process. Another source of inputs could encompass information concerning active threats provided by an Cyber Threat Intelligence Sharing enabler. The Privacy-aware Orchestrator utilizes the LoT and Privacy Index (PI) metrics to guide orchestration decisions, enhancing security and privacy through actions like live VNF migration. Deep Reinforcement Learning (DRL) and Explainable AI (XAI) provide visibility and traceability in this process [25].

4.2.4. CYBER THREAT INTELLIGENCE

Finally, in foreseen 6G networks, for the confidential and efficient exchange of threat intelligence among stakeholders, an establishment of a network, using a distributed index and proxy system, seems to be the ideal candidate. The establishment of such a privacy-friendly CTI Sharing system, uses MISP instances and CTI sharing proxies at each entity, allowing them to import/export data or use a distributed shared search index. Queries are relayed to all systems, and data control policies ensure only relevant information is shared. Confidential CTI sharing is achieved through multiple shared search indexes, utilizing reverse indexes with trapdoors representing Indicators of Compromise (IoCs) [24].

4.3. TRUSTWORTHINESS FRAMEWORK

To build a reliable and adaptable trust management system for 6G, a well-defined framework is crucial. A solid trustworthiness framework revolves around a Cognitive Coordination component. This component functions as an intent-handling mechanism, understanding complex and abstract trust intent semantics (via five user centric functions), determining the ideal goal state, and coordinating activities to achieve this trustworthy state [26]. Along with MLOps and the XAI component, having the capability to explore the potential of these key functions to provide the desired level of trustworthiness (LoT), learn from past experiences, and evaluate the feasibility of actions based on their expected results.

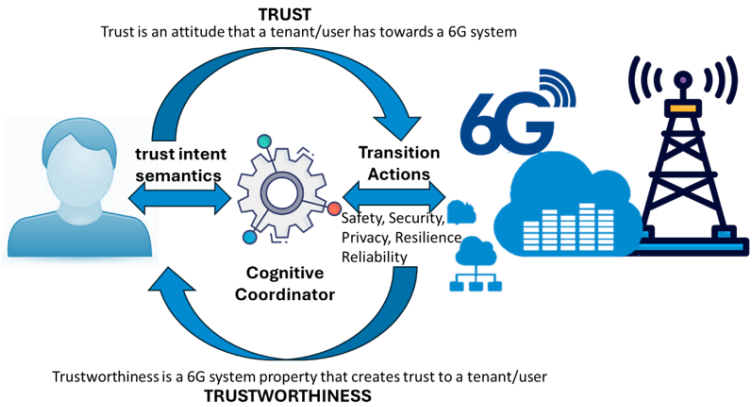


Figure 12: High level approach to the Trustworthiness framework

These five functions, can serve as the primary inputs for the cognitive coordination, are detailed below:

The development of a *Safety function* ensures the required Level of Trustworthiness (LoT) through proper resource isolation at the level of virtualized resources used for deploying User-Side Network (USN) and Network-Side Network (NSN) functions for each user in the 6G system. It begins by establishing the requested LoT, ensuring that the cloud continuum resources, utilized for USN and NSN functions, are securely isolated from unauthorized access and third-party resource sharing.

The *Security function* is essential due to the sensitive nature of the personal data it handles and the associated potential risks. Security breaches could compromise the system's integrity, lead to data leaks, and pose threats to the system and its users. To mitigate these risks, the development of a Security function shall emphasize measures across the entire 6G lifecycle, employing blockchain-based verifiable credentials within a zero-trust framework and action tokenization. Regular security audits to identify and address vulnerabilities and weaknesses should be included as well. By implementing these measures, the creation of a secure, transparent, and reliable system resilient to potential threats and attacks, ensuring consistent user trust and reliability, is feasible

A *Privacy function* is essential for gaining user trust and complying with emerging laws and regulations governing data collection and use. Moreover, privacy preservation in 6G is especially challenging due to user traffic potentially traversing nodes owned by multiple stakeholders, providers, and operators. In the light of the above, the integration of user privacy as a fundamental aspect of user-centric service provision is essential. To achieve this, the development and implementation of mechanisms, such a novel data schema, that will allow users to specify their privacy requirements for new or existing services via an auxiliary chatbot interface or the 6G Service Exposure Provider API, is crucial. This depends on the type of user (tenant or third-party application) and the degree of integration between the user and the system. These privacy requirements or intents can serve as input for a Cognitive Coordinator, influencing primarily the placement and resource management decisions of an AI Orchestrator. Additionally, these requirements will affect other components of the overall ecosystem through respective AI agents.

To address and specify desired network behaviours, such as "user-centric resilience", intent-based functions should be utilised. These specifications can be translated into actual network activities with the help of trained AI models. In this vein, a *resilience function* shall continuously monitor and orchestrate the network to ensure alignment with business intent through closed-loop automation, which includes capturing, translating, and activating trust

and resilience intents with minimal human intervention. For the resilience function to autonomously perform necessary resource orchestration, user-centric intentions must be specified in a machine-readable and processable format. To achieve this, an ontology of intent using knowledge management and semantic modelling methods, based on an expandable meta-model and utilizing the Resource Description Framework (RDF) and RDF Schema standards, is required.

Finally, to complete the trustworthiness state a *Reliability function* should be considered. This function focuses on two main aspects, the service profiling and the reliability profiling should be developed. Service profiling describes the collection of data from all the virtual resources for all the different workload parameters which consist of the diverse services that run on a node and deliver them to the local model training module. Next, the reliability profiling describes the division of the first service under different potential attacks and second under normal operating conditions. During this phase, the modular framework monitors and collects data from all possible layers of the service infrastructure creating and storing the dataset. This dataset can be then used as an input to the AI algorithms which will be then trained and deployed to detect these types of attacks at service run-time.

5. CONCLUSIONS AND KEY TAKEAWAYS

Recent developments in SNS JU projects are shaping the future of networks towards the 6G era. In this route, the critical role of APIs in enabling seamless interaction between software components and network services in 6G networks is highlighted. Key APIs for service and resource management are those from the TMForum; while for closed-loop runtime functions, APIs from ETSI GS NFV-IFA 022 and ETSI GR SAI 004, are the most relevant ones. Network telemetry and monitoring can still be facilitated by Prometheus, gRPC (OpenConfig or OpenROADM YANG models), and legacy protocols like NETCONF, RESTCONF, and SNMP. Transport network control shall be managed through ONF Transport API (TAPI) and TeraFlowSDN (TFS) Controller APIs; however, new challenges emerge when it comes to heterogeneous networks like the 3D networks. Given that, the Common API Framework (CAPIF) developed by ETSI SDG OCF is promoted as a standardised component for managing API publication, discovery, access control, and security.

In addition, the studies on service and resource management, revealed the need for a common service management and orchestration (SMO), which will take advantage of recent technologies and approaches that include intend-based networking, AI/ML decision making, and unified edge-to-cloud compute resources (compute continuum). In addition, it becomes apparent that enhanced security and privacy management are critical for 6G networks, with a focus on secure onboarding, privacy considerations, decentralized security analytics, and cyber threat intelligence sharing.

Overall, open sourcing has been proven to be a fundamental piece for a seamless evolution of the research work in SNS projects; thus, the use of and the contribution to the four running ETSI Software Development Groups (SDGs) (namely TeraFlowSDN, OpenSlice, OpenCAPIF, and Open Source MANO) are becoming a trend.

ANNEX A: OPEN-SOURCE PROJECTS CATALOGUE

Open-source software is revolutionizing the tech landscape, and this section explores some key players. This annex provides information of related open-source software projects that have been impacted and contributed from Reliable Software Networks Working Group. The presented projects hosted by multiple organizations, such as ETSI, the Linux Foundation, and TMForum showcase how collaboration drives innovation in networking and telecommunications.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE - ETSI

ETSI's embrace of open-source projects represents a strategic shift, leveraging the power of collaboration to accelerate innovation in the telecom industry. This approach fosters faster development cycles by drawing on a wider pool of developers, while simultaneously enhancing innovation. Open-source initiatives also promote industry alignment by encouraging widespread adoption of standardized solutions, ensuring interoperability between different vendors' equipment. The ETSI Software Development Group (SDG) is responsible for creating open-source platforms to support next-generation telecommunication networks. ETSI reduces development costs for its members, making participation in standardization activities more accessible. This multi-faceted approach positions ETSI's open-source efforts as a powerful driver for progress within the telecom landscape.

OPENSOURCE MANO

- Description: OSM is a framework for managing and orchestrating Network Functions Virtualization (NFV) and Software Defined Networks (SDN) infrastructure. It provides a vendor-neutral alternative to proprietary solutions.
- Use Cases:
    - Deploying and managing virtual network functions (VNFs) and containerized network functions (CNFs) applications.
    - Automating network service lifecycle management (NSLM) tasks.
    - Enabling multi-vendor and multi-technology deployments.
- Features:
    - Open architecture based on ETSI NFV and SDN standards.
    - Modular design for flexibility and customization.
    - Northbound APIs for integration with external systems.
    - Support for various VNF management and orchestration (MANO) frameworks.

- Ecosystem: A large and active community of developers, operators, and vendors contribute to OSM's development and adoption.
- References:
    - OSM Website: https://osm.etsi.org/news-events/news
    - OSM Documentation: https://osm.etsi.org/docs/user-guide/

TERAFLOWSDN

- Description: TeraFlowSDN is an open-source SDN controller designed for high-performance and scalability. It leverages SDN protocols to manage network traffic and it supports multiple network devices and services.
- Use Cases:
    - Building high-bandwidth and low-latency networks for data centers and cloud providers.
    - Implementing advanced traffic engineering and network control policies.
    - Supporting emerging network technologies like Network Function Virtualization (NFV).
- Features:
    - High-performance packet processing engine.
    - Scalable architecture for large networks.
    - Support for multiple network devices and services.
    - Programmable northbound APIs for customization.
- Ecosystem: A growing community of developers and researchers contribute to TeraFlowSDN's development.
- References:
    - TeraFlowSDN Website: https://tfs.etsi.org/
    - TeraFlowSDN Code Repository: https://labs.etsi.org/rep/tfs/controller

OPENSLICE

- Description: is a prototype open source, operations support system. It supports VNF/NSD onboarding to OpenSourceMANO (OSM) and NSD deployment management. Openslice allows Vertical Customers to browse the available offered service specifications and also allows NFV developers to onboard and manage VNF and Network Service artifacts.
- Use Cases:
    - Implementing network slicing for 5G and future mobile networks.
    - Providing dedicated network resources for specific use cases like IoT, industrial automation, and augmented reality.

  - Enabling network service providers (NSPs) to offer new and innovative services.
- Features:
  - Framework for automating network slice lifecycle management.
  - Support for multi-vendor and multi-technology deployments.
  - APIs for integration with OSS/BSS systems and cloud platforms.
- Ecosystem: OpenSlice is a relatively new project, but it's gaining traction with ETSI members and the broader industry.
- References:
  - OpenSlice Website: https://osl.etsi.org/
  - OpenSlice Documentation: https://osl.etsi.org/documentation/

OPENCAPIF

- Description: OpenCAPIF is an open-source Common API Framework, as defined by 3GPP allowing to expose and invoke Network APIs in a secure and consistent way. It aims to simplify and consolidate communication between network functions and network applications.
- Use Cases:
  - Service providers (telecom, content etc.) open their Network Functions to external domain users via APIs in a secure way, can leverage OpenCAPIF as API providers.
  - Verticals (e.g. SMEs developing Network Applications) can evolve their services and take advantage of the openness of contemporary networks, can leverage OpenCAPIF as API Invokers and acquire a seamless and standardized access to API providers' resources.
- Features:
  - RESTful API for accessing information about network resources and services.
  - Standardized data model for describing infrastructure and service capabilities.
  - Open specification for broad industry adoption.
- Ecosystem: OpenCAPIF is gaining momentum with participation from major network vendors and service providers.
- References:
  - OpenCAPIF Website: https://ocf.etsi.org/
  - OpenCAPIF Code Repository: https://labs.etsi.org/rep/ocf/

ZERO-TOUCH SERVICE MANAGEMENT

- Description: ETSI ZSM (Zero-touch Network and Service Management) is not an open-source project but an industry specification group that provides a framework designed to automate the management of 5G and beyond networks with minimal human intervention. Its goal is to enable autonomous networks that are self-configured, self-monitor, self-heal, and self-optimize through closed-loop automation, driven by AI/ML algorithms. This framework aims to improve the efficiency, agility, and scalability of network services, supporting next-generation service orchestration.
- Use Cases:
    - Telecom providers can utilize ZSM to automate end-to-end network and service management, reducing operational costs and enhancing service delivery speed.
    - Vertical industries (e.g., automotive, energy) can leverage ZSM for industry-specific network slicing, ensuring optimized and tailored connectivity for diverse applications.
- Features:
    - Closed-loop automation for service assurance, self-healing, and network optimization.
    - Support for multi-domain and cross-domain orchestration of both virtualized and legacy infrastructures.
    - AI-driven decision-making capabilities for network operation.
    - Secure management interfaces and open APIs to ensure flexibility and adaptability.
- Ecosystem: ZSM is supported by collaborations across the telecom industry, including service providers, network vendors, and AI developers. It is a key enabler of next-gen network automation, working alongside other initiatives like ETSI's NFV and MEC standards.
- References:
    - ZSM Website: https://www.etsi.org/technologies/zero-touch-network-service-management
    - ZSM Standards: https://www.etsi.org/committee/1431-zsm

LINUX FOUNDATION

The Linux Foundation hosts a wide variety of projects that span various industries. This commitment to open development fosters a dynamic environment where innovation thrives.

By leveraging the collective expertise of a global community, The Linux Foundation's projects address critical challenges and unlock new possibilities across diverse fields. In this section, related projects with smart networks and services are detailed.

SYLVA

- Description: Launched by the Linux Foundation Europe, Project Sylva aims to create a production-grade open-source Telco Cloud Stack. This software framework will reduce fragmentation in the cloud infrastructure layer for telecommunication and edge services.
- Use Cases:
    - Building and managing telco cloud infrastructure for next-generation mobile networks (5G and beyond).
    - Deploying and scaling network services on a common cloud platform.
    - Enabling efficient management of edge computing resources.
- Features:
    - Open-source framework for telco cloud deployments.
    - Reference implementation showcasing best practices.
    - Designed for scalability, flexibility, and interoperability.
    - Supports integration with existing open-source networking and virtualization projects.
- Ecosystem: Project Sylva is a collaborative effort with founding members including major European telecom operators (Telefonica, Deutsche Telekom, etc.) and network equipment vendors (Ericsson, Nokia). The project is open to participation from the broader industry.
- References:
    - Project Sylva Website: https://gitlab.com/sylva-projects/sylva

HYPERLEDGER

- Description: Hyperledger is an open-source collaborative effort hosted by The Linux Foundation, specifically focused on enterprise blockchain technologies. It fosters the development of various blockchain frameworks and tools for business use cases.
- Use Cases:
    - Building secure and transparent supply chain management systems.
    - Enabling efficient trade finance and cross-border payments.
    - Developing innovative solutions for identity management and data provenance.
- Features:

  - A collection of open-source blockchain frameworks, each with its own strengths (e.g., Hyperledger Fabric for permissioned networks).
  - Tools and libraries for blockchain development.
  - Collaborative community for knowledge sharing and project development.
- Ecosystem: Hyperledger boasts a vast ecosystem with participation from leading technology companies, financial institutions, and startups. This fosters a rich environment for innovation and development of enterprise-grade blockchain solutions.
- References:
  - Hyperledger Website: https://www.hyperledger.org/

TMFORUM

TM Forum is a global industry association that promotes collaboration between digital service providers and their technology partners to drive innovation and efficiency in the telecom and digital industries. The organization provides frameworks, tools, and standards, such as the Open Digital Framework, to support the transformation of networks and business operations, enabling companies to accelerate digital transformation. TM Forum's members include a wide range of telecommunications operators, software providers, and system integrators, working together to shape the future of the digital ecosystem. The forum is known for initiatives in areas like 5G, AI, and customer experience management.

OPENAPI

- Description: TM Forum OpenAPI is a suite of standardized REST-based APIs designed to enable seamless interoperability and integration across different systems within the telecommunications industry. It simplifies the management of complex digital ecosystems by offering open, vendor-neutral interfaces that ensure consistent communication between service providers and technology partners.
- Use Cases:
  - Service Providers can use OpenAPIs to integrate legacy systems with new digital platforms, enabling faster service delivery and improved operational efficiency.
  - Developers can utilize these APIs to create new applications and services that easily interact with existing telecommunications infrastructure.
  - Partners can collaborate and share data securely across various platforms through standardized interfaces.
- Features:
  - A wide range of APIs for managing customer, product, and service operations.

  - Standardized, REST-based design that facilitates ease of use and integration.
  - Modular APIs for flexible implementation in a variety of use cases.
  - Active support for cloud-native applications and 5G network operations.
- Ecosystem: TM Forum OpenAPI is supported by a large community of telecommunications operators, technology vendors, and service providers, who collaborate to expand and enhance the OpenAPI library.
- References:
  - OpenAPI Website: https://www.tmforum.org/open-apis/
  - OpenAPI Documentation: https://projects.tmforum.org/wiki/display/API/Open+API+Table

OPEN-SOURCE 6G EXPERIMENTATION TOOLKIT

Experimentation potential on top of 6G network and compute infrastructures faces two key challenges. The first challenge is to provide experimenters with access to the internal configuration of the network components; for instance, to test new AI/ML algorithms for any optimization at the network or service level, a fine-tuning of the underlay communication and compute infrastructure is required by the infrastructure owner. The second challenge is the lack of capability to run medium- or long-term experiments, or even complete projects, without the need for time-consuming manual reconfiguration and provisioning of the setup from time to time. Both barriers are related to the poor capability of the underlay infrastructure to automatically support pure automation and multi-tenancy in a secure way. By addressing these challenges, a more industrialized (automated-repeatable) way for 6G experimentation services is proposed by an open-source Toolkit, which realizes the concept of Trial Networks.

A Trial Network (TN) is defined as a fully configurable, manageable, and controllable network that combines virtual, physical, and emulated resources to enable experiments for validating 6G technologies and measure 6G KPIs. Instances of TNs might be offered targeting specific network domains and technologies. The Trial Network software components are described in a common repository, or 6G Library, which eases an experimenter to perform a modular and automatic deployment of a TN by selecting on demand the required elements from the library. The 6G library's objects are curated and designed to serve as the foundational building blocks for building the Trial Networks. For the library implementation Github serves as a sophisticated version control system essential for monitoring changes within computer files, primarily employed in managing source code during software development. Each element within the 6G library embodies the Everything as a code - EaC philosophy, designed

as self-contained unit equipped with the necessary automations and scripts for deployment in a network and compute infrastructure.

6G EXPERIMENTATION TOOLKIT

- Description: is a software package that can be installed in a network and compute infrastructure to enable the provisioning of "on demand testbeds" to experimenters.
- Use Cases:
    - The wide variety of potential experiments / interactions that a third party can apply in a 6G experimentation platform can form related use cases.
- Features:
    - The Installer, which drives the whole process of creating the platform by installing the core components provided in the package plus open-source automation tools from the Internet (Terraform, Ansible and Jenkins).
    - The core components, mainly the Trial Network Life Cycle Manager (TNLCM)[9] and associated tools like the Graphical User Interface and the Validator of Trial Network Descriptions.
    - The tester of the installation, which automatically deploys and tests a predefined set of Trial Networks.
    - Once the local installation is done, the TNLCM explores the library to identify which components are available for developing a Trial Network. The GitHub repository contains the 6G-library with many components, and each component contains many files with information and automation needed to be deployed.
- Ecosystem: Any owner/operator of an end-to-end experimentation platform/testbed who is interested in adopting the concept of Trial Networks.
- References:
    - Toolkit Website: https://github.com/6G-SANDBOX/6G-Library
    - Toolkit Documentation: https://6g-sandbox.eu/wp-content/uploads/2024/09/6G-SANDBOX-Toolkit_Installation-G-V1.0_F.pdf

[9] https://github.com/6G-SANDBOX/TNLCM

ANNEX B: OPEN-SOURCE TRENDS IN SNS PROJECTS

The Smart Networks and Services (SNS) community is both a major 'user' of open-source solutions as well as a significant contributor to the various open-source communities and (pre)standardisation bodies, showcasing the important part that open-source solutions are expected to play in future telecommunications networks. Based on a survey conducted by the SNS OPS Coordination and Support Action (CSA) project10, among the 33 SNS Call 1 R&I projects, that started their operations in 2023, more than 130 open-source solutions were used by the researchers. Figure 12 depicts the most popular open-source solutions among the SNS call 1 projects, with open5GS being by far the most popular, followed by Kubernetes, OSM, OpenSlice, Prometheus, Open CAPIF and more. Besides the solutions depicted in Figure 12, several other open-source solutions were utilized within SNS (only once by specific projects, hence not included in the graph) including InfluxDB, Sonata, OpenAirInterface (OAI) and many more, showcasing the tremendous variety and differentiation of available open-source solutions.

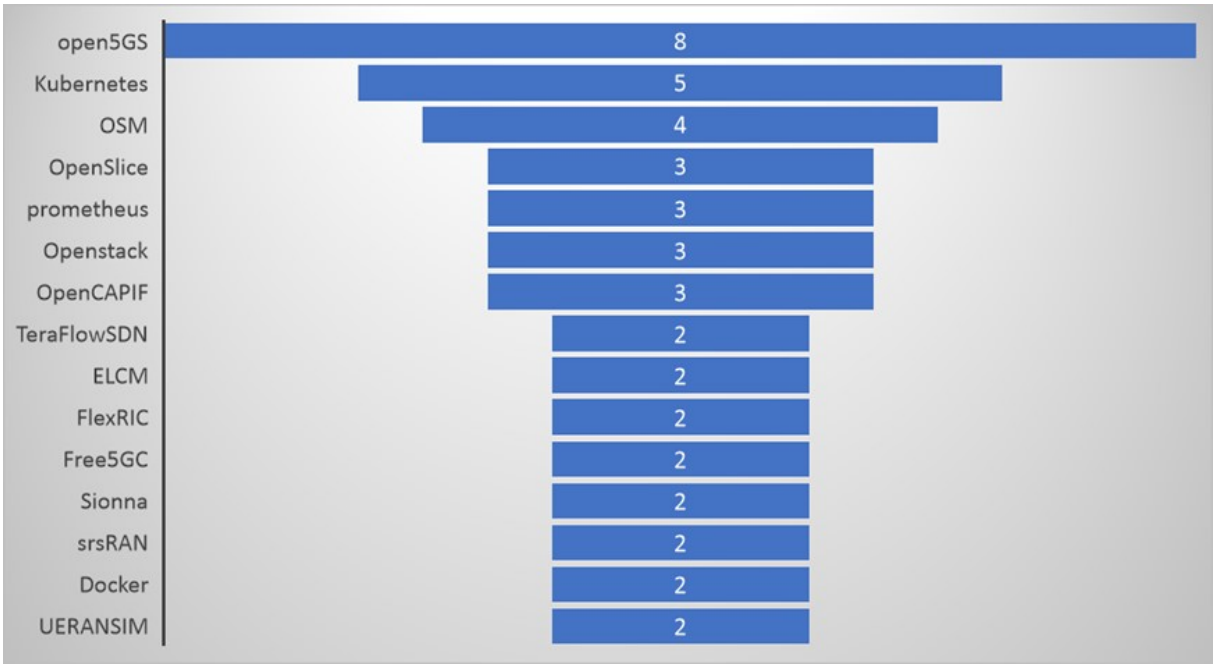


Figure 12: Distribution of Open-source solutions used by SNS Call 1 R&I projects

Despite the relatively short-life at the moment of the SNS OPS survey (approximately 1 year), the SNS Call 1 R&I projects already managed to leave their mark in the open-source community by actively contributing to relevant open-source bodies, with approximately 29 contributions. Figure 13 depicts the number of submitted and accepted contributions to

[10] https://smart-networks.europa.eu/csa-s/#SNS-OPS

open-source communities by SNS Call 1 projects during their first year of operation, categorized per project stream11. As there are more Stream B and stream A projects, the distribution depicted is reasonable, while the high percentage of accepted contributions (~80%) indicates that SNS researchers are conducting meaningful and relevant work. Some of the open-source communities targeted with contributions from SNS are INET, TeraFlowSDN, Open CAPIF, OpenNebula, OAI and more.

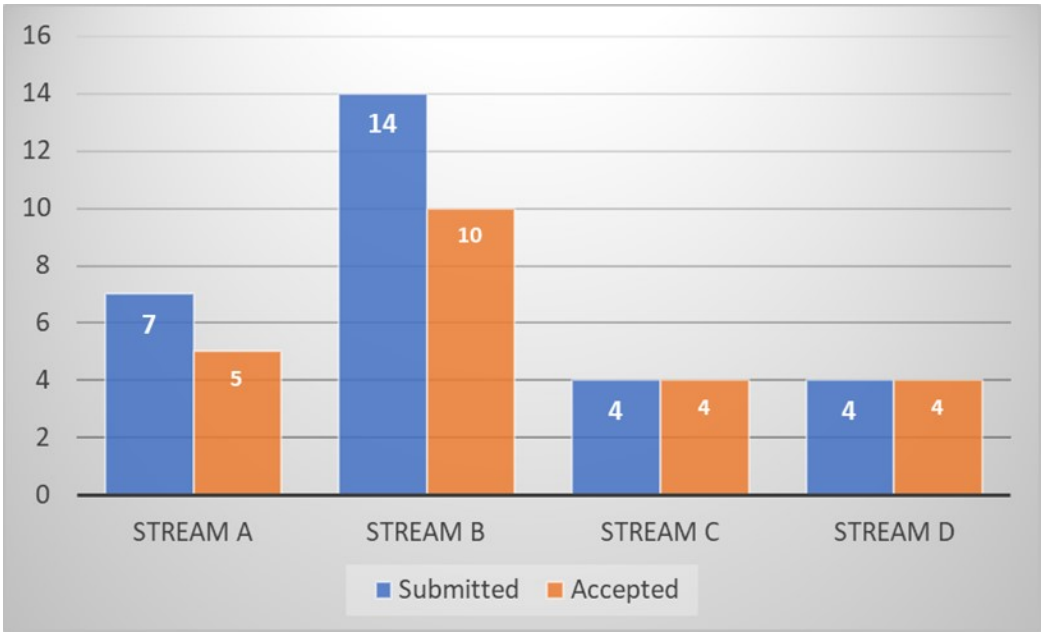


Figure 13: Open-source contributions by SNS Call 1 R&I projects in their 1st year of operation

[11] Focus of SNS Project Streams, **A**: Evolution from B5G, **B**: Revolutionary low TRL research, **C**: Experimental Infrastructures, **D**: Experimentation & Trials. More info: https://smart-networks.europa.eu/sns-call-1/

REFERENCES

[1]. TMF633 Service Catalog Management API https://www.tmforum.org/oda/open-apis/directory/service-catalog-management-api-TMF633/v4.0.0

[2]. TMF641 Service Ordering API https://www.tmforum.org/oda/open-apis/directory/service-ordering-management-api-TMF641/v4.1.0

[3]. TMF638 Service Inventory Management API https://www.tmforum.org/oda/open-apis/directory/service-inventory-management-api-TMF638/v5.0.0

[4]. TMF639 Resource Inventory Management model https://www.tmforum.org/oda/open-apis/directory/resource-inventory-management-api-TMF639/v4.0.0

[5]. ETSI GR NFV-IFA 022 Network Functions Virtualisation (NFV) Release 3. https://www.etsi.org/deliver/etsi_gr/NFV-IFA/001_099/022/03.01.01_60/gr_nfv-ifa022v030101p.pdf

[6]. ETSI GR SAI 004 V1.1.1 ETSI GR SAI 004 V1.1.1 (2020-12) Securing Artificial Intelligence (SAI); https://www.etsi.org/deliver/etsi_gr/SAI/001_099/004/01.01.01_60/gr_SAI004v010101p.pdf

[7]. A. -S. Charismiadis, J. M. Salcines, D. Tsolkas, D. A. Guillen and J. G. Rodrigo, "The 3GPP Common API framework: Open-source release and application use cases," 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Gothenburg, Sweden, 2023, pp. 472-477.

[8]. O-RAN Alliance, "69 New or Updated O-RAN Technical Documents Released since November 2023," 22 03 2024. [Online]. Available: https://www.o-ran.org/blog/69-new-or-updated-o-ran technical-documents-released-since-november-2023.

[9]. 3GPP, "3GPP TS 29.520, 5G System; Network Data Analytics Services; Stage 3, v18.6.0," 24 06 2024. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3355

[10]. Vaño, R.; Lacalle, I.; Sowiński, P.; S-Julián, R.; Palau, C.E. Cloud-Native Workload Orchestration at the Edge: A Deployment Review and Future Directions. Sensors 2023, 23, 2215. https://doi.org/10.3390/s23042215

[11]. European Commission, "Meta-operating Systems for the Next-Generation IoT and Edge Computing", Available at: https://ec.europa.eu/newsroom/repository/document/2022-25/Factsheet__Horizon_Europe_metaOS_projects_8aBnKLInqjY1Epj4HIvU4vzlY_87827.pdf

[12]. aerOS Continuum Ontology, Available: https://wp4.pages.aeros-project.eu/t4.1/aeros-continuum/

[13]. 3GPP, "3GPP TS 23.288: Architecture enhancements for 5G System (5GS) to support network data analytics services, v18.5.0," 27 03 2024. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3579.

[14]. N. Gritli, F. Khendek, and M. Toeroe, "Decomposition and Propagation of Intents for Network Slice Design," 2021 IEEE 4th 5G World Forum (5GWF), Montreal, QC, Canada, 2021, pp. 165-170, doi: 10.1109/5GWF52925.2021.00036.

[15]. 3GPP TS 28.812, "Technical Specification Group Services and System Aspects; Telecommunication management; Study on scenarios for Intent driven management services for mobile networks (Release 16)", March 2020.

[16]. M. Ruiz, F. Tabatabaeimehr, and L. Velasco, "Knowledge Management in Optical Networks: Architecture, Methods and Use Cases [Invited]," IEEE/OSA Journal of Optical Communications and Networking, 2020.

[17]. S. Barzegar, M. Ruiz, and L. Velasco, "Packet Flow Capacity Autonomous Operation based on Reinforcement Learning," MDPI Sensors, 2021.

[18]. L. Velasco et al, "Autonomous and Energy Efficient Lightpath Operation based on Digital Subcarrier Multiplexing," IEEE Journal on Selected Areas in Communications, 2021.

[19]. M. Wooldridge, An introduction to multiagent systems, John Wiley & Sons, 2009.

[20]. RIGOUROUS D3.1 Design plan of the multi-domain automated security orchestration, trust-management, and deployment, Zenodo, Dec 2023. DOI 10.5281/zenodo.10476147

[21]. RIGOUROUS D4.1 Design Plan of the AI-driven Anomaly Detection, Decision and Mitigation. Zenodo, Dec 2023. DOI 10.5281/zenodo.10476152

[22]. National Centre of Scientific Research "Demokritos", Space Hellas (Greece), Infili Technologies, IPO Portoand Telefonica Research and Development, "PRIVATEER White Paper: Security- and Privacy-related KPIs/KVIs for 6G", Zenodo, May 2024. doi: 10.5281/zenodo.11402378

[23]. PRIVATEER (101096110) Deliverable D3.1: Decentralised Robust Security Analytics Enablers - Rel.A.", Jun. 2024, Available online: Zenodo, doi: 10.5281/zenodo.12530825

[24]. PRIVATEER (101096110) Deliverable D5.1: Distributed attestation, identity and threat sharing enablers - Rel.A", Jun. 2024, Available online: Zenodo, doi: 10.5281/zenodo.12531624.

[25]. PRIVATEER (101096110) deliverable, "D4.1: Privacy-aware slicing and orchestration enablers" Rel.A, June 2024, Available online: Zenodo DOI, 10.5281/zenodo.12531563

[26]. SAFE-6G deliverable "D2.1: Definition of Technical Requirements for User-Centric 6G Trustworthiness

[27]. ETSI GR MEC 035, Multi-access Edge Computing (MEC); Study on Inter-MEC systems and MEC-Cloud systems coordination, Available online:

https://www.etsi.org/deliver/etsi_gr/MEC/001_099/035/03.01.01_60/gr_MEC035v030101p.pdf

[28]. ETSI GS ZSM 001, "Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios: ETSI GS ZSM 001 Vl.1.1", 2019.

[29]. E. Rojas, C. Guimarães, A. de la Oliva, C. J. Bernardos and R. Gazda, "Beyond Multi-Access Edge Computing: Essentials to Realize a Mobile, Constrained Edge," in *IEEE Communications Magazine*, vol. 62, no. 1, pp. 156-162, January 2024, doi: 10.1109/MCOM.017.2300056.

[30]. Bartzoudis N, Rubio Fernández J, López-Bueno D, Román Villarroel A, Antonopoulos A. Agile FPGA Computing at the 5G Edge: Joint Management of Accelerated and Software Functions for Open Radio Access Technologies. Electronics. 2024 Feb 9;13(4):701.

[31]. Tuli S, Casale G, Jennings NR. SplitPlace: AI augmented splitting and placement of large-scale neural networks in mobile edge environments. IEEE Transactions on Mobile Computing. 2022 May 24;22(9):5539-54.

[32]. Badia RM, Conejero J, Diaz C, Ejarque J, Lezzi D, Lordan F, Ramon-Cortes C, Sirvent R. Comp superscalar, an interoperable programming framework. SoftwareX. 2015 Dec 1;3:32-6.

[33]. Official website of oneAPI initiative: https://oneapi.io/ (Available: 04-DEC-2024)

[34]. Witt L, Heyer M, Toyoda K, Samek W, Li D. Decentral and incentivized federated learning frameworks: A systematic literature review. IEEE Internet of Things Journal. 2022 Dec 22;10(4):3642-63.

CONTACTS

WG Chair:

David Artuñedo Guillen, Telefonica

david.artunedoguillen@telefonica.com

WG Co-chair:

Dr. Dimitris Tsolkas, Fogus Innovations & Services P.C.

dtsolkas@fogus.gr

SNS WGs:

https://smart-networks.europa.eu/sns-ju-working-groups/

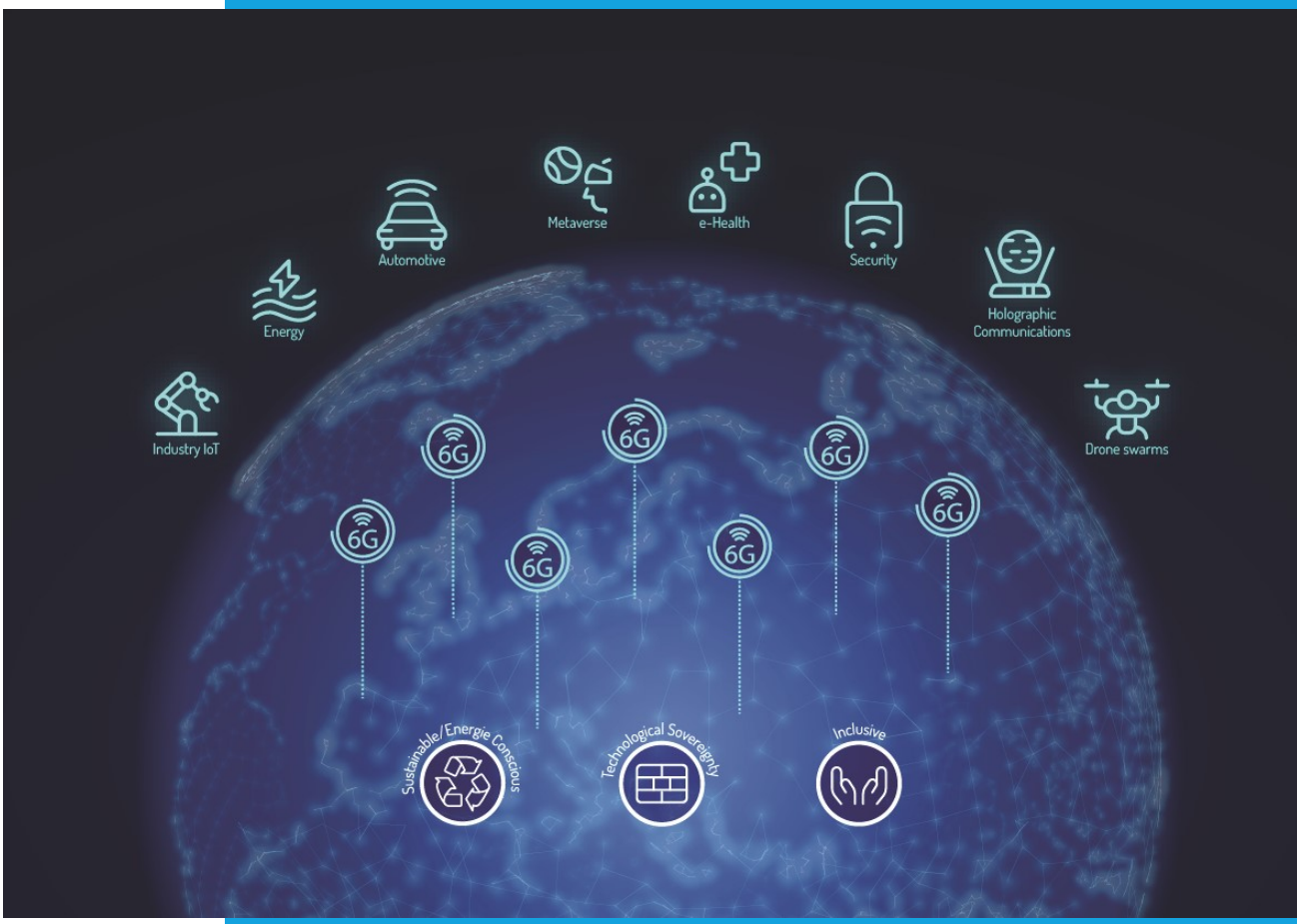
LIST OF EDITORS

Name	Affiliation	Country
Dimitris Tsolkas	Fogus Innovations & Services P.C.	Greece
David Artuñedo Guillen	Telefonica	Spain
Anastasius Gavras	Eurescom GmbH	Germany
Christos Tranoris	University of Patras	Greece
Sándor Laki	ELTE Eötvös Loránd University	Hungary
Antonio Skarmeta	Universidad de Murcia	Spain
João Paulo Barraca	Instituto de Telecomunicações, Universidade de Aveiro	Portugal
George Makropoulos	National Centre For Scientific Research Demokritos (NCSRD)	Greece
Ricard Vilalta	Centre Tecnològic Telecomunicacions de Catalunya (CTTC)	Spain

LIST OF CONTRIBUTORS

Contributors Name	SNS Project(s)
Dimitris Tsolkas	6G-SANDBOX, ORIGAMI
David Artuñedo Guillen	6G-SANDBOX, ORIGAMI
Anastasius Gavras	CENTRIC, 6G-SANDBOX
Christos Tranoris	ACROSS, FIDAL
Marius Iordache	ADROIT6G
Ramon Casellas	SEASON
Sándor Laki	DESIRE6G
Andrés Cárdenas	ETHER
Anastasios Zafeiropoulos	6Green
Maria A. Serrano	VERGE
Antonio De la Oliva	Hexa-X-II
Antonio Skarmeta	RIGOUROUS
Jorge Bernal	RIGOUROUS
João Paulo Barraca	RIGOUROUS
George Makropoulos	SAFE-6G
Harilaos Koumaras	SAFE-6G
Maria Christopoulou	PRIVATEER
Ricard Vilalta	Hexa-X-II
Alejandro Fornes Leal	SAFE-6G
Chrysa Papagianni	DESIRE6G
Luis Velasco	DESIRE6G
Marc Ruis	DESIRE6G
Simon Pryor	DESIRE6G
Kostas Trichias	SNS OPS
Alexandros Kaloxylos	SNS OPS

Smart Networks and Services Joint Undertaking (SNS JU)
Reliable and Software Networks Working Group (SoftNet WG)



Website: https://smart-networks.europa.eu/sns-ju-working-groups/

DOI: 10.5281/zenodo.14234897
URL: https://doi.org/10.5281/zenodo.14234897