5G-PPP Software Network Working Group

NetApp: Opening up 5G and beyond networks

5G-PPP projects analysis

September 2022

Date: 2022

Version: Draft/0.1

Abstract

As part of the 5G-PPP Initiative, the Software Network Working Group prepared this white paper to demystify the concept of the Network Applications. In fact, the Network Application ecosystem is more than the introduction of new vertical applications that have interaction capabilities. It refers to the need for a separate middleware layer to simplify the implementation and deployment of vertical systems on a large scale. Specifically, third parties or network operators can contribute to Network Applications, depending on the level of interaction and trust.
Different implementations have been conducted by the different projects considering different API types and different level of trust between the verticals and the owner of 5G platforms.
In this paper, the different approaches considered by the projects are summarized. By analysing them, it appears three options of interaction between the verticals and the 5G platform owner:

- ***aaS Model***: it is the model where the vertical application consumes the NetApp as a service. The vertical application deployed in the vertical service provider domain. It connects with the 3GPP network systems (EPS, 5GS) in one or more PLMN operator domain.
- ***Hybrid***: it is the model where the vertical instantiates a part of its Vertical App in the operator domain like the EDGE. The other part remains in the vertical domain. A similar approach has been followed in TS 23.286 related to the deployment of V2X server.
- ***Coupled/Delegated***: it is the model where the vertical delegates its app to the operator. The NetApp will be composed and managed by the operator. This approach is the one followed in the platforms like 5G-EVE.

In addition, the paper brings an analysis of the different API type deployed. It appears that the abstraction from network APIs to service APIs is necessary to hide the telco complexity making APIs easy to consume for verticals with no telco expertise and to adress data privacy requirements.

Table of Contents

List of Acronyms and Abbreviations

3GPP	3rd Generation Partnership Project
5G-PPP	5G Infrastructure Public Private Partnership
5GCN	5G Core Network
5GC	5G Core
API	Application Programming Interface
AR	Augmented Reality
AOEP	Automotive Open Experimental Platform
CAPIF	Common API Framework
CI/CD	Continuous Integration/Continuous Delivery
CNF	Container Network Function
CSP	Cloud Service Provider
EC	European Commission
EU	European Union
eNB	Evolved Node B
ETSI	European Telecommunications Standards Institute
ICT	Information and Communication Technology
IoT	Internet of Thing
IOPS	Isolated Operation for Public Safety
K8s	Kubernetes
KPI	Key Performance Indicator
LCM	Life Cycle Management
MANO	Management and Orchestration
MEC	Multi-Access Edge Computing
NEST	Network Slice Type
NetApp	Network Application
NFV	Network Function Virtualization
NFVO	Network Function Virtualization Orchestrator
NRF	Network Repository Function
NSD	Network Service Descriptor

NSMF	Network Slice Management Function
NSSMF	Network Slice Subnet Management Function
NWDAF	Network Data Analytics Function
PaaS	Platform as a Service
PPDR	Public Protection and Disaster Relief
OSS	Operations Support System
KPI	Key Performance Indicator
RAN	Radio Access Network
SBA	Service Based Architecture
SEAL	Service Enabler Architecture Layer
SFC	Service Function Chaining
SMO	Service Management and Orchestration
SLA	Service Level Agreement
SLO	Service Level Objective
SOA	Service Oriented Architecture
TETRA	TErrestrial Trunked RAdio
VAL	Vertical Application Layer
VNF	Virtual Network Function
VNFFG	Virtual Network Function Forwarding Graph
VNFD	Virtual Network Function Descriptor
VM	Virtual Machine
VR	Virtual Reality
UE	User Equipment
WAN	Wide Area Network
WG	Work Group
WP	White Paper

1 Introduction

Importance of Verticals in 5G/B5G System and Beyond: Verticals are an essential driving force behind 5G and Beyond systems. Whether it is augmented reality, IoT, Automotive, or any other application, it is clear by now that the human-to-human communication is only a fraction of what 5G promises to deliver. Most of the traffic or data flowing through 5G/B5G networks will be sourced from those different verticals business and applications.

Benefits of Cloud to Verticals: More than ever before, verticals are competing at an accelerated pace, each trying to get the biggest market share in its domain. There are currently vertical industries that rely on 4G systems and that will continue to exist in 5G/B5G System. Those verticals that built their software-based systems on “legacy” technologies will need to adapt or migrate towards newer technologies as 5G/B5G System matures. Newcomers to appear after 5G becomes massively deployed, however, must envision building their industry in the most flexible and adaptive way leveraging 5G/B5G system capabilities. These features as well as short time-to-market and other benefits that Cloud-Native principles and the “as a Service” model offer will keep verticals in the competition and allow them to deliver valuable quality services in a short time.

Are Verticals ready? Software networks provide high flexibility through implementation of virtual network functions (VNFs). VNF's may be chained across several domains to create Network Applications (NetApps) tailored to the requirements of specific tenants, as demonstrated under previous 5G PPP phases. This requires open platforms that provide access to networks resources which can then be used to develop NetApps supporting requirements and developments from specific vertical sectors. Different mode of interaction between verticals and 5G/B5G System are identified depending on the level of vertical platform control.

NetApp Challenge: As we move from the 5G era onwards to 5G-Advanced, and leading up to the 6G era, the communications fabric and the way the network services are consumed need to be architected differently. Technologies like Cloud-native, AI/ML, Software led, low touch operations and ultimately automation of every aspect of the network and the services it delivers, will be key and essential for this disruption. Previous 5G PPP phases demonstrated that software networks, the Service-Based Architecture (SBA) and network programmability through standard APIs, provide high flexibility to offer network services tailored to the vertical needs and the requirements of specific tenants.

As a response to this, last year a series of projects launched that offer experimentation facilities able to provide enhanced experimentation infrastructures on top of which third party experimenters SMEs or any service provider and target vertical entreprise customers will have the opportunity to test their applications in an integrated, open, cooperative and fully featured network platform running across multiple domains where needed and tailored to specific vertical use cases. Vertical sectors/entrprises have different needs which the NetApp ecosystem embraces with abstracted API sets and new business models. The aim of this white paper is to demystify the concept of the NetApp. The different technical frameworks behind will be captured through the analysis of the different implementations proposed by the different 5G-PPP projects mainly projects launched in ICT-41 Call. This paper targets to:

– Highlight experiences and lessons learned with NetApp development and its Lifecycle management

– Investigate how standards include related information to realize the NetApps

– Understanding of all related stakeholders

– Investigate cross-industry cooperation opportunities

– Promote the innovative services and new business models introduced by the NetApp concept and their evolution towards 6G

2 Network Application requirements

The vertical space targeted by 5G/B5G System is very large. It considers diverse use-cases belonging to the following domains: Smart Cities & Utilities, Transportation, Automotive, Media & Entertainment, Agriculture & Agri-food, Smart (Air)ports, Energy and E-health & Wellness as it is pointed out in [1]. One can ask:

- Does each vertical want to create its own solution for each service?
- Does each vertical want to negotiate with each communication service provider (CSP) on how best to utilize resources?
- Does each vertical want to convince each CSP to use its defined API interface?
- Does each application developer want to adapt to each required CSP API interface?
- Does each private 5G deployment want to negotiate and adapt to each infrastructure provider
- Does each infrastructure provider want to negotiate and adapt to each private 5G/B5G system deployment?

We need an application layer *in the middle* offering common or vertical specific application function or services (for simplicity we call this ***Middleware Layer)*** to simplify the implementation and deployment of vertical system at large scale and this what we call Network Application.

Although there does not yet exist a standard definition of what a NetApp is, in the 5G-PPP Software Working Group, we identified some key characteristics that shall aid to the definition of a NetApp in the context of the 5G/B5G System. Specifically, a Network Application is defined as set of services that provide certain functionalities to the verticals and their associated use cases**.**

The following are some identified characteristics of a NetApp. Specifically, a NetApp:

- Should deliver services to 5G/B5G vertical sectors;
- Must embrace the Service Based Architecture paradigm;
- May expose APIs to be consumed by other service consumers. The exposed APIs should be delivered in an Open API model and may follow the 3GPP recommended APIs for applications (i.e. 3GPP CAPIF, Service Enabler Architecture Layer for Verticals – SEAL);
- A NetApp may be part of one or more vertical application services;
- One or more services of the NetApp may be attached to one or more 5G User Plane Functions (UPF);
- May be part of one or more 5G slices. The slices may be shared or not;
- Part of a NetApp may reside at the (UE) side. The part of the UE side may interact with a NetApp service that resides within the domain network. The UE part may follow the definition of the Vertical Application Layer (VAL) client of 3GPP;
- May interact with the 5G/B5G System by consuming 5G/B5G System's APIs (i.e. the NEF), if the 5G system allows. When interacting with the 5G Systems, it must support relevant 3GPP standards. Such interactions may include location services, Quality of Services (QoS) management, Assured Forwarding (AF) traffic;
- May support service continuity by minimizing service interruption when transferring application context;
- May have resource and network requirements in terms of hardware, memory, GPU, CPU, etc.;
- May have placement requirements (e.g. edge, region, core, etc.). Additionally, a network latency KPI must be specified by the NetApp when requesting a slice with specific characteristics by the 5G/B5G System;
- May consume monitoring and telemetry data from the 5G/B5G System. Such data from the 5G/B5G System should be consumed by functions like the Network Data Analytics Function (NWDAF);

- May interact with the service orchestrator or resources Orchestrator of the domain if this is not restricted;
- Should follow relevant 3GPP security definitions and recommendations.

Software networks provide high flexibility through implementation of virtual network functions (VNFs). VNF's may be chained across several domains to create Network Applications (NetApps) tailored to the requirements of specific tenants, as demonstrated under previous 5G PPP phases. This requires open platforms that provide access to networks resources which can then be used to develop NetApps supporting requirements and developments from specific vertical sectors.

3 The marketplace for NetApp

One of the main challenges in the 5G context is the shortening the idea-to-market process through the creation of a European testbed for Small and Mid-size Enterprises (SMEs) that is fully automated and self-serviced, for rapid development and testing of new and innovative Network Applications (NetApps).

Several key marketing topics have been analyzed, as considered relevant for the research:

- analysis of the Cloud-Native 5G Context for enabling scalable, efficient and secure deployments of NetApps.
- initial analysis of the PPDR 5G Apps Market, including its overall Value, the trends in this Market, notable players, opportunities and challenges in developing NetApps and the Market Evolution.
- initial analysis of the Automotive 5G Market Value, trends, challenges and opportunities and to identify notable players and Market Evolution potential
- assessment of the overall 5G Apps Market Value Chain
- initial analysis of the business elements of each NetApp context

The market research [2] is focused on the Cloud-Native 5G architectures, technologies and processes able to support reliable, scalable and secure, cloud-oriented business models. The key models and components of Cloud-Native deployments consist of practices such as continuous deployments, microservices-based architectures, the use of containers and the achievement of elastic scaling capabilities with readiness to introduce new functionality with increased automation.

The 5GASP market research report is treating also the PPDR market overview, as in the industry the narrowband PPDR communication systems are mainly utilizing mission-critical voice and, in certain cases, low-speed data services. PPDR communications have over the years adopted digital technologies in order to improve voice quality, provide end-to-end encryption and some other advanced functionalities enabled by digital technology, as the PPDR vertical can benefit substantially on 5G when it is properly matured, (search and rescue support using emergency robots and unmanned aerial vehicles (UAVs), sensing of the affected areas using high definition (real-time) video streaming and massive Internet of Things (IoT), multimedia messaging, mobile office/field data applications, location services and mapping, situational awareness and other broadband capabilities, as well as mission-critical voice services provided by traditional system)

The market value for 5G PPDR Network and Services Market is not yet established, as the Market Value estimations can be made on the current situation and expected impact of gradually introducing 5G technologies into the PPDR sector, expect the evolution of 4G/LTE PPDR systems towards 5G systems, hybrid networks to be in use at a certain point.

The Market Trends, as a possible business opportunity for the 5G PPDR verticals and, especially, SMEs may be based on independent test/trial environments, including 5G Apps ecosystems, 5G-related knowledge and consultations. The opportunities identified for the evolution of 5G Apps Ecosystems are linked to the vertical of PPDR, as they are well behind the innovations brought upon the evolution of communication networks, as for example TETRA is used in many cases in many EU countries that still have not adopted 4G for their PPDR services yet, as the market for 5G in the PPDR sector is not established yet as not much 5G infrastructure for PPDR is in service. it has been identified the opportunity on short-term, that could be in establishing, operating, and supporting testing/trial environments for both operators and PPDR practitioners considering the ability to test and validate the behavior and performance under realistic circumstances. As these environments can be highly flexible, it could be expected that infrastructure vendors will have an interest in participating, due to the fact that the 5G facilities supporting PPDR-centric experimentation and trials are not representative, several potential issues being identified:

- unavailability of 5G infrastructures for test and verification for PPDR needs; limited locations where test/verification can take place
- unavailability of specific PPDR features (e.g., 5G IOPS) and components for 5G experimentation; unavailability of test/verification tools that are already integrated and easy to use; available 5G implementations typically don't support configuration flexibility,
- outdated ICT systems (e.g., TETRA and DMR), lack of technical knowledge.

As for the Market Evolution, the transition will last for a decade, during this time there will exist narrowband networks, broadband networks and hybrid networks utilizing a combination of narrow- and broadband services, it is expected that (at least EU member) states will remain independent in choosing their PPDR networks strategy, technology and legislation related to it. An example could be Automotive Market, the overview of the current 5G Apps Market, at European and country Level, expanding on the Market Value and Market Trends, indicating that the autonomous vehicles could potentially eliminate up to 94% of traffic fatalities**.** It is perceived as a large and fast-growing market, reaching over € 3 billion by 2025, as it can be deployed for current and future market opportunities, segments, and challenges. The Total Addressable Market is comprised of the relevant segments of the market, according to FIOR Market Research 2019, the Global Automotive Teleoperations Market will be valued at € 60 billion in 2030, the global autonomous vehicle market is projected to reach a market size of $ 888.40 billion by 2028 at a rapid and steady compound annual growth rate.

The **Market Value Chain** linked to telco industry has embarked on a transformation from purpose-built appliances, often in physical boxes, to virtualized, and later, containerized software applications that deliver Network Functionality, in line with the still ongoing trend of software transformation in many industries, including the telecom and service-provider related sectors, advances of transformation to software in four ways, based on Choice, Agility, Efficiency and Focus.

Despite the potential risks related to NetApps being adopted by PPDR and Automotive stakeholders, there is a high potential that NetApps can be soon adopted, based on:

- very fast development of the 5G market ecosystem and its proven business benefits in the verticals of telecoms,
- interest of major players to get involved in the early phases and playing a role in the definition of 5G cloud application development,
- need of all stakeholders to test new NetApps on mature 5G testbeds to advance their technology, even before it is market-ready,
- interest of increasing resiliency, efficiency, and public safety,

4 NetApp and the need for Exposure

4.1 NetApp Definition

Network Application is a piece of software that interacts with the control plane of a mobile network by consuming the exposed Application Programmable Interfaces (APIs), e.g., northbound APIs of 5G core and RAN Intelligent Controller (RIC), and edge computing APIs, in a standardized and trusted manner to compose services for the vertical industries. Network Applications can provide services to vertical applications, either as an integrated part within the vertical application or by exposing APIs (called business APIs).

The Network Application ecosystem is more than the introduction of new vertical applications that have interaction capabilities. It refers to the need for a separate middleware layer to simplify the implementation and deployment of vertical systems on a large scale. Specifically, third parties or network operators can contribute to Network Applications, depending on the level of interaction and trust. For instance, a Network Application residing in the operator domain, primarily considered for Non-Public Network (NPN) deployments, can potentially have further access to network capabilities in addition to the functionality provided through the northbound APIs available in third-party Network Applications. The same request triggers the development of Vertical Application Enablers (VAE) standardized by the third Generation Partnership Project (3GPP) SA6 working group in [3].

4.2 Common API modelling languages and protocols

Network control and management has evolved, and nowadays Multiple Standard Defining Organizations (SDO) have contributed with data modelling languages and the corresponding data models to describe a service and/or device capabilities, attributes, operations, and notifications to be performed or received from a device or service [4]. The Internet Engineering Task Force (IETF) has proposed Yet Another Next Generation (YANG) data model language. Later, the introduction of Protocol Buffers has signified a new step in data model definition. The proposed data modelling languages have an associated transport protocol, which provides primitives to view and manipulate the data, providing a suitable encoding as defined by the data-model.

Ideally, data models should be protocol independent. Each proposed transport protocol shall provide an architecture for remote configuration and control based on client / server. It should support multiple clients, provide access lists, include transactional semantics, and deploy roll-back functionalities in case of error. In practice, current data modelling languages and transport protocols are tightly interrelated. In the following subsections we present the most significant.

4.2.1 YANG and NETCONF/RESTconf

YANG is a data modelling language that is used to define a component configuration, state, and notifications. YANG structures data into data trees within the so called datastores, by means of encapsulation of containers and lists, and to define constrained data types. It allows the refinement of models by extending and constraining existing models (by inheritance/augmentation), resulting in a hierarchy of models. A YANG data model descriptor includes a header, imports, include statements, type definitions, configurations, and operational data declarations as well as actions (RPC) and notifications. NETCONF is a control and management protocol that supports the configuration of devices based on their known YANG-based data models. It is based on the exchange of XML-encoded RPC messages over a secure (commonly Secure Shell, SSH) connection. NETCONF offers operation primitives to view and manipulate data, which is arranged into one or multiple configuration datastores. Later, the RESTCONF protocol has been presented as a feasible solution to provide the benefits of NETCONF using Representational State

Transfer (REST) with Hypertext Transfer Protocol (HTTP). RESTCONF protocol organizes the datastore using Uniform Resource Identifier (URI) that reflect data hierarchy. HTTP REST operations such as Create, Read, Update, Delete (CRUD) are applied to the defined URI.

4.2.2 Protocol buffers and gRPC

Protocol Buffers (protobuf) are a language-neutral, platform-neutral extensible mechanism for serializing structured data. Its encoding in byte-oriented messages increases the efficiency compared to XML/JSON encodings.

Following the proposal of protobuf, novel protocols such as gRPC and gNMI have been proposed. Google Remote Procedure Calls (gRPC) is based on HTTP/2 and considers protocol buffer byte-oriented messages, thus introducing low latency. gRPC Network Management Interface (gNMI) is a protocol for configuration manipulation and state retrieval. It is built on top of gRPC and it is described using protobuf and it can use binary or JSON encoding for payload. This allows the usage of YANG data models, allowing the integration of all efforts for defining them in Standard Defining Organizations (SDO).

4.2.3 OpenAPI and HTTP

Finally, OpenAPI is a data modelling language that is provided through the HTTP protocol. It allows the definition of JSON/XML schemas for data exchange, the multiple defined URLs, and finally, the possible defined operations and the involved data in JSON/XML.

4.2.3.1 What is HTTP REST?

- Representational State Transfer (REST) is a software architectural style for Application Programming Interfaces (APIs) that consists of guidelines and best practices for creating scalable web services. REST uses simple HTTP to make calls between machines.
- This happens via a request/response mechanism between the server and the client. For example, a client, let’s say an Android application, makes a request for the most recent posts from the website. The server knows how to interpret this request, through REST, and satisfies the response by providing the most recent posts in a format understood by the client.
- REST requests interact with the resources in your application (e.g. a Post or Page). These interactions are typically Reading, Creating, Updating, or Deleting. Combined with HTTP, REST requests are formed using four verbs:
    - POST: Create a resource
    - GET: Retrieve a resource
    - PUT: Update a resource
    - DELETE: Delete a resource
    - The data retrieved is supplied in a machine-readable format, often JSON in modern web applications.
- REST was proposed by Roy Fielding in his 2000 dissertation Architectural Styles and the Design of Network- based Software Architectures

4.2.3.2 What makes an API RESTful?

- An API must have the following architectural features to be considered RESTful:
- Client-server: the client is separated from the server. This means that clients are not concerned with data storage and servers are not concerned with display. This

ensures that data is portable and can be reused in multiple clients, and servers are simpler and more scalable.

  - Cacheable: clients can, and should, cache responses to improve performance, and avoid the server with every request.
  - Stateless: the necessary state to handle the request is contained in the request itself, whether as part of the query parameters, URL, body, or headers.
  - Uniform interface: information transferred via REST comes in a standardised form, creating a simplified, decoupled architecture.
  - Layered System: the architecture is composed of hierarchical layers. Each component cannot "see" beyond its layer: a client cannot tell if it's connected to the server or to an intermediary.
- A separate, but closely related concept is hypermedia. Hypermedia allows a client to more fully discover a REST API without needing to know anything about the structure of the API. It's similar to hyperlinks on the human-readable web (which enable discovering new sites and content). The server provides the information the client needs to interact with it. This means that the client can interact with the server in complex ways without knowing anything beforehand about it.

4.2.3.3 What is an open API?

- Open APIs are publicly available APIs that give developers access to proprietary software information that they can make use of in their own software and applications. REST is the ideal architecture for creating an Open API for the web because, by using HTTP, it is built on the principles of the open web. To leverage an open REST API a developer just needs to make a HTTP request.
- By making data available for developers to use in their own applications, open APIs are transforming the internet. Developers can access data across services, creating applications that aggregate information from different providers. The impact of APIs cannot be overestimated; they are transforming the way businesses and services are run.
- In general, then Open API allows to describe, develop, test, and document APIs conforming to the REST architecture, so it allows to create RESTful APIs.

5 The 5G openness capabilities interpreted by the different projects

5.1 Introduction

5G is providing new experiences, such as AR and VR offerings, to our traditional consumer customers. But our mobile cellular industry is also pushing into multiple new verticals with distinctive service categories, like future factories, eHealth, automotive, Mission Critical, Immersive Media etc, with the expectation of addressing these markets in the next three years or so.

So how will the telco industry that has essentially created and matured three mobile services over the past thirty years (voice, short messaging and internet connectivity), deal with this huge challenge of developing multiple markets in a few short years?

To meet the scalability, the flexibility and the performance to cost-effectively deliver 5G services, a Cloud-Native framework able to integrate all VNFs is required. This would enable operators to create, contract for, or require as a condition of use, a standardized "adapter" that would expose all control, parametric, and management APIs and data in a common way

Only by redesigning the software architecture and core functions using Cloud-Native design principles and IT web-based development and methodologies, can CSPs gain the necessary agility to rapidly deliver new services and reduce their time-to-market.

In this section, we describe the approach followed by some 5G-PPP projects, namely: 5GASP [5], 5GMEDIAHUB [6], SMART5GRID [7], 5G-INDUCE [8], EVOLVED-5G [9], VITAL5G [10]. Section 5.8, summarize other view on the network application from projects which are not part of ICT-41 Call such us Affordable5G [11], DEAMON [12], TeraFlow [13] and 5G-VICTORI [14].

For a detailed presentation and explanation, we invite the reader to visit the website of the different projects respectively where they have access directly to the public documentation and to the contact names.

5.2 5GASP approach

5.2.1 The onboarding model

The overall 5GASP facility is composed of several interworking sites, each deployed at a different geographic location and defining a single administrative domain. Every 5GASP facility site includes at least the following components: i) a NFV Orchestrator, taking care of the lifecycle management of provided network services that comprise the host network slice, b) a Virtualized Infrastructure Manager, responsible for controlling and managing the NFV infrastructure compute, storage, and network resources within each site's infrastructure domain and c) a Testcase Execute Engine, which performs and executes automated tests against the deployed NetApp on the facility. In this context, 5GASP envisions the option to provide developers with a single entry-point to the facility by means of a portal. This portal will allow any developer to onboard its NetApp, specify the accommodating site to host it and the underlying Network Slice and describe the tests that should be triggered once the NetApp is deployed.

To provide a unified abstraction for all sites, a necessary experiment modelling and transformations need to be defined so that experiments can properly run on any 5GASP facility, regardless of the internal details. 5GASP envisages that this process can be related as a unified experimental model bundled together as a **"*triplet*"** triggering a service deployment order, as depicted in .

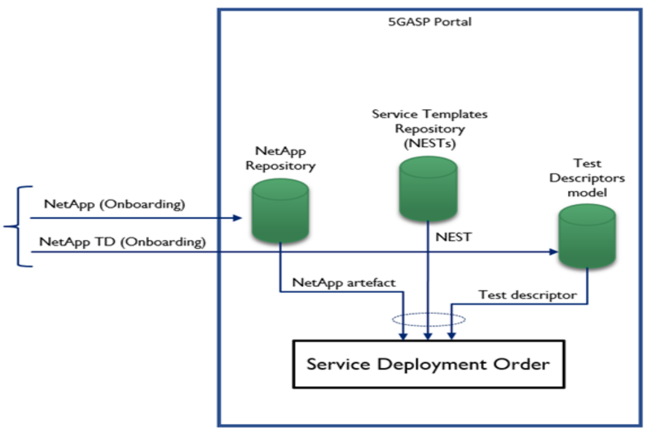

Figure 1 5GASP Onboarding triplet model

The portal solution is based on the open-source project, Openslice [16]. Openslice offers both a user-friendly UI, multi-tenancy, support for onboarding VNFs to target facility NFVO and an Open API based on TM Forum Open APIs making it a perfect candidate for facilitating the project's needs.5GASP's approach for each segment of the experimental "*triplet*", i.e. NetApps, hosting network slices and test descriptors, is to be defined under the TMF's Service Specification resource model [17]. Service Specification is a class that offers characteristics to describe a type of service. Functionally, it acts as a template by which services may be instantiated.

To support this approach, NetApps described as VNFDs/NSDs, depending on the defined model YANG or TOSCA, that will be onboarded through the portal will be referred as Resource Facing Service Specifications expressing the resource aspects of the NetApp with its respective requirements. As enhancements of the NFV architecture towards "*cloud-native*" are currently attempted, 5GASP aims to provide effortless transformation for already containerized applications to NSDs/VNFs via Kubernetes Helm Charts, leveraging deployment schemes described in [18].

Network requirements will be fully aligned with GSMA's Generic Slice Template (GST) properties, and each designated site will provide information on the range of network requirements it supports in form of ***NESTs***. Therefore, these templates will be either available to the developer to choose from or there will be automatically allocated, depending on the NetApp fulfilling its requirements. Each one of the populated properties in NESTs will be perceived as a Service Spec Characteristic resource class representing a key feature of the service specification describing the hosting network slice. Lastly, testing may be carried out through pre-defined automated test cases already described in each facility site [49]. The reference to each test case can also be achieved via the adoption of Service Test Specification (TMF653) model. Once all entities are expressed to the above models, then bundling to a single entity can be achieved and progressed through underlying components for fulfilment. The concept of this unique entity can be facilitated through TMF's Service Order model [19]. Once a Service Order is placed, service fulfilment process is instantiated by our Service Orchestrator and runs the delivery process as per the requested specification, gets the full decomposition up to the required network level operations and executes them onto an administrative domain. The fulfilment and delivery process are further elaborated in the next section.

5.2.2 NetApps deployment and orchestration

As Service Deployment Order is captured by the 5GASP system, the fulfilment process is instantiated as illustrated in Figure 2. Here, order fulfilment and delivery are happening in two layers: by the Service Orchestrator and then by the NFV Orchestrator. Although the Service Orchestrator resides within the 5GASP portal, the NFVO is facility site specific, thus the two-layer distinction. Service Orchestration is aware of all underlying facility sites and their respective network capabilities and is responsible of coordinating the service deployment through certain steps depicted in Figure 2, simultaneously ensuring that each step is successfully progressed through.

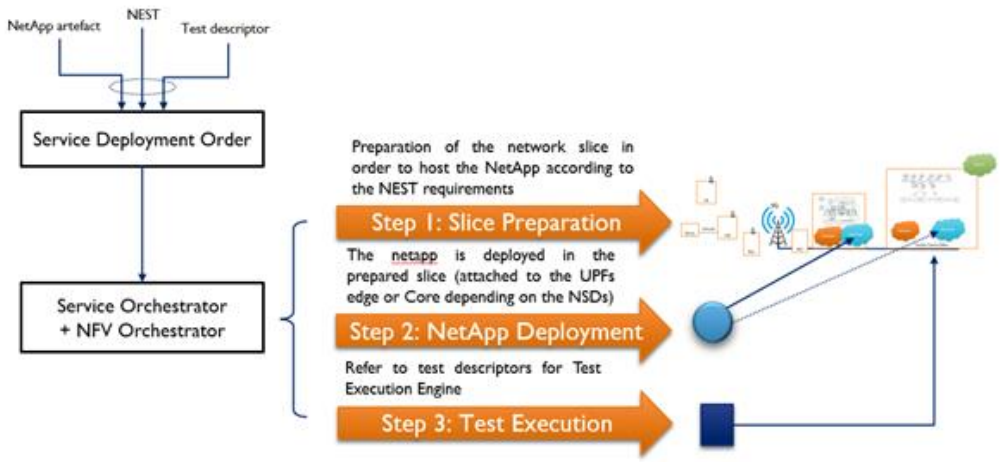

Figure 2: Service Order fulfilment and delivery

A service order may trigger orchestration process in a single facility site, or it may involve a cross-domain orchestration. In the latter case, Service Orchestrator may collaborate with a Network Orchestrator to establish a multi-site deployment. As outlined above, to begin the process, the Service Orchestrator transforms the properties of the provided NEST into network requirements which are then requested to be accommodated by the underlying facility site(s). Each testbed implements a set of these NESTs and once requested it deploys the respective service to facilitate the network requirements accordingly, e.g. 5G Core – Edge deployment, depending on latency inputs. Once the network slice is properly prepared on site's infrastructure, NetApp deployment request is expected and thus, the flow returns to Service Orchestrator for that matter. Eventually, NetApp is deployed on the previously prepared host network slice.

5.3 5GMEDIAHUB

5GMediaHUB [20] aims to accelerating the testing and validation of innovative 5G-empowered media applications and NetApps from 3rd party experimenters and NetApps developers, through an open, integrated and fully featured Experimentation Facility. This will significantly reduce not only the service creation lifecycle but also the time to market barrier. In particular, 5GMediaHUB builds and operates an elastic, secure and trusted multi-tenant service execution and NetApps development environment based on an open cloud-based architecture and APIs, by developing and integrating a testing and validation system with two existing well-established 5G testbeds (by CTTC and Telenor) for enabling the fast prototyping, testing and validation of novel 5G services and NetApps.

5GMediaHUB offers: (i) a DevOps environment for Testing as a Service; (ii) a rich set of Experimentation Tools that offer scheduling, validation, verification, analytics and QoS/QoE monitoring mechanisms; (iii) A set of re-usable vertical-specific and vertical agnostic NetApps with easy to use APIs that can be consumed by application developers, reducing the complexity and risk of integrations and operations; (iv) a re-usable open-source NetApps Repository; (v) an umbrella cross domain service orchestrator to deliver cross-domain orchestration of NetApps; (vi) an innovative security framework offering software defined perimeter protection and isolation of NetApps; (vii) incremental validation capabilities of the Experimental Facility evidenced through 3 novel media use cases with 2 scenarios each, over 3GPP Release 16 [21] and Release 17 [22] 5G testbed releases.

5GMediaHUB is designing and developing a set of open, standards compliant Northbound interfaces that will be made available to the application developers and expose the capabilities of the verified NetApps that are available within the NetApps Repository. These interfaces will support the development of media type applications following the 3GPP SEAL [23] and CAPIF [24] specifications and offer APIs for video streaming, user registration, reporting, discovery, event notifications, etc.

5GMediaHUB is aligned with ETSI's MEC vision of an evolved NFVI, with PaaS capabilities as illustrated in Figure 3. NFV was initially conceived as a paradigm shift from “black box” Physical Network Functions (PNFs) to software-based Virtualised Network Functions (VNFs) but has since gained a wider scope, aiming to also serve vertical industries. For this vision to succeed, next-generation NFVIs must offer feature parity with state-of the- art Public Clouds with PaaS capabilities (e.g., Microsoft Azure), as well as compatibility with the Cloud Native technology stack that powers the ongoing cloud computing revolution. 5GMediaHUB targets the media vertical industry and has a strategic vision to offer PaaS capabilities [25] by abstracting NFV complexities from the vertical application developers. This will be accomplished via NetApps, i.e. chains of application enablement VNFs that implement networking, security, resource management, load balancing and vertical specific functions on top of the NFVI, abstracting its details. Thus, vertical applications only interact with the NFVI via Northbound APIs, that will be offered by the NetApps. NetApps in 5GMediaHUB are mapped to Network Slice Instances that can span across different testbed facilities and NFVIs, to mimic real-world 5G infrastructures with multiple Data Centres and Multi-access Edge Computing (MEC) nodes, that are bridged by cross-domain slices. Thus, individual VNF instances can be optimally placed depending on resource availability, as well as on performance and latency constraints.

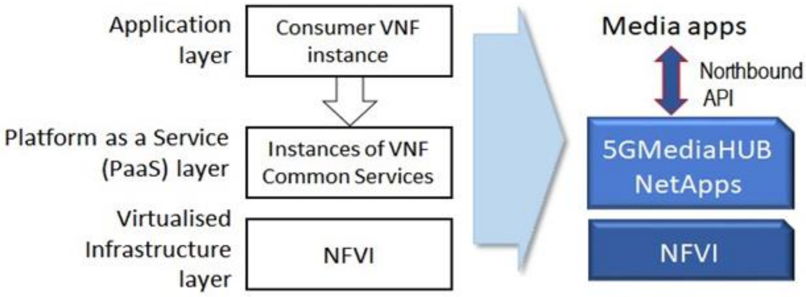

Figure 3: 5GMediaHUB 's alignment with ETSI MEC of evolved NFVI

The PaaS NetApp hosts 5GMediaHUB vertical applications within VMs or Docker containers, offering PaaS capabilities and abstracting SDN & NFV complexities in accordance with the ETSI MEC PaaS extensions. It is leveraging the OpenStack Zun framework. Workload-dependent load balancing, Scale-out and Scale-in of PaaS instances, and multi-domain Network Slicing are handled by the NetApp. The vertical SLA parameters are derived via the 5G Policy Control Function (PCF). Application developers simply provide their applications in the form of VM or container images, as well as their respective metadata (e.g., in Helm Charts). Containerised applications are served via a Container Infrastructure Service Instance (CISI) and a corresponding manager (CISM), i.e., the OpenStack Zun. The NetApp interacts with the latter to deploy the collection of micro services on top of the CISI.

The project will also leverage an umbrella ETSI OSM-based Cross Domain Service Orchestrator (CDSO) to deliver cross-domain orchestration of NetApps in a distributed, multi-tenant, multi-vendor environment. The CDSO is able to guarantee NetApps isolation and cross-domain resource allocation across heterogeneous 5G testbeds via 3GPP-compliant Network Slices, optimising and governing the usage of the underlying infrastructure resources. Specifically, each NetApp is mapped to a 3GPP Network Slice Subnet Instance (NSSI), which is composed of a chain of Network Service (or VNF) instances and is treated as a single entity. This functionality is implemented by the OSM Slicing Manager module, in accordance with the ETSI NFV EVE specifications [26]. Furthermore, the CDSO Slicing Manager will be extended with Deep CNNs, to drive the cognitive management of slice resources that underpin NetApps. To realise the cross-domain orchestration of slices, 5GMediaHUB leverages the OSM Multi-Site Extensions and WIM plugins to configure the underlay network fabric (e.g., via VPN tunnels, VLAN configuration, etc.), implementing support for different infrastructure domains via SDN southbound protocols. Thus, the CDSO has a dual role:

- as a resource orchestrator, it administers, monitors and optimises NFV infrastructure resources and provides an aggregated collection of VIM and NetApps related metrics across geographically distributed NFVIs.
- as a network service orchestrator, it onboards NetApps, which are a composition of VNFs, connected through forwarding graphs, which define service chains. It automates network service lifecycle management, including deployment, configuration, monitoring, updates, termination, and deletion.

In the framework of 5GMediaHUB, at least the following three sets of NetApps will be implemented by expert 5GMediaHUB consortium partners. These include both vertical-specific NetApps within eMBB slices (i.e., Streaming, ImmersiveMedia, MCDN, StreamSelector) as well as vertical-agnostic NetApps (i.e. PaaS orchestration, Web Application Firewall, IDS) that can support use-cases outside the media domain.

5.4 Smart5Grid NetApp

This section introduces the approach taken by Smart5Grid project to the concept of NetApps, conceived as bridges to the gaps between vertical industries and 5G networks.

The NetApps allow developers to concentrate on building the applications that are specific to the vertical domain on which they concentrate their expertise, while leveraging the features and performance that 5G networks offer. NetApps enable them to do so by creating an abstraction of the complexities of the 5G network into a set of requirements, captured formally in a NetApp descriptor.

A NetApp provides a service to the vertical but differs from a plain vertical application in the sense that it contains the necessary access performance requirements that are needed to fulfil the demanding performance constraints that applications in the vertical domain may request. In the case of Smart5Grid, the focus has been put on fulfilling the requirements captured in four use cases that are essential in the energy vertical domain [27], i.e., i) automatic power distribution grid fault detection, ii) remote inspection of automatically delimited working areas at distribution level, iii) millisecond-level precise distribution generation control, and iv) real-time wide-area monitoring in a cross-border scenario.

The Smart5Grid NetApp concept has been built around the Cloud Native paradigm [28][29], ETSI NFV framework [30] and edge computing concept [31]. With this approach, Smart5Grid defines its NetApp [32] as a vertical service comprising subservices modelled as cloud-native VNFs based on OSM Information Model (IM) (which is aligned with ETSI NFV IM **Error! Reference source not found.**) or Pure cloud Native technologies like Helm-charts that are chained together, allowing it to leverage 5G cloud-edge deployments by splitting its functions and indicating the service level objectives (SLOs) required by each of these functions, at network and service levels. It is worth mentioning that, although the NetApp offers a complete, standalone vertical service, this could potentially be an unattended service, or operated through a dashboard/API interface by an operator or even another system, easing its potential integration with legacy applications from the vertical industry. This is open to the developer's design decisions.

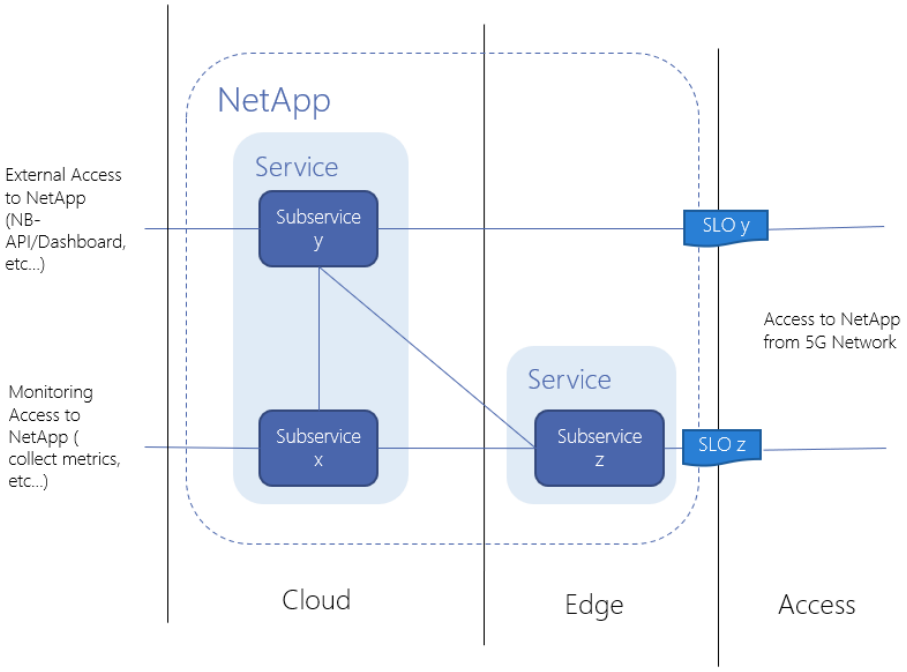

Figure 4: Basic NetApp representation (according to [32])

Splitting the NetApp into decoupled components, enables the Management and Orchestration (M&O) framework to influence traffic routing decisions and decide the correct placement of each function based on the requirements outlined in the NetApp descriptor. Similarly, changes in the load of the infrastructure may trigger a migration of these functions or offloading of the edge resources to guarantee that the requested SLOs are met. Figure 5 describes a scenario where a NetApp with multiple functions that request different SLOs is deployed over a 5G network. The placement decisions of each Service over the NFV infrastructure, as well as the traffic rules over the 5G network are influenced by the defined SLOs. Functions that require intensive usage of computing resources may be placed within the main datacentres, where resources are not constrained, while other latency-sensitive functions are placed at the edge to minimize network delays. The M&O framework manages the end-to-end lifecycle of the NetApp through a *NetApp Controller and MEC Orchestrator* component, whose functions include deployment, migration, termination, set and forward the required traffic routing rules, but also functions like node (re-)provisioning and configuration. This component works tightly with the NFV orchestrator and interacts also with the APIs that the 5G network exposes, potentially acting as an Application Function (AF) as specified in the 5G 3GPP specification.

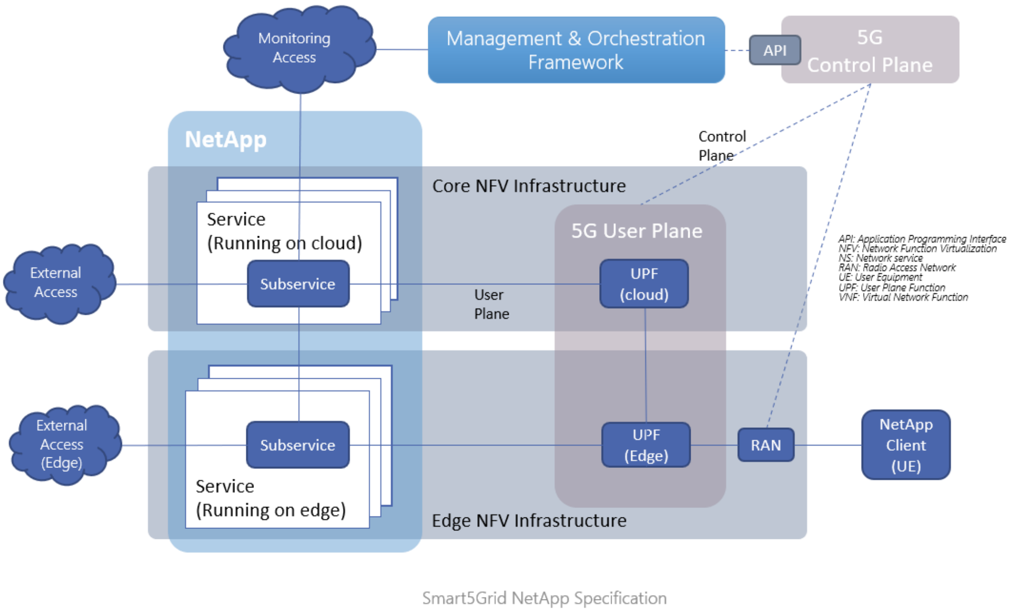

Figure 5: NetApp deployment over a 5G network (according to [32])

To achieve the set goal, Smart5Grid defines a NetApp descriptor that is aligned with ETSI NFV IM and acts like a wrapper of Network Services (NSs). With this approach, VNFs can be reutilized and incorporated into NetApps. The NetApp descriptor maps the scenario described in Figure 5: , specifying one or multiple services as NSs. The Service Access Points (SAPs) of these Network Services are then referenced by the NetApp endpoints. As shown in Figure 6, these endpoints indicate the different characteristics of a SAP, depending on whether it is used as: i) an *Access Endpoint*, in which case and Access policy is defined with the performance requirements to access the relevant function, ii) an *External Endpoint*, utilized to describe an interconnection point where the NetApp service may be available through a dashboard or API, and iii) a *Monitoring Endpoint*, which is used by the NetApp controller to monitor service-specific metrics. These service-specific metrics are defined by the application developer on the NetApp descriptor and allow the NetApp controller to perform actions (e.g., migration, scaling) over the deployed services.

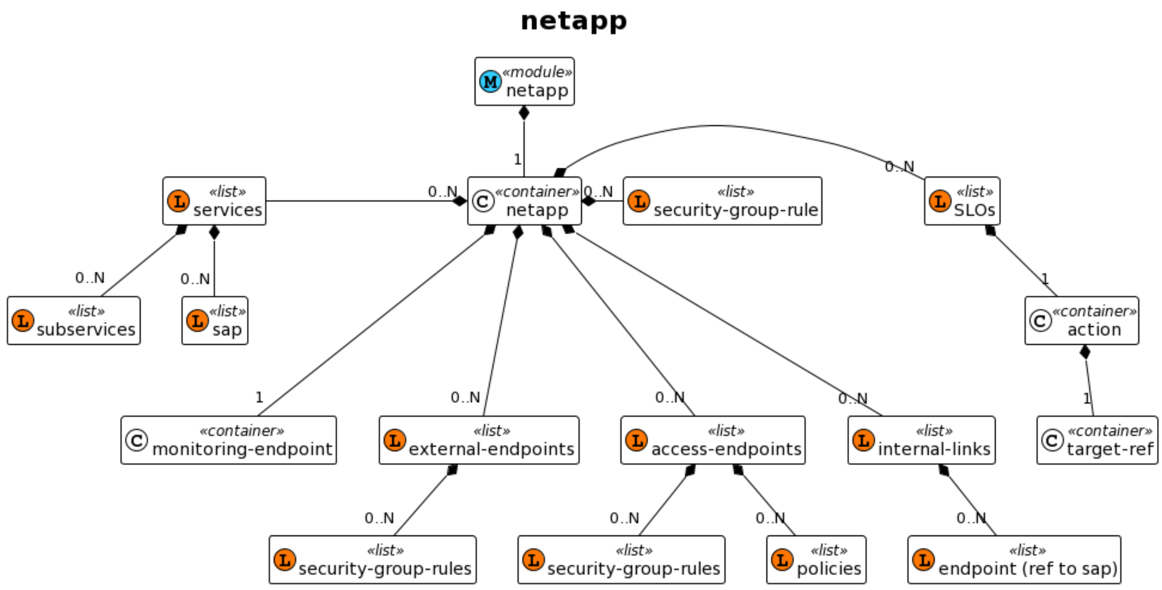

Figure 6: Smart5Grid NetApp Information Model and relation with ETSI NFV IM

5.5 5G INDUCE NetApp approach

The 5G INDUCE NetApps system architecture shown in Figure 7 would enable 1) various business roles to contribute to the NetApps ecosystem, including 5G and beyond network operators, vertical industries, and NetApp developers or service providers; 2) a full-stack NetApp management platform to facilitate the onboarding of NetApps over 5G and beyond networks; 3) advanced NetApps validation for validating the diverse industrial NetApps onboarded; 4) pre-deployment testing over industrial and 5G experimentation infrastructures for end-to-end business services.

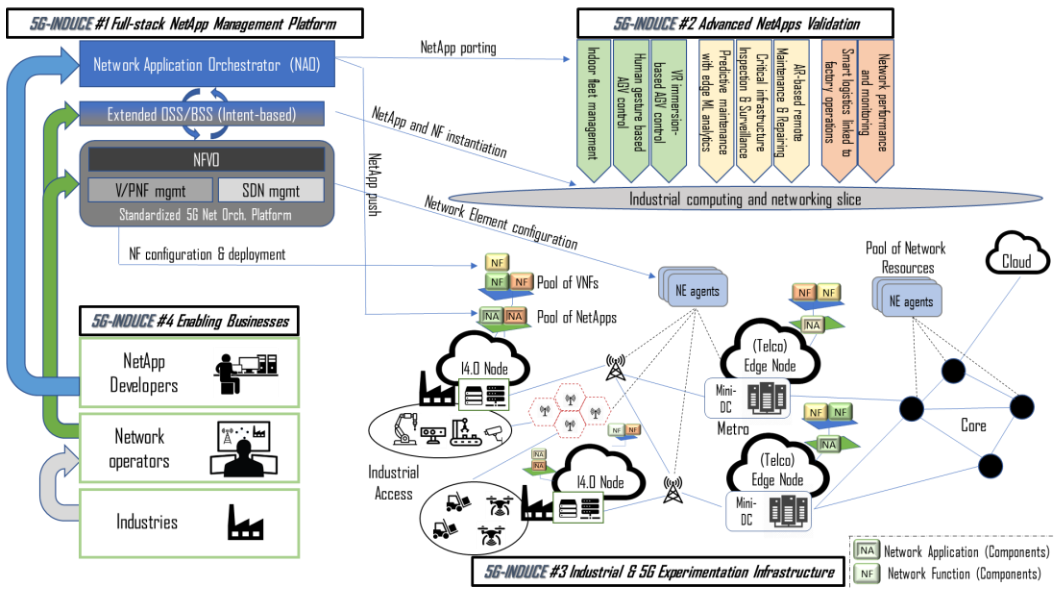

Figure 7: 5G INDUCE NetApp system architecture

In particular, 5G INDUCE promotes the decoupling of application orchestration and network orchestration in the NetApp management platform to separate the concerns between the application and network domains. Hence, a three-layer orchestration approach is proposed including the following three main components.

Network Application Orchestrator (NAO): It interfaces with the vertical industrial NetApp developers to allow them to onboard their NetApps and to assure that their application requirements will be fulfilled during the deployment of the NetApps. A NetApp Application Graph is used per NetApp to specify how the network functions involved in the NetApp are distributed over the various end-to-end network segments (Edges, Core, etc.). The NAO autonomously manages the lifecycle of the NetApp instances during runtime independently of the network functions. From the business perspective it is in line with the operator's role as manager of its own facilities, while it enables the exposure of open NetApp APIs to any developers and service providers through which tailored applications can be designed and deployed. Enable an application-oriented network management and optimisation approach that is in line with the operator's role as manager of its own facilities, while offering the development framework environment to any developer and service provider through which tailor-made applications can be designed and deployed, for the benefit of vertical industries and without any indirect dependency through a cloud provider.

Extended Operations Support System (OSS)/Business support systems (BSS): It provides the interface that translates the NetApp requirements into network connectivity and resource allocation requirements. It acts as a middleware to bridge the gaps between the reluctance of the 5G network operator in exposing any infrastructure details to end users and the demand from vertical industries to require such information for optimised business application deployment. It therefore enables NetApp developers to define and modify the application requirements, whilst exposing the network capabilities at the application level without revealing infrastructure related information.

NFV Orchestration (NFVO): It is based on the standardised ETSI NFV Orchestration (NFVO) framework to manage the lifecycle of the network functions involved in a NetApp and their associated resources distributed over the virtualised network infrastructure.

This three-layer NetApp orchestration scheme thus creates a complete vertical application-oriented 5G orchestration platform that includes the mechanisms of service deployment, network management and network resource orchestration. It enables developers and industries to create and manage respectively the NetApps that are requesting deployment over the network orchestrator, which in turn undertakes the placement of the VNFs (application and network) on the available resources. The NAO provides an API to NetApp developers for NetApp composition. This way NetApp developers can both turn existing unmodified applications into NetApps with minimum effort and develop new NetApps leveraging the rich yet abstract high-level APIs of the NAO. Consequently, the NetApp development model fosters NetApp portability.

5.6 EVOLVED-5G

For a 5G network, there are already standardized interfaces for interaction with verticals (using APIs). The main ones are the Network Exposure Function (NEF) APIs (referring to network core exposure) and also the ETSI MEC APIs (referring to edge exposure capabilities). There are also other interfaces that could be exposed to a vertical, referring, for instance, to the exposure of the business support system – BSS APIs, by providing service orchestration APIs. In the framework of the EVOLVED-5G project [33] APIs that refer to the above-mentioned interfaces are called as ***Native APIs.***

An EVOLVED-5G Network Application (NetApp) [34] is a software piece that composes a service for a vertical by consuming native APIs. For example, a NetApp could consume APIs that provide monitoring events and network slice configuration analysis to compose a service that guarantees Quality of Experience (QoE) for latency-sensitive applications in the manufacturing sector.

For the interaction of NetApps with the network (referring mainly to core network exposure through NEF), two additional aspects shall be considered:

- In 3GPP (SA6) there is ongoing work on developing Vertical Application Enablers (VAE) to facilitate that interaction [35].
- 3GPP has also specified the procedures and the information flows for a common API framework [36][37] (CAPIF) to address applicability, duplication and inconsistency aspects of the 5G native APIs (NEF APIs). Thus, CAPIF [38] (and its evolution as well, i.e., evolved CAPIF -eCAPIF-) shall be considered in the interaction of a NetApp with the mobile network for trust and security reasons [39]. Note that the VAE developments should also be CAPIF compliant.

Considering all the above, a NetApp is a software piece that interacts with the mobile network by consuming exposed native APIs in a standardized and trusted way (i.e., for a 5G network a NetApp should be CAPIF compliant) to compose services for vertical industries. A NetApp provides services to vertical applications either as an integrated part of the vertical application or by exposing additional APIs, which in EVOLVED-5G are referred to as ***business APIs*** (Figure 8).

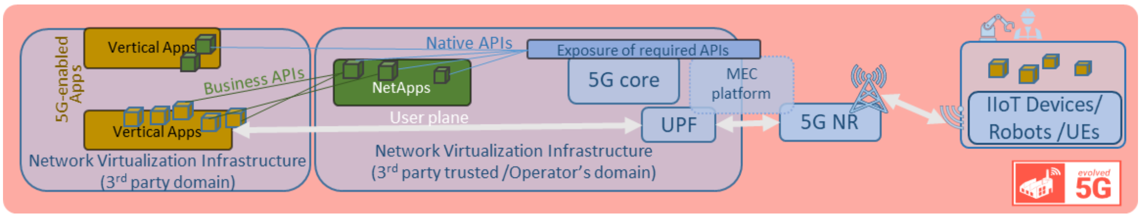

Figure 8: Evolved-5G NetApp concept

In principle, an EVOLVED-5G NetApp refers to the ***control plane***; and it enables network-aware service provisioning to verticals (vertical application providers) by providing network and end user-related information (currently unavailable at the verticals side). This information shall be useful for enriching the capabilities and for enhancing the performance of the vertical application. For instance, that information could be location awareness for a group of end devices or analytics/measurements from the NWDAF. In addition, the interaction that the NetApp enables shall be ***bidirectional***; this implies that a NetApp should realise both the API consumer and provider functions, for both the interactions with the vertical app and the mobile network.

5.7 5G-IANA

5G-IANA aims at providing an open 5G experimentation platform, on top of which third party experimenters in the automotive vertical sector will have the opportunity to develop, deploy and test their services. An Automotive Open Experimental Platform (AOEP) (Figure 9) is specified, including experimentation and orchestration functionalities on top of a computational and communication/transport infrastructure. One of the most relevant components of such architecture is the NetApp Toolkit, whose goal is to simplify the design and onboarding of new automotive services from third-party experimenters.

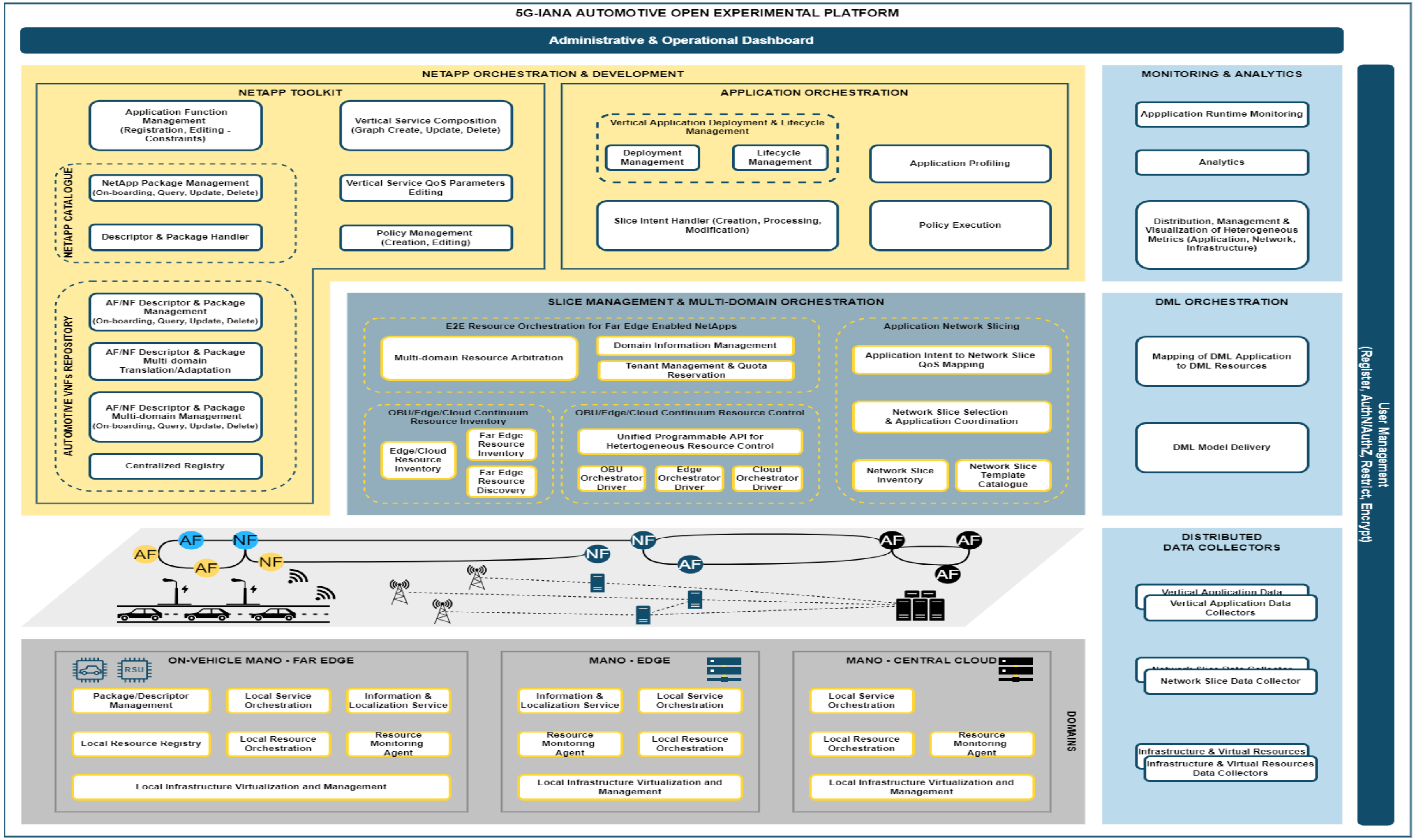

Figure 9 5G-IANA Automotive Open Experimental Platform System Design

The two main layers in 5G-IANA AOEP architecture are:

NetApp Orchestration and Development (NOD) layer: offers the functionalities to design, model, and provision a vertical service/NetApp. In particular, this layer includes a catalogue of available NetApps to be used to compose advanced vertical services. The functionalities are exposed through an enhanced GUI, which enables and facilitates the browsing of the available NetApps along with their on-boarding and composition into composite service-chains.

Slice Management and Multi-domain Orchestration layer: allocates and manages the 5G network slices and the compute resources of the 5G-IANA infrastructure. The AOEP integrates the ability to manage and orchestrate services/NetApps across an extended compute continuum, which comprises multiple interconnected and virtualized domains including centralized, edge and far-edge resources. Indeed, 5G-IANA targets the experimentation of distributed service-chains that can be deployed and orchestrated also making use of on-board units and roadside units' compute resources.

5.7.1 5G-IANA NetApp

In 5G-IANA, a NetApp is defined as a virtual application that can be deployed in a 5G infrastructure and can use 5G services (e.g., connectivity, localization etc.). The NetApp concept extends the typical orchestration-oriented descriptors proposed in ETSI NFV (e.g., Virtual Network Function Descriptors – VNFDs and Network Service Descriptors – NSDs) through the specification of additional information that should facilitate the NetApp re-usage, customization, integration, and provisioning.

Indeed, a NetApp can be composed of one or multiple Application Functions (AFs) or Network Functions (NFs) across different domains, as depicted in Figure 10. On one hand, the AFs correspond to the NetApp components that implement the application logic; on the other hand, NFs implement those functionalities of the NetApp that are related to networking and communication (e.g., ICT long-/short- distance communication functionalities).

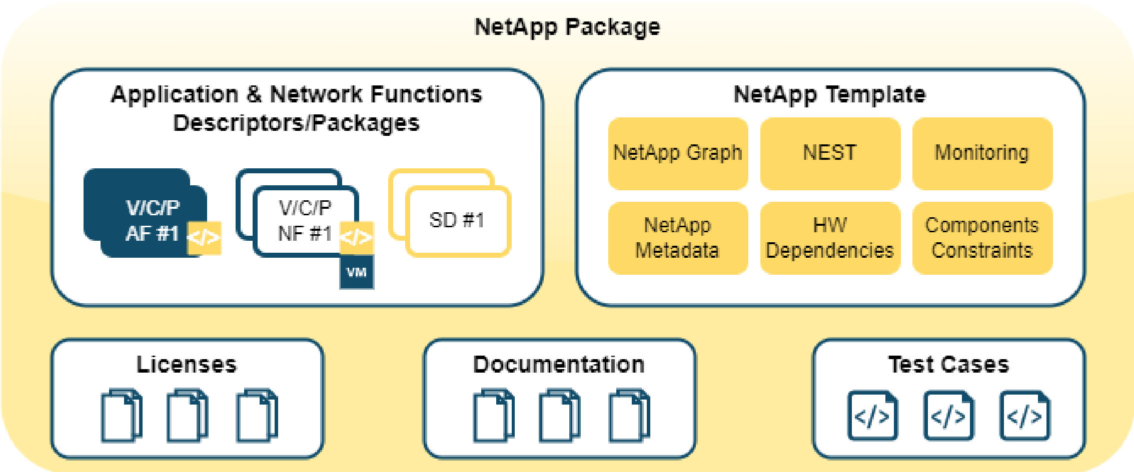

Figure 10 NetApp Package content

To facilitate the NetApp re-usage, the NetApp Package (Figure 10) specified in 5G-IANA includes service-level information such as the specification/documentation of supported interfaces to enable the sharing of the NetApp and its composition with other NetApps to build advanced vertical services, which result in a chain of multiple NetApps.

In addition, the NetApp Package also includes information about:

- high-level QoS parameters that correspond to the main characteristics of the required 5G slice profile and available interfaces for service-chains composition,
- 5G Core services and/or external services (e.g., AI-driven) integrated with the NetApp for optimized orchestration decisions,
- available interfaces that can be used to integrate the NetApp in a more complex service-chain,
- test cases related scripts, target metrics and KPIs that enable the assessment of the NetApp from a functional and performance perspective.

Furthermore, the 5G-IANA project offers a set of NetApp starter-kits that are baseline examples of different categories of NetApps that third parties can re-use to develop their own vertical services/NetApps. The starter-kits will be on-boarded into the NetApp Toolkit catalogue and made accessible by third-party experimenters.

5.8 VITAL-5G API and Interfaces

VITAL-5G project [50] is addressing specific R&D innovations and enhancements to Intent-Based APIs for NetApps: translation of high-level Transport and Logistics (T&L) -oriented intents in to 5G network components/VNF and NetApp deployments and configurations. It provides the functionality extensions to the intent-based APIs in order to accommodate the more complex multi-vertical environment of the VITAL-5G trials Figure 11.

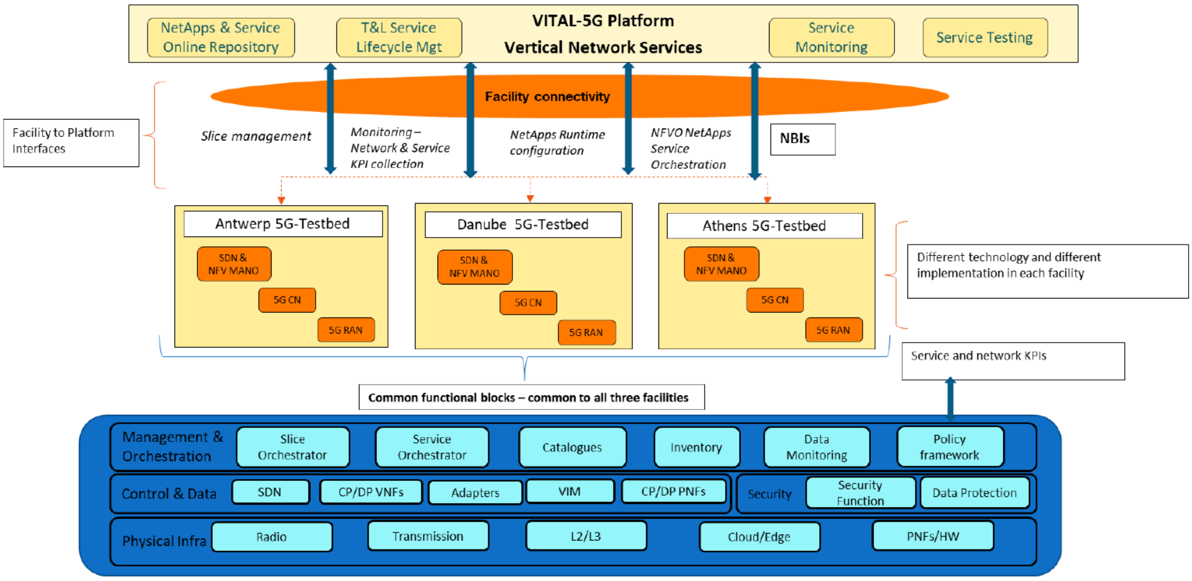

Figure 11: Vital-5G Architecture – functional blocks and interfaces

As described in [51], starting from VITAL-5G Platform Software Architecture, several key services have been identified to be available at the Facility to VITAL-5G Platform, through RESTful based interfaces, between the VITAL-5G Platform and VITAL-5G Testbeds designed as:

- *A-Interface*: the interface providing the facilities basic slice management information, acting like GET function to retrieve the 5G slicing characteristics of the facilities. In this context, the slicing is supposed to be manually configured (based on SST).
- *B-Interface*: the interface collecting the local facilities network and service KPIs, monitoring the facilities related parameters, by reusing the 5G-EVE already existing Kafka Broker. Each VITAL-5G facility is presenting own monitoring tool and PUSH the

data to the Centralized monitoring Platform. the interface exposes the network and the service data from 5G network elements as RAN, 5GC, Transport, Virtualized Infrastructure for service load (network resources, slice).

- *C-Interface*: the interface providing the NetApps experiment LCM, the NetApps Runtime configuration at facility level, facility orchestrator (OSM) related.
- *D-Interface*: the interface providing NetApps and service orchestration, NFVO for services LCM.

It is considered that each VITAL-5G facility has its own technology implementation (RAN, Core, Virtualization, Security) in terms of 5G infrastructure and network implementation, monitoring tools and related service KPIs. The NFVO function is provided through OSM on each testbed, linked to the virtualized infrastructure for NetApps service deployment and to the VITAL-5G Platform through NBIs for NetApps configuration and NetApps service configuration. The C-Interface and D-Interface support the NetApps LCM and onboarding process, interfaces linked to the targeted facilities through the Restful APIs. RESTful standardizes protocols specification for D-Interface is the Os-Ma-nfvo OSM IFA013 SOL005 for CNF/VNF NFVO and for C-Interface is the Ve-Vnfm-em IFA008 SOL002 for NS LCM, for the two main functions: (1) On-board NSD and VNF Package and (2) VNF LCM. The goal beyond is to provide Open APIs to access VITAL-5G platform functionalities in a programmable manner, APIs to trigger lifecycle management actions on the instantiated service and NetApps in a programmable manner, APIs to retrieve monitoring data for service and network KPIs. VITAL-5G is also including the onboarding of Vertical Service Descriptors, the blueprints experiment design, Vertical Service Instantiation and experiment execution via REST APIs on each of the three project's testbed.

The functional architecture of the VITAL-5G system is structured in two main components, the VITAL-5G Portal backend and the Open Online Repository (called also VITAL-5G Catalogue), each of them including a number of functional elements and supported by a set of management backend services. Both Portal backend and Open Online Repository provides north-bound interfaces (NBI) that allow the VITAL-5G users to securely access the authorized VITAL-5G services in a programmable manner, mostly via REST APIs. On top of these interfaces, a unified web-based GUI offers an additional graphical Portal with dedicated tools, designed to simplify the users' manual interaction with the VITAL-5G platform, for both VITAL-5G Portal and Catalogue. On its south-bound interface (SBI), the VITAL-5G Platform interacts with the platforms, services and tools deployed in the VITAL-5G testbeds. This interface is designed with a modular and plugin-based approach that deals with the diversity of capabilities and APIs related to the three testbeds while exposing a uniform layer towards the functional elements of the VITAL-5G platform. The design of the VITAL-5G Platform architecture follows the principles of a Service Based Architecture, with all its functional elements exposing open interfaces to provide access to their services and functionalities. All the consumers of these services can simply implement the client side of such interfaces. In VITAL-5G, some VITAL-5G Platform functional elements provide interfaces which can be consumed by the platform users; the whole set of these interfaces constitutes the VITAL-5G Platform North-bound interface (NBI). All the requests received on the NBI must be authenticated and authorized, on the basis of the user's profile and associated groups. Access to the NBI can be performed in a programmable manner or through the mediation of the VITAL-5G Platform GUI. In the former case, the user will need to compose the message and trigger the request. For example, assuming the adoption of REST APIs, the requests can be issued via REST clients embedded in users' applications or via stand-alone REST clients.

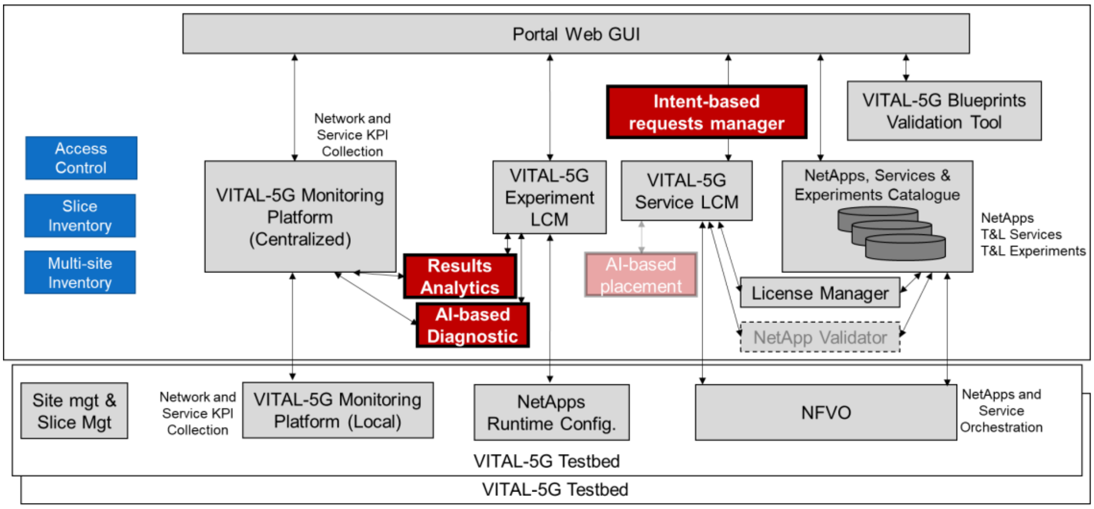

Figure 12: VITAL-5G Platform key software components

The software components depicted in Figure 12 are classified in three main categories:

- The core components of the VITAL-5G Platform, represented in grey, which provide the baseline functionalities to enable the experimental validation of vertical services composed of NetApps in a 5G-enabled infrastructure.
- The management services, represented in blue, which support the core components with transversal functionalities related to the management of the users and their access to the VITAL-5G services, as well as the management of various aspects of the VITAL-5G testbeds, required to properly interact with them.

The advanced functionalities, represented in red, provide added-value services to facilitate and improve the definition of the experiments, the management of the vertical services and the analysis of the experiment results.

The South-bound Interface (SBI) of the VITAL-5G Platform enables its interaction with the VITAL-5G Testbeds, to support the following types of functionalities:

- The selection and/or management and configuration of network slices over the shared 5G infrastructure available in the VITAL-5G testbeds.
- The onboarding, provisioning and management of NetApps and Vertical Services to be deployed as VNFs and NFV Network Services in the virtual computing infrastructures offered by the VITAL-5G Testbeds.
- The collection of monitoring metrics from the 5G infrastructure, addressing both the 5G network performance or load and the usage of computing/storage resources of the virtual computing nodes where the NetApps are running.

An additional interface may be provided as optional, to collect information related to the hardware devices (e.g., IoT sensors, AGVs, video cameras) installed in the T&L facilities at the VITAL-5G testbeds, with all the details required to properly interact with them. At the VITAL-5G Platform level, a unified SBI presents an abstract and common interface for towards the platform components that need to interact with the VITAL-5G testbed.

5.9 Other views on NetApp

5.9.1 Affordable5G view on xApps

Affordable5G aims to provide cost-efficient deployments of private 5G networks, deliver a complete and disaggregated solution through technical innovation across all parts of the 5G network, including radio access, edge, 5GC, and orchestration, and is able to support a variety of applications and use cases.

The system architecture of Affordable5G is introduced in Figure 13, differentiating essentially three main layers, namely (1) Management, Orchestration and Automation Layer, (2) Network Function Layer, and (3) Infrastructure Layer. In this general architecture, the CU connects to a fully virtualised mobile core (5GC) via the N2 and N3 backhaul interfaces (NG-C/NG-U). Core network functions, particularly the User Plane Function (UPF), can be distributed to the edge of the network, bringing them closer to end users. In this way, edge computing can be enabled, steering traffic directly towards the servers where edge applications run.

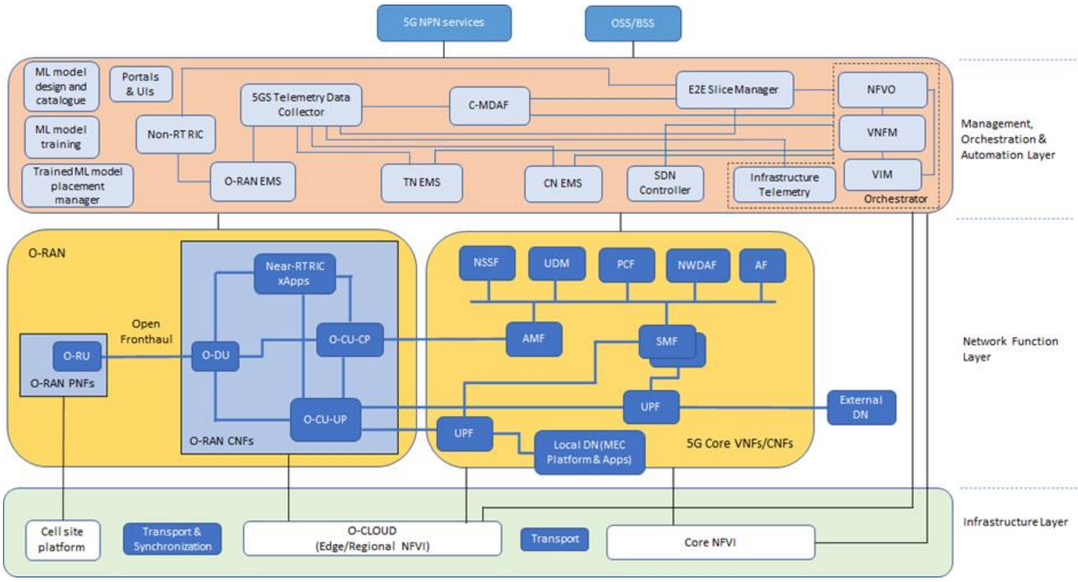

Figure 13: Affordable5G system architecture

Affordable5G solution for 5G RAN follows the specifications provided by the O-RAN Alliance [49] and includes components and open interfaces for the management of the O-RAN network functions and the underlying cloud infrastructure, as well as for the incorporation of intelligent closed-loop automation targeting at cost-efficient network operation. The RAN is connected to a 5G SA core, which quickly brings on the field the latest innovations from the newest 3GPP technical specification releases, including network exposure and extensions for multiple PDU session types that are exploited in the new 5G Quality of Service (QoS) architecture.

An O-RAN Near-Real Time (RT) Radio Intelligent Controller (RIC) is connected to the underlying nodes through the E2 O-RAN interface (divided into the Application Protocol (E2AP) and the Service Model (E2SM)). The E2 interface connects the O-RAN Near-RT RIC to the underlying E2 nodes, enabling the xApps loaded in the RIC to intelligently control the RAN functions as indicated in the Figure 14.

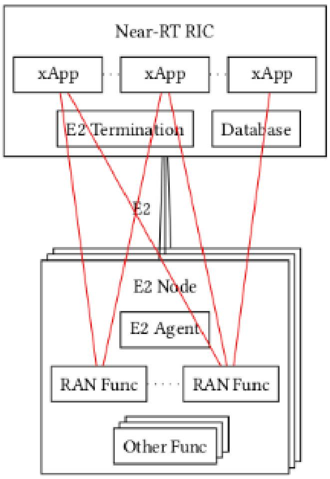

Figure 14: O-RAN Near-RT RIC, E2 interfaces, and xApps

To facilitate network automation towards zero-touch network provisioning, the Affordable5G solution includes building blocks supporting network and management data analytics services, recently standardized by 3GPP, as well as components for AI/ML-based O-RAN optimization while executing vertical 5G services. In addition, to address the diverse requirements of different types of 5G services, the system includes a network slicing component, which can exploit AI/ML and provision end-to-end slices in the compute, network, and access network domains. AI/ML models (from Tensorflow ecosystem) are executed in the O-RAN Near-RT RIC declaring and employing the xAPP API framework as mechanism to open 5G radio network functionalities. Within O-RAN, discussions are still ongoing to standardize the APIs provided by the Near-RT RIC towards xApps.

The required resource and service orchestration in Affordable5G is undertaken by an end-to-end solution operating on top of 5G infrastructures, composed of heterogeneous components like virtual network functions (VNFs), edge resources and hardware devices. The orchestration solution (SMO/MANO) is aligned with the latest O-RAN specifications and compatible with the relevant interface for managing the edge-cloud infrastructures.

5.9.2 DAEMON view on NetApp

Fundamental to the optimal operation of the softwarized, cloudified and atomized network infrastructure will be the Network Intelligence (NI) responsible for managing the composite mosaic of network functions and associated resources in presence of a surging mass of services, tenants, and slices. Present trends in NI for next-generation network orchestration promoted by major standardization bodies pivot on the notion of closed-loop AI. According to this paradigm, the NI instances deployed at centralized orchestrators and controllers work in closed control loops: abiding by the learning principles of modern AI, they record the context of management decisions, collect observations about the quality of such decisions via continuing monitoring, and then use the feedback to improve future choices. The current vision for closed-loop NI contemplates instances located centrally in the control plane that interact with VNFs deployed in the data plane. This model requires that network state information be exposed from different VNFs and transported to a central entity, where they are processed by the pertinent AI algorithms; decisions are then travel back across the network to take effects.

While with current standardization efforts, we recognize that the architecture still yields the following two major limitations. First, there is a risk that the latency in data transfer and decision communication ensuing from a strongly centralized closed-loop model hinders the effectiveness of NI and limit its application in several critical network management scenarios. Second, current architectural models do not foresee any interaction among NI instances, despite the fact the actions they take often yield reciprocal impact. Therefore, for NI to operate at its best, it is critical that NI instances can cooperate to ensure end-to-end synchronization, convergence, and global optimality of the zero-touch network management process.

To overcome the limits of control plane-centric closed-loop approaches, we posit a new **NI-native architecture** that enables a more systematic integration of NI as illustrated in Figure 15, in which three different levels of NI operation timescales are identified (i.e., NI at orchestrators, non-real-time controllers, and near-real-time controllers) and the **NI orchestration layer** introduces feedback loops across NI instances deployed throughout the network, including the new ones implemented at VNF level. Such NI orchestration layer is responsible for supervising intelligence in the network, ensuring the ideal functioning of each closed-loop NI instance, and overseeing interactions across closed loops that run NI at different timescales.

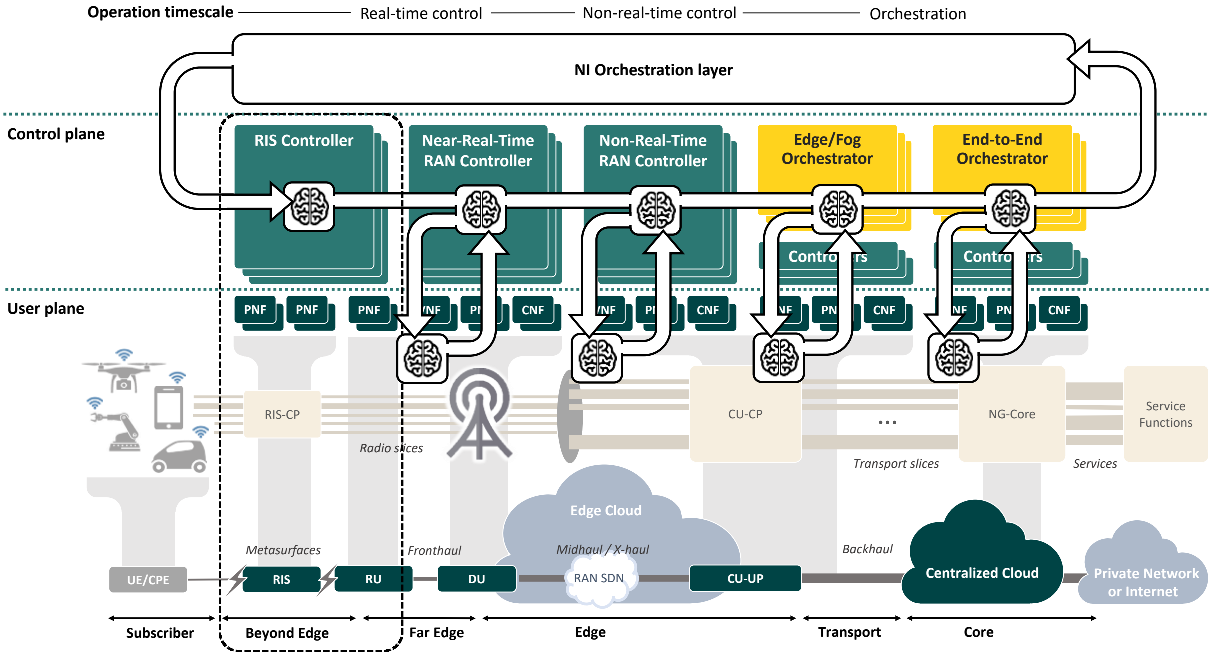

Figure 15: Concept of the DAEMON NI-native architecture

Based on the DAEMON NI-native architecture, eight different use cases are identified in [40] across different timescales over respective domain(s). These use cases aim to exploit "**Network Intelligence-as-a-Service**" to vertical 3rd parties. Such exploitation is of concern by allowing vertical services to be included in the network operation through specific APIs used to (1) manage the kind of provided NI, and (2) ensure that the resources are provided to them. By doing so, new NI instances can provide intelligence directly to the vertical service (e.g., video analytics directly in the user plane) and allow the efficient and secure resource provisioning through the usage of solutions based on e.g., distributed ledger platform. In particular, it is aligned with the scope of NetApp to inject verticals services' components to complete an end-to-end application process with the requested NI among concerned domain(s).

Consider a video streaming service provider as an example, it can exploit NetApp(s) for richer interfaces compared to over-the-top (OTT) operations by subscribing to continuous monitoring from the underlying network domain(s) to monitor the mapped Quality of experience (QoE) metrics available at the application layer. The service provider can also subscribe via developed NetApp to dynamic SLA events from the network operator BSS to be aware different subscription options. Therefore, it may offer the service using different user packages (e.g., gold, silver, or bronze plans) with different costs and QoE improvements. Finally, the NetApp can also offer NI in terms of different **decision-making models** according to the requests from the service provides. As depicted in Figure 16, based on the collected data characteristics (i.e., data sampling rate, data richness, and data distribution) and the decision enforcement limitations (i.e., delay, granularity, and availability), several decision-making models are populated and can be selected according to service-specific time constraints. Finally, a class of NI is selected and exposed to be subscribed by service provider posing a trade-off among control time scale, optimality, and robustness. These trade-offs will be address by the NI orchestration layer within the architecture Figure 15 to offer different levels of automation.

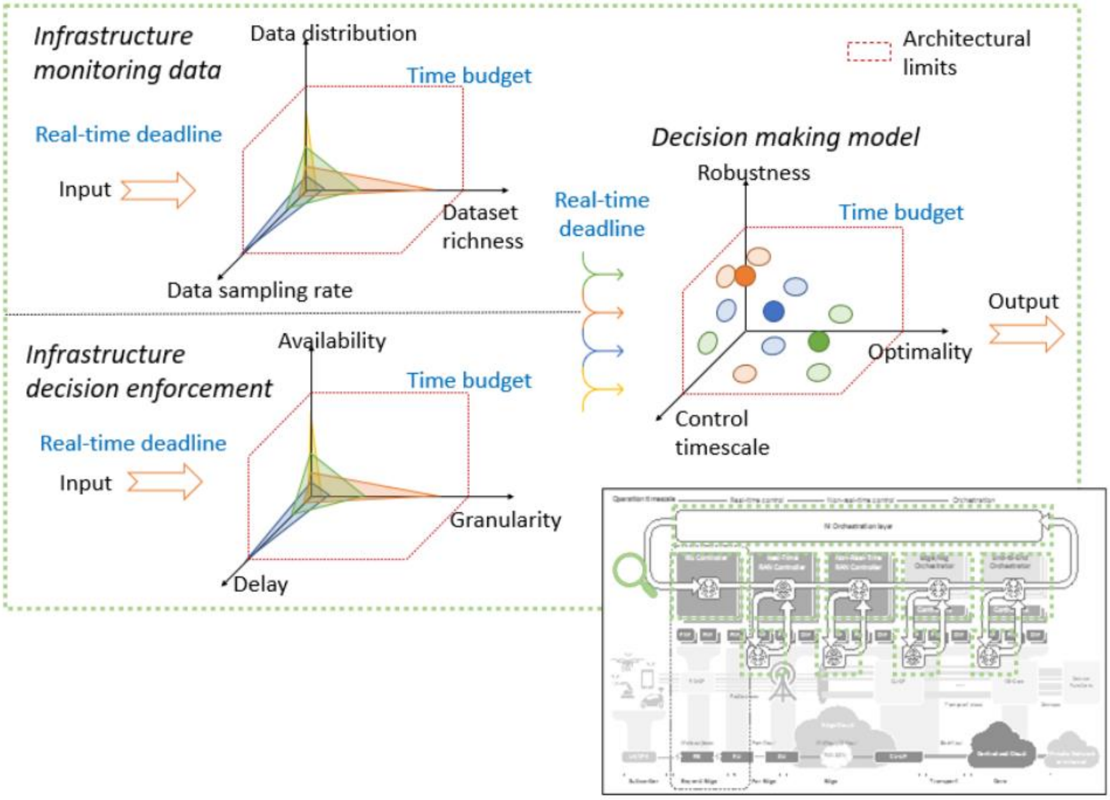

Figure 16: Network Intelligence degrees of freedom, input-output relationship, and real-time constraints subject to infrastructure observability and controllability

5.9.3 TeraFlow view on NetApp

The cloud-native software architecture of TeraFlow is based on container-based services (containers are a lightweight virtualization technique), which are deployed as microservices and managed on elastic infrastructure through agile DevOps processes and continuous delivery workflows. These micro-services are software development techniques that structure an application as a collection of interconnected and related services. In a micro-services architecture, services are simple and detailed, and the protocols are lightweight.

Figure 17 provides an overview of the proposed TeraFlow OS architecture. The TeraFlow OS is a cloud native SDN controller that is composed of multiple micro-services. Microservices interact with each other using a common integration fabric. Moreover, in the context of B5G networks, the TeraFlow OS is able to interact with other network elements, such as NFV and MEC orchestrators, as well as OSS/BSS. The TeraFlow OS controls and manages the underlying network infrastructure, including transport network elements (optical and microwave links), IP routers, as well as compute nodes at edge or public cloud infrastructures.

The TeraFlow OS cloud-native architecture provides multiple benefits which have already been clearly demonstrated in other cloud computing applications. The most important benefit is application resiliency, where microservices are monitored and restarted in case of misbehaviour. Another benefit is application scalability, which accommodates an increasing number of requests (i.e., load), with the deployment of new microservice instances when required. In order to detail the different TeraFlow OS functionalities (each one based on a single or multiple micro-service(s)), they have been divided into two categories: core and NetApps functionalities. This classification is based on the degree of inter-relationship of these micro-services, as explained below.

TeraFlow core micro-services are tightly inter-related and collaborate with each other in order to provide a complete smart connectivity service. Once a transport network slice request is received, the slice manager translates this request to the service component. Moreover, the slice request is recorded by the Distributed Ledger Technology (DLT) component in the blockchain. The service component computes the necessary connectivity services and requests the necessary network element configuration (e.g., NETCONF, P4, OpenFlow), or interacts with underlying SDN controllers through the device management component. These configurations are also recorded using the distributed ledger component. Policies per flow are computed in Traffic Engineering (TE) component and verified, and network elements are monitored for anomalous behaviour in automation and policy management components. The context manager is responsible for handling the distributed non-relational database that contains all necessary information (including slice and/or flow requests, network topology, and network elements' configuration).

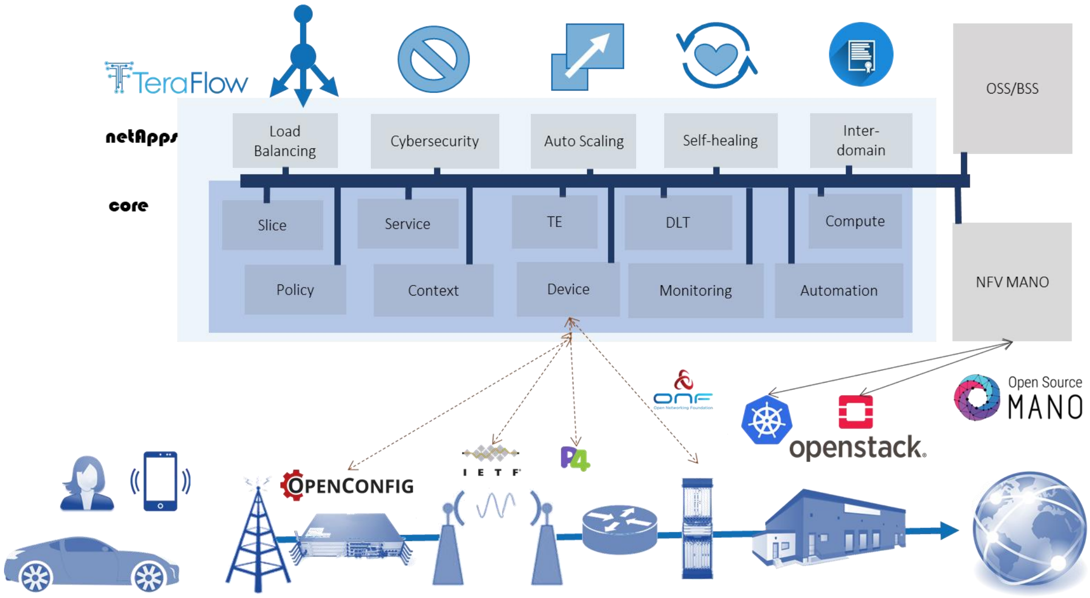

Figure 17: TeraFlow architecture

TeraFlow NetApps consume TeraFlow core micro-services. The TeraFlow NetApps provide the necessary carrier-grade features with a dedicated focus on: load-balancing, cybersecurity, auto-scaling, self-healing, and inter-domain smart connectivity services. Load-balancing allows the distribution of flow and slice requests among the micro-services component replicas. The cybersecurity component provides AI/ML-based mechanisms to detect network intrusions and harmful connections, and it provides countermeasures to security incidents. Moreover, the cybersecurity component will be able to protect itself against adversarial attacks that try to spoof the detector's ML components. The auto-scaling component focuses on the autonomous replication of micro-services to support high numbers of incoming requests. The self-healing component monitors micro-services and per-flow status in order to apply healing mechanisms (e.g., component restart, flow redirection) both from a control and a data plane perspective. Finally, the Inter-Domain micro-service allows the interaction of a TeraFlow OS instance with peer TeraFlow OS instances which manage different network domains.

5.9.4 5G VICTORI – 5G-VIOS view on NetApp

As described in [41], the 5G-VICTORI solution aims at supporting both ICT and vertical services through the deployment of 5G and vertical NFs. This is achieved by taking advantage of the capabilities that the overall 5G architecture offers in support of the vertical service requirements. The 5G-VICTORI architectural enabler that supports this vision is the creation of repositories comprising programmable NFs, both 5G and Vertical service specific (i.e., synchronization, positioning, signaling, etc.), as well as vertical industry specific Application Functions (AFs). Combinations of the functional elements of these repositories that may be associated with different facilities and geographical locations will form one common repository through which they can be accessed and deployed for service provisioning at any location of the 5G-VICTORI infrastructure.

To make vertical applications deployable over the 5G-VICTORI platform, suitable application packaging is provided through the development of AFs and Network Services (NS) descriptors. These descriptors facilitate applications to be deployed in a single domain/site but will be also extended to enable platform NSs. This functionality is supported through 5G-VIOS, the inter-domain orchestrator developed in the framework of the project and described in detail in deliverable D2.6 [41]. In summary, 5G-VIOS enables management of slices, resources, and orchestration of services across different 5G sites/platforms. It provides NS deployment across different facilities, inter-site service composition and on-boarding, E2E slice monitoring and management for the deployed E2E services and facilitates end-users (facility administrators and vertical users) to interact with the 5G-VICTORI infrastructure and services. Facility administrators are able to onboard their facilities onto 5G-VIOS and expose the capabilities they offer through a common service repository that can also host AFs developed by the external Vertical SPs, which can then be used to deploy new NS to other facilities. In addition, 5G-VIOS is responsible to automate the Life-Cycle Management (LCM) of these inter-domain NSs.

The 5G-VICTORI platform also acts as a single cloud-based contact point for multi-national system developer teams and integrators. This eases the development process and reduces time-to-market as APIs and Service Development Kits (SDKs) are offered using a programming language understandable to cloud-service developers. In addition to cross platform service exposure and Open API capabilities, the 5G-VICTORI platform also provides tools to manage services throughout their entire lifecycle. To achieve this, the platform relies on a set of dedicated components that have been developed to perform a set of actions, including monitoring and configuration of the underlying infrastructure as well as maintenance of the managed servicers.

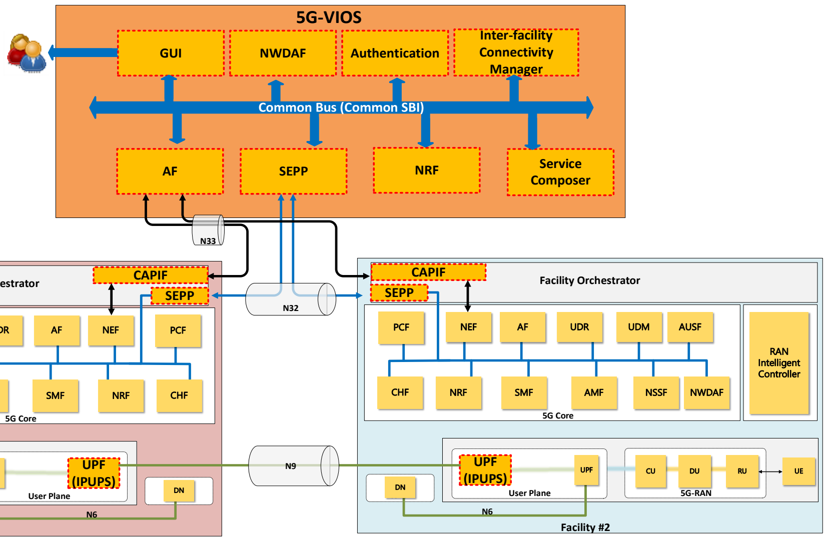

Figure 18: 5G VICTORI multi-domain reference architecture

5G-VIOS is responsible to automate the LCM of these inter-domain NSs. The 5G-VIOS deployed at the edge of each facility has appropriate interfacing mechanisms supporting the connectivity with 5G-VIOS and the remote 5G facilities. The Inter-edge Connectivity Manager (ICM) is responsible to establish secure connections between different facilities. Dynamic Multipoint VPN (DMVPN) is used to enable this connectivity on top of which appropriate interfaces are overlaid based on exposed functions, i.e., N32 for the control messages, N9/N6 tunnels for UPF (IPUPS) -UPF(IPUPS)/ UPF-DN connectivity, N33 for the exposure of the capabilities of each facility through NEF to the AF hosted in VIOS. Furthermore, 5G-VIOS offers a centralised data monitoring and analytics platform, extending the Network Data Analytics Function (NWDAF), with data collected across facilities from different components, including the 5GC NWDAF, MANO, and application specific monitoring data. AI and ML algorithms are employed to analyse and generate performance profiles for NSs used to optimize the deployment of such services across the facilities. Finally, a common exposure function provides access of the AFs available to the facilities. Information is shared per facility through the local orchestrators that interact with the local 5GC systems and expose the necessary information to 5G-VIOS.

The key building blocks of the 5G-VIOS interfacing the individual facilities include:

- The edge proxy providing interfaces for Security Edge Protection Proxy (SEPP) and CAPIF. SEPP is part of the roaming security architecture enabling 5GC signalling traffic to be transferred across remotely located 5G facilities. CAPIF is used to expose functionalities of each facility through NEF to the common AF repository hosted in 5G-VIOS. To implement SEPP and CAPIF an authentication mechanism is required that enables effective filtering of traffic coming from the interconnect between different facilities and 5G-VIOS. SEPP to SEPP and NEF to AF through CAPIF is implemented through a new application layer security solution on the N32 and N33 interfaces, respectively, providing protection of sensitive data attributes while still allowing mediation services throughout the interconnect. 5G-VIOS edge proxy and API gateway implement basic SEPP and CAPIF functionalities and extending it to communicate with the NFVO and other services running at each facility.
- An Network Repository Function (NRF) providing a single record of all NFs available in each facility, together with the profile of each and the services they support. It supports the following functions:
    - Maintains the profiles of the available NF instances and their supported services in the 5GCN.
    - Allows consumer NF instances to discover other providers NF instances in the 5GCN.
    - Allows NF instances to track the status of other NF instances.

The common repository component implemented in 5G-VIOS, is able to interact (upon approval by facility owners) with individual NRFs and thus facilitate inter-domain NSs. It registers itself with local NRFs as another NF allowing it to discover available NFs instances on each facility. In addition, it maintains a repository of NS descriptors advertised by the NFVO at each facility.

- A network data analytics function (NDWAF) colleting high and low level statistics and aggregating monitoring data across the different facilities from individual sub-systems including 5GC and MANO. Then through AI/ML algorithms implemented generating performance profiles for individual NSs that are used during the LCM of those services.
- The NEF providing the tools to vertical application developers to securely and developer-friendly expose the services and capabilities provided by 3GPP NFs (3GPP TS 29.522). This access is provided by a set of northbound RESTful APIs from the network domain to both internal (i.e., within the network operator’s trust domain) and external applications. This functionality is expanded to multi-domains with the aid of the Service Broker (SBR) components in 5G-VIOS. SBR enables different edge facilities to expose

their capabilities and services in a common infrastructure (5G-VIOS) that can be used to instantiate inter-domain services in collaboration with the service composer and other 5G-VIOS components. Particularly, as part of the experiment LCM, which relates to a network slice LCM, Network Slice Management Function (NSMF) and Network Slice Subnet Management Function (NSSMF) can be exposed in order to perform the appropriate operations.

6 NetApp classification

By analysing the different approaches considered by the different projects and their use-cases described in section 5, it appears different approaches.

Considering the level of interaction and trust, the NetApps could be classified following their architectural position:

- NetApp as part of 5G/B5G System
- NetApp adjacent to (after) the 5G/B5G System,
  - still in the CSP domain, typically as part of a Network Operator network slice
  - in interconnected (CSP / Service Provider) Domain, typically as part of a tenant / application slice

Following the level of NetApp integration, it results three categories, as depicted in Figure 19:

- **aaS Model**: it is the model where the vertical application consumes the NetApp as a service. The API is offered by a (Mobile / Communication) Service Provider (CSP) or a Vertical (Sector) specific Digital SP (DSP). The vertical application deployed in the vertical service provider domain. It connects with the 3GPP network systems in one or more PLMN operator domain.
- **Hybrid**: it is the model where the vertical instantiates a part of its Vertical Application in the operator domain like the EDGE. The other part remains in the vertical domain. A similar approach has been followed in TS 23.286 related to the deployment of V2X server.
- **Coupled/delegated**: it is the model where the vertical delegates its application (in short app) to the operator. The NetApp will be composed and managed by the CSP. This approach is the one followed in the platforms like 5G-EVE.

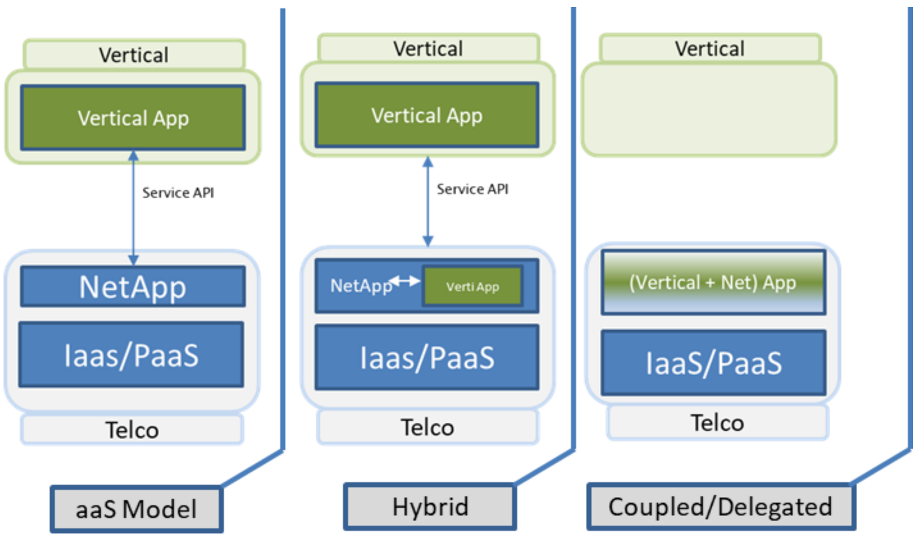

Figure 19: NetApp classification

Following the use-case, one of these three options is implemented. A complete survey has been circulated among the projects to collect their views. Table 1 summarizes the different approaches selected to design the Network Application according to the use-case.

More than 70% of the implementations follow the aaS Model, 20% coupled and the rest, 7%, the hybrid mode.

Table 1: NetApp classification per use-case

			Category		
Project Name	**Vertical Type**	**NetApp**	**aaS Model**	**Hybrid**	**Coupled**
5GASP	**Automotive**	Virtual On-Board Unit provisioning NetApp		x	
		Virtual RoadSide Unit provisioning NetApp		x	
		ITS station NetApp			x
		Multi-domain Migration NetApp			x
		Vehicle-to-Cloud Real-Time Communication (V2C R2C)		x	
		Remote Human Driving NetApp - Teleoperation for assisting vehicles in complex situations		x	
		Efficient MEC handover NetApp			x
		Vehicle Route Optimizer NetApp	x		
	PPDR	PrivacyAnalyzer NetApp	x		
		5G Isolated Operation for Public Safety NetApp (5G IOPS NetApp)	x		
		Fire detection and ground assistance using drones (FIDEGAD)			x
5GMEDIAHUB	**Media**	Streaming NetApp	x		
		Immersive Media NetApp	x		
		Multi CDN NetApp	x		
		Stream Selector NetApp	x		
	Vertical Agnostic	PaaS NetApp	x		
		Security NetApp, inlcuding Web Application Firewall NetApp and DPI NetApp	x		
EVOLVED-5G	**Industry/Smart Factories -** Interaction of Employees and Machines pillar	Remote assistance in AR			x
		Digital/physical twin			x
		Chatbot assistant	x		
	Industry/Smart Factories- Factory of the Future operations pillar	Occupational Safety Analysis			x
		Anomaly Detection	x		
		Industrial grade 5G connectivity	x		

		Smart irrigation for agriculture			x
	Industry/Smart Factories- Security guarantees and risk analysis pillar	Traffic Management			x
		ID Management and Access Control	x		
		5G SIEM add on	x		
	Industry/Smart Factories- Production Line Infrastructure pillar	Teleoperation	x		
		Localization	x		
	Agriculture - Operations pillar	Smart irrigation for agriculture	x		x
VITAL5G	**Transport/Logistic**	Indoor robot navigation & coordination with task planning	x		
		AI/ML based vessel/warehouse automated fault detection	x		
		Warehouse/vessel IoT environment technical visualization	x		
		Remote vessel navigation	x		
		Autonomous vessel navigation control	x		
		Navigation speed optimizer	x		
		On board data collection & interfacing for vessels	x		
	Industry	Human-robot collaboration	x		
5G-VICTORI	**Industry (Factory of the Future)**	Digitization of Power Plants	x		
	Media	CDN Services	x		
		Digital Mobility (infotainment)	x		
	Energy	Smart Energy Metering (Low Voltage)	x		
		Smart Energy Metering (High Voltage)	x		
	Transport/Logistic (Rail Transportation Service)	Rail operation non-critical services	x		
		Rail operation critical services	x		
		Communication services for passengers	x		
		Future Digital Mobility	x		
		Immersive Media service for travellers	x		

7 Standard status

In this section, we outline the standard status on the 5G API requirements for services definition and common API framework.

7.1 5G Telco API requirements for services definition

5G system architecture is the new communication service enabling model that leverages service-based interactions between 5GC control plane and the network functions through secured and exposed platform's APIs. In principle, it is based on the Service Based Architecture (SBA) framework concept, creating the modularized services deployment, on-demand networks implementation, fast deployment cycles, dynamic services launch in the network. The main API requirements are focused on the 5GC functions, interaction between components in SBA and on the management and orchestration capabilities of the 5G network. Thus, a Service Based Interface (SBI) represents how a given NF exposes a set of services for 5GC5GC interfaces specified in 3GPP TS 23.501. A sketch of SBA framework in 5G system control plane can be found in Figure 20. Among these NFs, both Network Repository Function (NRF) and Network Exposure Function (NEF) are of concern.

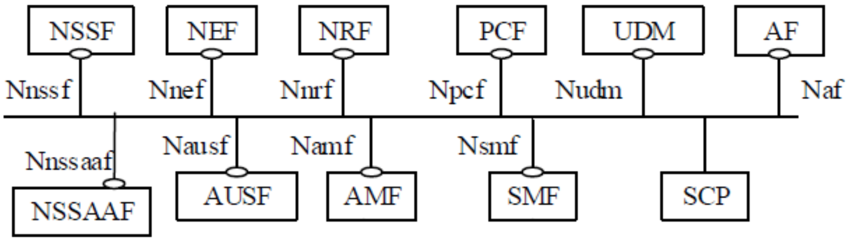

Figure 20: 5G System Control Plane Architecture

The NRF is the entity responsible for selecting the network functions for the PDU session based on services profiles, network states, policies, or other goals, viewed as an evolution of the existing 3GPP DNS systems combined with the selection logics in MME in 4G, integrated with additional intelligence for NF policy selection. Note that the NF Service Framework should include service registration, update and deregistration in order to make the NRF aware of the available NF instances and supported services. This can enable a NF service consumer to discover the NF Service Producer that can provide the expected NF service (with access authorization), through three main services offered by NRF: (1) Nnrf_NFManagement (2) Nnrf_NFDiscovery and (3) Nnrf_AccessToken. A depict of the three main service is in Figure 21, and more services can be found in 3GPP TS 29.510.

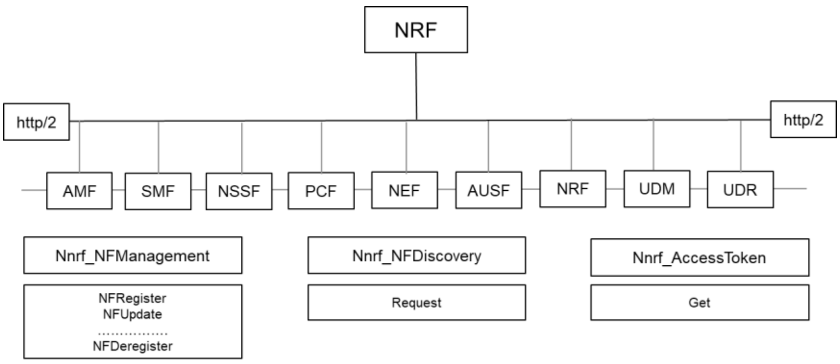

Figure 21: 5GC NRF Service Based Interfaces

The main tasks of NRF are to maintain the NF profiles of available NF instances, enable new NF subscription and registration, support service discovery functions, and interact with every NF in the 5GC. The services offered by NRF to the NF (e.g., the three aforementioned service in Figure 21) are using the open API, which is defined in 3GPP TS 29.510, e.g., nnrf-nfm, and nnrf-disc.. The design details for the SBIs specified by 3GPP includes: (i) API purpose, (ii) URIs of resources, (iii) HTTPs supported methods and supported representation (e.g., JSON), and (iv) Request/response body schema. A depict of 5G NRF service APIs can be found in Figure 22.

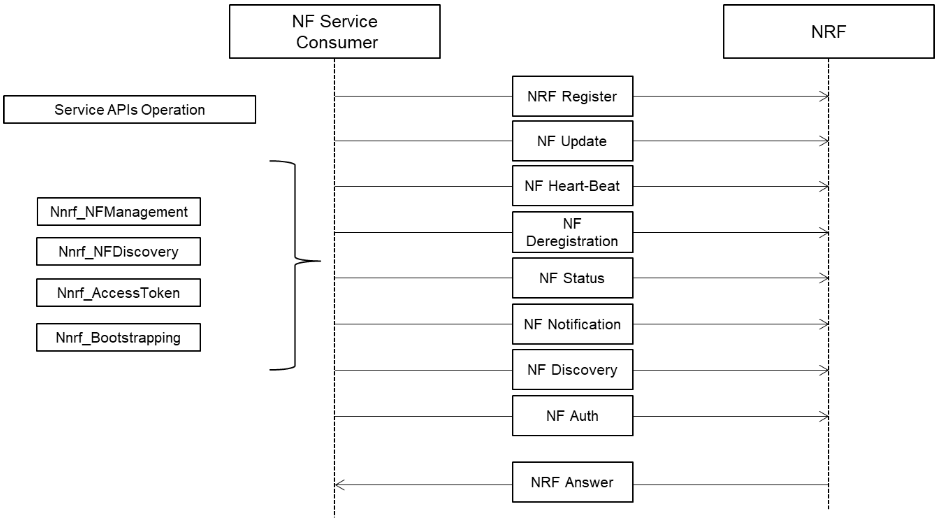

Figure 22: 5G NRF Services APIs

The NEF is the entity responsible for securely exposing different network capabilities, services and functions provided by 3GPP NF to the 5G customers (e.g., 3rd party, Application Function [AF], Edge Apps). And it leverages the exposed APIs to expose the required network information, as the architecture depicted in Figure 24.

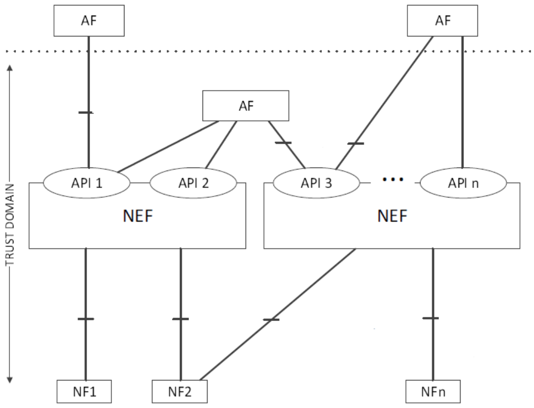

Figure 23: 5GS 3GPP Architecture for Network Exposure

NEF comprises two main exposure function services: NEF northbound APIs and NEFNEF southbound services. The NEF Northbound Interface is the RESTful API interface between the NEF and AF that supporting several procedures, such as monitoring, triggering, provisioning, traffic influence and AF session QoS, corresponding to the supported NEF servicers, i.e., Nnef_Interfaces between NEF and AF, as described in TS 23.502 and represented in Figure 24. Moreover, it supports functionalities related to secured network capabilities exposure, AF to 3GPP network authentication, and authorization information. The security is offered by using secured communication between NEF and AF over the NEF northbound Interface, accessing the SCEF authorized APIs (OAuth2 protocol).

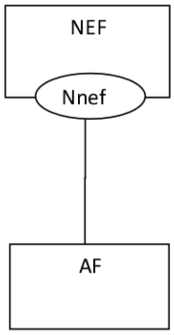

Figure 24: NEF Services SBI representation

In addition, NEF Northbound APIs supports the common API framework (will be tailored in section 7.2) and is based on the service-based interaction, as presented in Figure 25. It relies on a series of services operation activities between NEF and the consumers in place, such as Service Subscribe, Service Unsubscribe, Notify, Update through the REST APIs.

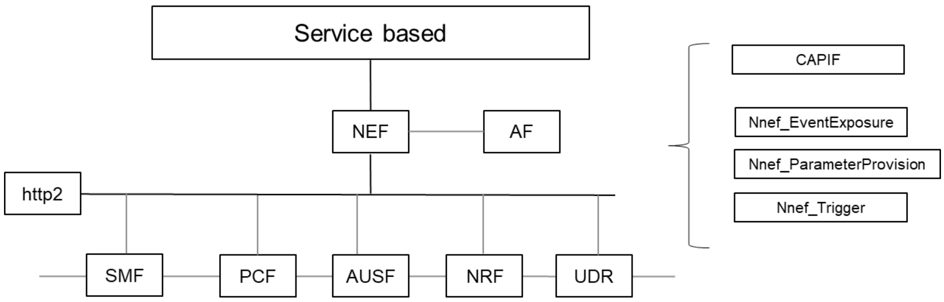

Figure 25: NEF Services Interaction

7.2 Common API Framework

The Common API Framework (CAPIF) [43] is a set of specifications from 3GPP to standardize some common capabilities exposed by 5GC northbound APIs. Its objective is to provide a unified and standardized northbound API framework across several 3GPP functions that allows for the utilization of 5G capabilities exposed on 5G networks. CAPIF specification [43] was first published in 3GPP Release 15 and has been updated with several enhancements in subsequent Releases 16, 17, and onward. Moreover, the CAPIF framework has been integrated within the northbound APIs developed by 3GPP SA2 (SCEF/NEF) and 3GPP SA4 (xMB).

3GPP has specified the procedures and the information flows for CAPIF to address applicability, duplication, and inconsistency aspects of 5G northbound service APIs. CAPIF provides a single and harmonized approach for API development and a framework to host APIs of PLMN, allowing third parties to leverage the standardized access to the exposed 5GC functionality. 3GPP TS 22.261 [44] states the requirements for the related API calls, and 3GPP TS 23.434 [45] defines the required interfaces under the term Service Enabler Architecture Layer (SEAL). The implementation of SEAL in an Application Function (AF) entity interface with NEF and enables network programmability features. The CAPIF architecture is specified in 3GPP TS 23.222 [46], addressing key features provided: on-board and off-board API invokers (i.e., vertical applications), registration and release of APIs to be exposed, 5GC API discovery, measures for framework security such as authentication of API invokers, and support for distributed deployments on third party domains and for the federation of CAPIF.

The advantages of using a standardized common API framework are numerous. First, it provides a unified and standardized access to 5G exposed capabilities, sparing verticals to deal with different and heterogeneous 5GC northbound frameworks. In this way, vertical applications do not require profound changes to their software to utilize 5G capabilities, maximizing solution reusability and facilitating 5G programmability. Furthermore, CAPIF set the grounds for the SA6 request of a middleware layer between 5GC and applications that will simplify the implementation and deployment of vertical systems at a large scale, as well as the creation of a common service platform for verticals to use 5G systems, incorporating an abstraction layer hiding the underlying heterogeneity and providing a unified/standardized access to 5G functionality. This is the same request that triggered the development of Vertical Application Enablers (VAE) by 3GPP SA6.

The CAPIF architecture is composed of several entities or blocks, as shown in the architectural model of Figure 26**Error! Reference source not found.**. Some brief introductions are described as follows:

- API Invoker refers to the vertical application consumer of the 5GC service APIs utilizing CAPIF. The API Invoker provides the CCF with the required information for authentication, discovers APIs through this orchestrator, and invokes the available service APIs. A NetApp is a 5G Native API invoker.
- CAPIF Core Function (CCF) can be seen as a central repository for all the APIs from PLMN and third parties. 3GPP has defined CFF as the entity that governs the relationship between API Invokers and AEFs. This entity acts as an orchestrator that manages the interaction between service consumers (vertical applications) and service providers (e.g., NEF, SEAL). The main responsibilities of CCF are authentication of the API invoker, authorization of the API invoker to access the available service APIs and monitoring the service API invocations, and aspects related to logging, on-boarding and charging.
- Three functions are within the API provider domain
  - API Exposure Function (AEF) is responsible for exposing the service APIs. The AEF wraps around the 3GPP functions to enable APIs to be exposed. If API Invokers are authorized by the CCF, AEF will validate the authorization and subsequently provide the direct communication entry points to the service APIs. AEF may also register the invocations in log files. In sum, AEF is the entity that exposes APIs to be consumed by other entities. AEF is typically associated with an APF that publishes API information in CFF and an AMF that controls the access to the exposed APIs **Error! Reference source not found.**.
  - API Publishing Function (APF) is responsible for the publication of the service APIs to CCF in order to enable the discovery capability to the API Invokers.
  - API Management Function (AMF) supplies the API provider domain with administrative capabilities (e.g., auditory of the service API invocation logs from the CCF, on-boarding/off-boarding new API invokers and monitoring service APIs status).

Moreover, several architectural deployment models are considered by 3GPP. First, two models exist between CCF and API provider domain functions:

- Centralized model where the CCF and API Provider domain functions are co-located
- Distributed model where CCF and API Provider domain functions are not co-located, and they are interacting through CAPIF-3/4/5 interfaces. Therefore, multiple CCFs can be deployed in the same PLMN trust domain.

Second, the API invokers can be co-located within the same PLMN trust domain or be external to the PLMN operator network where the CAPIF resides. As mentioned before, NetApps are API

Invokers and thus they can be deployed inside the PLMN trust domain of the operator or outside of the PLMN trust domain – typically, a 3rd party trust domain that can be a public or private cloud environment such as Azure, AWS or private Kubernetes cluster. These NetApps will consume APIs exposed by AEFs – in particular, the ones exposed by 5GC such as NEF or SCEF. Also, NetApps can become AEF entities if they are using CFF to expose those APIs.

Finally, 3GPP TS 29.222 [47] defines a set of reference points (interfaces), with associated management APIs, for enabling the interaction between NetApps (5G Native API Invokers) and AEFs. Those interfaces go from CAPIF-1 to CAPIF-5 for NetApps inside the PLMN trusted domain, and from CAPIF-1e to CAPIF-5e for NetApps outside the PLMN trusted domain.

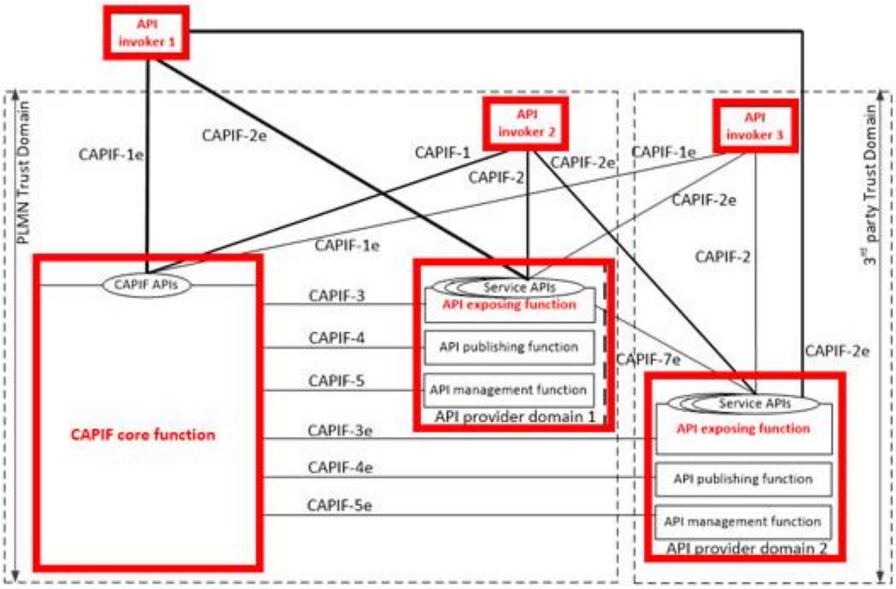

Figure 26: Overview of CAPIF architecture

8 Other initiatives like 5GACIA

In 5G-ACIA white paper [42], the functional requirements for exposing the capabilities of non-public 5G systems to connected industries and automation applications are shown. By utilizing exposure, industrial applications can have access to communication service monitoring and network management capabilities. In specific, two major groups are summarized for exposed capabilities as well as particular operational use cases (cf. Annex B of [42] for detailed use case or this two groups): (i) Device management that is related to the management of communication services for devices, and (ii) Network management focuses on the operations and maintenance tasks for the non-public network. Note that the considered use case is to allow factory operators to perform their daily tasks without the need to involve the network operator.

Specifically, the 5G exposure services are available via two reference points: Ed and En, as depicted in the following Figure 27 across different domains: Operational Technology (OT), Information Technology (IT), Service Provider (SP) domain. These reference points are situated between the IIoT application and the 5G system, in which Ed lies between a UE and an IIoT application, and En is the reference point between the 5G NPN and an IIoT application. Therefore, the 5G NPN user plane is managed by the services exposed through the reference points.

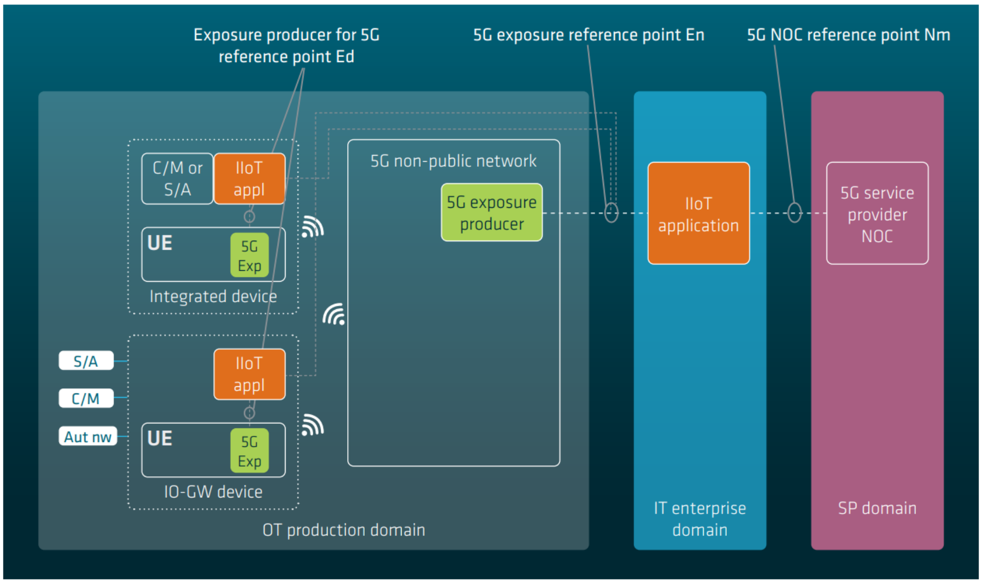

Figure 27: 5G exposure architecture

To provide more details, 5G-ACIA identifies the requirements for implementation of 5G exposure reference points. These requirements are designed to reflect the following four principles: (a) Usability and simplicity via proper levels of abstraction understandable for non-5G experts , (b) Modularity and extensibility to make certain functions optional and future extension with backward compatibility, (c) Service-based interfaces implemented in a service-oriented manner (e.g., by means of open RESTful APIs), and (d) A common time base must be applied to enable IIoT applications correctly correlate exposed events. Finally, 5G-ACIA provides a non-enumerated list of connectivity parameters and performance indicators of interest to IIoT applications for QoS monitoring. These listed parameters can follow the capabilities defined by 3GPP to be exposed to IIoT applications via network exposure functions (NEF) and via the SEAL framework or CAPIF.

Based on the above-mentioned 5G-ACIA view, we can observe that it can be mapped to two different classes of NetApps in Section 6: aaS model or hybrid model. When the IIoT application is in the device, for example an 5G UE that serves as the input-output gateway function (IO-GW) or integrated with sensors/actuators (S/A) and/or controllers/managers (C/M), it will leverage the hybrid model by instantiating a part of its application in the OT domain and still use the Ed reference point to be locally executed on the device. Note that the authentication of these locally deployed IIoT applications is not divulged to 5G system. Instead, it connects to the device management application in the enterprise network, and the network management server maps the IIoT application identifier to the UE identifier. Whereas the IIoT application on the network side can be mapped to the aaS model, and the exposed 5G services (subject to authorization) via the En reference point can be accessed by IIoT applications running on any compute node in its domain. Notice that even with the integration of 5G NPNs with Industrial Ethernet networks (i.e., 5G system as an Ethernet bridge) to support deterministic and time-sensitive traffic, the En interface is still necessary to expose Time-Sensitive Networking (TSN) application function capabilities using the aaS model.

9 Conclusion

This paper is prepared by 5G-PPP software network Working Group, and it complements a series of white paper published by the WG related to the cloud native transformation and the role of the vertical. The aim of this white paper is to demystify the concept of the Network Application. The important point of the concept is related to how the telco exposes the capabilities of the 5G/B5G platform, to others business platforms owned by the verticals to enhance their services. This mix and match between services from the telco and services from the verticals is the main driver of the concept of the NetApp. Open platform, API, service exposure, abstraction etc are different topics on which different projects, mainly ICT-41, worked out through diverse vertical use-cases. It results different mode of interaction between verticals and 5G/B5G system leading to three main categories: as a service, hybrid and coupled/integrated models.

10 References

[1] 5G-PPP White Paper, "Service performance measurement methods over 5G experimental networks", May 2021 [online]. Available: https://5g-ppp.eu/wp-content/uploads/2021/06/Service-performance-measurement-methods-over-5G-experimental-networks_short_version_08052021-Final.pdf

[2] 5GASP D7.3 Deliverable, "Market Research Report", Sept 2021 [online]. Available: https://www.5gasp.eu/assets/documents/deliverables/D7.3%20Market%20Research%20Report.pdf

[3] [online] https://www.3gpp.org/news-events/conferences/2082-sa6_verticals

[4] R Vilalta et al, "Experimental evaluation of control and monitoring protocols for optical SDN networks and equipment", Journal of Optical Communications and Networking 13 (8), D1-D12, 2021.

[5] http://5gasp.eu/

[6] https://www.5gmediahub.eu/

[7] https://smart5grid.eu/

[8] https://www.5g-induce.eu/

[9] https://evolved-5g.eu/

[10] https://www.vital5g.eu/

[11] https://www.affordable5g.eu/

[12] https://h2020daemon.eu/overview/

[13] https://www.teraflow-h2020.eu/

[14] https://www.5g-victori-project.eu/

[15] https://www.gsma.com/futurenetworks/wp-content/uploads/2020/01/3.0_Characterisation-of-Network-Slices.pdf

[16] http://openslice.io

[17] TM Forum, "TMF 633 – Service Catalog Management"

[18] ETSI NFV ISG, "GR NFV-IFA 029, Architecture; Report on the Enhancements of the NFV architecture towards

[19] TM Forum, "TMF 641 – Service Ordering Management"

[20] 5GMediaHUB: 5G Experimentation Environment for 3rd Party Media Services, available online: https://www.5gmediahub.eu/

[21] 3GPP release 16, available online: https://www.3gpp.org/release-16

[22] 3GPP release 17, available online: https://www.3gpp.org/release-17

[23] 3GPP SEAL "Service Enabler Architecture Layer for Verticals", available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3587

[24] 3GPP CAPIF "Common API Framework", available online: https://www.3gpp.org/common-api-framework-capif

[25] Network Functions Virtualization (NFV) Release 3; Architecture; Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS", available online: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=50985

[26] ETSI NFV EVE, available online: https://www.etsi.org/deliver/etsi_gr/NFV-EVE/001_099/012/03.01.01_60/gr_NFV-EVE012v030101p.pdf

[27] Smart5Grid deliverable D2.1 "Elaboration of Use Cases and System Requirements". Available at: https://smart5grid.eu/wp-content/uploads/2021/07/Smart5Grid_D2.1_Elaboration-of-UCs-and-System-Requirements-Analysis_V1.0.pdf

[28] Kepler/Cannon (2020). The Cloud-Native Paradigm. Evolving enterprises and the new business-IT convergence. Available at: https://www.keplercannon.com/cloud-native-paradigm/

[29] 5G PPP (2020). 5G PPP Software Network WG Paper, "Cloud-Native and 5G Verticals' services". Available at: https://5g-ppp.eu/wp-content/uploads/2020/02/5G-PPP-SN-WG-EV5G-and-Cloud-Native.pdf

[30] ETSI (2014). ETSI GS NFV-MAN 001, "Network Function Virtualisation (NFV); Management and Orchestration,"V1.1.1, December. 2014. Available at: https://www.etsi.org/deliver/etsi_gs/nfvman/001_099/001/01.01.01_60/gs_nfv-man001v010101p.pdf

[31] ETSI (2018). ETSI White Paper No.28: "MEC in 5G Networks", June 2018. Available at: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

[32] Smart5Grid deliverable D2.2 "Overall Architecture Design, Technical Specifications and Technology Enablers". Available at: https://smart5grid.eu/

[33] EVOLVED-5G Project: https://evolved-5g.eu/

[34] EVOLVED-5G deliverable D4.1 "5G Exposure Capabilities for Vertical Applications (Intermediate)" [online]. Available : https://evolved-5g.eu/wp-content/uploads/2022/03/EVOLVED-5G-D4.1_v2.0-final.pdf

[35] D. Fragkos, G. Makropoulos, P. Sarantos, H. Koumaras, A. Charismiadis, D. Tsolkas, 5G Vertical Application Enablers Implementation Challenges and Perspectives, IEEE MeditCom 2021.

[36] Common API Framework (CAPIF): https://www.3gpp.org/common-api-framework-capif

[37] 3GPP TS.23.222, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3337

[38] N. D. Tangudu, N. Gupta, S. P. Shah, B. J. Pattan and S. Chitturi, "Common Framework for 5G Northbound APIs,"2020 IEEE 3rd 5G World Forum (5GWF), 2020, pp. 275-280, doi: 10.1109/5GWF49715.2020.9221161.

[39] EVOLVED-5G Project (2021). EVOLVED-5G deliverable D2.1 "Overall Framework Design and Industry 4.0 requirements". Available at: https://evolved-5g.eu/wp-content/uploads/2021/11/EVOLVED-5G-D2.1_v1.4.pdf

[40] I. Paez, et al., "DAEMON Deliverable 2.1: Initial report on requirements analysis and state-of-the-art frameworks and toolsets", Jun. 2021.

[41] 5G-VICTORI, "D2.6 5G-VICTORI Infrastructure Operating System – Final Design Specification", 2021

[42] 5G-ACIA White Paper, "Exposure of 5G Capabilities for Connected Industries and Automation Applications", 2021

[43] Common API Framework (CAPIF) https://www.3gpp.org/common-api-framework-capif

[44] 3GPP TS 22.261

https://www.etsi.org/deliver/etsi_ts/122200_122299/122261/16.14.00_60/ts_122261v161400p.pdf

[45] 3GPP TS 23.434 https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3587

[46] 3GPP TS.23.222 https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3337

[47] 3GPP TS.23.222 https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3337

[48] O-RAN Alliance, “O-RAN Architecture Description v1.0,”. Feb. 2020.

[49] 5GASP deliverable D4.1 [online]. Available : “Initial Methodology for Designing and developing NetApps”, https://www.5gasp.eu/assets/documents/deliverables/D4.1%20Initial%20Methodology%20for%20Designing%20and%20Developing%20NetApps.pdf

[50] VITAL-5G project: https://www.vital5g.eu/

[51] VITAL-5G D1.2 deliverable, “System Specifications and Architecture”, [online] available: https://www.vital5g.eu/wp-content/uploads/2022/01/VITAL5G-D1.2-5G-system-specifications-and-architecture_Final.pdf

11 List of Contributors

Name	Company / Institute / University	Country	Project
Editorial Team			
Overall Editor			
Bessem Sayadi	NOKIA Bell-Labs 5G-PPP Software Network WG Chairman	France	
Contributors			
Chia-Yu Chang	NOKIA Bell-Labs	Belgium	DAEMON
Christos Tranoris	University of Patras	Greece	5GASP
Marius Iordache	Orange	Romania	VITAL-5G/5G-VICTORI
Kostas Katsaros	Digital Catapult	UK	5G-VICTORI
Ricard Vilalta	CTTC	Spain	Teraflow
Hamzeh Khalili	CTTC	Spain	5G-MediaHUB
Hakon Lonsethagen	Telenor	Norway	5G-SOLUTIONS/ 5G-MediaHUB
Josep Martrat	ATOS	Spain	Affordable5G
Thanos Xirofotos	UBITECH	Greece	5GIANA, 5GINDUCE
Qi Wang	University of the West of Scotland	UK	5GINDUCE
Jose M. Alcaraz Calero	University of the West of Scotland	UK	5GINDUCE
Antonello Corsi	ENG	Italy	Smart5Grid
Borja Otura Garcia	ATOS	Spain	Smart5Grid
Paula Encinar Sanz	ATOS	Spain	Smart5Grid
Regel G. Usach	Polytechnic University of Valencia	Spain	EVOLVED-5G
David Artunedo	Telefonica	Spain	EVOLVED-5G
Dimitris Tsolkas	Fogus Innovations & Services	Greece	EVOLVED-5G
Harilaos Koumaras	National Scientific Research Center Demokritos	Greece	EVOLVED-5G

George Makropoulos	National Scientific Research Center Demokritos	Greece	EVOLVED-5G

Acknowledgment

We would like to thank all the project contributors that are indirectly involved in this White Paper and not cited directly in the list above.