Challenges in (selected) Cloud-native adoption in (distributed & disaggregated) MNOs 5G and B5G Networks need for Synergy between Compute, Storage, Networking and Communications

Ike Alisson

2022 - 12- 08 Rev PA06

Table of Contents (ToC)

1. Cloud & Communications Systems' (current) Challenges & Issues

Today's Cloud and Communications Systems are NOT CAPABLE of

- *Capturing,*
- *Transmitting,*
- *Storing, and*
- *Analysing*

the Petabytes of Data generated by the soon-to-be trillions of Sensors operating 24/7.

They are also NOT PREPARED to deliver the Compute needed for Real-Time AI/ML Inferencing required to drive such demands that we anticipate will come from our

- *FoF (Factory of the Future)*
- *VR/XR/MR (Virtual, Extended, Mixed Reality and Extended Reality) with Haptic Interactions,*
- *(V2X) Connected Vehicles,*
- *Assisted living, or*
- *Merging of Physical & Digital worlds with 5G & B5G*

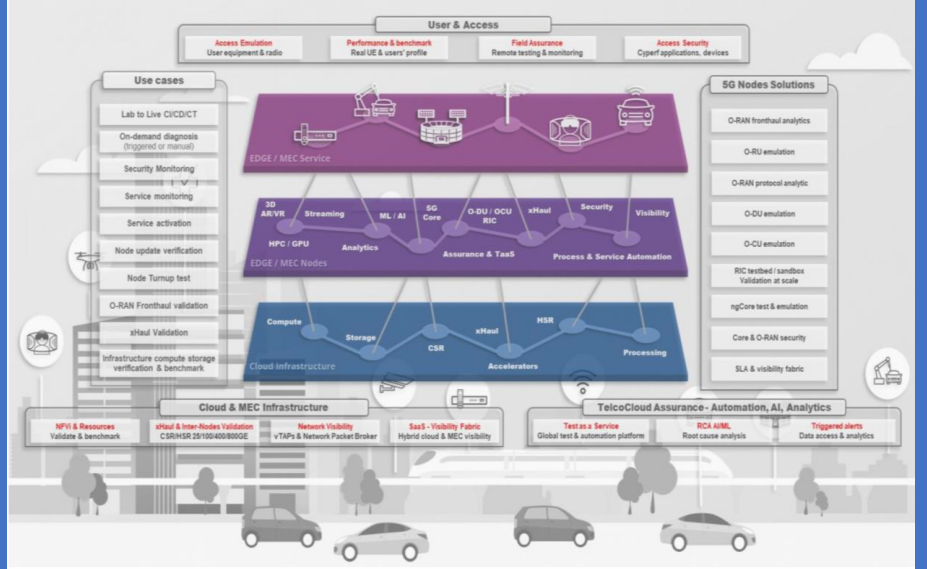


Figure – Telco Edge Cloud, Next-Gen Service Assurance at Scale

The Cloud is "Changing"

1st - Applications want to be deployed anywhere & change deployment anytime.

The **focus moves from "sharing resources to Composing Dynamic Capabilities, even after Deployment.**

Applications will be Delay- and Latency sensitive, on varying Time-scales with different Hard- & Soft boundaries.

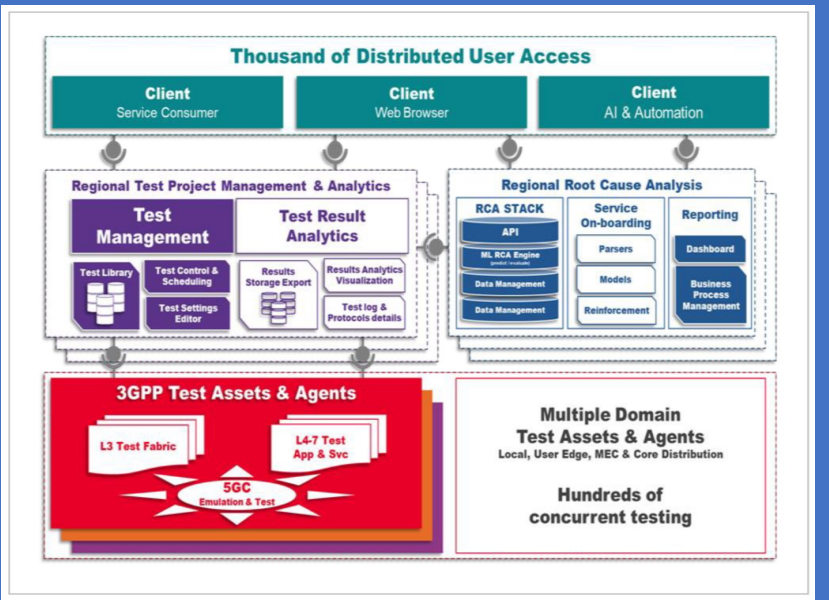


Fig – Nationwide Distributed Cloud based Network Test Bed Orchestration

Communication, Compute, and Storage must be considered as an **Integrated Set of Changeable Configurations** that provide the required service to an application.

2nd - "Center of Gravity is moving toward the Devices ("Edge"), & interactions in a Cyber-Physical World best suited for these tasks and configure any required communication between all end points in important areas such as

- IoT,
- Industry 4.0,
- Private 5G, or
- Retail and Public Services.

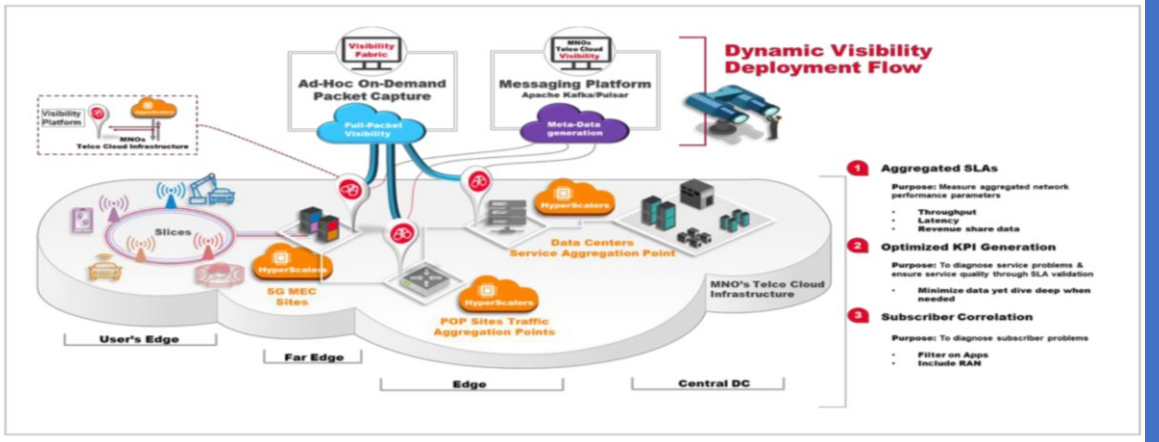


Figure : Hybrid Network Visibility Platform architecture

Management of Resources and Workloads:

Most Orchestration Frameworks today use a Centralized Approach (where) One (1) Entity has knowledge of all the Resources in the System and Plan how the Workloads will be mapped.

With the start of Docker & containers, the Kubernetes Project was started to provide a lightweight & scalable Orchestration solution.

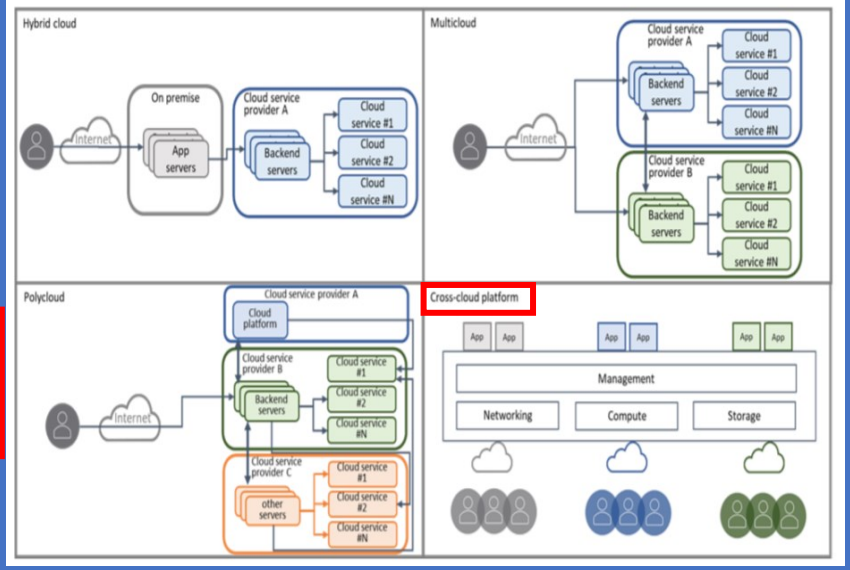
Most existing Compute Systems today, including Edge Computing Systems, rely **on static provisioning**.

Thus, the SW & the Services needed to perform the Compute are already residing at the Edge Server prior to an Edge node requests a Service & the pool of HW resources is also known a priori to Kubernetes.

This architecture works well for Cloud & the MEC where a Centralized Orchestration is used.

Since the Resources of the Pervasive Edge are independently owned, the **Orchestration Frameworks need to be extended to handle Dynamic and Multi-Tenant Resources** in a secure manner.

Figure multi-cloud deployment models



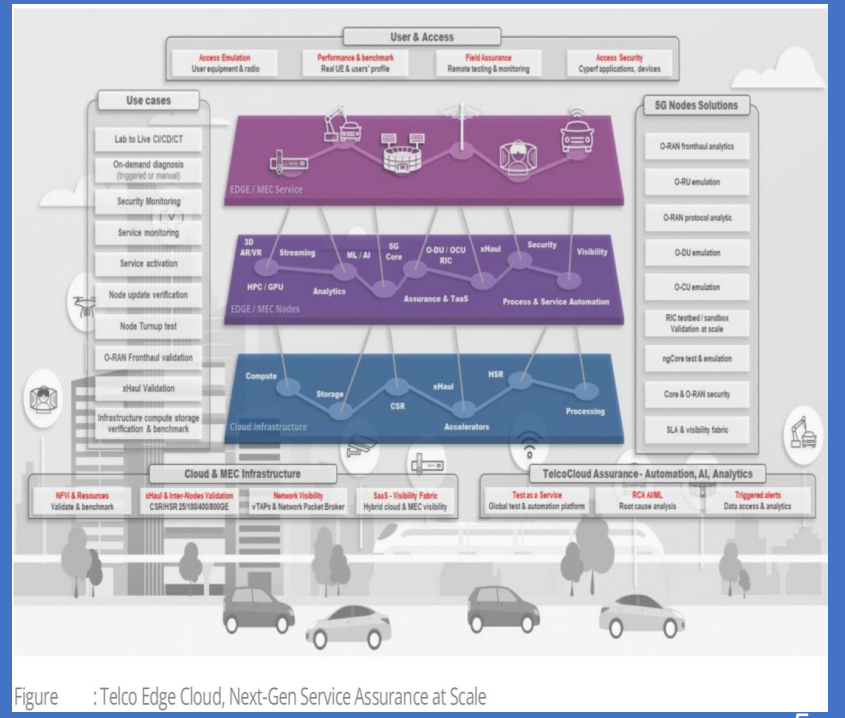


Figure : Telco Edge Cloud, Next-Gen Service Assurance at Scale

Management of Resources and Workloads:

it is important for the Orchestration Architecture to be able to support Dynamic Discovery & Use of (HW) Resources distributed in the edge.

Kubernetes and Docker are both centralized Architectures, which need messages exchange and synchronization before a new Service can be configured on a server.

Hence, new approaches have to be investigated to discover and deploy new (HW) Resources in Real-Time within the Multi-site & Multi-Edge Infrastructure of 5G & B5G Systems.

Content Sharing and Resource/Service Orchestration in 5G & B5G

New innovations in terms of **Data Movement & the Orchestration of Resource and**
Compute Services will be required.

a few new exemplary approaches on **Network - & Application - Layers** are detailed such as ……..

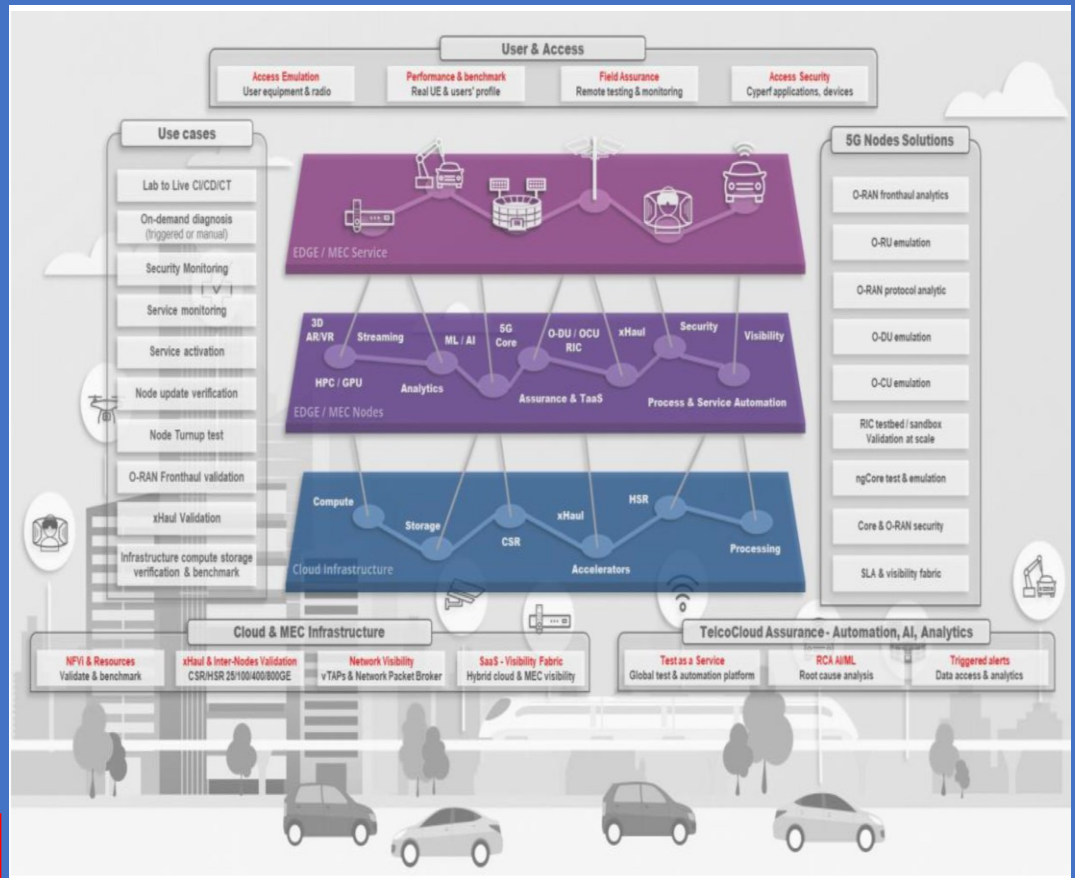


Figure : Telco Edge Cloud, Next-Gen Service Assurance at Scale

2. ETSI MEC design & implementation example

3GPP EAS and ETSI MEC Application Profile Provisioning

The MEC Application can start "producing" or "consuming" MEC Services after the MEC Application is instantiated & running.

The Application Information (AppInfo), which can be regarded as the MEC Application Profile, represents the information provided by the MEC application instance as part of the "Application Registration request" message.

Some fields in AppInfo are intentionally not duplicating the EAS profile (if present) with conflicting parameters but should be consistent with them.

It can be seen that unlike AppD, which is mainly used in the Management Plane for instantiating an Application, and is static in nature, AppInfo carries the runtime information about the MEC application instance.

In 3GPP EDGEAPP, the EAS profile is provided in the EAS registration request.

[Observation 1] The R17 of EDGEAPP only defines the functionality of EAS acting as an invoker, which is similar to MEC Application that consumes MEC Services defined in ETSI MEC. According to the Key issue #2 in clause 4.2, The EAS acting as a service provider is expected to be defined in R18 and expose service APIs.

[Observation 2] According to the Key issue #2 in clause 4.2, the EAS can act as a service provider and EES can act as CAPIF core function so different services will be discoverable at different EESs. How the information of a service registered at one MEC platform is made available to other platforms in the same MEC system is not explicitly specified within ETSI MEC, while in EDGEAPP, as EES supports CAPIF core function, the EAS service published on EES1 can be discovered by EAS registered on EES2 through CAPIF-6 or CAPIF-6e.

EAS/MEC application profile provisioning

ETSI MEC and EDGEAPP defined different style of EAS/MEC application profile provisioning. The information flows for lifecycle management of MEC applications is described in ETSI GS MEC010-2 [13]. The informational flows for the optional MEC Application registration are described in ETSI GS MEC 011 [14]. The MEC application can start producing or consuming MEC Services after the MEC Application is instantiated and running. The application information (AppInfo), which can be regarded as the MEC application profile, represents the information provided by the MEC application instance as part of the "application registration request" message. The attributes of the AppInfo are available from the clause 7.1.2.6 of ETSI GS MEC011 [14]:

Some fields in AppInfo are intentionally not duplicating the EAS profile (if present) with conflicting parameters but should be consistent with them. This is highlighted in NOTE 1 and NOTE 2, for example. It can be seen that unlike AppD [13], which is mainly used in the management plane for instantiating an application, and is static in nature, AppInfo carries the runtime information about the MEC application instance.

Ref.: 3GPP, Rel. 18 (5G Adv), Nov., 2022

… in current ETSI MEC specification, no APIs for MEC Application Registration is defined because it is assumed that all MEC Applications are on-boarded and managed by MEC Orchestrator.

API for MEC Application discovery is not defined since the existing MEC Service is either defined from the MEC Application's perspective or it is consumed by the MEC Application rather than the UE.

Therefore, the comparison EAS Registration and EAS discovery of EDGEAPP and ETSI MEC specification shows that:

[Observation 2] ETSI MEC platform(MEP) supports service registration. In the registration parameter "ServiceInfo", there is a mandatory field "consumedLocalOnly" used to indicate that the service can only be consumed by the MEC applications located in the same locality, which means ETSI MEC services (produced by Authorized MEC APPs) registered and exposed on MEP can be invoked by MEC consumer APPs deployed on the same or another MEC host.

EAS registration and EAS discovery

However, in current ETSI MEC specification, no APIs for MEC Application registration is defined because it is assumed that all MEC Application are on-boarded and managed by MEC Orchestrator, which was specified in ETSI GS MEC 010-2 [13]. API for MEC Application discovery is not defined since the existing MEC service is either defined from the MEC Application's perspective or it is consumed by the MEC Application rather than the UE.

Therefore, the comparison EAS registration and EAS discovery of EDGEAPP [2] and ETSI MEC specification [13] shows that:

[Observation 1] The EAS registration and EAS discovery mechanism is defined in R17 of SA6 and ETSI MEC introduced MEC application registration (ETSI GS MEC 011 v3.0.6). It is FFS whether and how to address such differences in SA6, e.g. in support of ETSI MEC.

[Observation 2] ETSI MEC platform(MEP) supports service registration. In the registration parameter "ServiceInfo", there is a mandatory field "consumedLocalOnly" used to indicate that the service can only be consumed by the MEC applications located in the same locality, which means ETSI MEC services (produced by Authorized MEC APPs) registered and exposed on MEP can be invoked by MEC consumer APPs deployed on the same or another MEC host.

Ref.: 3GPP, Rel. 18 (5G Adv), Nov., 2022

6 Reference architecture

6.1 Generic reference architecture

The reference architecture shows the functional elements that comprise the multi-access edge system and the reference points between them.

Figure 6-1 depicts the generic multi-access edge system reference architecture. There are three groups of reference points defined between the system entities:

- reference points regarding the MEC platform functionality (Mp);
- management reference points (Mm); and
- reference points connecting to external entities (Mx).

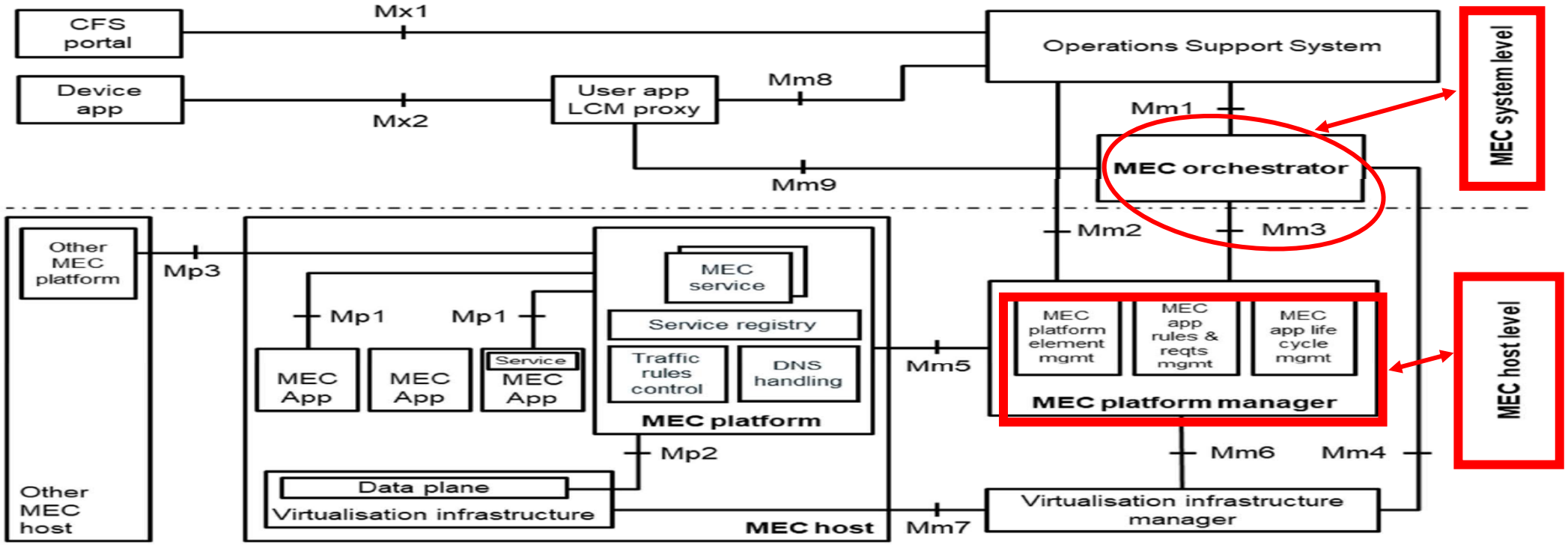


Figure 6-1: Multi-access edge system reference architecture

4.3.2 Application descriptor requirements

Table 4.3.2-1 specifies requirements related to application lifecycle management applicable to the application descriptor.

Table 4.3.2-1: Application descriptor requirements

Numbering	Functional requirement description
AppDesc.001	The application descriptor shall contain a description of minimum computation resources required by the application, e.g. amount, characteristics and capabilities for virtual compute.
AppDesc.002	The application descriptor shall contain a description of minimum virtual storage resources the required by application.
AppDesc.003	The application descriptor shall contain a description of minimum virtual network resources required by the application.
AppDesc.004	The application descriptor shall support describing a list of services a MEC application requires to run.
AppDesc.005	The application descriptor shall support describing a list of additional services that a MEC application may use if available.
AppDesc.006	The application descriptor shall support describing a list of features a MEC application requires to run.
AppDesc.007	The application descriptor shall support describing a list of additional features a MEC application may use if available.
AppDesc.008	The application descriptor shall support a description of Traffic Rules.
AppDesc.009	The application descriptor shall support a description of DNS Rules which provide specific FQDNs to be registered into the MEC system (e.g. for redirection of traffic to local host).
AppDesc.010	The application descriptor shall support a description of latency required by the MEC application.

4.4 Requirements for reference point Mm3*

4.4.1 General requirements

The Mm3* reference point between the MEC Application Orchestrator and the MEC Platform Manager - NFV is used for the management of the application lifecycle, application rules and requirements and keeping track of available MEC services, etc. Table 4.4.1-1 specifies requirements related to application lifecycle management applicable to the Mm3* reference point.

Table 4.4.1-1: Mm3* reference point requirements

Numbering	Functional requirement description
Mm3*.001	The Mm3* reference point shall support the application Lifecycle Management interface produced by the MEC Platform Manager - NFV.

4.4.2 Application lifecycle management interface requirements

Table 4.4.2-1 specifies requirements applicable to the Application Lifecycle Management interface produced by the MEC Platform Manager - NFV on the Mm3* reference point.

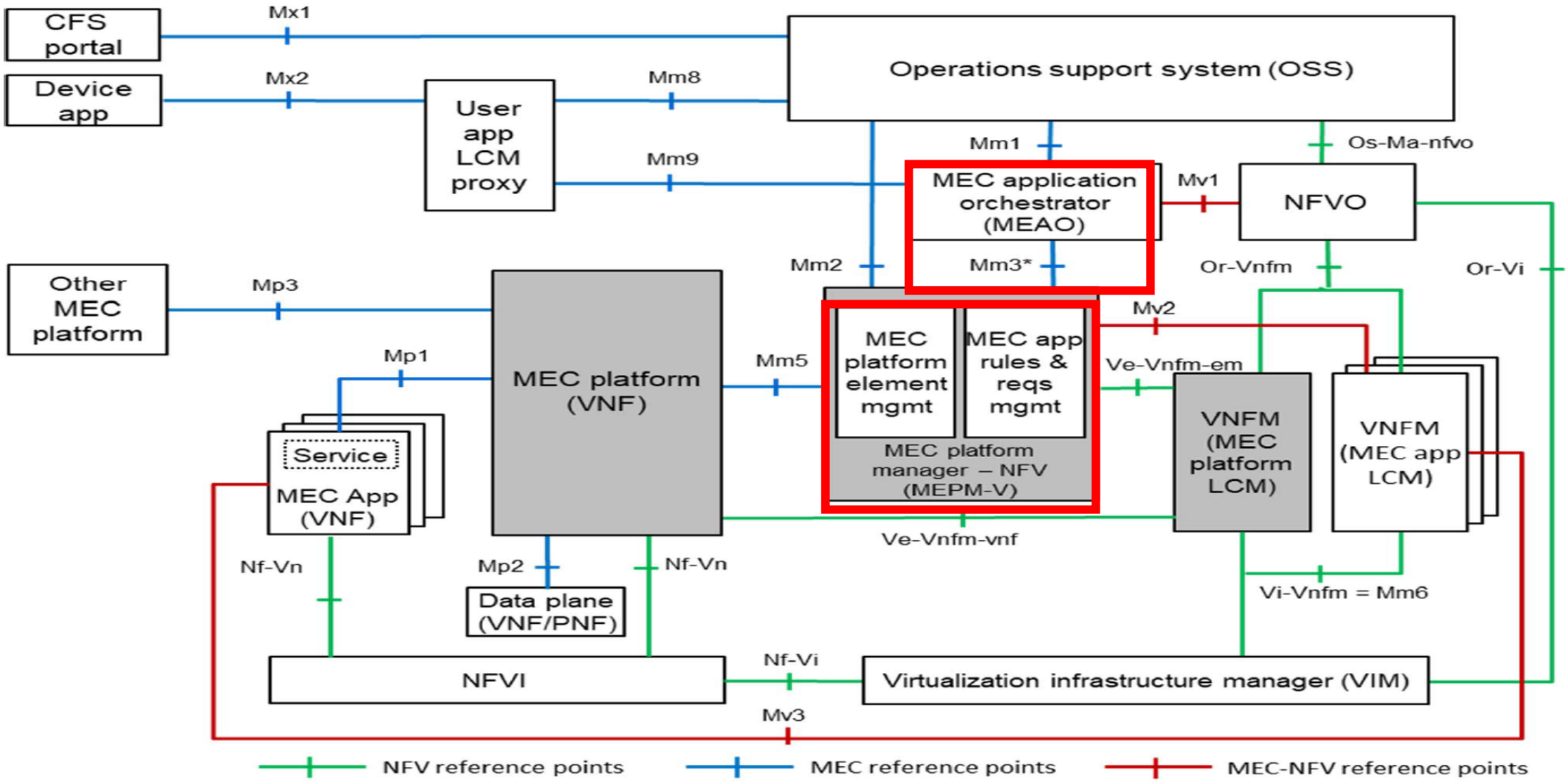


Figure 6-2: Multi-access edge system reference architecture variant for MEC in NFV

Input on MEC System Architecure Management & Orchestration mapped into the NFV Architecture Management and Orchestration

Akraino API TSC × ETSI MEC ISG × ETSI NFV ×

Ike Alisson <ike@alicon.se>
till mehmet.toy, Jie, Jeff, Tina, Aaron, wdudhnath, api@lists.akraino.org, mig

14 nov. 2020 13:1

Dear Mr. Toy (Cc et al.,),

With reference to your question to me during the TSC meeting on Friday, Nov., 13th, on the MEC Architecure Management and Orchestration Functions (with interfaces) integrated/mapped into ETSI NFV Architecure and my verbal reply, please see below in written (to read and have a quick insight into it) and also attahced in *.word format to use in and personal choice.

Hope and wish that it might be of interest and use to you.

Sincerely yours,
Ike

The MEC Architecture has been designed in such a way that a number of Different Deployment Options are possible.

ETSI MEC & ETSI NFV (Network Functions Virtualization) are complementary concepts as seen in the diagram (Fig.) attached further below.

A specified **MEC Architecture** variant **allows the instantiation of MEC Applications & NFV** (Virtualized Network Functions) **on the same Virtualization Infrastructure**.

Also, **ETSI NFV MANO Components are reused to fulfil a part of the MEC Management & Orchestration Tasks**.

Fig. below is *a variant of the Multi-access Edge System Architecture for the deployment of NFV Functions*.

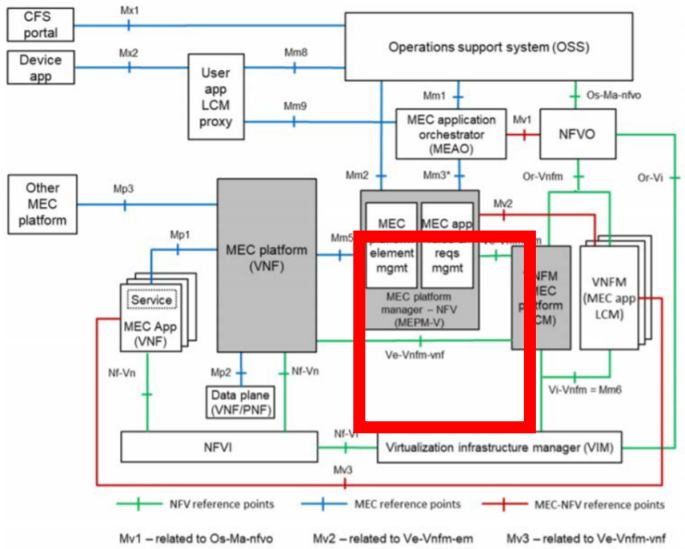


Fig. Multi-access Edge System Reference Architecture Variant for MEC in NFV.

The following assumptions also apply to the *Variant Reference Architecture for MEC in NFV*:

1. The MEC platform is deployed in a VNF

Inquiry on the NFV&MEC IOP Plugtests 2021

ETSI NFV × NFV × One M2M ×

Ike Alisson <ike@alicon.se>
till Laurent, Miguel, Silvia, Tina, Oleg, wdudhnath, mig

22 juli 2021 11:18

Hello Laurent (Cc Miguel, Silvia et al.,),
Oleg B. shared with me a piece of your correspondance on the ETSI MEC & NFV plugtests.

On personal basis, due to our previous acquaintance and interaction, I kindly would like to share with you my spontaneous reaction and thoughts that arised with the purpose just to convey them to you so that you are aware of the questions that I spontaneously have with respect to MEC & NFV implementation. I will deliberately leave RAN aspects out (related to LADN, DNN, DNNAI, NSSAI, S-NSSAI, RAN RIC, CU-DU/RU Geographical coverage and RT/nRT Communication and impact on Latency as well as the 3GPP SST and GSMA NEST & GST that have an impact on the Service deployment and latency as specified in the 5QI values).

On the list that you had sent, I wonder if you include in the test between MEC & NFV:

1. Is the MEC Platform (MEP) implemented on the 5G SBA CN SMF as a NF or just a demo set up platform?
2. Is the ETSI NFV implemented as a 5G SBA CN standard specified VNF or it is a demo set-up test simulation platform?
3. On the Management, do you utilise OSM Rel 10 features? If "Yes", which one and is there anything related to ETSI ZSM?
4. On the MEC/MEP Application selection and re-selection of UPF/PSA, do you test all three SSC Modes 1-3 or you just test SSC Mode 1?
5. Do you test with UE Application set on with checking the registration (Authentication, Authorization and Accounting) of the UE and allowed Service Access Identiy and Service Access Category as well as Subscriptions (SUPI, SUCI, GUTI) for the HPLMN, VPLM interaction and interrogation in the PCF as well as NRF and UDM for the respective NF and Resources invoked due to PCF defined subscription in the UDR)
6. Do you test all the all four (4) PDU (standard specified) session Data types, namely , IPv6, IPv4v6, Ethernet, Unstructured. For the last type of PDU data type, do you have any interrogation via UDM to UDSF where the NF Appplication's Context is separated from the NF Application Business Logic and stored separately as Unstructured Data in the UDSF?
7. For the MEP Application Multi-access, do you utilize the feature ATSSS (currently deployed as part of Rel 16 for for handling Multi-access through 3IWG and N3IWG with support for "Structured Data" as M and "Unstructured Data as"O" in the 3GPP System Architecure specification.
8. Do you use SCP and if it is only one or you have several in Domain as defined by the PCF?
9. Do you have defined and test MTU (Maximum Transfer Units) with GTP Packets, e.g. if you would test "Slicing" (anyone of the standard specified in 3GPP 5 SST Categories) with simulation of having RAN (NR) and 5G CN, transferred over IPSec tunnel in an IPv6 deployment with User Packet first encapsulated in a GTP tunnel which results in the overhead for IPv6 header, which is 40 octets, UDP overhead, which is 8 octets, Extended GTP-U header, which is 16 octets.

The above points are just spontaneous thoughts that I wanted to share with you, as there might be some other people that may address some of the above and/or similar aspects. As you well know, my fosu is on the Service E2E deployment (with focus on Data-centric) and since I am not a Technical person, but I am privileged to interact with extremely talented and World-class Technical System E2E expert, who puts me "on track" when I get "lost", I can get some insights that may affect the Service implementation

Laurent Velez <Laurent.Velez@etsi.org>
till Miguel, Silvia, ike@alicon.se, Tina, Oleg, wdudhnath, mig

30 juli 2021 18:46

Hello Ike,

Thank you for all these inputs , suggestions and questions. I will share them with the rest of the NFV&MEC Plugtests team.
Of course the Interop testing will depend on the products that the companies bring. And following the supported features, reference points or APIs, we have a list of tests in both NFV and MEC IOP Test plans. It is also possible to run conformance testing on standardized NFV and MEC API.
The scenarios you propose are "advanced" and more complex that what we used to run. In Plugtests, we more focus to validate the standards and if it is correctly implemented.
Anyway, there are good input and we will have a look on this.
Best regards.
Laurent.

•••

Ike Alisson <ike@alicon.se>
till Laurent, Miguel, Silvia, Tina, Oleg, wdudhnath, mig

30 juli 2021 19:10

Hello Laurent et al,
Thank you for your reply with an elaboration. It is appreciated.

I kindly would like to share with you two more issues in case that you might be in need of assistance.

First, there are some improvements related to 3GPP 5G NR Rel. 16 and Rel. 17 related to UE RM (for initiating/enabling PDU sessions transfer) and CM and RRC states defined as "idle", "connected" and "inactive". These enhancements are done to target the Latency and Security (for the UE defined RNA - RAN Notification Area) and while you have Application session management and throughput and latency defined for respective UC Service 5QI, it might be good to be aware of these depending on the UC Service categories that shall be run.

In case that you might be in need to get in contact with some representative at LFN ONAP, please let me know if I may help and assist you.

Have a nice weekend

ETSI MEC deployment/commissioning issues/challenges by May-June 2021

Datum: 7 juni 2021 11:50:20 +02:00

Ämne: Lunchtime Webinar 5GCroCo: Mobile Edge Computing/Cloud (MEC) Architecture (Part-1).

Till: Webinar@5g-ppp.eu

Thank you for registering for the Lunchtime Webinar 5GCroCo: Mobile Edge Computing/Cloud (MEC) Architecture (Part-1).

The webinar was held on Monday, 31 May 2021.

The recorded video from this Webinar is now available via the link before, with the indicated username and password.

http://5gcroco.eu/images/vv4/5GCroCo%20Lunchtime%20Webinar%2061-20210531%201002-1.mp4

user: trident

password: Rr6tadNk

Best wishes,
5G-PPP and 5GCroCo webinar team.

Ämne: 5GCroCo Lunchtime Webinar 6-2: 7 June 2021

Till: Webinar@5g-ppp.eu

Thank you for your interest in the 5GCroCo Lunchtime Webinar 6-2: Mobile Edge Computing/Cloud (MEC) Architecture (Part 2).

The recorded video from this 5GCroCo Lunchtime Webinar, held on Monday 7th of June, is now available via the link below, using the indicated user and password.

https://5gcroco.eu/images/vv5/5GCroCo_Lunchtime_Webinar_62-20210607.mp4

user:

password:

Can we also remind you that future events in this series and from other projects are available via the 5G PPP events page: https://5g-ppp.eu/event-calendar/

The 5G PPP and 5G CroCo webinat team.

The MEC system level management includes the **MEC orchestrator** as its core component, which has an overview of the complete MEC system. The MEC system level management is further described in clause 7.1.4.

The MEC host level management comprises the **MEC platform manager** and the **Virtualisation infrastructure manager**, and handles the management of the MEC specific functionality of a particular MEC host and the applications running on it. The MEC host level management is further described in clause 7.1.5.

6.2 Reference architecture variant for MEC in NFV

6.2.1 Description

MEC and Network Functions Virtualisation (NFV) are complementary concepts. The MEC architecture has been designed in such a way that a number of different deployment options of MEC systems are possible. A dedicated Group Report, ETSI GR MEC 017 [i.5], provides an analysis of solution details of the deployment of MEC in an NFV environment.

In clauses 6.2.2, 7.1.8 and 7.2.4 of the present document, a MEC architecture variant is specified that allows to instantiate MEC applications and NFV virtualised network functions on the same Virtualisation infrastructure, and to re-use ETSI NFV MANO components to fulfil a part of the MEC management and orchestration tasks.

6.2.2 Architecture diagram

Figure 6-2 depicts a variant of the multi-access edge system reference architecture for the deployment in an NFV environment [2].

In addition to the definitions for the generic reference architecture in clause 6.1, the following new architectural assumptions apply:

- The MEC platform is deployed as a VNF.
- The MEC applications appear as VNFs towards the ETSI NFV MANO components.
- The Virtualisation infrastructure is deployed as an NFVI and is managed by a VIM as defined by ETSI GS NFV 002 [2].
- The MEC Platform Manager (MEPM) is replaced by a MEC platform manager - NFV (MEPM-V) that delegates the VNF lifecycle management to one or more VNF Managers (VNFMs).
- The MEC Orchestrator (MEO) is replaced by a MEC Application Orchestrator (MEAO) that relies on the NFV Orchestrator (NFVO) for resource orchestration and for orchestration of the set of MEC application VNFs as one or more NFV Network Services (NSs).

Open Source MANO

by ETSI

OSM RELEASE TWELVE

RELEASE NOTES

Open Source MANO

Technical Steering Committee

June 2022

In addition to the definitions for the generic reference architecture in clause 6.1, the **MEC Federator** (MEF) functional element is introduced, including **MEC Federation Broker** (MEFB) and **MEC Federation Manager** (MEFM) functionalities. The MEF provides the functionality required to interface with other MEFs and in that capacity can act as a broker between MEFs. It interfaces to at least one MEO.

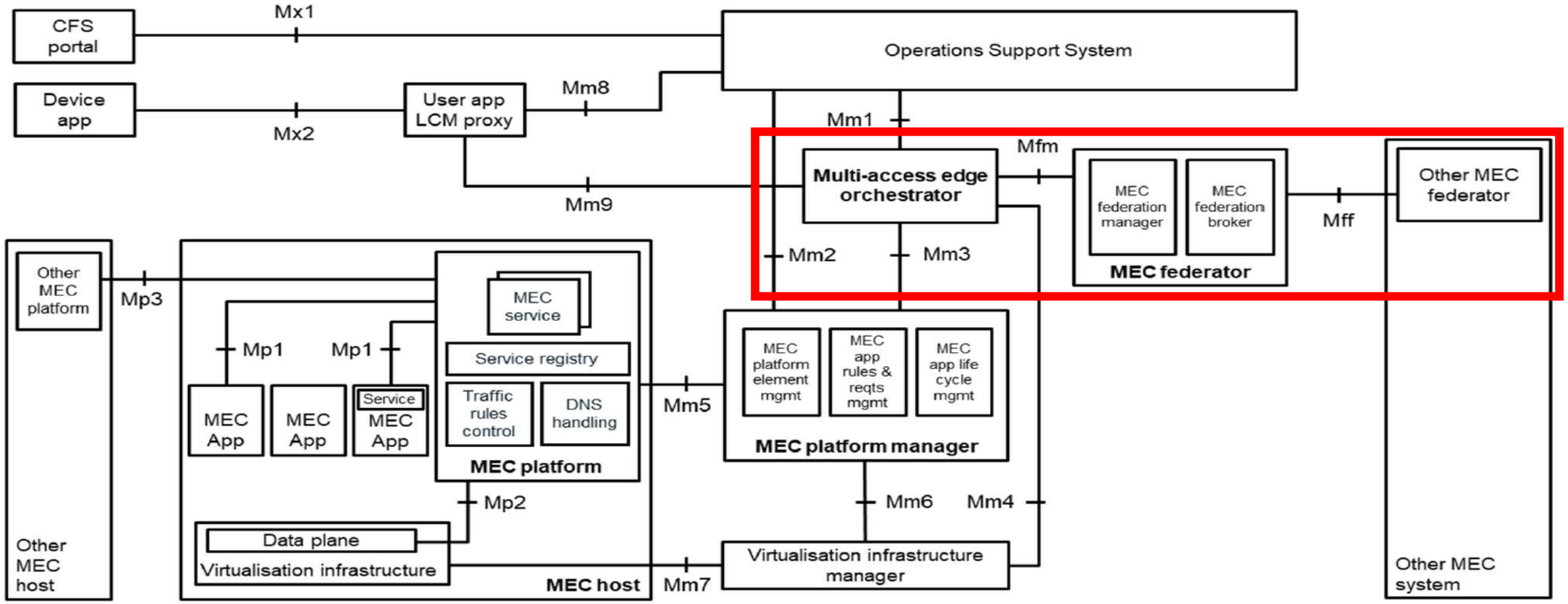


Figure 6-3: Multi-access edge system reference architecture variant for MEC federation

Enterprise open source for innovation

Consider the following findings from our survey:

Two years ago, lower cost of ownership was cited as the top benefit of enterprise open source. This year it's fallen to the sixth spot, well below "access to the latest innovations" in second. This year, 82% of IT leaders also agreed with the statement that "enterprise open source is used by the most innovative companies." About the same number, 81%, said that it "provides flexibility to customize solutions to meet company needs."

We see specific examples of enterprise open source adoption in emerging technology areas. 79% of respondents expect that over the next two years, their organization will increase use of enterprise open source software for emerging technologies. In the two most prevalent emerging tech areas, edge computing/IoT and artificial intelligence/machine learning (AI/ML), use of enterprise open source is expected to significantly outpace proprietary software over the same period. In edge computing/IoT, enterprise open source is expected to increase from 55% of cases to 72% two years from now. And, for AI/ML, our survey found that proprietary software use is actually expected to decrease, while enterprise open source use shoots up from 48% to 65%.

The benefits are broad and strategic

When we began running this survey four years ago, the top benefit of enterprise open source was clear: lower total cost of ownership (TCO). This result was likely a surprise to no one. Linux, along with enterprise open source more generally, was adopted by companies in no small part because it was a less expensive alternative to proprietary UNIX and proprietary networking-related applications. Even if this view of enterprise open source began to increasingly diverge from reality, it remained a stereotype. However, we have seen a steady shift away from enterprise open source being defined as cheaper software rather than better software. Of course, this is not to say that enterprise open source can't be less expensive to acquire and operate than proprietary software. But price is not how IT leaders generally frame their thinking about enterprise open source today.

This year's top two benefits? Better security and higher quality software. By contrast, lower TCO has declined dramatically in importance. It is now near the bottom of the benefits list in ninth place.

Red Hat

The State of Enterprise Open Source

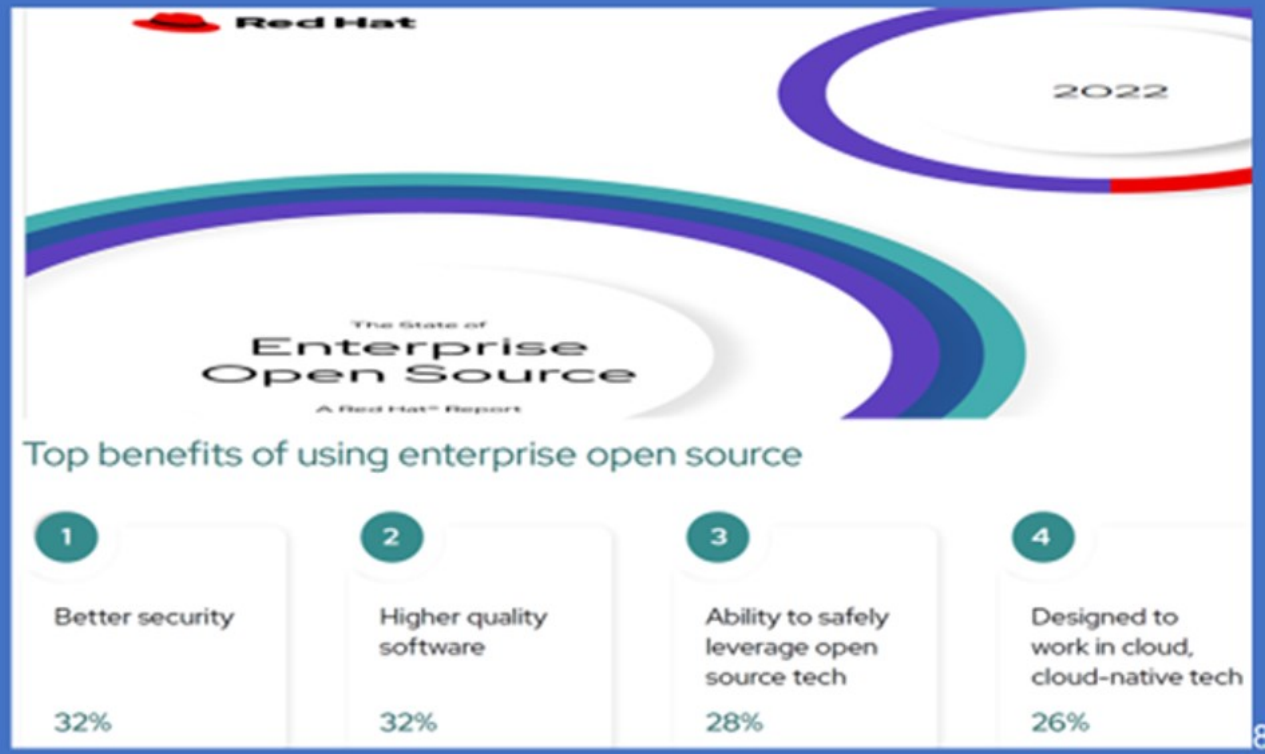
The State of Enterprise Open Source

A Red Hat® Report

2021 | Research conducted by Illuminas

Top benefits of using enterprise open source

1. Higher quality software **35%**
2. Access to latest innovations **33%**
3. Better security **30%**
4. Ability to safely leverage open source technologies **30%**



DISAGGREGATION IMPACT TO NETWORK ACTIVITIES

Operations Layers

The overall network operation includes 3 layers:

- **Business Operation Layer**
  Business operation is about CSP's Product Portfolio planning, development, operations and other roles, information or activities toward market and customer requirements.

- **Service Operation Layer**
  Service operation layer represents roles, information and activities that are involved in the strategic planning, definition, development, and operational aspects of services that are used to realise product offerings to the market.

- **Resource Operation Layer**
  Resource operation layer is about the activities related to the enterprise infrastructure, e.g., computing, networking, and storage resource capabilities to support the operation of the services.

the following analysis is limited to resource and service operation layers only.

Ref.: ODiN, Sept., 2022

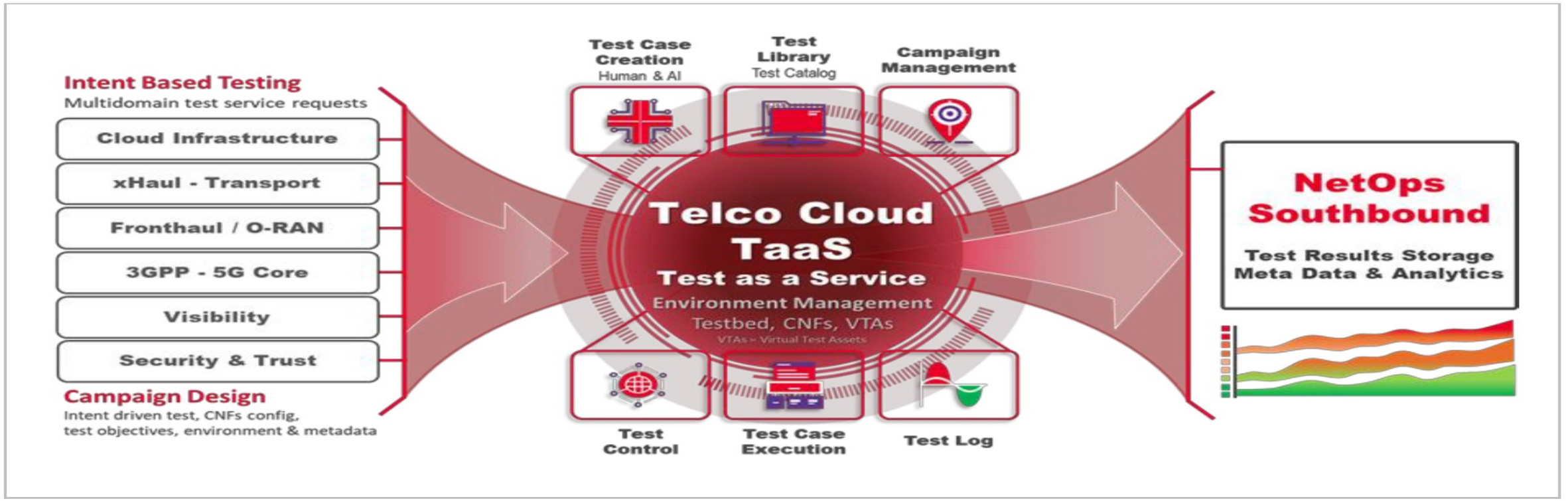


Figure : A TelcoCloud TaaS Platform

System Under Test (SUT) and Monitoring requirements:

- Isolation mode testing interfaces, functions & system interaction emulation
- End to End mode testing in Lab to Live context in pre-production & production mode
- Test agents and Assets distribution automated test agent distribution across the telco cloud architectures

For the special **MEC/Hybrid Cloud Assurance UC** - CI/CD/CT, **MEC assurance** becomes essential for *critical Edge Compute Applications & Performance* & particularly in a *Multi-Cloud Environment at the Carrier/Hyperscale Gateway.*

An MEC Validation Platform provides Full Stack MEC Testing & Performance coverage including Global Security assessment.

This is divided in **3 Main Categories** starting from the ground floor with **Cloud Infrastructure Validation** including:

1. **Capacity & Performance for Latency**, Bandwidth & Resiliency, Benchmarking, Scaling and Secure Access Service Edge (SASE).

2. **MEC Nodes Validation need to be conducted for QoS / QoE Validation, Jitter Latency, Video & Audio Processing, O-RAN RIC, 5G Core UPF split / N9 interface, xHaul Transport as a Service, Extended Visibility and Security Assurance Specification (SCAS).**

3. MEC Vertical Services & Applications with QoS / QoE Validation, Jitter Latency, O-Cloud, Video & Audio Processing, all the Verticals like C-V2X, industry 4.0, Video surveillance etc. and Network Security.

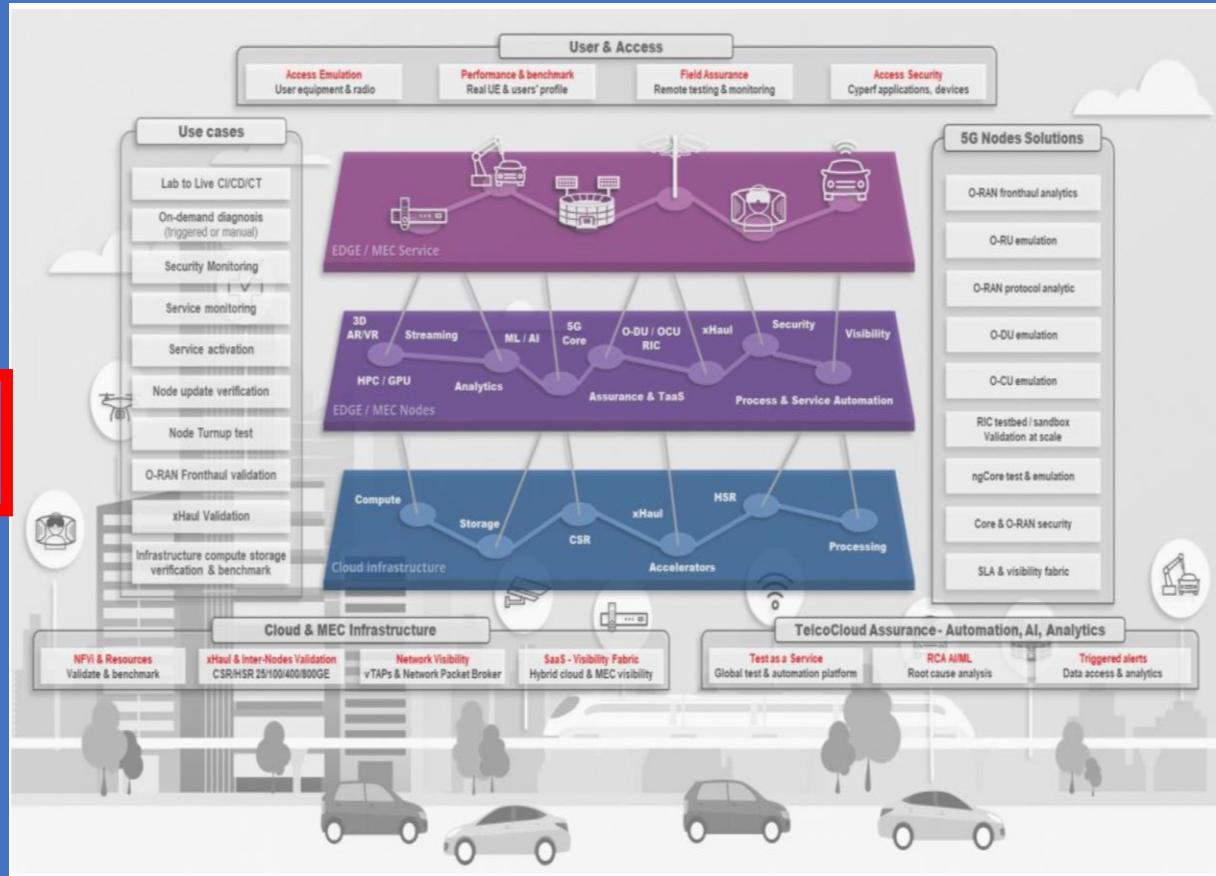


Figure : Telco Edge Cloud, Next-Gen Service Assurance at Scale

The O-RAN WG4 Conformance Test Specification ensures the O-RU's compliance with the O-RAN Fronthaul (**FH**) Standards.

The 3GPP (Test) Specifications requires a full gNB since 3GPP does not recognize the open nature of O-RAN.

3GPP does not separate the Radio from the BaseBand processing Unit (**BBU**) as required by O-RAN. However, it is possible to leverage the *3GPP Transmitter & Receiver (***TRU**) Tests (Chptrs 6 & 7 of 3GPP Specifications) when validating the **O-RAN FH**.

All test waveforms specified by the O-RAN Conformance Test Specification use the same test waveforms used in 3GPP tests.

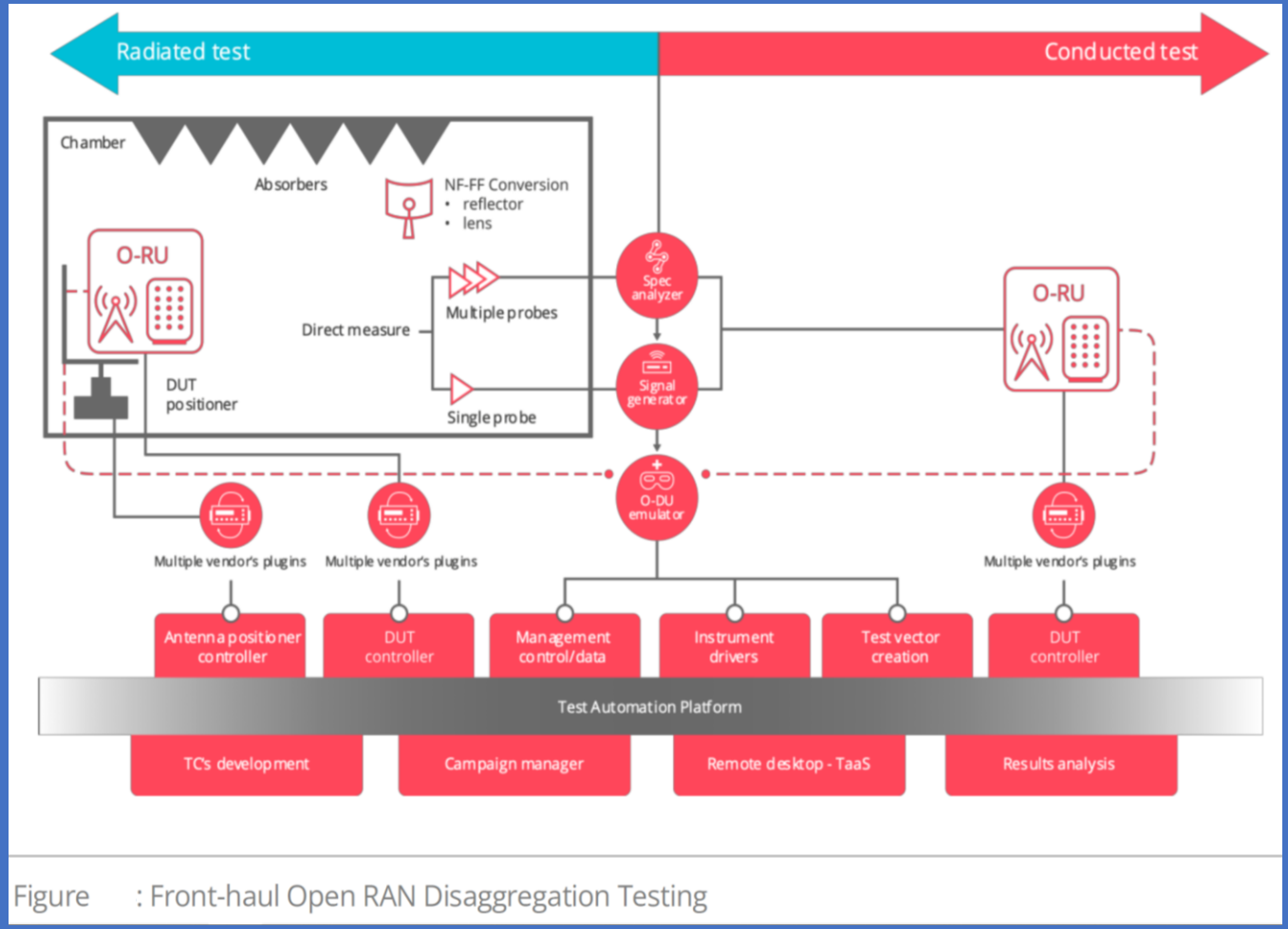


Figure : Front-haul Open RAN Disaggregation Testing

The Test set-up can test a Radio for 3GPP TRU performance and O-RAN conformance. The only difference is that 3GPP expects the tests to run on a **gNB** *that is in test mode*.

The **O-RAN tests the Radio using an O-DU emulator** and does not require a *test mode*.

It is not possible to perform 3GPP Chapter 8 conformance tests using the **O-DU emulator because it requires MAC layer processing, which is not present in the O-DU emulator**.

Autonomous Service Management (enabling Autonomous Networks) tries to put Analysis & Decisions into Machines, so it becomes a “Zero-touch” System for the Operator – more correct: the operator’s touch moves from the Network to the Design of the Automation.

- The Management Systems need to provide Capabilities to enable Autonomy, but also to accelerate and simplify the DevOps process

- System interactions need to be simplified at API level and allow autonomous decisions in requested systems at different levels On the path to full cloudification, hybrid situations will appear.

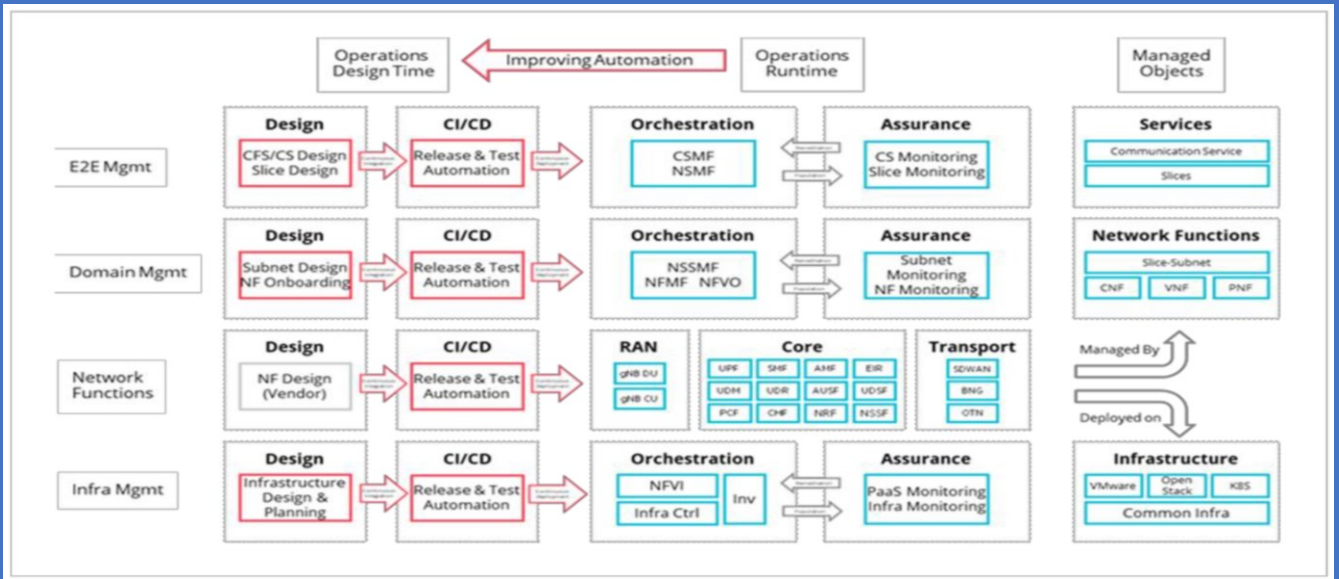


Figure Operations Processes from Design to Runtime

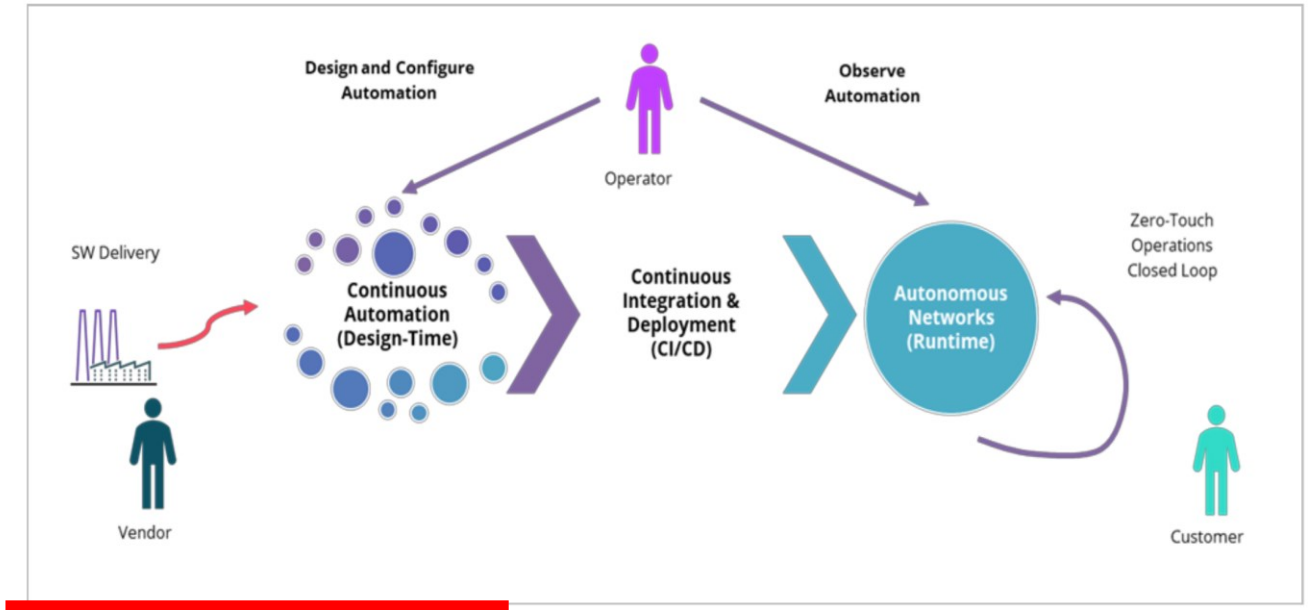


Figure Operations becomes DevOps

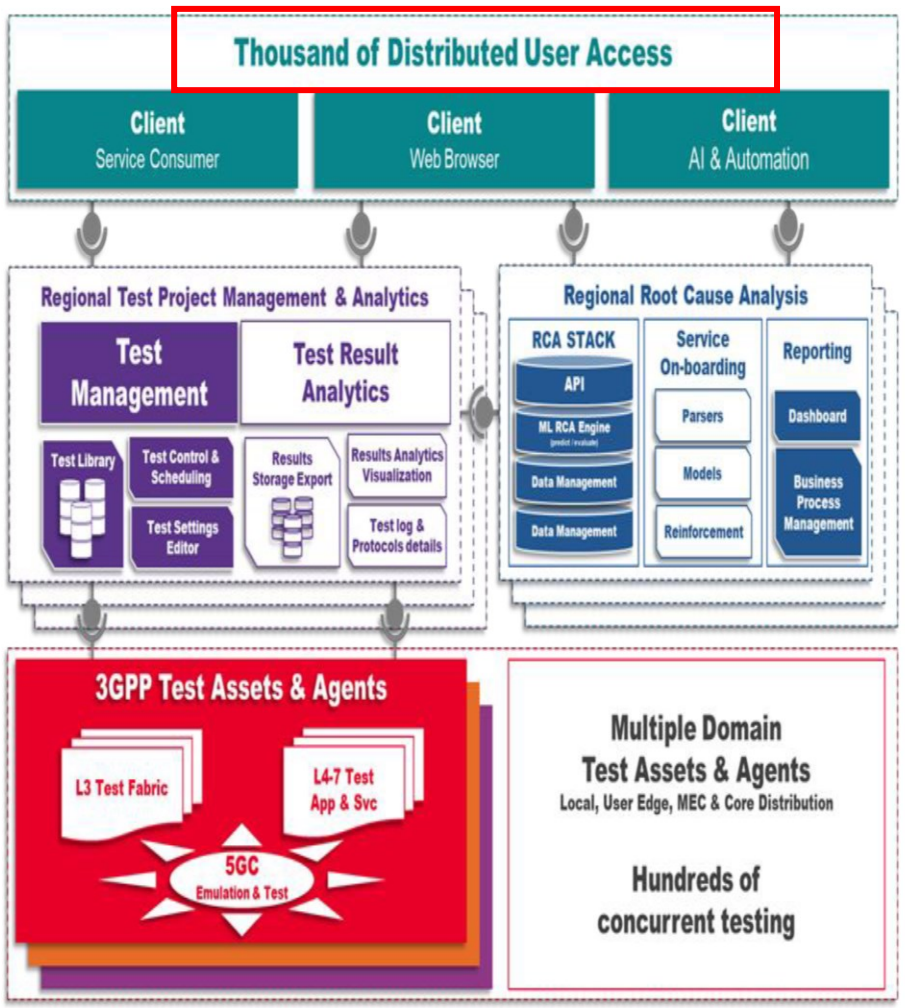
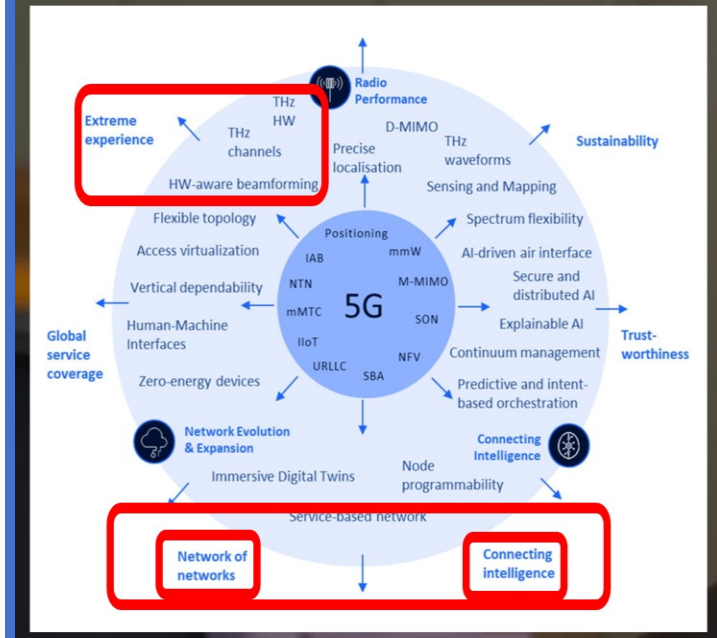


Fig – Nationwide Distributed Cloud based Network Test Bed Orchestration

Ericsson 6G Vision - 1



Magnus Frodigh
Head of Ericsson Research

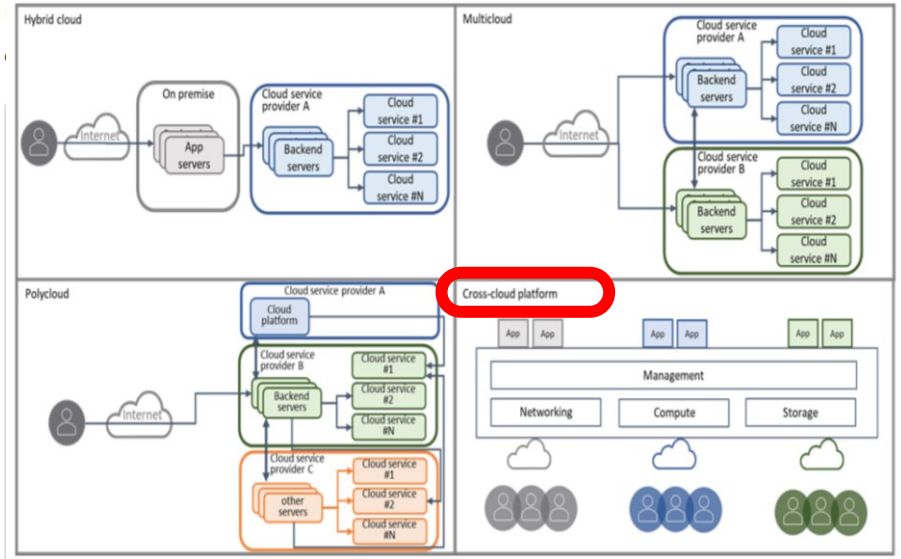
Ref. 5G++ Summit in Drezden, Magnus Frodigh Keynotes, May 2021

TIP Community Labs

TIP Community Labs were created to support TIP's overall mission of working together to develop, test and deploy open, disaggregated, and standards-based solutions that deliver the high quality connectivity that the world needs. A Community Lab is dedicated to TIP projects, but the space and basic equipment are sponsored by individual TIP participant companies. Our Community Labs are a new approach to testing and deploying telecom network infrastructure which encourages the industry to adopt open and collaborative practices for developing new technologies.

It's through the TIP Community Lab framework that TIP participant organizations can more seamlessly collaborate on disaggregated solutions,

Figure multi-cloud deployment models



Community Lab Locations

Madrid, Spain
Sponsored by Telefónica

London, UK
Sponsored by Facebook

Adastral Park, Ipswich, UK
Sponsored by BT

Turin, Italy
Sponsored by TIM

Berlin, Germany
Sponsored by Deutsche Telekom

Manesar, India
Sponsored by Airtel

Tokyo, Japan
Sponsored by KDDI

Menlo Park, California, USA
Sponsored by Facebook

Kansas City, Kansas, USA
Sponsored by Sprint

Louisville, Colorado, USA
Sponsored by CableLabs

São Paulo, Brazil
Sponsored by CPqD

Rio de Janeiro, Brazil
Sponsored by TIM Brazil

Bandung, Indonesia
Sponsored by Telkom University

Santa Rita do Sapucaí, Minas Gerais, Brazil
Sponsored by Instituto Nacional de Telecomunicações

Lima, Peru
Sponsored by Pontifical Catholic University of Peru

Zhudong Township, Taiwan
Sponsored by Industrial Technology Research Institute

Paris, France
Sponsored by Orange

Use case examples

AF-originated API invocation (Gaming)

General

This use case is an example of AF-originated API invocation with a gaming application. In this use case, the end user (also a subscriber of the MNO) allows the AF (game provider's server) to invoke the QoS API (offered by MNO) to modify the QoS of the end user.

Pre-conditions

An end user (also a subscriber of the MNO) is playing a time-sensitive game using a game client application on the end user's UE communicating with a game provider's server. The end user wants to have a high-quality and low-latency communication for better service experience, so the game server (AF or API invoker) tries to invoke the QoS API provided by the 5GC of the MNO to change the end user's QoS according to the request from the game client application on the end user's UE. Changing the QoS may affect the charging rate to the end user, so the game server needs to get authorized to invoke the API by the end user.

Service flows

1. The game server triggers an authorization procedure of the QoS API provider where the MNO subscriber (end user) is asked to confirm whether the game server can invoke QoS API with extra charge.
2. The MNO subscriber (end user) authorizes the game server to apply the QoS change with extra charge.

Post-conditions

After receiving this authorization as per the authorization procedure, the game server invokes the QoS API.

NOTE: This is an example of real-time or near real-time request of authorization, but the game server may also use the authorization information given by the MNO subscriber in the past authorization procedure.

Use case examples

UE-originated API invocation (Location tracking)

General

This use case is an example of UE-originated API invocation with a location tracking application. In this use case, the end user (also a subscriber of the MNO) on UE X allows the end user on UE Y to invoke an API to track the location of the end user on UE X.

Pre-conditions

A tracking application enables the user on UE Y to track the location of a user on UE X. An API Provider AP provides location APIs for the end users on UE X and UE Y, and the tracking application on the UE utilizes the location APIs to provide the tracking functionality.

Ref.: 3GPP 5GAdv, Nov., 2022:

1. List of Equivalent PLMNs, as specified in TS 5G System Architecture Rel. 17, clause 5.18.2a.

5.18.2a PLMN list handling for network sharing

The AMF prepares lists of PLMN IDs suitable as target PLMNs for use at idle mode cell (re)selection and for use at handover and RRC Connection Release with redirection. The AMF:

- provides the UE with the list of PLMNs that the UE shall consider as Equivalent to the serving PLMN
  and
- provides the NG-RAN with a prioritised list of permitted PLMNs. When prioritising these PLMNs, the AMF may consider the following information: HPLMN of the UE, the serving PLMN, a preferred target PLMN (e.g. based on last used EPS PLMN), or the policies of the operator(s).

For a UE registered in an SNPN, the AMF shall not provide a list of equivalent PLMNs to the UE and shall not provide a list of permitted PLMNs to NG-RAN.

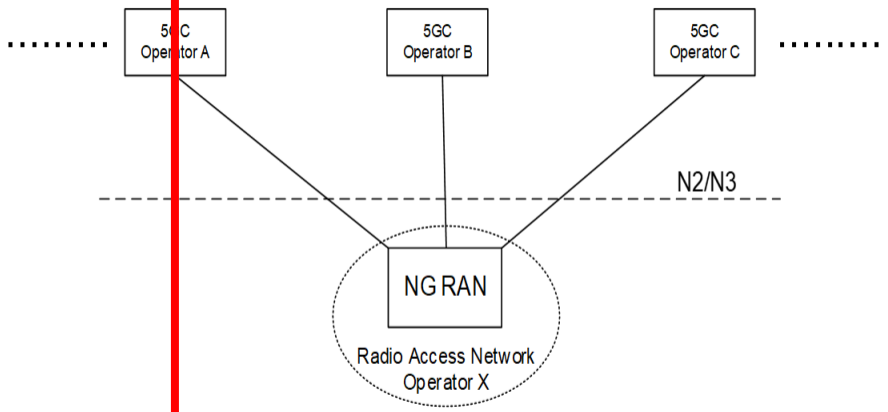


Figure : A 5G Multi-Operator Core Network (5G MOCN) in which multiple CNs are connected to the same NG-RAN

2. The Solution re-use existing Function as specified in clause 5.18.1 of TS 5G System Architecture, Rel. 17, where different combination of PLMN ID and NID can point to the same 5GC.

5.18 Network Sharing

A Network Sharing Architecture shall allow Multiple Participating Operators to share resources of a Single Shared Network according to agreed allocation schemes. The shared network includes a radio access network. The shared resources include radio resources.

The shared network operator allocates shared resources to the participating operators based on their planned and current needs and according to service level agreements.

In this Release of the specification, only the 5G Multi-Operator Core Network (5G MOCN) network sharing architecture, in which only the RAN is shared in 5G System, is supported. 5G MOCN for 5G System, including UE, RAN and AMF, shall support operators' ability to use more than one PLMN ID (i.e. with same or different country code (MCC) some of which is specified in TS NAS for UE in Idle mode and different network codes (MNC)) or combinations of PLMN ID and NID. 5G MOCN supports NG-RAN Sharing with or without multiple Cell Identity broadcast as described in TS NG RAN.

5G MOCN also supports the following sharing scenarios involving non-public networks, i.e.NG-RAN can be shared by any combination of PLMNs, PNI-NPNs (with CAG), and SNPNs (each identified by PLMN ID and NID).

NOTE 1: PNI-NPNs (without CAG) are not explicitly listed above as it does not require additional NG-RAN sharing functionality compared to sharing by one or multiple PLMNs.

In all Non-Public Network sharing scenarios, each Cell Identity … is associated with one (1) of the following Configuration options:

- one or multiple SNPNs;
- one or multiple PNI-NPNs (with CAG); or
- one or multiple PLMNs only.

NOTE 2: This allows the assignment of Multiple Cell Identities to a Cell and also allows the cell identities to be independently assigned, i.e. without need for coordination, by the network sharing partners, between PLMNs and/or non-public networks.

NOTE 3: Different PLMN IDs (or combinations of PLMN ID and NID) can also point to the same 5GC. When same 5GC supports multiple SNPNs (identified by PLMN ID and NID), then they are not used as equivalent SNPNs for a UE.

NOTE 4: There is no standardized mechanism to avoid paging collisions if the same 5G-S-TMSI is allocated to different UEs by different PLMNs or SNPNs of the shared network, as the risk of paging collision is assumed to be very low. If such risk is to be eliminated then PLMNs and SNPNs of the shared network needs to coordinate the value space of the 5G-S-TMSI to differentiate the PLMNs and SNPNs of the shared network.

5G Architecture for Hybrid and Multi-Cloud Environments

The Main Challenges to overcome in a Hybrid & Multi-Cloud Strategy are:

1. Maintaining Portability; 2. Controlling the Total Cost of Ownership (TCO); 3. Optimizing Productivity & Time to Market (TTM).

DevOps – *a Set of Practices* that brings together *SW Development & IT operations* with the Goal of Shortening the Development & Delivery Cycle & increasing SW Quality **- is** often thought of and discussed **in the Context of a Single Company or Organization. The Company usually Develops the SW, Operates it & Provides it as a Service to Customers,** according to the **SW-as-a-Service (SaaS) Model. Within this context**, it is easier to have **Full Control over the Entire Flow**, including **Full Knowledge of the Target Deployment Environment.**

In the **Telecom Space**, by contrast, we typically follow the **"as-a-Product (aaP) Business model**, in which **SW is developed by Network SW Vendors** e.g. as Ericsson (Nokia, Huawei, ZTE) & provided to Communication Service Providers (CSPs) that Deploy & Operate it within their Network. This **Business Model requires the consideration of additional aspects**.

The most important contrasts between the Standard DevOps SaaS Model & the Telecom aaP Model are the **Multiplicity of Deployment Environments & the fact the Network SW Vendor Development Teams cannot know upfront exactly what the Target Environment looks like**.

Although a SaaS Company is likely to Deploy & Manage its SW on two (2) or more different Cloud Environments, **this is inevitable within Telco**, as each CSP creates &/or selects its own Cloud infrastructure (Fig. 1 below).

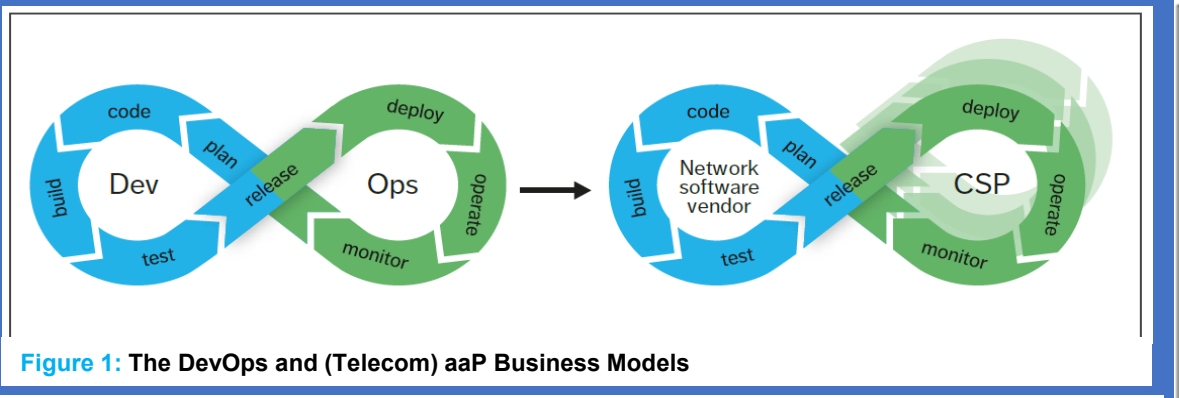


Figure 1: **The DevOps and (Telecom) aaP Business Models**

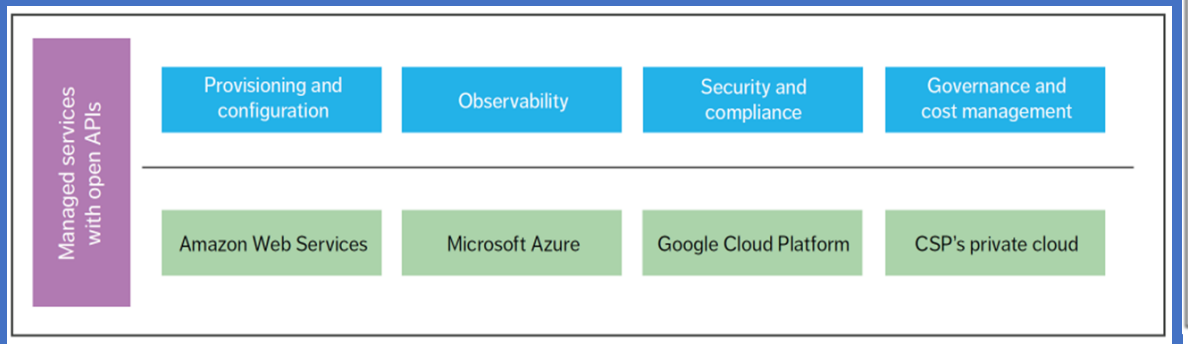


Figure 3: **Key Enablers for a Multi-Cloud Native Application**

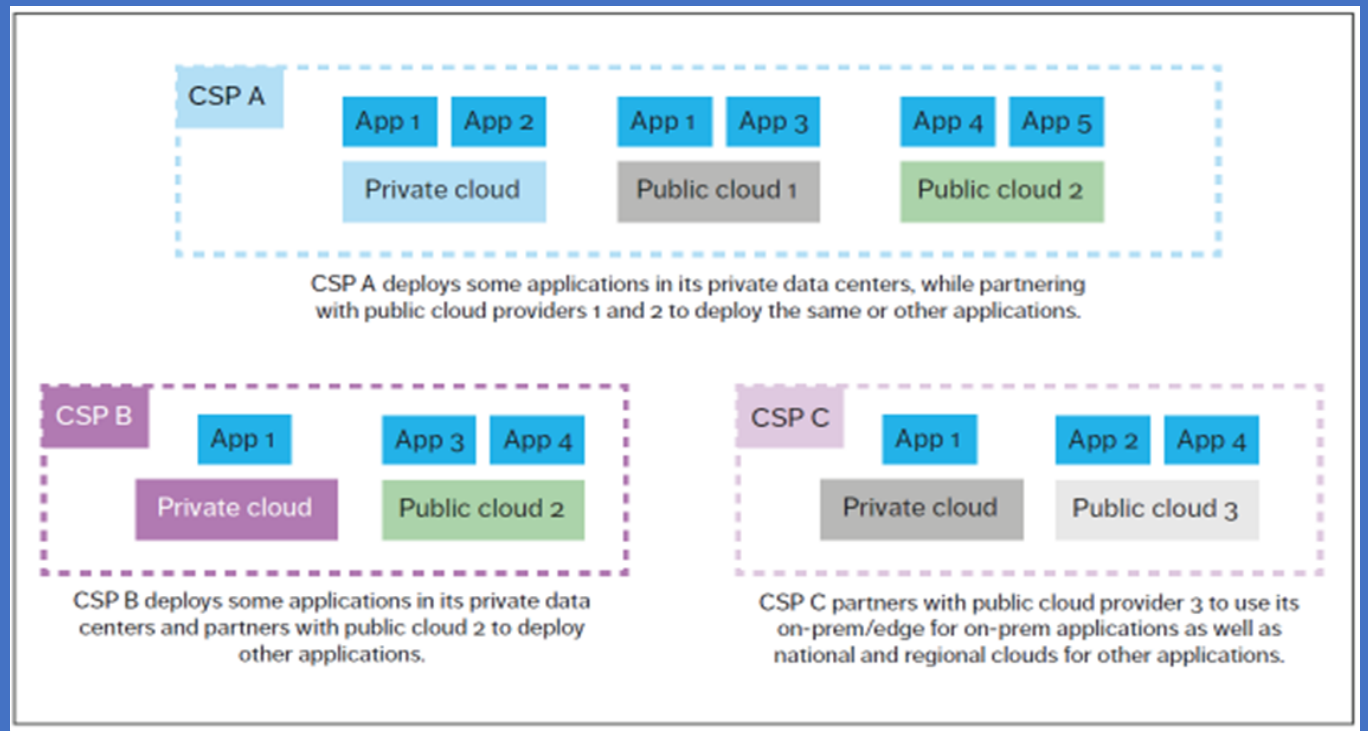


Figure 2: **Examples of Hybrid and Multi-Cloud Deployment Scenarios that Applications must be able to support**

Remarks & Questions?