ODiN - Operating Disaggregated Networks

—

v2.0
www.ngmn.org

WE MAKE BETTER CONNECTIONS

ODIN – OPERATING DISAGGREGATED NETWORKS

by NGMN Alliance

Version:	2.0
Date:	20.09.2022
Document Type:	Final Deliverable (approved)
Confidentiality Class:	P - Public
Project:	ODiN – Operating Disaggregated Networks
Leadership:	Carlos Fernandes (Deutsche Telekom) Javan Erfanian (Bell Canada) Lennart Olaivar (Smart Communications)
Editor / Submitter:	Carlos Fernandes/Javan Erfanian/Lennart Olaivar
Contributors:	Deutsche Telekom, Bell Canada, PLDT Smart, BT, China Mobile, Orange, TIM, TELUS, 1&1, US Cellular, Chunghwa Telecom, Turkcell, Keysight technologies, InterDigital, Hewlett Packard Enterprise, Juniper Networks, Fraunhofer FOKUS
Programme Office:	Chris Hogg (NGMN)
Approved by / Date:	NGMN Board, 20th September 2022

NGMN Alliance e. V.
Großer Hasenpfad 30 • 60598 Frankfurt • Germany
Phone +49 69/9 07 49 98-0 • Fax +49 69/9 07 49 98-41

Contributors:

Osman Akkaya (Turkcell)

Afrim Berisa (Turkcell)

Jason Budloo (BT)

Chiung-Jang Chen (Chunghwa Telecom)

Vincent Danno (Orange)

Lingli Deng (China Mobile)

Javan Erfanian (Bell Canada)

Carlos Fernandes (Deutsche Telekom)

Varun Gowtham (Fraunhofer FOKUS)

Erdal Harput (Turkcell)

Kevin Holley (BT)

Jinri Huang (China Mobile)

Han-Peng Jiang (Chunghwa Telecom)

Wei Jiang (China Mobile)

Chien-Hua Lee (Chunghwa Telecom)

Jian Li (China Mobile)

Ting Li (China Mobile)

Weiyuan Li (China Mobile)

Fabrizio Moggio (TIM)

Weichen Ni (China Mobile)

Joseph Lennart Olaivar (Smart Communications)

Weisen Pan (China Mobile)

Frank Qing (Telus)

Roy Reyes (Smart Communications)

Cheng Choon Si (Singtel)

Arvin Siena (Smart Communications)

Stephan von Malottki (1&1)

Tse-Han Wang (Chunghwa Telecom)

Ming-Yen Wu (Chunghwa Telecom)

Pin-Hua Wu (Chunghwa Telecom)

Han Yan (China Mobile)

Zhiqiang Yu (China Mobile)

Herve Oudin (Keysight technologies)

Sebastian Robitzsch (InterDigital)

Andreas Krichel, (Hewlett Packard Enterprise)

Sridar Gopalaswamy (Hewlett Packard Enterprise)

Graziano Catucci (Hewlett Packard Enterprise)

Andreas Volk (Hewlett Packard Enterprise)

Pavan Kurapati (Juniper Networks)

Andreas Meisinger (Juniper Networks)

Yuhan Zhang (China Mobile)

The information contained in this document represents the current view held by NGMN Alliance e.V. on the issues discussed as of the date of publication. This document is provided "as is" with no warranties whatsoever including any warranty of merchantability, non-infringement, or fitness for any particular purpose. All liability (including liability for infringement of any property rights) relating to the use of information in this document is disclaimed. No license, express or implied, to any intellectual property rights are granted herein. This document is distributed for informational purposes only and is subject to change without notice. Readers should not design products based on this document.

ABSTRACT

Network Disaggregation is one of the mobile telecommunication industry's biggest opportunities while also being a major challenge.

The opportunities coming with Network Disaggregation are appealing: a healthier and more resilient ecosystem and supply chain, lower barriers to market entry for new players enabling increased competition whilst also fostering increased innovation with potentially faster time to market for new products and services.

However, disaggregation presents several new challenges, which operators, along with their suppliers, need to address. To ensure disaggregation can be achieved whilst maintaining service levels it demands, a new way of working is needed, most likely significant additional integration efforts, changes in the operational model to embrace new processes, as well as the adoption of new skills and new tools.

There is also a need to validate whether the benefit of lowering the TCO (Total Cost of Ownership) can be achieved for operators and if it will outweigh the complexities involved.

Each operator will need to eventually make its choices, depending on its strategy, its starting point (e.g. greenfield or brownfield), its geolocation, competition, market, etc. However, there are many topics which need to be analysed and addressed jointly to support global standards, economies of scale and to enable competition.

'Mastering the Route to Disaggregation' is a key strategic focus topic of NGMN. This deliverable - the second white paper in the series - has been developed by NGMN partners - operators, vendors, and system integrators. Whilst the first white paper [1] outlined the opportunities and challenges of network disaggregation, this paper provides a detailed breakdown of how network disaggregation impacts the network, the organisation and the processes that support the planning, deployment, service providing, optimisation and maintenance of the disaggregated network. RAN, Core and Transport disaggregation is covered as well as complementing topics and activities to the network such as Cloudification, Network Automation, DevSecOps and interoperability and performance testing. In covering - in a methodical way - the impacts to both the network and to the operator's organisation, it is hoped that the paper can act as a reference for operators that covers both network disaggregation technology and process issues.

NGMN plans to provide a third white paper to further build on this work and extend it to provide further and more detailed guidance by outlining network disaggregation architectural options and related operating models matched to specific deployment scenarios and operator needs. It is anticipated that 'Operating Disaggregated Networks White Paper 3' would be released in 2023.

CONTENTS

1 BACKGROUND AND INTRODUCTION

1.1 A New Operating Model

Mobile network operators have optimised their way of work, leveraging multiple key criteria when planning, deploying, and running their networks. Criteria such as ease of integration, performance, capacity, security, and resilience are important to ensure, a high-quality customer experience can be delivered using proven processes and procedures that can cope with the multiple technology vendors and technology generations involved.

Digital Transformation observed in several domains and areas (e.g. automated industries, market and societal needs, environment, etc.) has required technologies such as 5G to provide solutions to cope with a growing number of use cases with diverse needs such as requiring increased levels of agility, flexibility, scalability, as well as being responsive and cost / energy efficient. This not only applies to the technology but will also impact the teams, processes, and partnerships needed to bring new solutions and services to market. Ultimately, this digitization points to a great deal of prospects but not without complexities and risks in the absence of sufficient insights, tools, operating models, and end to end alignment.

In parallel, the IT and mobile networking technologies which operators rely on to provide their services are in moving to cloud-based solutions. This has resulted in:

- Separation of functions from underlying hardware; cloudification, and orchestration of containerized functions
- Service-based architecture, stateless functions, exposure, discovery, and consumption of capabilities
- Separation of monolithic services into granular micro-services with open APIs
- Flexible and agile teams combining both software development and IT operations (DevOps), providing continuous integration and delivery (CI/CD) of new features and software; use of open-source automation and orchestration platforms
- Open, interoperable and multi-vendor interfaces, and granular components in a broad ecosystem

Network operators are following these trends while having high expectations of reliability, resiliency, speed, and low latency, among others, essential for telecommunications networks.

As a response to these factors and challenges, the industry continues to drive network disaggregated solutions. As these solutions mature and become increasingly competitive versus the established monolithic integrated ones, operators start to incorporate them in their portfolio. However, this adoption (one can even say transition) of new network capabilities presents several challenges to the established ways of working. Are operators able to use those capabilities without jeopardising their quality of service and operational excellence while at the same time remaining or becoming even more cost effective? Is there a need to adapt the current operating model and how can they decide what, how and when to do it?

1.2 Network Disaggregation - the Transformation Catalyst

Network Disaggregation can be seen as both a consequence of the Digital Transformation as well as an accelerator of that journey, and it can be observed broadly from two perspectives:

- vertical disaggregation, where network functions decouple software from hardware, allowing multiple combinations to be used
- horizontal disaggregation, where established network functions are decomposed into more granular elements and new interfaces are designed and specified

Ultimately, this creates more players, able to develop specific components of the overall architecture, broadening the ecosystem, and leading to an acceleration of innovation. As a consequence, networks are expected to become increasingly agile, flexible, and responsive. All of these factors provide the means to deliver new communication services tailored to the user needs. This leads not only to new business opportunities but also to many different services which needs to be managed and operated. Considering that those services are based on a multi-vendor ecosystem and on new self-caring technologies, it is evident that there is huge impact on operations. This, in a broad sense, involves people, processes, technologies and the ecosystem.

Disaggregation enables this end-to-end, particularly through openness, cloudification and softwarization, providing network features such as:

- Separation of control and user plane, programmability and software-defined networking, including SD-RAN
- Flexibility of the user-plane function, hybrid cloud and edge

- System flexibility, composable core, granular QoS architecture, multiple-access Network slicing

As mentioned above, this leads to potentially significant benefits to performance, user experience, and business opportunities, which will be further detailed. These also leads to the necessity to define and adopt a new operating model, as the deployment and leveraging of such capabilities is deeply intertwined with the way operators are able to control and exploit them.

Since 2021, NGMN has identified 'Mastering the route to Disaggregation' as one of its strategic imperatives creating a new programme named "ODiN" (short for Operating Disaggregated Networks) to address the issue of how to successfully plan, deploy and manage disaggregated networks. The ODiN programme will provide a solid and meaningful guide to operators, industry partners and telecommunication ecosystem players in general on how to successfully execute this journey. This is the second document from the ODiN programme.

2 EXPECTED BENEFITS OF NETWORK DISAGGREGATION

The agility and flexibility of disaggregated networks has the potential to provide many benefits, as identified below. It is also expected that a parallel and equal improvement in how operators can operate those networks will depend on the native tools and best practices that come within a disaggregated and cloudified ecosystem. Many of these aspects have an impact on the operating model in terms of for example new technologies to master or new processes to set up to take full advantage of the provided benefits.

2.1 Adoption Flexibility

2.1.1 More Solution Choices and Flexibility

Disaggregation further enables a multi-vendor environment. Vendors can focus on a subset of the whole pack of solutions which once was expected to be provided by a single vendor. This in turn will allow vendors to specialize on specific products and allocate their resources on those. It is expected this will provide more focus and more competitive products for similar functionality. When this is replicated by more companies, there will be more competing brands and products in the telecommunication market. This has not happened in the past to such extent.

Now, with lowered entrance barriers and, consequently, more suppliers in the market, we expect there will be more choices for the operators to select from. This will also enable them to mix and match based on their needs (best of breed approach). Operators for example can now source a Radio Unit (RU) from a different vendor than those of a Distributed Unit (DU) and Centralized Unit (CU). They could choose the best RU, DU or CU and they could do more combinations for each area or cluster type. The same way with Core, operators can now source the hardware from a vendor different than their software or functions vendor. Some operators who have internal Research and Development Teams and are engaged in industry testing and development initiatives may be able to develop solutions faster and customize solutions based on their needs. Bottom line is, it is expected that users get more value for their subscription as disaggregation allows more opportunities to make operator networks more efficient with improved performance.

One of the many advantages of disaggregation is the separation of software from hardware. This is actually the key factor that allows more flexibility because hardware and software are now developed separately. This allows more innovations on both.
Aside from allowing more developments in software, operators will also have more choices or options in terms of hardware. Since COTS (Commercial Off-The-Shelf) can now be used, IT branded hardware could also be used for telecommunication applications. This should enable operators to acquire the best, latest and most technologically advanced and efficient hardware. The latest technologies and functionalities could then easily be deployed using software upgrades. It is expected this will also lead to a faster time to market.

2.1.2 Supply Chain Benefits

On one hand, disaggregation adds the possibility and capacity to ensure operators can access a more diverse supply chain, sourcing components from multiple vendors and multiple geographies and therefore allowing for more resilient networks and processes.

On the other hand, global operators could have more opportunities to localize the supply, giving opportunities to competent local companies. This may encourage more local suppliers to develop solutions and join the telecommunication business even if they are from other industries.

2.2 Innovation Acceleration

2.2.1 Better Functionality, Features and Solutions

Disaggregating or breaking the network components into more parts and opening the interfaces will allow more companies, including disruptive and emerging ones, to develop solutions as well as hardware and software products. This will allow faster development of technology as more minds, teams and companies are working towards one goal – improving solutions, customer experience, and making networks more efficient.

Disaggregation will also allow for more and better customization of products based on the specific needs of each operator. Operators are able to buy only the features and functionalities that they need. It is expected that this will translate to a more efficient solution.

2.2.2 Better Performance, Improved User Experience

Increased innovation in each part of the network is expected to cause better KPIs and improve performance in mobile networks. These developments will allow each network component to contribute to a better performing system and will ultimately lead to better end-user experience and improved services.

2.2.3 Speed of Change

Increased competition due to lowered barriers to market entry will also provide incentives to vendors who will develop better and more efficient products that in effect develops the market as a whole. This will benefit the operators even more as it is expected that technology will keep on getting better in a shorter span of time. The level of flexibility and agility, which affects the speed of change, will be dependent upon the development of each vendor. It is assumed that some will be more flexible, and some will be less flexible. With this, some will be capable of being faster than others. At any rate, changes to the network will be faster compared to today. This will allow operators to scale their networks better based on their needs.

Due to more granularity and flexibility of solutions, operators will be able to do expansions, upgrades or any changes with less effort and faster. By disaggregating the network, operators can better manage network demand by scaling up network functions as needed. Upgrades and maintenance can also be better managed as operators can upgrade each part singularly as opposed to upgrading the entire network. This greatly improves the life cycle of network services and time-to-market when providing new services to new customers.

2.3 Cost efficiency

2.3.1 Lower Cost Attributed to Improved Competition

One of the promises of disaggregation and open interfaces is lowering cost, with expectations - based on the experiences of one greenfield operator - for specific network domains such as RAN to reach 30% to 40% lower CAPEX and OPEX [2]. As networks continue to expand, develop, and transform, operators need to invest significantly. Operators are simultaneously trying to ensure cost efficiency and disaggregation is the best candidate solution to fulfil that.

2.3.2 Assumed cost gains attributed to improved Resource Efficiency

Disaggregation allows operators to centralize functions and control. This enables better efficiency by leveraging on pooling gains which could also translate to lower CAPEX and maintenance cost. Since software and functionalities are disaggregated, they could be installed or housed on shared hardware. With this, operators could implement a common hardware or infrastructure from RAN, Edge to Core in order to simplify engineering, implementation and operations. It is assumed this leads to reduced costs by leveraging on economies of scale.

2.4 Openness for Further Innovation in Automation and AI Platform

By disaggregating the business capabilities and control capabilities in the network, common capabilities are achieved and provided in a “platform” way. A unified AI platform is built, where specific services could be called through network elements. The unified AI platform can provide intelligent application R&D with infrastructure services including centralized computing power, algorithm frameworks and general AI capabilities, realizing one-stop management of network intelligent application R&D, operation and maintenance.

After disaggregation of the network’s business capabilities and intelligent capabilities, independent R&D can be carried out based on the AI platform, promoting R&D efficiency improvement and cost reduction.

3 CONTEXT, CURRENT CHALLENGES AND NEEDS OBSERVED BY THE OPERATORS

Benefits outlined in the previous section will not be achieved unless the industry manages to overcome a number of challenges.

3.1 Impacts to the Network

Making solutions more flexible and scalable has an inherent challenge which is complexity. As hardware and software are separated, as well as their individual development, the overall solution becomes more complex because there are more and more solutions available that need to be able to work together. As each company developing different parts has different roadmaps, the complexity that it will bring will add to the challenge of ensuring compatibility and interoperability between different vendors' solutions. This will have significant impacts on the options operators have for managing this complexity. This compares to the present situation where the operator manages this complexity themselves or (more often) appoints a single or small number of system integrators or vendors to have oversight of the solution. The system integrator(s)/vendor(s) then work closely with the other partners in the project to manage the complexity.

3.1.1 Interoperability and compatibility

The move to a disaggregated network solution needs to go hand in hand with the assurance of interoperability and compatibility. Operators must not find themselves in a situation where vendors are pointing at each other on how to integrate or problem solve when the customer experience and brand value is on the line. This is the part where operators need to be assured as this will impact network quality, customer experience, time to implement, optimization and maintenance. In having multiple and many suppliers, one of the major concerns is interoperability.

Interoperability issues can only increase in the near term with the longer-term aim to reduce these issues.

Currently, most if not all, traditional partnership model vendors who are complying to 3GPP and other telecommunication standards are also performing interoperability tests with each other. Yet, operators are still encountering interoperability issues especially on inter domain connections or interfaces. This is for instance caused by each vendor applying their own interpretation of the standards. It is anticipated that this will escalate further, rather than improve, when disaggregation is introduced into the networks since there will be more types of solutions and vendors to connect. Each of these solutions may have different and independent developers, roadmaps and interpretations of the standards leading to different implementations. They also have different timelines in terms of development, e.g., typically software has a faster development cycle than hardware. Therefore, it has to be expected that compatibility and interoperability will be a huge challenge.

3.1.2 Security

Operators must continue to ensure that their networks and services are secure. This is even more important when mobile networks are increasingly becoming critical national infrastructure – providing services to a wide range of industries. Although operators and vendors have a long-established history of managing the security of mobile networks, the systems and processes used are likely to come under additional strain as the number of vendors, functions, and interfaces in a typical mobile network increase.

For example, as more components and functionalities are introduced, the network potentially becomes vulnerable as there are more integration points. This could arise in the open interfaces in any network domain (RAN, Core, Transport), open-source software and off the shelf solutions. Functional splits and Edge computing could also contribute to wider physical attacks.

Disaggregation, if hosting software to the public cloud, could also introduce more vulnerabilities and attacks as the network tends to be more exposed to the public domain.

Different software and different hardware might cause new vulnerabilities as they are developed separately. Each of these vendors or companies have different experiences towards attacks. This is where consolidated monitoring becomes essential. Each of the software and hardware needs to be fully monitored to detect any possible intrusion.

Multiple patches and updates could also introduce incompatibility and security risks across different versions. The need to maintain backwards compatibility and have a strict regression testing regime will be key to maintain security.

3.2 Impacts to the Organization and Processes

3.2.1 Impact to Procurement Processes

Disaggregation will have a huge impact in the supply chain and procurement strategies and processes. The number of suppliers will increase, and this may mean that the procurement team needs to expand to be able to handle more suppliers.

Though disaggregation brings a huge benefit by expanding the telecommunication ecosystem, it will also cause complexity to the system and processes, as more vendors would need to be managed. Different vendors/suppliers have different SLA's, hence the variables in purchase and delivery will tend to broaden. More bricks lead to bigger challenges - both technical and legal/contractual.

Responsibility delineation is also expected to be a huge challenge to the supply chain. Procurement teams may encounter difficulties in identifying who should be responsible for a specific purchase, warranty, operations, etc.

More and smaller components mean more parties (either new players, or existing players that were masked by integrators/vendors in the past) to deal with. There will be new software components which again means more parties to cooperate with. New players (including possibly start-ups) will impact our current processes/habits to interact with the industry players.

3.2.2 Newly Added System Integration Processes

3.2.2.1 Changes in the Organization and Processes

The huge impact and changes brought about by disaggregation will cause an impact to the organisation of each of the operators. System integration is one of the biggest challenges in adopting disaggregation, since this was not typically part of the organisation during the traditional or legacy days. So, the operators would need to either build their own team of system integrators or tap an external entity or company that will do system integration for them. Both options will entail huge effort, adjustments, changes in the organisation, and potentially additional cost.

Today, almost all the system integration work is being done by the vendors of the respective equipment. Typically, operators' biggest responsibility is interfacing and understanding the needs of the business, translating them to technical solutions, planning the implementation, decision making and governance. The rest is mostly passed on to the vendor for execution –

from detailed design, to implementation, optimisation, and maintenance. Now that with disaggregation networks are broken into smaller parts, the responsibility of bringing everything together cannot be passed on anymore to a single vendor because of this new multi-vendor environment. There will no longer be a single vendor taking care of the overall solution and its management. The responsibility of successful integration will now be on the shoulders of the operator. If the operator decides to build its internal system integration team, it will have to make either major rearrangements to re-purpose manpower or hire significant resources to fill the gaps. There will also be a massive change and adjustments in the processes of the organisation. Coming from a set-up where much is done by the vendor, to the operator playing a bigger role in terms of putting everything together, from design to operations and management, will entail change at all organisational levels of the operator.

Integration is said to be a huge challenge for the operators. On the other hand, it will also be challenging to the vendors. They would need to be more conscious of what the other vendors are doing and developing as they need to interoperate. This fact would need to be considered also by procurement to ensure nothing is missed in the process or purchase.

3.2.2.2 Many Components and Companies to Deal With

At the moment, operators are talking to two to four vendors per domain. With disaggregation, operators could be talking to more than five for RAN alone. That could even go higher if they choose to be more flexible and choose more vendors. That will add to the complexity, not only to the solution, but also to the organisation and processes of the company. Firstly, it is assumed that operators need to add more manpower to handle such vast number of vendors. Secondly, operators need to adjust their procurement processes and strategies to adopt to more vendors supplying the requirements. The separation of software and hardware alone will instantly add to the complexity as operators are historically used to buying both software and hardware from the same vendor. Having them separate would mean there will be separate services for each. This may not only add to the cost but make things more difficult as operators will talk to more people and have more interfaces.

The challenge will truly come during implementation, troubleshooting and problem resolution. Operators would need to talk to at least two entities for a single node.

3.2.3 Potential Additional Cost

3.2.3.1 Integration Cost

System integration of different parts of each domain is normally not part of what operators spend on at the moment, as the same vendor is supplying both the hardware and the software, and most solutions are integrated. There is no integration needed because software is already integrated in the hardware. The beauty of the current set-up is its simplicity.
With disaggregation, since software is separated from hardware and functions are separated, operators would need to have an integration team that will combine or install the software to the hardware making sure of its compatibility, facilitate proper operation of the equipment and proper interoperation of all network functions as well as ensure functionalities work together as a whole. This will either need a separate vendor or a formation of a new team within the company. This will translate to additional effort and potentially additional cost.

With all the additional efforts and costs, it is imperative that the benefits outweigh the challenges. The expected cost effectiveness and the new business possibilities enabled by the new ecosystem, attributed to the separation of hardware and software, should offset the operational changes that need to be made. Cost reduction needs to cover for the needed offset and still maintain a worthwhile net decrease in TCO. All the efforts should be compensated in the long term. Otherwise, the decision making will be very hard as everything needs to be justified given that the current set-up and system is working well. There is a saying that goes "Do not fix something that is not broken". The current system and solutions are not broken but are not flexible enough to sustain new possibilities and services of the upcoming years. Disaggregation is there because of the industry's desire to make things better and more efficient.

3.2.4 Need for training and competency development

Training and competency development are efforts that are needed in disaggregation. Most of the engineers are more familiar with integrated solutions as they worked on them for many years. Disaggregation is new to most of the engineers in the network. This is why there needs to be proper education within the organization and industry in order for the manpower to be better equipped to operate the new network.

If operators decide to build a new integration team within their company, operators would need to spend time and budget to build the competency and expertise of that team. On the other hand, if operators decide to outsource system integration, they will still need to develop the competency of manpower who will govern external SI.

3.2.5 Shift of Scope and Responsibilities

3.2.5.1 Who is responsible?

The breaking of a whole system into parts raises the question “Who is responsible?”. This will be highlighted especially when there are network issues or collective customer complaints where there is a problem in the network that hasn’t been identified yet.

In the traditional process, a single vendor would conduct tracing of the whole network and identification of problem and isolation is easier because that vendor has all the counters and measurements for each part of the network, therefore it is easier to identify which part of the network is causing problems. Since that vendor is providing all the parts and solutions to the whole system, only one entity or company is responsible. Therefore, escalation and troubleshooting is simpler.

With disaggregation, even in one node, several vendors might be involved. For example in a gNodeB, one vendor might be supplying hardware for the CU, another for the DU and another for the software of both or one of these functions. Then another vendor is supplying the RU and another for the antenna. If say that gNode B or site is having performance issues, it is not straight forward to tell which component is problematic. Is it hardware or is it software? Or is it the combination of the two that causes the trouble? Even when the problem is identified, the escalation and troubleshooting won’t be as easy as several teams from different parties may need to cooperate to solve the issue.

Let’s take for example an extreme case in traditional solution having only one vendor for all the RAN components in the network. Since that single vendor handles and is responsible for the RAN of the whole network, it will have a large support system in terms of resources, tools, manpower, technical support, ticketing system that escalates all the way to R&D and the main office. In that case, any issue in the network will be identified, troubleshooted and resolved by that single vendor who might have significant resources that could respond to an issue anywhere in the network, quickly. On the other hand, when network is disaggregated and the components of the network are handled by different vendors, each of those vendors would most likely have less or fewer resource supporting the networks. This might cause them to respond slower. This goes back to the bottom line and question again of “Who is responsible?”.

To resolve this, there should be a central team that oversees and monitors all components. Then again, building and equipping this team won’t be as easy as there are many different components in the network with different brands. That would mean additional effort as the team should be capable of monitoring and understanding all the components in the network. This again would imply effort on training and competency development and translate to OPEX.

One of the common questions is when there are major issues in the RAN network, who would identify if the issue is caused by the software or the hardware? There should be a way or a tool that could easily pinpoint that. Now the question arise on who will develop that tool and if that tool supports any software or hardware vendor, given the vastness of the ecosystem that is continuously growing until now?

Troubleshooting will eventually be more complex when networks get disaggregated. With that, it can be expected that vendors can differentiate themselves through support offerings.

3.2.5.2 Software Asset Management (SAM)

Dealing with software components will require proper licensing and asset management: The choice of licensing model should be adjusted to the use cases. Concerning the duration of the rights of use, the "rental" model (i.e., subscription) could be considered with caution to avoid explosion of OPEX and perpetual rights should be preferred to optimise investments. On the other hand, as cloud services are generally monetised based on their usage, it is logical to reflect this model on the licenses of network functions, which will have to be based on "Pay-as-you-Use" models. This means that usage rights must be quantified based on usage metrics related to the value generated by the network function.

- The potential impact of a significant increase in operational costs related to the SAM process throughout the life cycle of Virtualised Network Function (VNF)/ Cloud-Native Network Function (CNF), from procurement to decommissioning, could be mitigated by an adapted tooling approach, to guarantee usage compliance while controlling operational costs. Automation of SAM processes is therefore essential, just like other business processes of the operator. This automation is only economically feasible if this process can be applied in a unified manner to all network software and regardless of the suppliers. This is best possible if this is based on standards.

- The purchase of licenses adapted to the usage implies being able to estimate this usage at a certain time in the future. This can be done by observing the evolution of current usage, but this is not sufficient. Network functions can be viewed as being “organized/deployed” as “stacks” (in a “client/server” or “vertical” type of association) and “service chains” (i.e., in a “horizontal” type of association). To simplify, it can be said that it is useless to buy usage rights for a function if the usage rights of the one(s) on which that function relies would not allow to exploit them. On the other hand, it is useless to buy usage rights for a function that is part of a chain of functions (Network Service), if the usage rights of one of the functions in the chain would not allow to exploit them. It is therefore considered necessary to be able to consider the management of usage rights for network functions in a comprehensive way.

4 DISAGGREGATION IMPACT TO NETWORK ACTIVITIES

This section introduces the overall organisation of the network operation, and further analyses the potential impact to the existing operation and organisation from the disaggregated activities in various domains.

4.1 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.

In the context of our focus on operational models in this document, the following analysis is limited to resource and service operation layers only.

4.2 Operational Processes

Each operation layer includes several vertical operational processes including: planning, deployment, maintenance, optimisation, and service providing. The following technical-agnostic descriptions are applicable:

- **Planning**
  Based on market and product portfolio strategy and forecasts, research & analysis is performed to determine service and resource targets as well as strategies. This includes expansions of the existing service and resource capabilities and the identification of new service and resource capabilities, service and resource support levels and approaches

required, service and resource design elements to be developed, as well as service and resource cost parameters and targets and defining the way that new or enhanced infrastructure may be deployed. These processes also define the policies relating to technical services or resource and their implementation.

- **Deployment**
  Based on demand, plan and deliver the total capabilities required to deliver changes to service, as necessary. This may involve integration of capabilities delivered from within the MNO, and capabilities delivered from an external party.
  This also involves the use of capability definition or requirements to deploy new and/or enhanced technologies and associated resources, ensuring that network, application and computing resources are deployed according to the plans set. It also entails delivering the physical resource capabilities necessary for the ongoing operations and ensuring the basis on which all resources and services will be built.

- **Maintenance**
  Managing Service and Resource infrastructure, ensuring that the appropriate service capacity, application, computing, and network resources are available and ready to support Fulfilment, Assurance and Billing processes in instantiating and managing service and resource instances, and for monitoring and reporting on the capabilities and costs.

- **Optimisation**
  Managing, tracking, monitoring, analysing, improving and reporting on the performance of specific services and resources. Collect and/or distribute management information and data records between resource and service instances and other operator IT processes.

- **Service providing**
  Manage problems associated with specific services. The objective of these processes is to respond immediately to reported service problems or failures to minimize their effects on customers, and to invoke the restoration of the service, or provide an alternate service as soon as possible.

4.3 Disaggregation activities and impacts to operating a network

4.3.1 RAN disaggregation

4.3.1.1 RAN Disaggregation activities

RAN is a challenging and complex domain to disaggregate due to the legacy and the number of moving parts within the system. RAN disaggregation will involve a broad and diverse ecosystem providing flexibility and choice.

Disaggregation considerations in RAN

There are a number of considerations with respect to disaggregation in RAN such as:

a) Operators need to maximize their investment on Distributed RAN (DRAN) since legacy technologies (4G, 3G, 2G), and even 5G, were deployed using DRAN. Transitioning to virtualised RAN (vRAN) or Open RAN (O-RAN) would entail a total change in architecture and cause major adjustments in operators organisation, processes, planning, dimensioning and more. There are still many unknowns that translate to challenges, particularly for brownfield operators. There may also be factors that are unseen or not visible at the moment that may cause major impact in the future once disaggregation in the RAN starts and matures.

b) Transitioning to Centralised Unit – Distributed Unit – Radio Unit (CU-DU-RU) in the Radio Access Network and (in the transport network) to Front Haul-Mid Haul-Back Haul (FH-MH-BH) will greatly impact transport configurations and topology as well as requirements on bandwidth and latency. This is one of the most important considerations during disaggregation. Over the years, most operators have simplified their architecture so as to become more efficient and simpler in terms of operations, yet disaggregation impacts this trend. Disaggregation may require transport reconfigurations with potentially significant and costly effort. In the past, 1G was enough for back-haul. Now, the minimum has become 10G and the ideal is 100G. This is because of the huge bandwidth requirement of 5G especially in the millimetre wave band and even in sub 6 GHz band. Along with that, strict latency requirements will now need to be considered for front haul. This will again require huge cost and reconfiguration of transport. So, there is a risk the savings from RAN may be challenged by the transport cost.

c) The dimensioning principle will become totally different. As complex as the technologies from 3G to 5G have been, operators did manage to simplify the dimensioning in order to be flexible especially in budgeting and allocating resources. With vRAN/O-RAN, operators will need to dimension even the smaller parts of the hardware such as the processors/compute and storage.

Despite these many challenges, if RAN disaggregation proves to be beneficial in terms of performance, customer experience, better services, energy efficiency, and lower costs, it will have a huge positive impact to the network and to operators' businesses.

RAN Function Disaggregation (Horizontal Disaggregation)

In RAN function disaggregation or Horizontal disaggregation, the functions of the BBU, where the processing of baseband signals and intelligence are done, is split into CU and DU. This divided the RAN architecture from BBU-RU to CU-DU-RU. The split of functions allows the operators deployment flexibility in a way that each function could be positioned in different parts of the network. This means that, aside from separating the functions, the hardware can also be separated. For example, DU and CU can now be placed either on site or further away, e.g. at a Data Centre. Another option is to place CU and DU separately closer or farther from the site. The positioning of these functions will impact or potentially make the deployment cost become lower. If it is positioned in a way that the DU or CU functions are centralized, cost will potentially decrease since the resources are pooled and more sites are sharing the same hardware and software. This is called pooling gains for which its notable gains need to be validated. Different positions require different transport requirements in terms of bandwidth and latency. This would require a conscious decision by the operator on which topology or configuration to use as one would be less expensive in the RAN but might cause higher cost in the transport. A balance of this would be required to achieve the most cost effective and efficient solution.

A distinct benefit of horizontal disaggregation is flexibility, choice and diversity of providers to maximize performance, capabilities and efficiencies. Operators now have the liberty to choose different vendors for CU, DU and RU thereby giving flexibility in terms of solution and costing. Doing such may come with challenges to be addressed, in terms of visibility, management, and integration, among others.

Introduction of RAN Intelligence

Another advantage of disaggregation is that it enables operators to easily inject intelligence into the RAN network. ORAN developed RAN Intelligent Controller (RIC) which incorporates Artificial Intelligence (AI) and Machine Learning (ML) for dynamic, intelligent, and predictive allocation, policy, management, optimization, and operation.

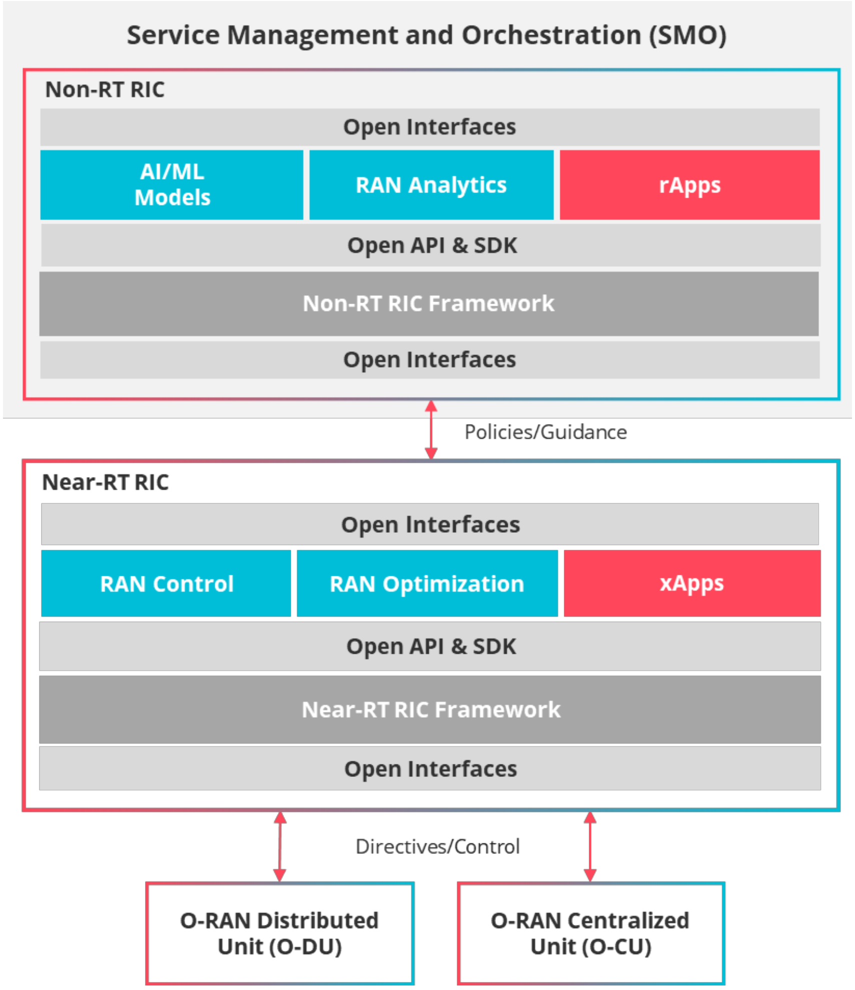


Figure 4-1: RAN Intelligence

As a software-defined platform, the RIC brings intelligence, programmability, and extensibility to radio access networks. RIC uses AI and machine learning (AI/ML) applications that automate RAN operations and support innovative use cases. With the RIC, network operators have a platform to deliver new functions and user experiences with greater agility and ease.

RIC comes in 2 forms - Non-real time RIC and Near-real time RIC. Non-real time RIC integrates intelligence into RAN system design in performing network management tasks and work for control loops over 1 second. Near-real time RIC controls CUs and DUs and performs network improvement and optimization decisions that happens between 10 milli seconds to 1 second. In addition, there are specialized applications called rApps and xApps.
The Non-RT RIC, expected to run in a cloud, enables greater-than-one-second control and policy guidance over the RAN elements and their resources through rApps. It also enables AI/ML capabilities for the RAN. The Near-RT RIC is responsible for fast loop control of the RAN

network functions. It provides less-than-one-second control over the RAN nodes and resources which are driven by the non-real-time RIC. It can host and deploy specialized xApps. The Non-RT RIC communicates with the Near-RT RIC over the A1 interface to provide policy-based guidance to the xApps running on the Near-RT RIC to optimize RAN behaviour, such as for capacity, customer-specific service levels, or energy efficiency. The Non-RT RIC uses long-term network data, such as performance metrics as well as enrichment data from external applications to train and generate AI/ML-driven applications. The RIC platform is based on a cloud-native microservices architecture and needs to be fully compliant with the O-RAN specifications and interfaces. It needs to support both an open API and a software development kit (SDK) for integration with any third-party O-RAN-compliant xApps or rApps, giving network operators greater flexibility and choice of suppliers.

rApps and xApps are the foundation for innovation and agility in the RAN. These specialized, AI-driven applications, allow operators to enable new business models, personalize the service experience, and optimize CapEx and OpEx. Key use cases include RAN slice SLA assurance, tenant- and slice-aware admission control, traffic steering, energy efficiency, M-MIMO optimization, and quality of experience (QoE) optimization.

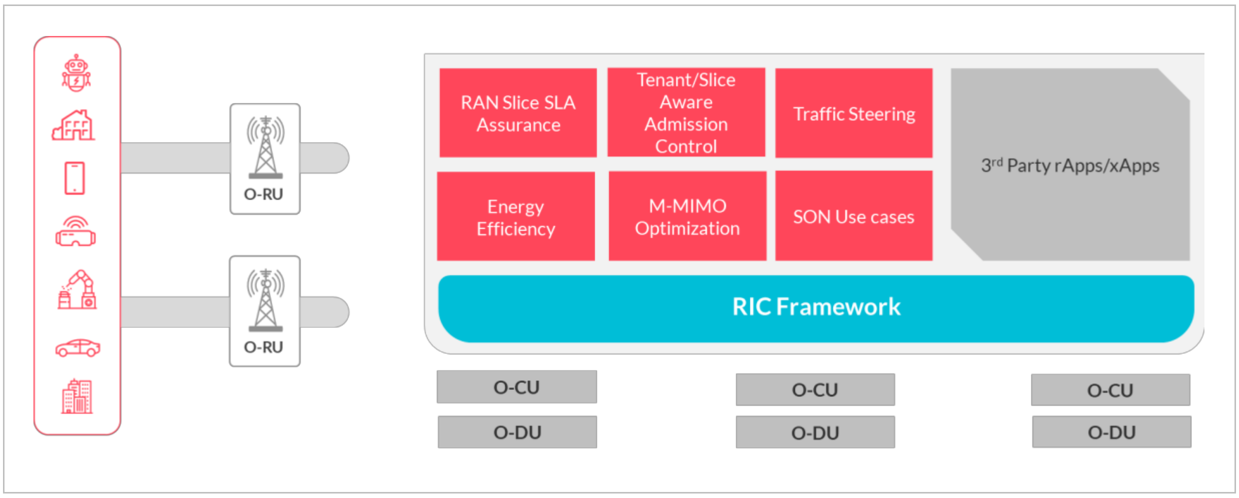


Figure 4-2: RIC Framework

As mentioned above, rApps are running on the Non-RT RIC since they are less low latency critical. Examples for rAPP use are:

- Network deployment use-cases
- Network automation use-cases
- Network optimization use-case

- Network healing use-cases

xApps are addressing use cases which are more time critical, not necessarily but very often they work in a combination between xApps on Near-RT RIC with the support of rApps from the non-RT RIC.

Some example use-cases, which are using a combination of xApps and rApps are:

- Network Slicing—Network slicing is a key advancement in 5G networks, with end-to-end connectivity and data processing tailored to specific customer requirements or workloads. The service levels are guaranteed and must be continuously assured across the delivery chain. rApps/xApps can continuously monitor each slice and collect slice-specific performance metrics. If the application detects a SLA violation, it can immediately initiate corrective action by making the appropriate configuration changes to the centralized and distributed units (CUs and DUs) and updating the policy accordingly. The changes are monitored and confirmed as meeting the specified service levels.
- Tenant- and Slice-Aware Admission Control—This application allows for real-time tracking and enforcement of radio resources such as packed data units (PDUs) per slice, and user equipment per slice. This use case is required to provide priority services for hospitals, schools, public safety, and other high priority users to ensure that communications are delivered with efficiency and predictability.
- Steering—Traffic steering allows operators to meet capacity demands while avoiding additional capital investments. The RIC and the associated apps can monitor the dynamically changing network load, using AI/ML-based steering algorithms to distribute the load to different frequencies within the same base station, to neighbouring base stations, or even to different radio access technologies, resulting in efficient utilization of operator resources.
- Energy Efficiency—AI-driven predictions and controls can be used to optimize energy efficiency of the RAN, switching off antennas as needed to increase energy efficiency. Insight into traffic, coverage, interference, and other factors can also be factored in to identify long-term trends and enable strategic planning. Massive MIMO Coverage—A key advantage of 5G, massive multiple input and multiple output (M-MIMO) provides greater capacity and minimizes interference. By applying AI/ML and decision-making in real time in conjunction with M-MIMO and beam forming, the RIC can proactively and continuously improve the subscriber's experience even in dense areas or at times where demand is surging, such as in crowded cities or entertainment venues. This could potentially

contribute to energy efficiency as the beams are efficiently utilized to capture or cover more users and traffic while using the same or even lower power.

- Quality of Experience (QoE)—Intelligent, real-time controls allow a better user experience for latency-sensitive or bandwidth-intensive applications like cloud virtual reality, drones, or autonomous vehicles. The RIC and associated applications can use analytics to take policy-based actions, ensuring that priority users maintain a satisfactory QoE and experience even during peak loads.

Software Disaggregation from hardware (Vertical disaggregation)

In vertical disaggregation, software becomes independent of hardware. This means that operators could choose different vendor for hardware and for software. This allows operators to choose the best of breed solution. They could choose the best and most economical hardware based on the needs of their network and subscribers. They could also choose the most flexible and cost-effective software that will allow them to be agile in terms of developing and releasing new services.

Just like Horizontal disaggregation, the flexibility of vertical disaggregation comes with a price, which is complexity. Since software is developed independently of hardware, the possibility of interoperability issues is higher. This could be countered though through testing and certification.

4.3.1.2 Disaggregation impacts on RAN operational process

Impact on RAN Planning

The overall architecture will change from RU-BBU to CU-DU-RU to implementing the different functional split options. This will significantly impact the planning, dimensioning, and engineering of sites. From simply putting RU-BBU to each of the sites and just dimensioning the number of bands and carriers based on the expected and future traffic that needs to be supported and carried, to dimensioning the DUs depending on how many RU's and how much traffic will be homed/connected or supported. CU's will also have to be dimensioned separately depending on how many sites or DU's will be homed to it. These will all depend on what functional split options operators choose to implement.

Additionally, when planning the new RAN – in addition to normal engineering based on traffic profiles and available sites, frequency bands and carriers, operators will now also need to consider the impact on the Resource Operation Layer to ensure that sufficient computing power, networking and storage is available to support the Services that comprise the disaggregated RAN. The amount of traffic that a specific Service instance (e.g. DU or RU) can support will depend on the number of cores/processors in the instance.

Planning and Engineering teams need to learn different styles of dimensioning that is similar to IT and apply it to network.

Impact on RAN deployment:

RAN deployment in disaggregated network becomes flexible and complex at the same time. In the traditional networks all RAN components (BBU and RU) are installed to each site, which is costly because each site needs all the supply and services for all RAN components. In disaggregated RAN, operators can choose to either replicate the traditional, which is deemed costly, or centralize DU and CU. In centralised architectures, the site could consist only of RU, antenna and ancillaries which will be faster in terms of implementation. BBU functions, which now becomes the CU and DU could be placed in a central location or Data Centre which could handle more sites. This is like how the RNC is positioned in 3G and the BSC in 2G. The difference is that this new architecture could centralise more sites as it allows stacking up of servers. In this case, the deployment of massive number of sites could potentially be faster and cheaper.

The challenge here is the resiliency of the solution. Since the network functions are centralized, it is prone to more down time during disasters. To counter this, a good resiliency or multi-homing architecture would be required. In addition, further approaches to resiliency such as 'hot-standby' should be considered.

Impact on RAN maintenance

Since RAN is broken down to more parts horizontally and vertically, RAN maintenance will become more tedious as more expertise and tools are needed for the operations or field teams. Disaggregation will cause operators to use more brands therefore requiring operations engineers and staff to have more knowledge and skills both in hardware and software of each brand. This impact would have to be managed properly to ensure cost and organisational effects will be at an acceptable level.

The current set-up that could manage 3 to 5 vendors won't be sufficient anymore. The team has to be capable of handling multiple hardware and software vendors. This would require more training and even more people. With this, huge and proper preparations are needed by operators in order to ensure down times and service interruptions are avoided. The whole organization has to be ready when disaggregation is adopted.

Impact on RAN Optimisation process

Since hardware and software is separated during disaggregation, optimisation will be done separately. Optimisation will also become more complex as there is more hardware and software to measure, monitor and troubleshoot. The optimization team would need capabilities to build expertise on hardware and software separately. That would at least be twice the effort and might be twice the cost as well. The optimisation engineer and teams would need to fully understand the topology in the areas he/she handles for him/her to determine where the problem, bottleneck or failures are. This would be simpler if the monitoring and service assurance would be connected to just one platform where the CU, DU and RU hardware and software can be viewed. Otherwise, it will be more difficult for the optimisation engineer and team because he/they would have to look at many monitoring tools. This also needs understanding and expertise in each of the software and hardware brand for each functional element so intense training and competency development is required.

Separation of function in disaggregation will also impact the operations team as they need to build expertise in all the new brands or vendors that will be integrated in the network to ensure all issues will be addressed or resolved.

Impact on RAN Service providing

Service providing impact needs to be determined to ensure disaggregation will not affect problem management and troubleshooting of services, functions, or features in a negative way. Disaggregation should help expedite the process and make it more efficient. The operations team should be able to respond quickly to any service problems or failures and ensure there is no, to minimal, effect to subscribers whenever there are service interruptions. There is a hope that complexity of disaggregation will not make matters worse.

Need for Identification of applicable and best topology/configuration

There were originally several functional splits/options to choose from that were identified by 3GPP (see figure 4-3) in RAN which allows horizontal flexibility in a way that operators have the option to place RAN functions anywhere in the network depending on what is best in terms of flexibility and efficiency.   The industry has adopted an upper and a lower functional split approach. In particular, Option 2 is standardized by 3GPP and O-RAN has adopted option 2 (upper split) or option 7.2x (lower split).

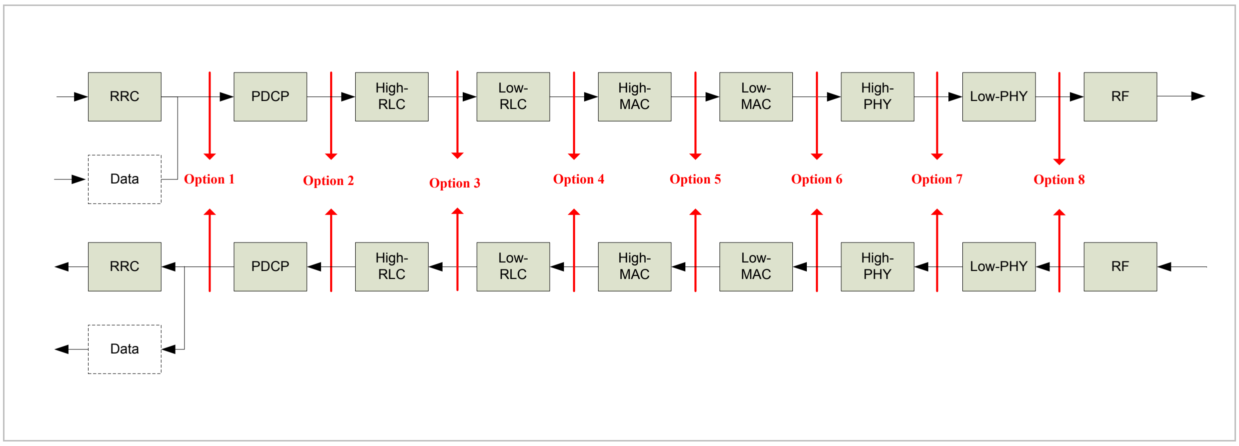


Figure 4-3 – RAN Functional split options [source: 3GPP TR38.801]

Operators could formulate several topology and configurations based on the upper and lower splits and be able to come up with models that will be applicable to different situations in the network that considers flexible use of resources while maintaining high performance and user experience.

Need for Selection of vendors

Vendor choice for each part

Operators need to formulate several options and analyse its Pros and Cons so they could decide which best will fit their network requirements, future plans and the current capabilities of their organization similar to the following extremes:

Option 1: Use same vendor for hardware and software

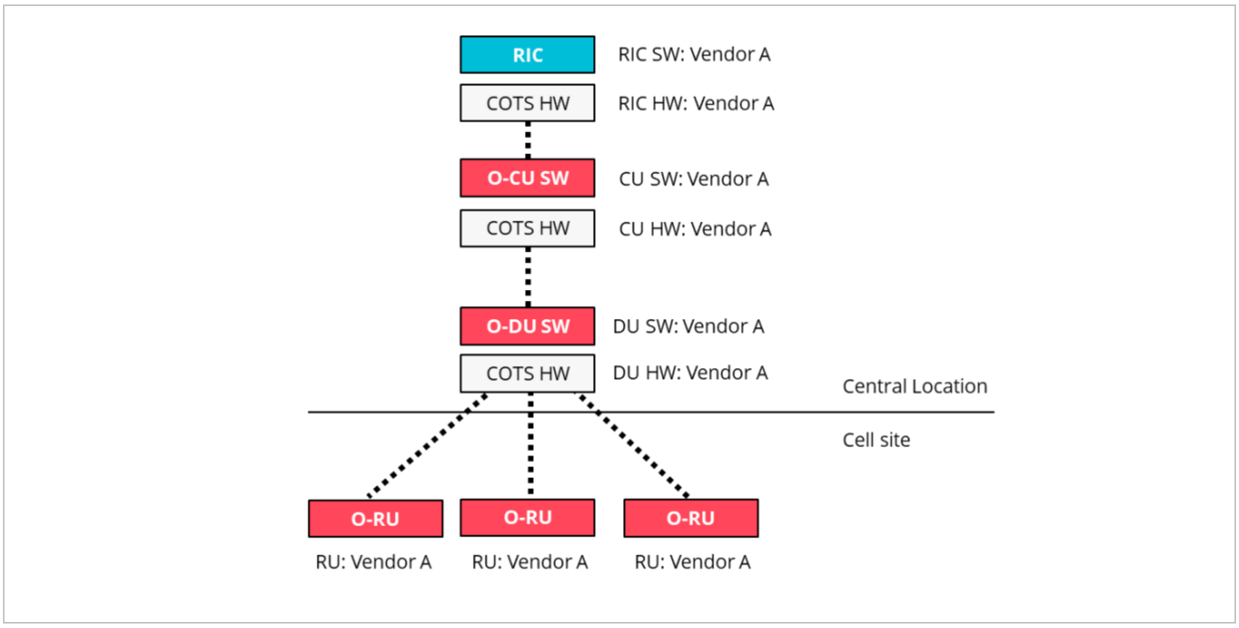


Figure 4-4: Use of same vendor for Hardware and Software

The advantage of this option is that the coordination, planning and engineering is simpler since we coordinate and work with fewer vendors and type of hardware and software.
The disadvantage is that it somewhat defeats the purpose of disaggregating which should allow us to choose more vendors/suppliers and be able to mix and match them.

Option 2: Use Totally Different Vendors

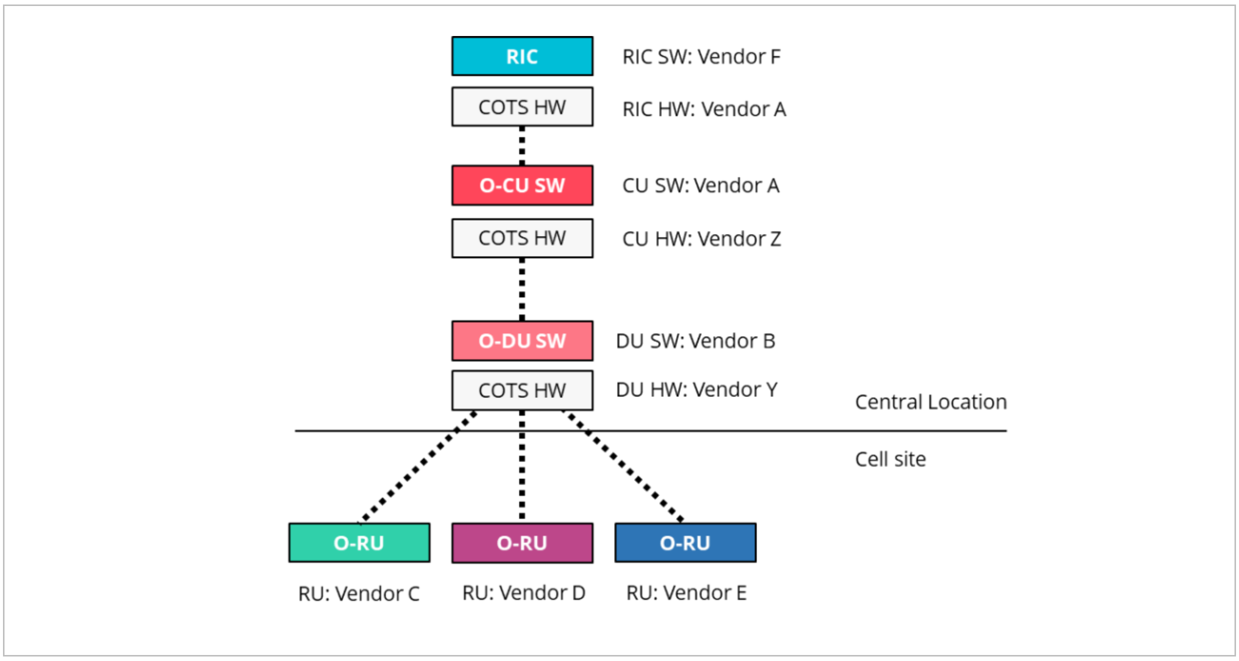


Figure 4-5: Use of totally different vendors

The advantage of this option is that we are able to take advantage of the disaggregation in a way that we are able to choose the best vendor for each part.
The disadvantage is that we are talking, coordinating, planning, engineering and implementing with too many vendors. This is very complex and would require more manpower and effort, not only to planning, engineering, build and operations team but also to procurement and other parts of our organizations.
ODiN project will be developing such models in the next Phase.
The vendor selection process for functional RAN disaggregation should strongly focus on standard based compliance. New disaggregated RAN components such as RIC (Near- and Non-RT RIC) are being specified in industry forums such as the O-RAN Alliance (https://www.o-ran.org/).

The O-RAN Alliance also runs, interoperability tests and PlugFests which are being performed in open Testing and Integration Centres (OTIC).

- Support wide adoptions of O-RAN specifications
- Organize and run PlugFest and proof of concepts
- Test RAN equipment based on O-RAN specifications
- Run test between different RAN vendors to verify interoperability
- Provide feedback to O-RAN community according to test results and potential interoperability gaps.

For more details please refer to the corresponding O-RAN Alliance description (i.e. https://www.o-ran.org/testing-integration)

Here are a few important points to consider for operators when selecting a RIC:

- Strong standards compliance with O-RAN
- Openness (Open & standard APIs, Ability to work with any O-RAN compliant 3rd party systems (RAN NFs, x/rApps, SMOs, etc.)
- RAN vendor independence & continuous support/contribution to O-RAN toward fully interoperable RAN (e.g. continuous extension of O-RAN E2SMs)
- RIC as a platform to enable RAN innovation
- Flexibility and support for x/rApps developers to develop new use-cases (both SDK and API based)
- Portfolio of x/rApps, and ability to develop more
- Support for in-house and 3rd party x/rApps
- RIC as a platform for AI/ML-driven RAN
- Proven interop in plugfests, PoCs, etc.
- Engagement in the O-RAN community

It is also worth to mention that a simple DIY (Do it yourself) or non-standard RIC platform, may come with the promise of an easy and non-complicated start, which may even promise a quick and easy win. However, since the main goal of the RIC platform is to leverage the innovation power of an entire industry eco-system, it will be important to consider standardization and world market acceptance over implementation speed to leverage the innovation power of multiple industry partners.

The vendor selection process for hardware and software disaggregated IP&Optical Transport Networks should follow a pragmatic approach, which systems offers the best solution for the operator's preferences.
HW&SW disaggregated solutions are functional comparable with non-disaggregated solutions, therefore, they can be easily compared on a functional and commercial basis. However, if new aspects such as cloudification, the introduction of containerized networking functions, are being introduced, this will also influence other operational aspects which will require more complex commercial TCO evaluations.

Let's have a look on the example at a typical Cell-Site router:
One option is a non-disaggregated legacy Cell Site Router which is provided by a single vendor with a specific set of required Network functions (i.e. IP/MPLS, SR/MPLS, SRv6, etc.). The same functions could be also provided by a disaggregated Cell-Site Router, where the dNOS is provided by vendor A, the required hardware by Vendor B and the integration of HW&SW by a specific System Integrator (S.I.). Since the required networking functions are the same, a simple commercial and operational comparison of the disaggregated and non-disaggregated solution would be sufficient. The picture is changing in case the Cell-Site Router function is being performed by containerized Software running on COTS based Hardware platform, which is at the same time being used to host other functions, such as CU or DU. In this case, the comparison becomes more complex and requires the consideration of multiple factors such as:

- Reduced Set of hardware
- Reduced Maintenance Cost
- Reduced Truck Roll costs during Roll-out and Hardware repair.
- Leveraging Cloud native tools such as CI/CD pipelines, which are already being used for other cloud based solution components.

HW&SW disaggregation in the IP&Optical Transport domain, is not the primary goal by itself, the various pros and cons of disaggregation need to be evaluated against operator specific preferences.

4.3.2 Core Disaggregation

Similar to the RAN domain, 5G has brought a tremendous change to the Core Network domain too: the move towards a Service-Based Architecture (SBA) and leveraging numerous cloud principles. This actually came ahead of RAN disaggregation and now RAN is following a similar journey. SBA essentially breaks up the static one-to-one relationship between two functions, allowing any service to be consumed by any other function. This is achieved through the unification of the communication, i.e. utilising HTTP/2 with JSON-encoded payloads. Furthermore, compared to 4G's Evolved Packet Core (EPC), 3GPP has defined a much larger set of Network Functions for 5G which have a much smaller scope of functionality. This follows the idea of a standardised methodology to disintegrate the 4G EPC with each 5G Core Network Function offering a Service-Based Interface (SBI) which 3GPP defines. The reason for such effort is driven by:

a. The desire to enable multi-vendor deployments where a 5GC is not necessarily composed of a single vendor solution but offered by more than one vendor based on the operator's needs. Ultimately, it should be the operator's (or vertical's) choice of required functionality that dictates which Network Function is acquired from which vendor

b. Adoption of cloud principles (cloud-native procedures, DevOps workflows for implementing 5GCs, and utilising microservice-targeted software design patterns) is the second key driver behind the shift towards SBA allowing 5GC vendors to scale their software solutions similar to cloud solution providers (i.e. a service can scale on demand). However, not all 5GC Network Functions utilise SBA principles (in particular SBIs) and there is further standardisation work required to fully arrive at a disintegrated 5G Core Network.

c. The softwarisation of Network Functions combined with cloud-native workflows also eliminates the necessity for customised hardware and a tightly interlinked software development process. With virtualisation technologies heavily adopted in the cloud domain, e.g. Linux Containers, Docker or Kernel Virtual Machines, the separation of hardware and software is key towards fully (vertically) disintegrated 5G Cores.

4.3.2.1 Core Disaggregation Activities

To comprehend the missing pieces in the Core Network to enable a fully SBA-driven 5G Core, Figure 4-6 illustrates the current (Release 17) 5G system architecture with blue interface lines indicating the availability of a Service-Based Interface and green lines the existence of a Non-SBI. Note, it is only N4 that is the last remaining Non-SBI that interconnects 5GC Networking Functions, i.e. the SMF and UPF.

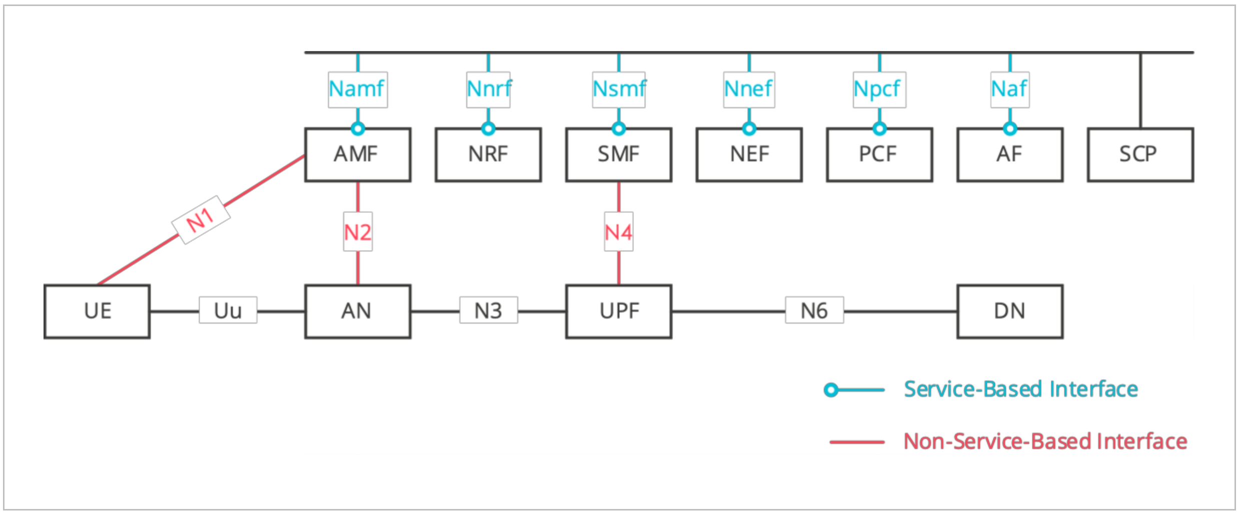


Figure 4-6: 5G Core Network System Architecture with Emphasis on Service-Based (blue) and Non-Service-Based (green) Interfaces [4]

Approved Study Item in 3GPP [4] focuses on enhancing N4 to support event exposures and real-time service flow information (for Network Data Analytics Function (NWDAF) purposes) marking a small step towards the N4-to-Nupf transition.
Equally important, but with much larger impacts, is the N1 interface allowing UEs to communicate to the 5G Core via Non-Access Stratum (NAS) procedures. This part of the control plane remains untouched so far and poses a challenge to the Access and Mobility Management Function (AMF) as the single point of entry into an SBI-enabled 5G Core. The AMF essentially operates in two separate worlds (SBA and non-SBA) imposing challenges to 5GC vendors who have adopted microservice software architectures for their products (more information on that in Section 5). And the N2 interface between the Access Network (AN) and the AMF (as the underlying protocol stack for N1 communications) plays a significant role in the complexities AMF vendors face when implementing the AMF as a Cloud-Native Network Function (CNF).

4.3.2.2 Disaggregation Impacts on Core Operational Process

This section describes the impact of disintegration on 5GCs with regards to planning, deployment, maintenance, optimisation, and provisioning.

Impact on Core Planning Process

The planning of resources (compute, storage, networking) has changed in a way that the system can be scaled up and down based on demand and a 5GC NF can exist as a set of instances across different locations. While the input to such planning is still the number of users that are expected to connect in a given amount of time, potential fail over scenarios or system upgrades through DevOps procedures impacts the calculation and differs from pre-5G Core planning procedures.

The flexibility of disintegrated 5GCs also allows operators to plan for a multi-vendor 5G Core where NF1 (e.g. AMF) comes from Vendor 1 and NF2 (e.g. NWDAF) from Vendor 2. This decision is driven by the NF functionalities offered by a specific vendor.

Impact on Core Deployment Process

Disaggregation has allowed flexible deployment of Core Networks. Since Core Network software and functionalities are now independent of hardware and is now getting more cloud native, core functions can now be installed or hosted either in a private cloud/premise or in a public cloud that is not in the premise of the operators. Hosting the Core functions in the cloud potentially reduce CAPEX and convert spend to OPEX.

The adoption of cloud principles and the realisation of 5GC NFs using a microservice-based software architecture allows the deployment process to be automated using cloud-native procedures. Using orchestration frameworks that focus on container-based service provisioning, the deployment process is a defined through a workflow identical to the one of cloud service providers. In that workflow a descriptor is defined which declares the required microservices (container names/packages) in use and their properties (CPU, RAM, Storage) combined with policies how the orchestrator should react to a change in load. These deployment procedures also cover scenarios of hardware failures or system failures increasing the capability to react to system changes in a robust and automated fashion. Furthermore, this also enables the deployment of 5GC Network Functions implemented by multiple vendors or the choice to only deploy the 5GC Network Functions required for a specific network. For instance, in a Private Network setting only a handful of Network Functions could be required to provide the capabilities needed.

5GC as a service is also now possible wherein the 5GC functions could be outsourced.

Impact on Core Maintenance Process

DevOps has become the norm to realise a continuous development and integration of software without the need to bring down an entire service. Tightly linked with cloud-native orchestration workflow, microservice-based software realisations can be upgraded for a subset of service requests allowing to observe whether the upgrade causes unexpected service behaviour. Such maintenance workflow has been only possible due to the disintegration of the 5GC and the creation of SBIs. Furthermore, if vendors choose to adopt a microservice software architecture for the realisation of their NF, issues in maintenance are always limited to the scope of the microservice instead of the entire NF. The same applies to each NF, as they are separated through standardised SBIs.

Hosting Core NF's in the public cloud will help reduce the efforts of operators in maintaining the network as many of the responsibilities, especially with the hardware, are now passed on to the cloud provider. This will help ease operations and maintenance.

Impact on Core Optimisation Process

The disintegration of 5GCs enabled vendors to optimise their NF to a greater extent, allowing operators to pick a specific NF from a specific vendor, if desired. In particular for user plane specific QoS requirements around optimised latencies, local breakout or customised capacities, the disintegrated 5GC allows fine-tuned UPF realisations. For instance, if a Private Network owner or operator of a Public Network aims to deploy 5GLAN with support for Time Sensitive Networking, only the SMF and UPF must support such feature, while preserving any other 5GC NF required to operate a fully-fledged 5GC. Another example of how important the disintegration enabled optimised deployments could be is to consider a manufacturer utilising 5G for the communication technology of their robots: in such scenario billing and mobility is not required and can be removed as functionality from the 5GC without affecting the operations of other NFs.

Impact on Core Service Provisioning Process

When considering the 5GC as a service, the disintegration of 5GCs enables never before seen provisioning possibilities due to the flexibility the system architecture permits. In particular for verticals, there is a range of questions that must be evaluated related to the service provisioning and is commonly discussed under Public Network vs Non-Public Network service provisioning concepts:

- If coverage is not an issue, verticals may choose a network slice in an operator's public network offering including a defined set of NF instances exclusively available to handle control plane communication of the vertical's UEs

- Alternatively, verticals may deploy their own gNB on premise and connect it to a 5GC deployed in a cloud or to the 5GC of an operator (where the operator also provided the gNB).

- To demonstrate even greater flexibility, the vertical could choose a sub-set of 5GC NFs to be owned and deployed locally (e.g. UPF and UDM for performance and data protection purposes), while utilising the remaining necessary 5GC NFs from a third party in a public cloud or from an operator.

As the entire 5GC is pure software without any hardware dependencies, the service provisioning may be compared to typical cloud offerings.

4.3.3 Transport disaggregation

In the fast-changing digital transformation, we see an agile network Evolution of the end-to-end Communication Service Provider. We've seen how the transport network domain continues to evolve as it adapts to the new services and applications requiring low latency and massive bandwidth. As the transport network evolves, we need a separation of different functional components that is fulfilled by network disaggregation.

We have seen giant hyper scalers such as Google, Facebook, Amazon, and Microsoft implement the first large-scale disaggregation of network and software in the data center and wide area network deployment that drives service innovation and market differentiation.

The disaggregation of hardware and software is the critical enabler for deploying each functional component of the network device. Each element delivers specific roles and functions that separate the control and user-plane traffic. Transport disaggregation is in all forms of the transport networks such as Ethernet , Optical and IP. It’s an open networking device consisting of IP routers, optical systems build on open APIs for software-defined networking (SDN)..

4.3.3.1 Transport disaggregation activities

Telecommunication providers adapt to the emerging hardware and software separation ecosystem in their domains such as IP core, transport, and access networks.

Standards Development Organizations (SDO) create standards for the Disaggregated Transport Networks. See different organizations below.

- Telecom Infra Project
- Internet Engineering Task Force (IETF)
- Broadband Forum (BBF)

- Open Networking Foundation (ONF)
- Open Compute Project (OCP)
- Optical Internetworking Forum (OIF)

Disaggregation in Transport Network – ONF

ONF's target is to bring the approach of open networking to the optical network layer. The initial phase of Open Disaggregated Transport Network (ODTN) project will disaggregate transponders from open line systems to enable data centre interconnection to evolve at the speed of transponder improvement.

The ODTN project is an ONF operator-led initiative to build data centre interconnects that will use disaggregated optical equipment, open and common standards, and open-source software. The objective is to drive innovation by disaggregating the components of the network and provide open software to control a multi-vendor assembly of components.

ODTN will enable a white-box optical 'peripherals' ecosystem allowing multiple components to be combined and built into a complete solution. Vendors can then focus on building a specific component (for example, transponder) without the need to build a complete solution which leads to accelerated innovation and lower costs. This will allow operators to integrate the latest technologies once they become available rather than waiting for them through the previous siloed method.

ODTN Phase 1 will focus on point-to-point data center interconnection. The open-source network controller controls the network infrastructure with well-defined open transport APIs, which allows a mix of paired transponders from different vendors running on the same physical links.

We can see the role of SDN technology in the Telecommunications ecosystem of Communication Service Providers, and it is the critical enabler for transport automation and disaggregation.

The Transport domain is evolving into disaggregated hardware and software parallel to the Access and Core domain. Like the ODTN initiatives of ONF, The Telecom Infra Project (TIP) has the Optical & Packet Transport Project (OOPT) with the common goal of disaggregation from software and hardware.

The open-source community is driving the innovations for Disaggregated network operating system. It complements our transport domain to adapt to the open networking wave that is fast evolving in the disaggregated transport network. Many hyperscalers and tech giants like Google, Amazon, and Facebook run their network operating systems using commodity networking switches which helps drive open networking innovations.
Decoupling hardware from the Network Operating System (NOS) to allow a more diverse eco-system is introducing new opportunities but also new operational challenges. In general, under the term 'Transport' different device classes operating at the OSI-Layer 1-4 are being summarised to one solution domain. According to operator preferences, Optical Transport systems as well as Ethernet Switching and IP-Routing devices are being used in this domain.

Before we elaborate on the operational challenges it is also worth to mention, that meanwhile the next iteration of Transport disaggregation is taking place and is introducing stronger cloudification aspects.

One good example is the OCP (Open Compute Platform) industry standardisation group, which is hosting the Software for Open Networking in the Cloud (SONiC) Opensource initiative, which is not only disaggregating the NOS from the Hardware, here also the NOS itself is divided into multiple functional parts in order allow Network functions to run as a containerized functions on top of a Linux based operating system. This will allow a more cloudified approach with the usage of standard Cloud technologies and their widely used tool chain.

Another example, which goes into the similar direction, is to take those containerized network functions (i.e. dynamic Routing Stack) and to run them on standard X.86 COTS Server which are using as well a LINUX based operation system. With this, it now becomes possible to run the identical network functions on either networking specialized white-boxes or on COTS standard servers.

An example of these multiple disaggregation steps is illustrated in the following diagram, which shows the multiple steps from simple disaggregation towards cloudification on the example of a Cell-Site-Router.

In the figure 4-7, the Cell-Site Router is taking the transport function to connect the Cell-Site with the aggregation network, while the first approach of disaggregation just focused on separating the underlying Hardware from the "monolithic NOS. This allows the flexibility to pick and choose Hardware and Software from different suppliers (dNOS). This flexibility comes with the cost of re-integrating it into a single working system. The next step of cloudification shows that the transport function becomes now just a containerized Software, which can also run on the already existent Hardware to power CU/DU functions on the corresponding sites.

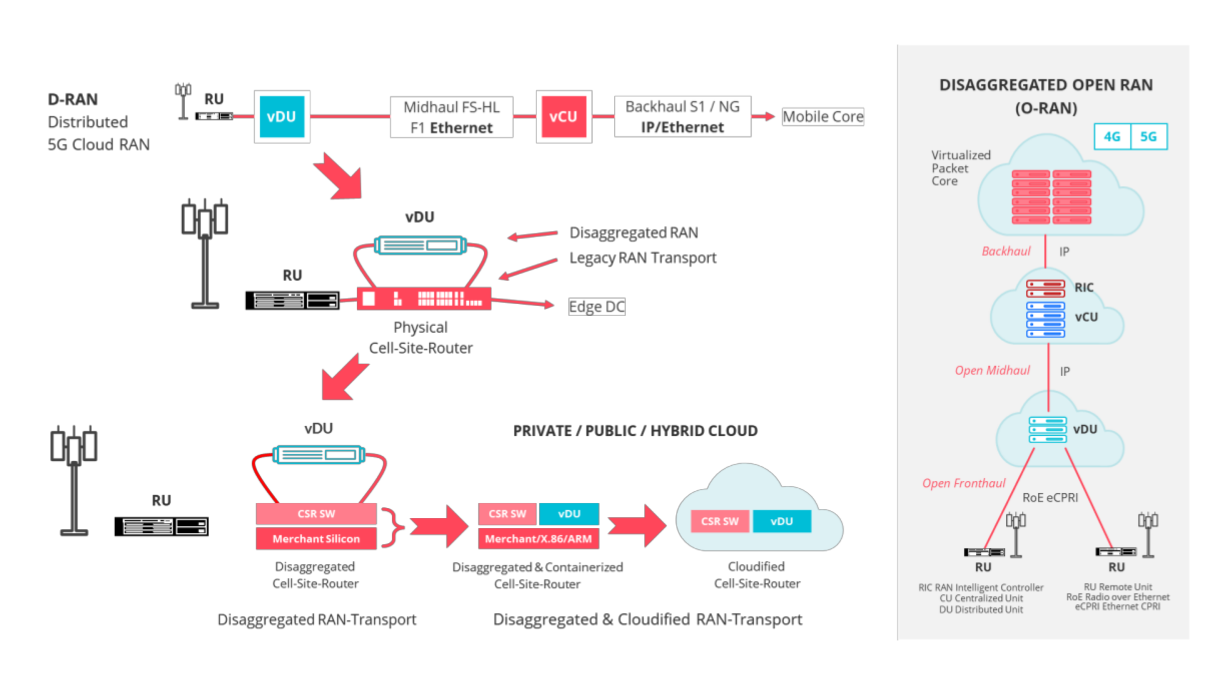


Figure 4-7: Disaggregated Network Operating System

With this additional step of cloudification, new operational models which follow cloud principles, will be required. Details of cloudification in the Transport domain will be described in the following chapter of cloudification.

4.3.3.2 Disaggregation impacts on Transport operational processes

Impact on Transport Planning process

Disaggregated Transport is introducing a new architecture and will require different methods of planning and dimensioning. In the traditional architecture, Transport dimensioning mostly focuses on the capacity planning of the metro aggregation Network, which consist typically of optical Transport devices and/or Routing and Switching devices for Cell-Sites and aggregation locations (sites). Since disaggregation does introduce more potential variables in terms of which hardware and which software can be combined with each other and in general as a larger eco-system of suppliers will be able to provide their solutions, this will also impact the planning process. Potentially, also the role of a system integrator needs to be considered and responsibilities need to be clearly divided between the systems integrator and MNO. Once the desired combination of hardware and software has been selected, the planning process remains largely the same as with non-disaggregated solutions. This will change, if cloudification also comes into the picture. Cloudification is covered in the next chapter.

Impact on Transport Deployment process

It can safely be assumed that the deployment process of the disaggregated Transport, with its disaggregated hardware- & software, remains largely the same as with the non-disaggregated legacy approach. This is due to the fact that the re-integration of the separated HW & SW packages takes place before the actual deployment is going to happen, therefore a plain disaggregated Transport solution will behave very much like the legacy Transport solutions. Again, the major change will come with the cloudification of the transport.

Impact on Transport Maintenance process

In the disaggregated model, as the Transport is broken down to more parts horizontally and vertically, Transport maintenance will become more tedious as more expertise and tools are needed for the operations or field teams. Disaggregation will cause operators to use more vendors therefore requiring operations engineers and staff to have more knowledge and skills both in relation to the hardware and the software of each vendor. This impact would have to be managed properly to ensure cost and organisational effects will be at an acceptable level.
However, here again in the model of cloudified disaggregated Transport the picture is changing. The maintenance process of hardware will be aligned with the RAN and cloud infrastructure. The maintenance of the Transport itself, will be reduced to primarily software aspects. This step will offer massive operational benefits in this domain

Impact on Transport Optimisation process

Identical to the previous chapter, since hardware and software is separated during disaggregation, optimisation will be done separately also with hardware and software given that the two are potentially provided by multiple different suppliers. The optimisation team would need to build expertise on hardware and software separately.

Separation of functions in disaggregation will also impact the operations team as they need to build expertise in all the new vendors that will be integrated in the network to ensure all issues will be addressed or resolved.

Impact on Transport Service provisioning process

Due to the fact that in the disaggregated transport re-integration (of separated HW and SW packages) will take place prior to deployment, the service provisioning process for disaggregated Transport remains largely unchanged in comparison with previous “integrated” models.

4.3.4 Non domain specific Operational Activities

4.3.4.1 Integration of parts

There are 2 options for each operator to address integration of different parts and vendors to have a complete solution. One is to develop an internal team that will be responsible for integrating the solutions of all the participating vendors to build the full set-up. The other is to outsource or hire an external entity that will be tasked to do all the integration works and services. That same entity will be the one responsible for any fault in the system, be it hardware or software for any part - CU, DU, RU as well for for the RAN-Transport systems and Core which might come disaggregated as well, as described in previous sections.

The first one is quite tedious and costly because it will require hiring new resources that should stay for a long time, training them and building their competencies. Rather than making the organization lean, it requires now to beef up in order to support the disaggregated architecture. The second option might be easier and simpler although it will be very costly and would require governance

4.3.4.2 Interoperability and Compatibility Assurance

As outlined in other chapters, interoperability is a huge challenge. Horizontal interoperability, i.e. between functions building up the network end-to-end remains business as usual. In addition, disaggregation brings the need for vertical interoperability.

This is addressed by integration and testing. Due to the increasing number of tests, this calls for automation, typically in a CI/CD (Continuous Integration/Continuous Delivery) pipeline.

The industry is organising activities to achieve interoperability, by initiatives such as TIP international labs and testing efforts as well as cooperation being done between operators and vendors. Some hardware vendors are also doing certifications with software suppliers to ensure their hardware are always updated and are always capable of supporting any new functions and features that comes with the new software release. This will help a lot, but then again this will not completely assure compatibility and interoperability.

Telecom Infra Project (TIP) has 14 labs (https://telecominfraproject.com/test-and-integration/), sponsored by individual TIP participant companies that test interopeability. There are three types of labs:

- TIP product labs - focused on Proof of Concepts (PoC's).
- TIP integration labs - focused on end to end testing to evaluate a product's maturity toward commercial readiness.
- TIP deployment labs - focused on people (education and technology spread out), processes and tools.

TIP certification and badging (https://exchange.telecominfraproject.com/).

TIP Badges and Ribbons are awarded depending on the level of maturity of products and solutions against the technical requirements that is evaluated. Only those products with market availability are qualified to be evaluated. Awarded products and solutions are then listed to the TIP Exchange (https://exchange.telecominfraproject.com/) with the corresponding awarded badges. Aside from badges, products on TIP Exchange may also be awarded ribbons.

Badges:

- **Supplier Validated Product (Bronze)**
  This is being awarded to the products that technology suppliers have tested in their own laboratories, This is primarily applicable to individual network products and components. Products are required to be commercially available even on its early stages
- **TIP Validated Product (Silver)**
  This badge is awarded to integrated network layers. It is awarded to the products that were validated in a TIP Community laboratory or it could also be validated by an approved 3rd party laboratory. Products has to be commercially available with the minimum product support in order to qualify for this badge.
- **TIP Validated Solution (Gold)**
  Gold badge is awarded to products that were validated in a TIP Community laboratory or it could also be from an approved 3rd party party laboratory. This is primarily applicable to end-to-end solutions, integrated network layers, or it could be individual products tested in an end-to-end environment that is representative of actual service provider conditions. Solutions are required to be commercially available with full product support to qualify

Ribbons:

- **Operator tested Ribbons**
  Ribbons are awarded to listed products on TIP Exchange that were tested in an actual field trial conducted by an operator.

- **Requirements Compliant**
  This is the minimum requirement to get listed to the TIP Exchange. Individual network components or products should be compliant to the requirements that was set by the associated project group.

For a more detailed information, it is advised to visit the TIP website (https://telecominfraproject.com/test-validation/)

4.3.4.3 Joint DevSecOps Pipeline

Disaggregation is very different from the development model of existing networks. In order to ensure that the network quality, customer experience, implementation time, optimization and maintenance will not be affected by technological changes, the network operation mode also needs to be changed and new processes, skills and tools needs to be adopted. Operators will face challenges at two levels. First, in terms of technical complexity, disaggregation increases the complexity of integration testing, compatibility, and security prevention and control. Second, in terms of organization and process, disaggregation will have a significant impact on procurement, integration, and operations.

Therefore, DevSecOps is a necessary means to comply with the trend of Disaggregation. The introduction of DevSecOps will help operators improve efficiency and reduce costs. On the one hand, cross-organizational DevSecOps application scenarios are required to solve the contradiction between the complexity of network evolution and network management efficiency; On the other hand, it is necessary to introduce the cross-organization standard pipeline general solution R&D tools into the testing and certification system to solve the problem that the test environment adapts to the frequent upgrade of the existing network equipment.

4.3.4.4 Upgrades and expansions

New education must be done in doing upgrades as it is not the same anymore as the way we do it with traditional solutions. It is not simply upgrading the hardware and buying software and licenses. Now, the number of processors must be accounted and dimensioned accordingly. It is now like buying computer for your home and ensuring you bought the correct processor specification and quantity, memory and storage that will suffice for your everyday needs. So our traffic requirements and projections should be translated to hardware requirements up to the chip level.

4.3.4.5 Troubleshooting and disaster recovery

Once we implement disaggregation, as complex as it may be, we are compelled to have a troubleshooting and disaster recovery plan.

Troubleshooting is included in the main course and action of operations and daily activities. This is why troubleshooting for every group of hardware and software should be planned well. There should be enough manpower to do that and they should be equipped with the right knowledge and tools. Each of the brands, hardware type and software type might need different types of tools. If there is a single or universal one that could support all types of hardware and software, then that would be the most ideal. Otherwise, there should be proper grouping and minimization of tools used so there is not too many that the troubleshooters need to learn. This will avoid confusion which could potentially lead to errors later.

Due also to the new architecture and splits, a new resilience plan would have to be developed. This is especially true if CU's and DU's are centralized. Since more sites will be home to a single DU and/or CU, there has to be a secondary homing plan to a different DU and/or CU that could support transferred traffic in cases of disaster or any down time.

Nowadays, we experience more and more devastations from storm, earthquakes, volcanic eruptions. Therefore, it is a necessity to have a very strong disaster recovery plan that could minimize the service down time no matter how bad the situation is. Operations team should know each and every hardware and software by heart so the decision-making during disasters would be fast and easy. Fast decision making and correct judgement are the two important things during disaster recovery. Our teams should be equipped in ensuring these two are achieved even when the architecture of the network has significantly changed.

4.3.5 Support for Green Technology

In all the improvements being done to the network ensuring flexibility and efficiency, minimization of carbon emissions and energy efficiency should always be considered as these are the key factors to sustainability. To enable MNOs and the wider mobile and IT industry to meet their sustainability goals, the design, manufacture, deployment and operation of disaggregated networks will need to go hand in hand with the adoption and advancement of new 'green' technologies and processes. NGMN Alliance, through its Green Future Networks strategic programme is providing industry leadership in this area and has already published a number of white papers outlining the overall challenges and opportunities [5] as well as addressing how to make networks more energy efficient [6]. Further work in this programme is expected to address wider issues related to how MNOs and the entire mobile industry value chain can reduce carbon emissions; use advanced technologies and processes to further improve network energy efficiency; and provide guidance on how the industry can reduce its overall environmental impact.

The impact of network disaggregation on the energy efficiency and carbon emissions of the network requires further study. At a high-level, the key issue is the extent to which energy efficiency gains from pooling lots of different network function compute tasks in the cloud (where they are run on general purpose compute resources) are offset by the energy efficiency losses in moving these tasks from highly optimised (and presumably energy efficient) dedicated compute resources (often using systems on chips designed for the specific task).

Although it is anticipated that future phases of NGMN's Mastering the Route to Disaggregation programme will address specific disaggregation challenges in relation to Green Future Networks it is worthwhile pointing out two existing industry initiatives that address data centre energy efficiency. These are:

- Redfish, a REST API used for platform management and standardized by the Distributed Management Task Force, Inc.[7]
- Scaphandre, an open-source metrology agent that can be deployed on a CaaS platform (Kubernetes) to collect power metrics related to the overall cluster and the individual CNFs running on it.[8]

4.3.6 Integration to End-to-End Service Orchestration and Common Management and Service Assurance System

While parts are increasing, and network functions are being distributed to more nodes, we need to ensure that all network elements are connected and covered by the overall management and service assurance system. This will ensure proper monitoring, alarm management, troubleshooting and control. This will also ensure proper operation of all elements as well as overall visibility ensuring expected and target availability.

All functions should also be connected to and covered by End-to-End Service Orchestration to ensure all parts of the network are participating in the automation process and services are instantiated and defined in all parts of the network – RAN, Core, Transport, billing, etc.

5 CLOUDIFICATION OF DISAGGREGATED NETWORKS

Cloudification is the next step in the evolution of a disaggregated network. This evolution is not only on network functions design and implementation, Cloudification also brings new tools supporting automation and orchestration that have a relevant impact on operation. NGMN published in 2021 an extensive study on the target picture provided by Network Disaggregation and Cloudification for the overall Telco Platform [9]. This chapter summarises the main aspects on the Cloudification of a disaggregated network and suggests possible impacts/challenges on operation.

5.1 The overall Blueprint

5G is designed with open interfaces and a service-based architecture allowing services to be delivered via a network that is 'disaggregated' in nature compared to previous generations.

These aspects well match a Cloud Native approach. The evolution from disaggregation towards Cloudification is a process encompassing the whole Telco Platform. A cloudified Telco Platform leverages on unique Telco assets from one side and on common IT/Telco technologies from the other side. Enhanced by this evolution the Telco Platform is evolving to further simplify operation. It is becoming closer and closer, in terms of technology and automation, to the cloud platforms supporting information, communication and social media services provided by companies such as Google, Meta, Microsoft, and Amazon. The enhancement of the 5G network in terms of performance and deployment flexibility allows the Telcos to support new business models. This requires an evolution of the supporting systems to keep the pace.

A cloudified Telco Platform must exploit openness both internally and toward the external ecosystems. The basic characteristics for such an openness are the same whenever you are considering internal optimization or external federation and interoperability. The new 5G mobile network indeed foresees a microservices based architecture that aligns the different domains and vendors' solutions leveraging on common hardware and decoupled software for the network application by exposing standard interfaces. On top of the disaggregated network, Open-Source communities are delivering IT solutions supporting this evolution on top of the experience made on cloud architecture management. From physical to Cloud Native Network Functions the current evolution path is fostering Cloud Native concepts becoming deeply embedded everywhere in the Telco world, from the central data centres to the regional and edge ones.

For this new Telco Platform to allow partners into the service ecosystem, openness is key for these partners (internal and external). Many of the new partners that will leverage 5G for their services will have limited or no knowledge in Telco networks or how they are operated. This is where network cloudification becomes vital – it enables those partners to leverage the network as a resource in a software defined manner.

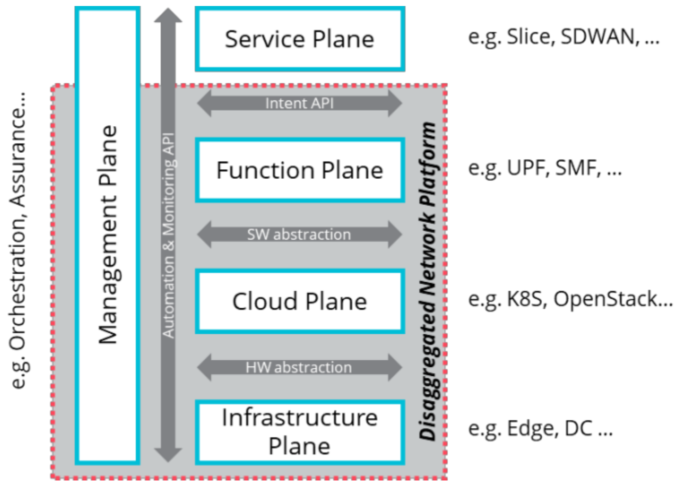


Figure 5-1: Disaggregated and cloudified Network Platform interacting with the service plane and Automation/orchestration

To operate a Disaggregated network in cloudified context a few aspects need to be considered. As shown in the picture above the management plane extends into the service plane since an E2E management needs to be in place for the service ecosystem to work. But this also implies an important aspect on tooling. If the tools used for the Cloud plane are not consistent, operations will be complicated. The methods of these planes as well as the tools established could be different – nonetheless they will sit on the same network infrastructure.To enable operation teams to deliver services across the planes it needs a common set of tools, processes and APIs to be used by these tools.

The next important part of operating the disaggregated network is the SDN structure. This also is an aspect of the Cloud Plane. K8s and Openstack use different methods to deploy an overlay network. The solution could be to have each cloud plane use its own infrastructure – but this will create multiple siloed Disaggregated network platforms and is contradicting the cloud native concept of micro services creating enriched service offerings stretching across the entire network from edge to core. Aligning the operation of multiple SDNs on top of the same network infrastructure is a critical challenge in the disaggregated networking space.

A key enabler for evolving networks supporting both NFs and applications is Cloud Native orchestration. Cloud Native orchestration has the capability to support standardised deployment and operational procedures across various cloud data centres leveraging open multi-vendor physical infrastructure. This disaggregated model allows an independent deployment paradigm without having dependencies on hardware and applications typical of a legacy, single vendor solution. Without such an orchestration integrating autonomous deployment and closed loop assurance, these complex and integrated services could not be efficiently operated.

5.2 Cloudification domain impacts to essential activities in operating a network

Cloudification is a technological innovation that is pervasive in different Telco domains. The fundamental pace of this innovation is the evolution of the Network Function from physical assets to Virtual Network Function and then to Cloud Native Network Function though with some intermediate steps. Decoupled from the hardware, the application component of a NF is evolving adopting different models in terms of software engineering. The first step in this evolution is simple porting of the NF logic, decoupling the functionality it offers from the compute hardware it operates on. With this basic approach, these functions retain their monolithic characteristics that makes it hard or impossible to easily decouple services. The second step is the redesign of the software to run as Virtual network Function (VNF) over a shared platform. The ability to virtualise a softwarised network function allows to offer the compute hardware resource to more than one softwarised function and abstracts its underlying operating system. The optimal design for a 5G network function follows the Cloud Native paradigm. At the core is the idea to decompose a function into microservices that can exist as multiple instances to allow to scale on demand. Each of these steps introduces new enablers for an innovative operation of the network. The final step, where a network is cloudified, brings many tools supporting automation and orchestration that can really change the paradigm of network deployment and assurance.

These new implementation of the NFs leverages on complex infrastructures that provide specific tools according to the specific NF virtualisation technology (e.g. VM based or Cloud Native). A disaggregated system indeed highly leverages on Infrastructure as a Service (IaaS) to host the applications and leverages on Container as a Service (CaaS) in a Cloud Native environment. Platform as a Service (PaaS) gives even more common tools for application deployment and monitoring. Operating an infrastructure or a platform is facilitated when a common solution is adopted by the different domains. The same tools with advanced diagnostic features and auto healing features can be used. This allows to set up a cross domain group of technicians, for operation, with homogeneous skills, adding flexibility among the operations teams. It could be an added complexity if different solutions, infrastructures or platforms are instead adopted in different domains. Fortunately, open source and IT platforms and tools adoption is providing a sort of "standard de facto" operating environment that would also allow the teams to leverage the same framework of operational processes. This is especially important since from a Cloud Native perspective as operating the PaaS includes the operation of infrastructure as well as the Cloud Stack. In the networking world the infrastructure (transceivers, switch backplanes and Network OS) is often dealt separately by subject matter experts and hence needs new processes and structures to establish an operational approach for a PaaS.

Each of the different infrastructures (e.g. IaaS or CaaS) provides very powerful tools to orchestrate the NF life cycle. Having disaggregated network components means that operations can leverage on software orchestration for O&M. The current model for software orchestration in a Telco network adopts a hierarchical approach both for provisioning and for assurance. Requirements are passed to a specific domain that is able to substantiate them into actual configuration parameters for provisioning purposes. With the same approach performance assurance is built around the closed loop approach where each domain, even if coordinated, is in charge of guaranteeing the performances in its scope.
A key characteristic of Cloud Native concepts for orchestration is the ability to follow standardised deployment and operational procedures across various cloud data centres. The orchestration procedures are fully decoupled from the service that implements how to respond to requests. In more detail, for both operations the key is the separation of deploying and managing service instances, and the operation of the service itself inside an instance. In a Cloud Native orchestration world, services are pre-packaged (offline or at run-time) images that have no notion of the deployment and operational procedures required to orchestrate a service, to scale it based on demand, failover procedures, or economic incentives. The ability to build services in such a way is what the paradigm shift from monolithic functions to microservices entails. When mapping this to the Telco, it means that a service is simply waiting for a service request to arrive to process it without any additional logic to talk to the underlying system for location, billing, orchestration, identity management, or any other purposes.

When you have so many systems that must work together, the adoption of standard interfaces and architectures is an important success factor. There are many activities around the Telco Ecosystem evolution toward cloudification - some are carried out by standardization bodies such as ETSI or 3GPP, others are forged around the Open Source communities such as ONAP or Anuket. These two approaches to create and promote innovation, once very far from each other, are currently, more and more, leveraging on one another. Standardization is important at any level starting from the physical infrastructure to have just one set of HW components leveraging any kind of application. In terms of operation this is extremely important. Standardization is important as a basis to have shared and multi-vendor APIs, to create a solution that is composed by elements from different Vendors. The general architecture itself is worth to be discussed and defined in the standard bodies to give guidelines to Operators. Having a reference architecture is indeed fundamental to set-up a common ground for everyone to discuss with colleagues and vendors.

One of the main outcomes in standardisation is the adoption of an architecture providing a common approach that can be adopted by different platforms. For example, 3GPP structures the 5G Management System around the concept of Service Based Architecture (SBA) opening it to be customised according to the Telco needs. The SBA concept is based on the idea of having specific Management Services (MnSs) that offer capabilities for management and orchestration of network and service. This paradigm well matches with a cloud native approach. It is important to define the system in terms of services rather than of predefined building blocks strictly coupled, to have an open and flexible architecture. Web technologies and cloud concepts, i.e. *-as-a-Service, have a relevant impact on the Telco world and have seen a significant adoption. This leads into a simplification in the operations because of the adoption of a common approach and API technologies (http based) in the different domains. The availability of APIs that can be consumed by other systems is the base to create automated and orchestrated solutions that an operator can shape accordingly to its operational blueprint.

The evolution of a cloudified Telco network can also foresee the integration with hybrid Cloud solutions. Hybrid is indeed a key word in the cloudification process of the Telco Platform and it covers different aspects. One aspect is the coexistence of hybrid cloud solutions such VM-based and Containers-based NFs deployments. Another aspect is the coexistence of Telco oriented and Service oriented Cloud Native integrated environments. The coexistence and integration of Centralized, Edge and Cloud based deployments are another aspect that fits in the hybrid scenario. Hybrid resource managers are responsible for this complexity and are key technologies supporting the operation of different virtualisation technologies spread in different location, both private and public (e.g. provided by Hyperscaler cloud service providers).

6 ROLE AND IMPACT OF DISAGGREGATED NETWORK TESTING

Disaggregated networks pose new challenges and opportunities in relation to network testing. This chapter explores these challenges and opportunities and the impact on the operations and processes required to manage network testing and assurance as illustrated in figure 6-1.

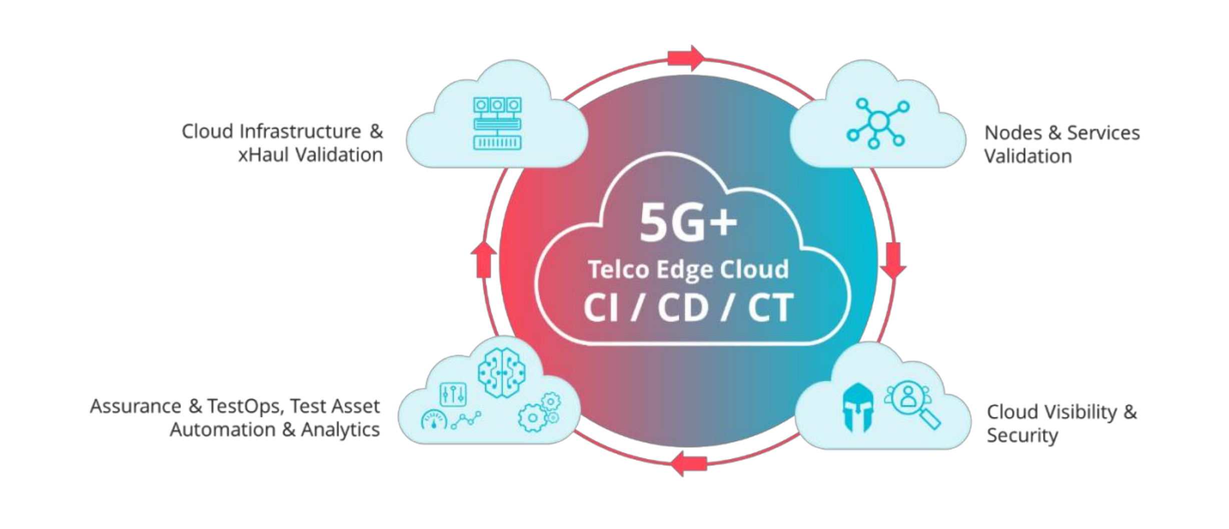

Cloud Infrastructure & xHaul Validation
Nodes & Services Validation
5G+
Telco Edge Cloud
CI / CD / CT
Assurance & TestOps, Test Asset Automation & Analytics
Cloud Visibility & Security

Figure 6-1: Telco Edge Cloud Validation coverage

5G disaggregated network architectures exist in a highly virtual and automated environment and Service Providers are using Continuous Integration and Continuous Deployment CI/CD pipeline processes. To reliably deploy, operate and maintain mobile network services in such environments these processes now need to encompass Continuous Testing (CI/CD/CT) (figure 6-2).

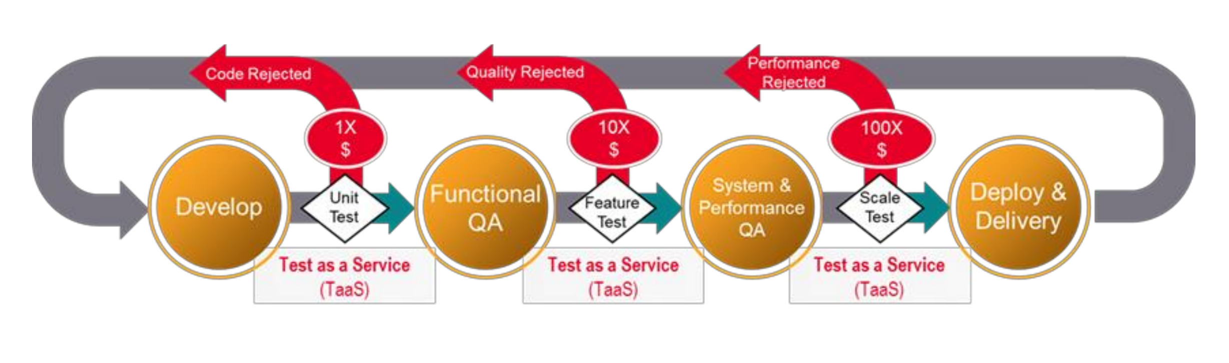


Figure 6-2: Continuous Testing & Test as a Service

These changes are driving the transformation of MNOs global work flow and organisation: from Lab to Field operation and from classical network equipment selection, integration and deployment to network assurance and network visibility platform including test asset disaggregation, distribution and automation supporting intent-based testing "Test as a Service" (TaaS) and advanced analytics.

In this context, Network Assurance, Troubleshooting and Network Visibility are no longer silos, bringing together modular and instant service access from network planning to operation and commissioning, and supervising from user/devices through to RAN/OpenRAN, Transport xHaul, Core/5GCore, data network (DN) and end-user applications.

This common Telco Cloud testing and automation framework spans from passive to active testing and from Multi-access Edge Computing (MEC), 5G Core and xHaul to Open Radio Access Networks (Open RAN) as well as to Private 5G wireless network architectures including hybrid public hyperscaler and private cloud, disaggregated and distributed cloud infrastructure.

6.1 The Importance of Test for Disaggregated Network from Design, Integration to Operation

Network disaggregation is spreading across the entire network from access, transport, core to OSS/BSS to services. This requires new certifications, performance and network assurance schemes including:

- Network technologies and performance level mix definition
- Device and subsystem selection, to badging and validation
- Multi-vendor and functions interoperability and troubleshooting
- System integration and performance validation
- Hybrid cloud Infrastructure mix validation, partners selection and performance assessment
- Extended and distributed network visibility
- Extended "SecOps" and "ZeroTrust" policy introducing security by design and throughout the application life-cycle (development, deployment and operations)

- Assurance and network operation based on on-demand service delivery and AI/ML based network Operation

In effect the aim here is to ensure that the MNO's expectations (cost, interoperability, resiliency, power efficiency, features etc) in relation to deploying and managing the multi-vendor infrastructure can be assured (see figure 6-3).

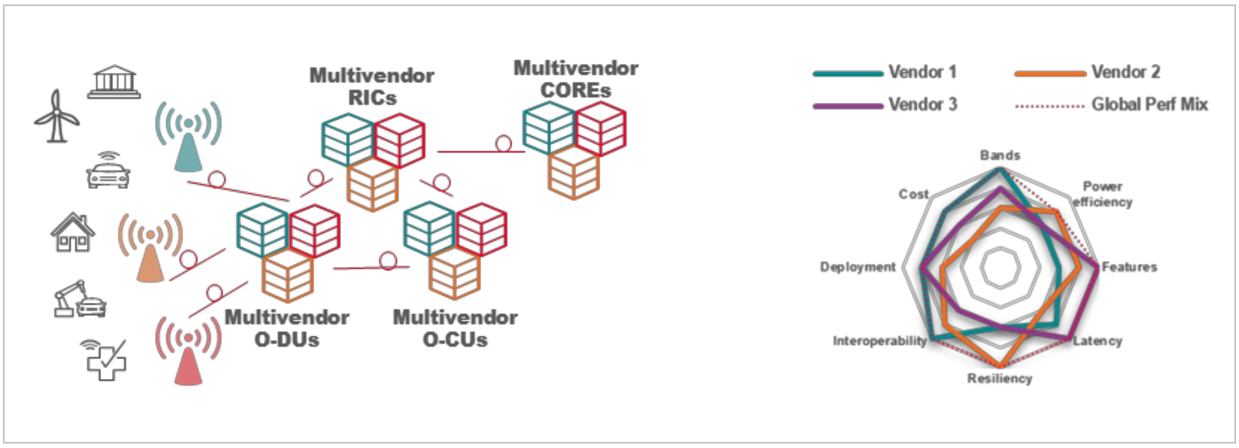


Figure 6-3: A Multi-Vendor Architecture Mix

6.1.1 Front haul Open RAN Disaggregation testing

To ensure a multi-vendor Open RAN works properly, it takes more than merely placing multiple instruments together and running through a few calls.
Testing each section individually to the maximum of its capabilities is particularly important for Open-RUs.

When testing O-RAN compliant radios, you need:

- to go beyond the test protocol because the radio does not return any status messages.
- Easily simulate the radio with the correct protocol messages containing valid 4G and/or 5G waveforms.
- Then, measure and coordinate what occurs on the RF side of the radio with the protocol side.

Proper testing ensures you choose the right network equipment for your requirements and architecture as illustrated below (figure 6-4).

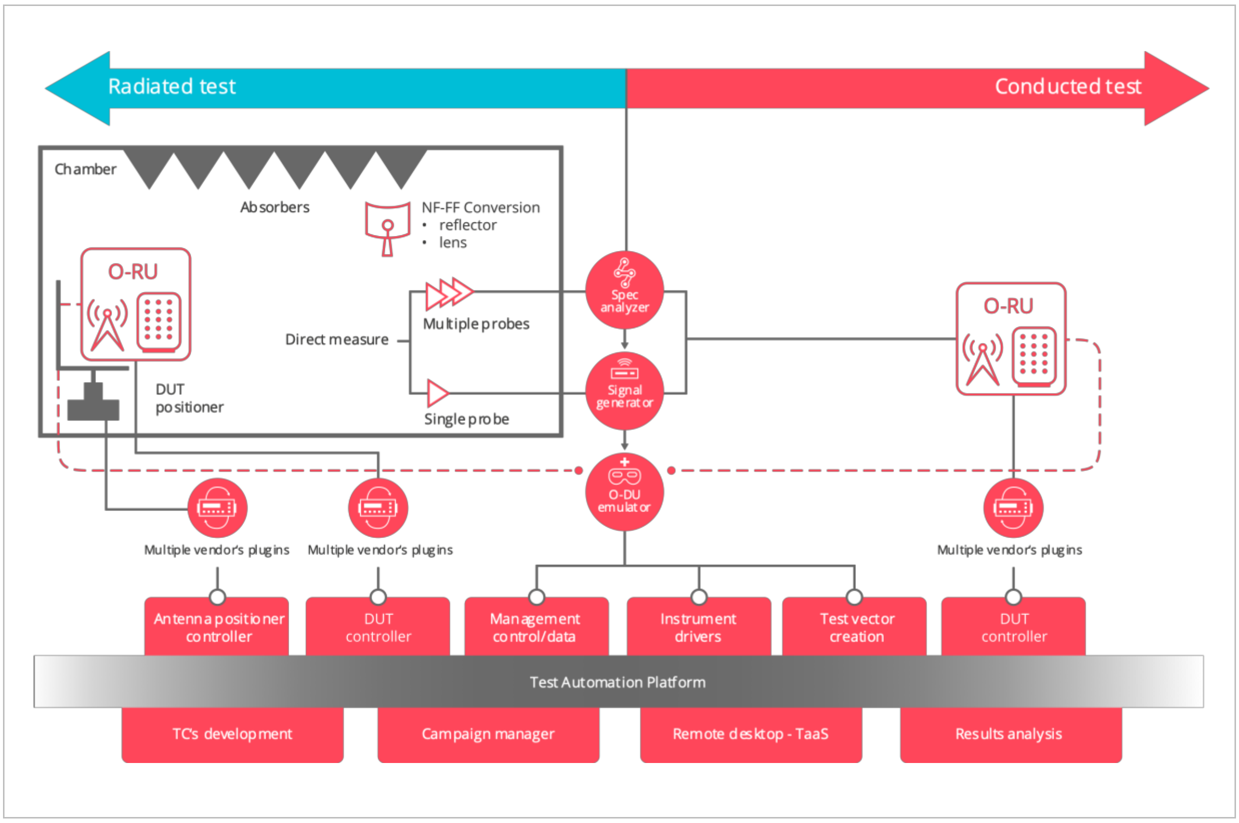


Figure 6-4: Front-haul Open RAN Disaggregation Testing

The O-RAN WG4 conformance test specification ensures the O-RU's compliance with the O-RAN fronthaul standards.

The 3GPP (test) specifications 38.141-1 and 38.141-2 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 as required by O-RAN. However, it is possible to leverage the 3GPP transmitter and receiver tests (Chapters 6 and 7 of 3GPP 38.141-1/2) when validating the O-RAN fronthaul. All test waveforms specified by the O-RAN conformance test specification use the same test waveforms used in 3GPP tests.

The test set-up can test a radio for 3GPP transmitter and receiver 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.

6.1.2 xHaul – Transport Disaggregation Testing

There are couple of challenges when we are talking about transport layer validation in a disaggregated network context.

As there is no common architecture in real life, the network architects need to allocate more time and attention in designing, deploying and more precisely in testing functions, performances and vulnerabilities for all the new network segments that are going to be deployed to support network disaggregation.

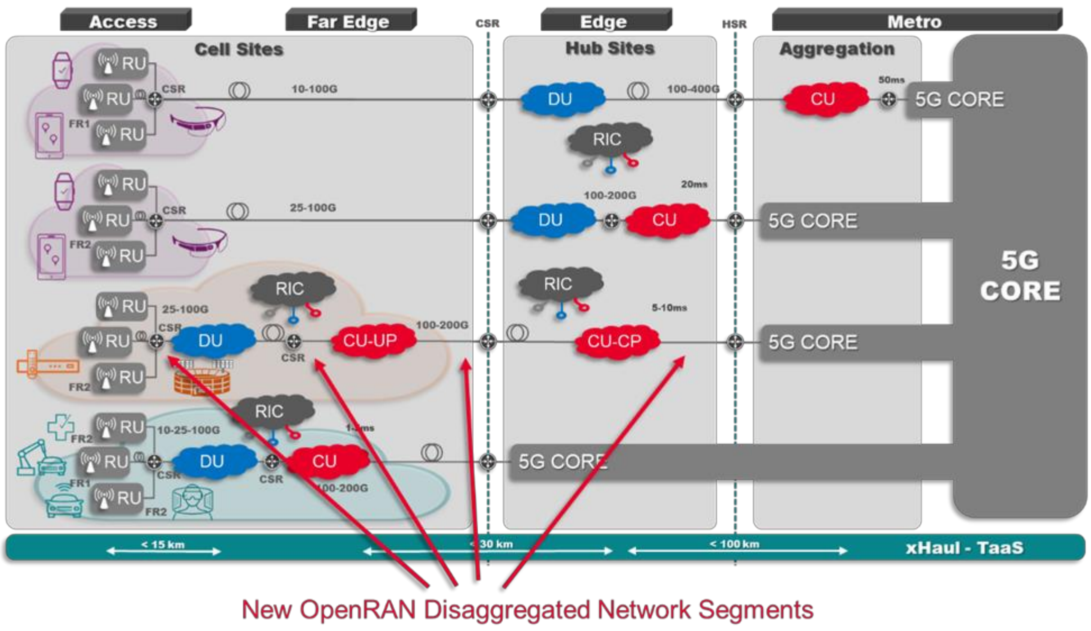


Figure 6-5: OpenRAN Disaggregation and New transport Segments

In this context, the MNOs need to verify the various transport layer technologies and engineering options before moving to production. Particularly, if we look at 5G ORAN as a whole, the transport chain is divided into 3 different network segments for Fronthaul, Midhaul and Backhaul as part of the O-RAN architecture (figure 6-5 and figure 6-6).

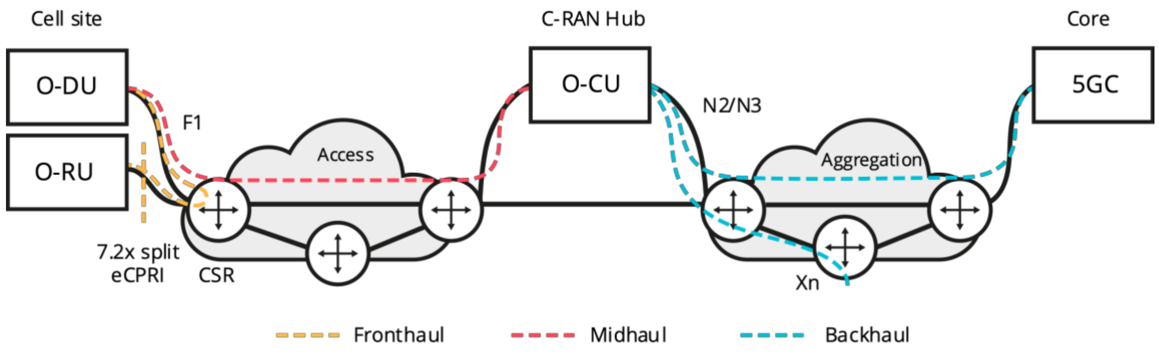


Figure 6-6: O-RAN Disaggregation Transport Segments

And with this transport disaggregation comes associated challenges:

- Multiple service levels objectives: measure the throughput, delay, jitter, and frame loss
- Variable fibre deployment models and associated impairments
- Various technologies: eCPRI, eth/IP packets, TSN
- Numerous protocols/encapsulations to carry the packets in all these network segments: Eth vs IP/UDP for eCPRI, Vlan, SR-MPLS, SRv6, Ipv4/v6
- Complex topologies: P2P, Ring, Star or Daisy Chain
- Co – existence and interworking with 3G/4G/5G and slicing
- Multi-vendor interoperability and performance validation

Therefore, it will be essential to allocate resources and new methodologies like creating dedicated xHaul sandboxes (see figure 6-7) to validate a specific mix of distributed solutions, functions, technologies, and performance level that would secure the deployment in a multivendor environment with full confidence.

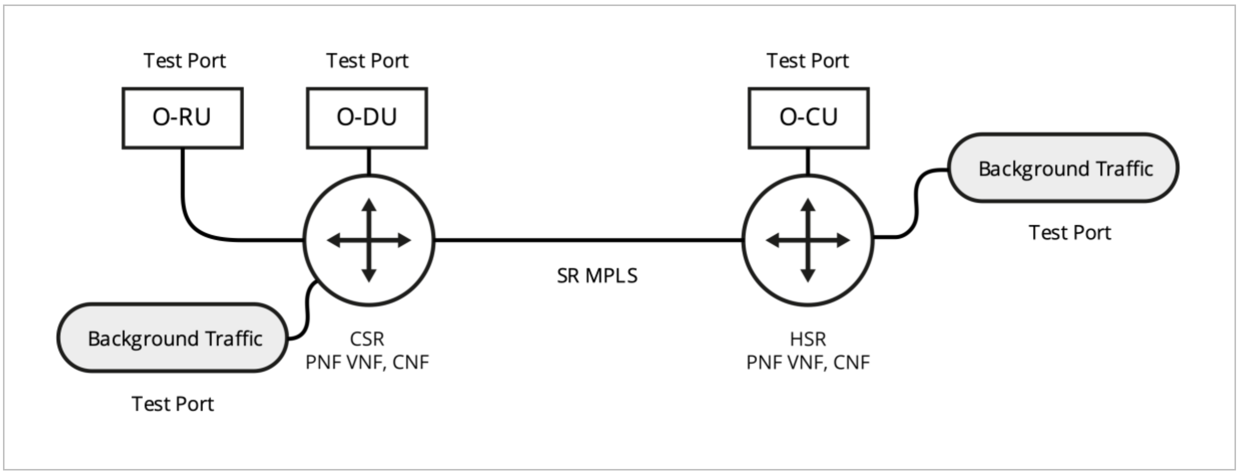


Figure 6-7: O-RAN Transport Sandbox example

6.1.3 Disaggregated Core Network Test

MNOs need to characterize and continuously validate their 5G Core (5GC) network in lab and in pre-production and deployments phase.

There are 3 main testing domains that need to be addressed for ngCORE test:

- NFVi and Cloud Infrastructure Performance & Capacity Benchmarking
- 5G Core VNF & Performance Testing
- 5G CORE testing at Scale, hybrid and distributed deployment

6.1.3.1 NFVi and Cloud Infrastructure Performance & Capacity Benchmarking

Virtualisation and Network Functions Virtualisation Infrastructure (NFVi) benchmarking enables performance characterization of a shared platform, which is critical to understanding the Total Cost of Ownership (TCO). However, benchmarking a shared platform proves to be error-prone and unpredictable due to the mystification of the individual physical components. Therefore, the use of a test application designed to rigorously benchmark the performance of virtualized network infrastructures is required. By deploying real virtual machine or docker container workloads on top of the NFVI system under test (SUT), key insights are provided into the capability of the NFVI to sustain the required VNF and cloud-native network function (CNF) workloads.

For service providers who are migrating to 5G Core, it is important to use automated test libraries that will stress the processing, the networking and the storage capabilities of the NFVI to drive proper NFVi benchmarking and in all aspects of NFVI such as:

- Complete Coverage
- Multiple VNFs for workload simulation
- VM activation and termination tests
- Noisy neighbour tests
- Open-source tools for computer, storage, memory

The aim is to set-up a Cloud Infrastructure Test and Benchmarking Platform (figure 6-8) designed to address any cloud deployment models: Telco / Edge / Public / Private / Hybrid in order to compare, optimize and identify bottlenecks.

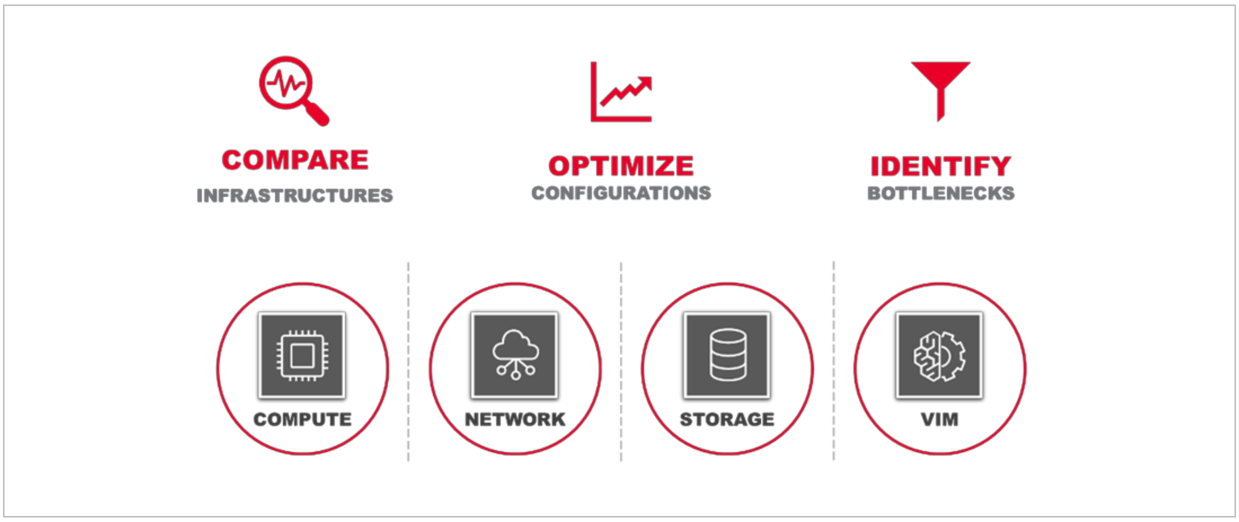


Fig 6-8 – Cloud Infrastructure test & benchmarking platform

A benchmarking platform (see figure 6-9 for an example architecture) includes the need to model Virtual Machine / Docker Container behaviour by generating synthetic workloads and delivers quantifiable KPIs used to characterize:

- Cloud solutions
- Compare infrastructure providers
- Identify configuration issues
- Assess performance bottlenecks

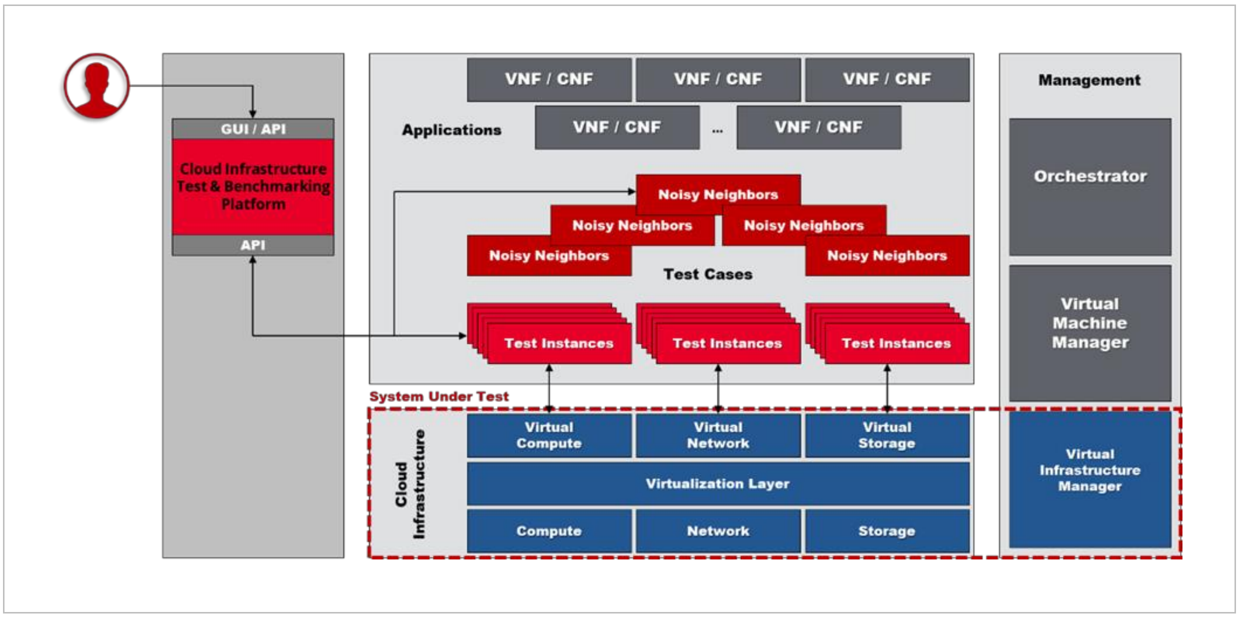


Fig 6-9 – Cloud Infrastructure test & benchmarking system architecture

The Linux Foundation Anuket group has been working on defining test suites for the purpose of verifying and benchmarking NFVi and Cloud infrastructure. Namely, the Functest project provides the means to verify any kind of OpenStack or Kubernetes deployment, including in production. It includes over 3000 functional tests and 3 hours upstream API and dataplane benchmarks. It's completed by Virtual Network Function deployments and testing (vIMS, vRouter and vEPC) to ensure the platform meets Network Functions Virtualization requirements.

In order to assist with the CI/CD pipeline, Anuket also provides the Xtesting project. By managing all the interactions with the CI/CD components (test scheduler, test results database, artifact repository), it allows the developer to work only on the test suites without diving into CI/CD integration.

6.1.3.2 5G Core VNF & Performance Testing

The importance of the one-stop-shop for testing 5G Core from end-to-end to node isolation, that simultaneously simulates multiple nodes and interfaces to validate core network virtual functions is now evident.

Re-creating entire networks in the lab enables engineers to validate critical 5G requirements to maximize network reliability and performance. They can leverage the solution's built-in per-UE detection mechanism to validate QoS enforcement at a high-performance level at the UPF.

Testing can use real-world subscriber modelling to perform capacity tests, device's throughput, measure voice and video quality, and model a wide variety of mobility scenarios.

Full automation via REST API and Python allows users to create regressions for continuous validation of product quality and to adapt their environments to the CI/CD lifecycle demands.

Key 5G Core sandbox capabilities:

- Simulate UE behaviour in multiple 5G use cases: Network slicing, multi-access edge computing (MEC) low latency and offloading, video optimization
- Scale up to millions of subscribers using stateful application traffic mixes that can interact with real servers and peers
- Perform service quality validation with subscriber modelling, multiplay traffic, and quality of experience (QoE) measurements

- Validate complex scenarios for service-based architecture (SBA)
- Control test traffic mix and intensity using network objectives to independently manage control and user plane

6.1.3.3 5G CORE testing at Scale, hybrid and distributed deployment

Due to the dynamic nature of network slicing and new, fully virtualised architecture of 5GC, validating both functionality and especially individual, per slice KPIs at scale is a challenge.

Hundreds of dynamically created and destroyed instances of tens of newly introduced network elements in the SBA architecture must work together at scale to provide a seamless, lower latency, higher capacity 5G network. It is no longer sufficient, for example, to test individual network functions such as the UPF in isolation or to push out line rate throughput to validate QoS.

Instead, Mobile Network Operators have to execute End to End system tests that exercise slices via the appropriate traffic as well as evaluate any impacts from one slice to others. This requires a test platform that can enable the design and run of test suites for performance, conformance and regression testing including negative testing and that exercises all the functionality of the SBA nodes.

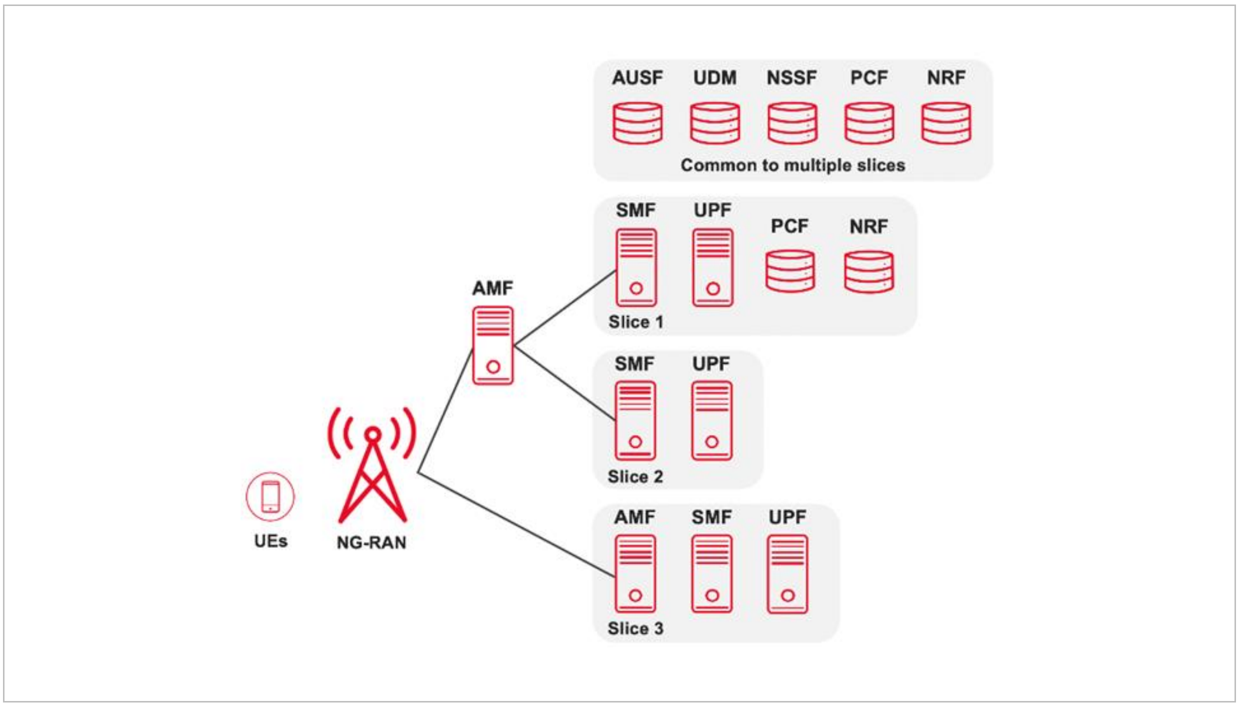
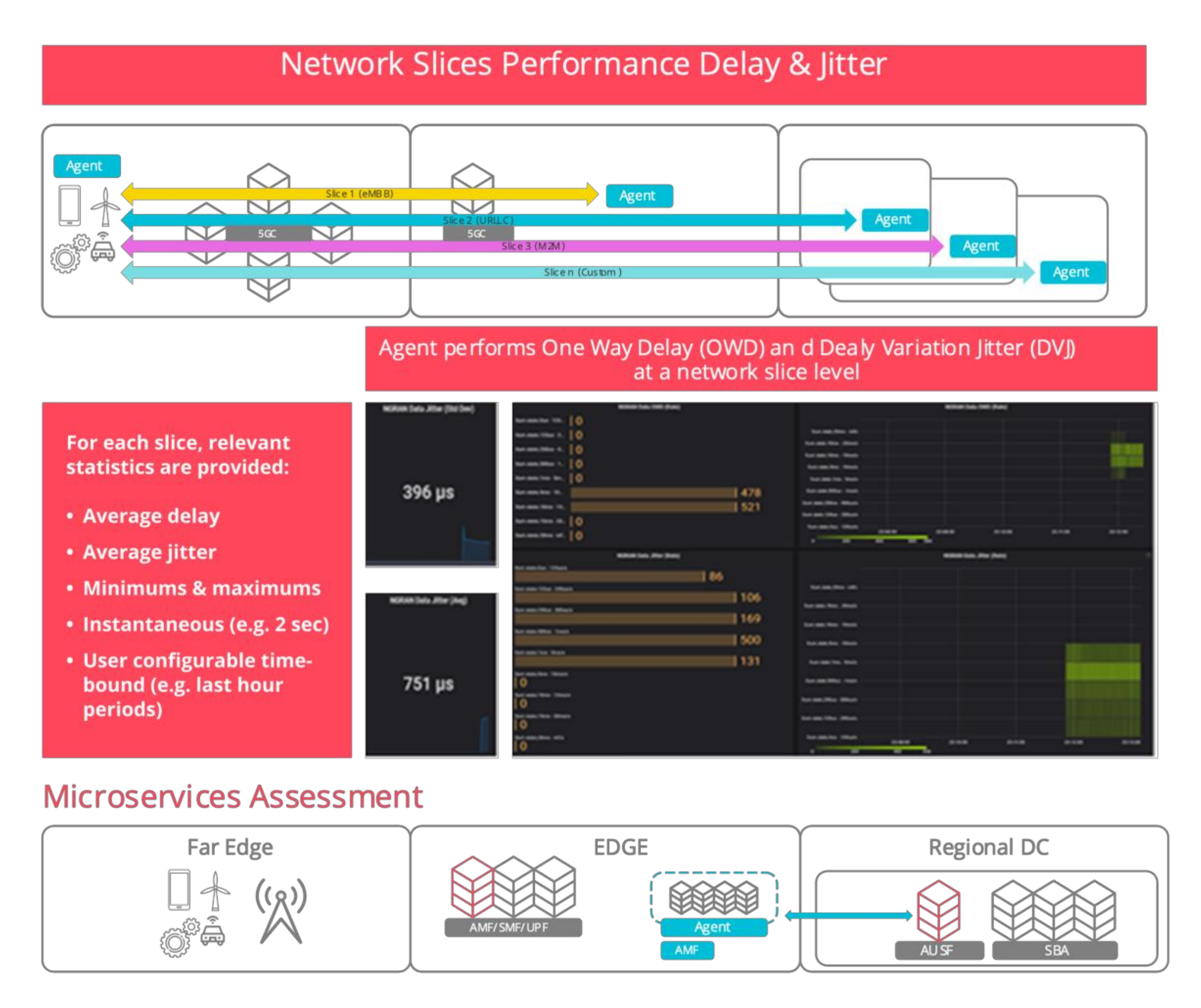


Fig 6-10 – Multiple Slices topology and distribution deployment validation

Figure 6-11 below illustrates the deployment use case and dedicated KPI that need to be addressed for a proper validation.



Network Slices Performance Delay & Jitter

Agent performs One Way Delay (OWD) an d Dealy Variation Jitter (DVJ) at a network slice level

For each slice, relevant statistics are provided:

- Average delay
- Average jitter
- Minimums & maximums
- Instantaneous (e.g. 2 sec)
- User configurable time-bound (e.g. last hour periods)

Microservices Assessment

Fig 6-11 – Hybrid distributed SLA and KPIs Validation

To succeed at core network testing in the 5G era, operators' engineers need to:

- Replicate real life in the laboratory to eliminate quality issues, benchmark network solutions, and validate network vendors' software updates
- Test nodes in isolation to ensure all network elements perform as expected
- Test and validate the QoS implementation and CUPS to reduce network delay

6.1.4 O-Cloud O-DU / O-CU / RIC Validation at Scale

Fronthauling, disaggregation, distribution and intelligence are key foundations of the network transformation and Next Generation Networks for 5G and beyond.

Nowadays, functional, interoperability and performance validation at scale is a major subject for network disaggregation transformation and distribution characterization.
O-Cloud infrastructure matters and impacts performance and latency in sensitive applications.
O-RAN WG-6 cloud architecture (CAD) provides dedicated recommendations.

The recommendations are based on these infrastructure deployment models:

- Non-Uniform Memory Access (NUMA) Zones
- Noisy Neighbours Hyper-Threading
- Hyper-converged Cloud
- Horizontal Scaling

Validation Scenarios:

- Measure latency within one single compute node (Non-Uniform Memory Access)
  Determine the impact of NUMA placement and CPU Hyper-Threading on latency performance.
- Measure latency across different compute nodes.Determine the impact of cloud size and scaling on latency performance.
- Measure latency with different number of applications
  Determine the impact of cloud resource utilization on latency performance.
- Measure latency with different payload sizes
  Determine the impact of payload size and fragmentation on latency performance.

Based on this, some obvious outcome and infrastructure guidelines have emerged:

1. NUMA Zone Validation: It is critical to be able to ensure that low latency applications are associated with cores which are connected to the same NUMA zone.

2. Compute Nodes Validation: O-DU / O-CU are performance sensitive and require the ability to consume a large amount of CPU cycles to work correctly.

3. Resource Utilization Evaluation: Enabling CPU Hyper-Threading has a detrimental effect on latency consistency.

4. O-RAN Hyper-converged Cloud (all-in-one Controller / Worker / Storage): Active Controller + Worker Node scenario incurs a very minor overhead.

5. Inter-nodes Transport Layer Validation: Scaling out applications across the cluster must consider the network latency overhead between nodes.

Performance level of such diverse and hybrid architecture must be assessed and characterized to guarantee the service level agreement are as expected by the end service users.

All these services and hybrid configuration and as well as Open RAN system architecture deployment strategies need to be validated:

- O-Cloud Validation including O-DU / O-CU / RIC
- Hybrid Architecture Performance Validation
- SLAs Performance Validation & Statistics

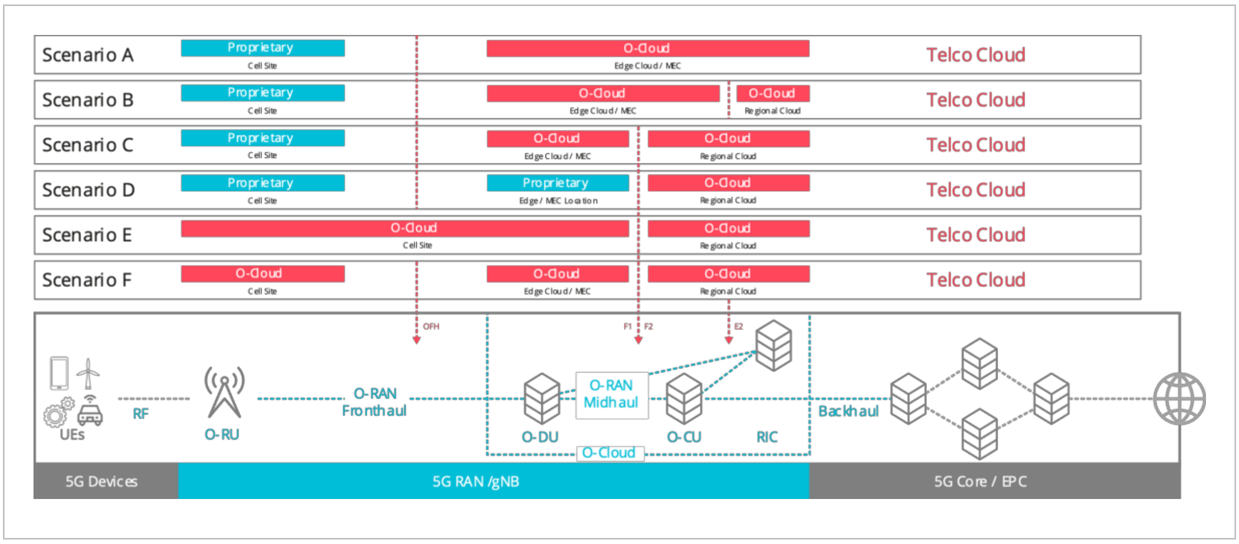


Fig 6-12 – O-Cloud deployment strategies validation - Private / public

The industry has established a number of initiatives to promote interoperable O-RAN bricks:

From the O-RAN alliance:

Plugfests

- Focused on PoCs. Support the ecosystem players in testing and integration of their solutions, ensuring the openness and interoperability of O-RAN solutions from different providers.

OTICS (Open Testing and Integration Centers)

- Test and verify the conformity of RAN equipment to O-RAN interface specifications
- Test and verify the interoperability of RAN equipment from different vendors (or the same vendor) using O-RAN interface specifications, based on O-RAN interoperability test specifications
- Test and verify the end-to-end system integration of groups of Devices under Test (DUT), based on O-RAN interfaces, using O-RAN E2E test specifications

O-RAN Alliance Certification and badging

Certification is applied on conformance tests, which involve only a single Device Under Test (DUT). A verification that the DUT behaves according to a concrete O-RAN technical specification
Badging is applied on interoperability tests (IOT) and end-to-end (E2E) tests. As the IOT and E2E tests involve multiple DUTs (from different vendors)

Type of Certificates/Badges:

- Certification of Conformance: verification of compliance of the device under Test (DUT) to O-RAN interface or reference design specifications, using O-RAN conformance test specifications.
- Interoperability Badge. Defined as an assessment of interoperability of pairs of devices under Test (DUT), which are implemented according to O-RAN interface specifications, using O-RAN Interoperability Test (IoT) specifications.
- E2E System Integration Badge. It is defined as an assessment of end-to-end system integration of groups of Devices under Test (DUT), which are implemented according to O-RAN interfaces, using O-RAN E2E test specifications.

6.1.5 Disaggregated Network Visibility

Network visibility is also quite impacted by network disaggregation, multi-vendor and distributed virtual functions.

Within virtualised, cloud-native environments:

- Topology (physical and virtual) is hidden
- Interfaces are hidden
- Flows are hidden (packets, octets, and protocols).

The fundamental of visibility, data access, has changed, which creates a whole new set of challenges for operators:

- Physical taps will no longer be an option for virtual workloads
- CNF-to-CNF
- Pod-to-pod
- Pod-to-service
- External communications
- Encryption
- Dynamic scaling (up and down)

With few exceptions tapping network connections and leveraging packet brokers and probes will no longer be practical and would not provide the necessary visibility into virtualized network resources and communications, dynamically changing/scaling network topologies, resource utilization or network slicing-related SLA metrics.

The ability to access, capture, and continuously monitor data at any point across the virtualize cloud-native environment needs to be the primary focus, and legacy solutions fall short in this regard.

A new network visibility platform is needed (figure 6-13):

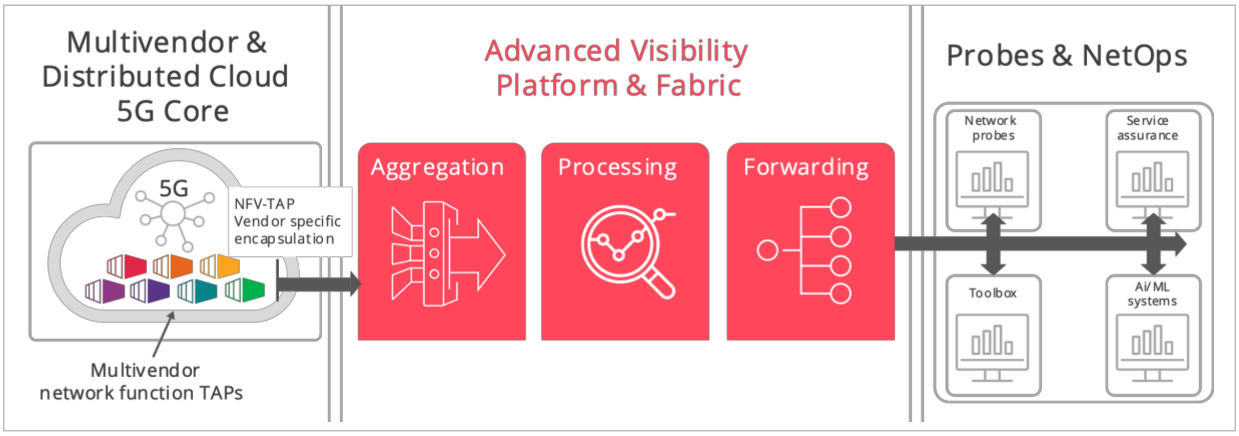


Figure 6-13: Next Generation Visibility Platform architecture

On the left section multi-vendor 5G Core NFV-TAP vendor-specific encapsulation and Multivendor network function vTAPs and version management.

Middle section: 5G Visibility platform & Fabric which is responsible for Trusted delivery channel, Visibility enrichment, Secure delivery, Context Filtering & sampling and KPI & Meta data generation

Finally, the right section is handling NetOps consistent flows toward Network probes, Service assurance, Toolbox and AI/ML systems.

The hybrid network distributed visibility use case:
Today it no longer makes sense to talk about computing at a single “edge.” A modern network consists of multiple layers, each with its own compute capabilities and latency trade-offs.

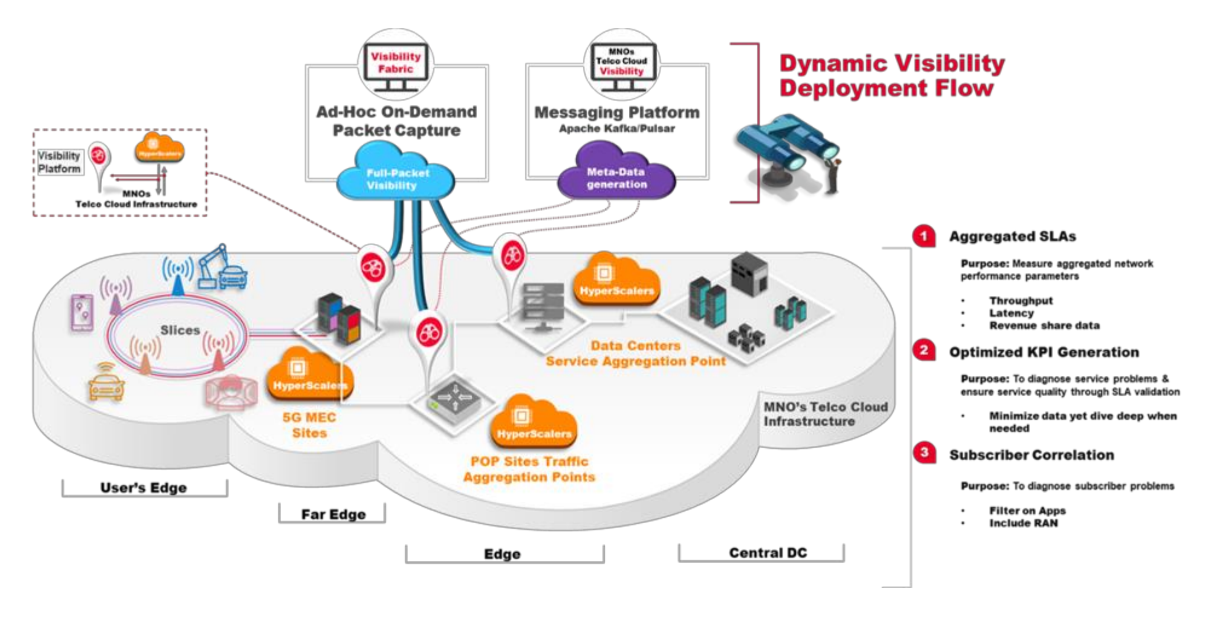
Traditionally, MNOs has been managing these trade-offs and interactions between the two innermost layers:

- Large and Sparse public cloud data centres
- Content Delivery Networks (CDN’s)

The challenge is, MNOs would like to deploy the same probes and visibility they have already for the rest of their TAP and C-RAN sites, however, due to the sheer number of sites it’s cost prohibitive.

However, the rise of 5G and multi-access edge computing (MEC) using hybrid (private and public clouds) creates new capabilities, with corresponding set of complexities.

The introduction of distributed Visibility enables operators to access and understand the nature of the traffic passing between their network and their MEC hyperscale partners by simply collecting network statistics.



Aggregated SLAs

Purpose: Measure aggregated network performance parameters

- **Throughput**
- **Latency**
- **Revenue share data**

Optimized KPI Generation

Purpose: To diagnose service problems & ensure service quality through SLA validation

- **Minimize data yet dive deep when needed**

Subscriber Correlation

Purpose: To diagnose subscriber problems

- **Filter on Apps**
- **Include RAN**

Figure 6-14: Hybrid Network Visibility Platform architecture

The trend now is in enabling visibility as a dual action solution where we combine metadata generation with full packet analysis. The metadata delivery will focus on high level statistics to help locate problem areas, and once one is detected a deep-dive on specific subscriber traffic on interest can be conducted.

6.2 The integrated test workflow CI/CD/CT

This introduces what is called "Lab to Live" concept which is a tight integration and path between lab and live network operation which now are part of CI/CD integrated processes.

In addition, another new concept is in use by MNOs which is "constant testing" lifecycle and complementing the "CI/CD" process automation with "CT" as part of "Lab to Live" cloud network lifecycle framework. Figure 6-15 shows this workflow from Day 0 through to operation and optimization.

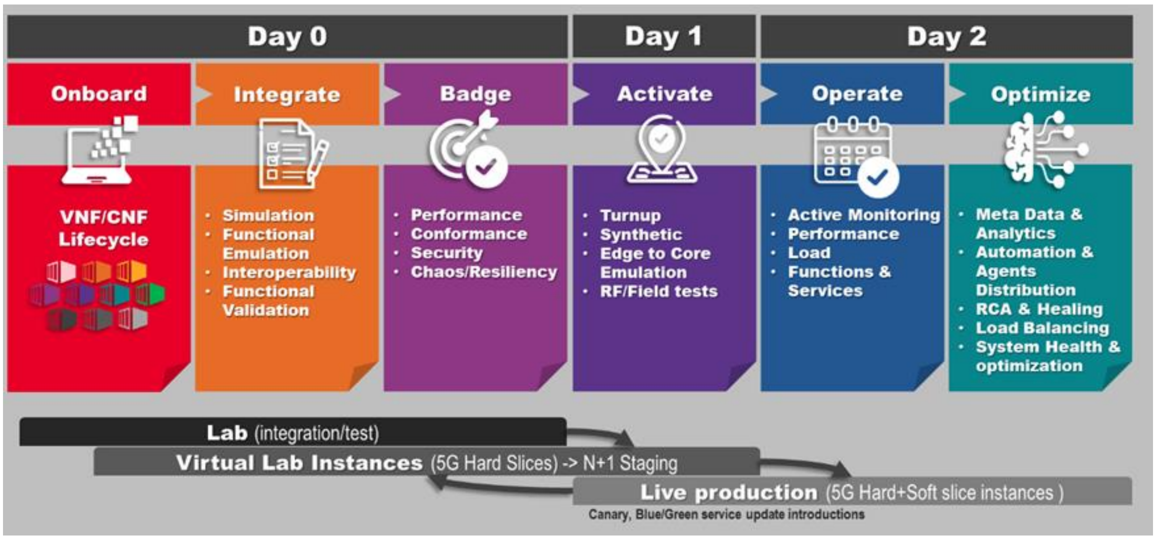


Fig 6-15 – Lab to Live cloud network testing lifecycle

The CI/CD/CT workflow and from “Lab to Live” to network operation mode includes the following:

- CI/CD/CT (Continuous Testing)
- Service activation
- Service monitoring
- Triggered diagnostic
- Extended visibility meta data & analytics
- Telco Cloud Security Towards “Zero Trust” SecOps
- Administration & System Health

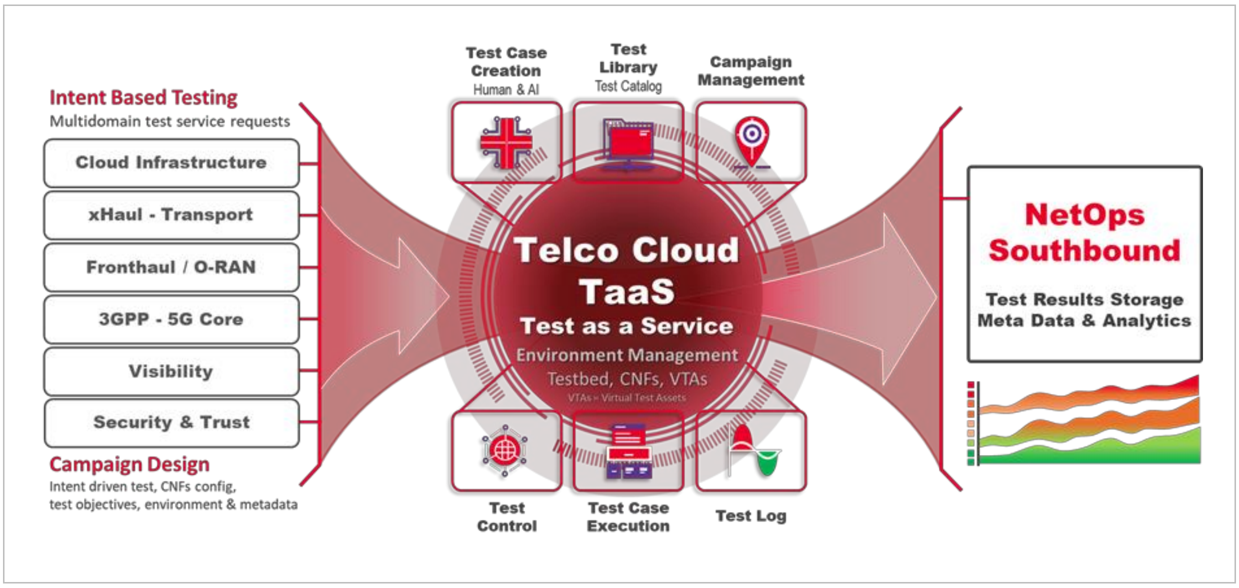


Figure 6-16: A TelcoCloud TaaS Platform

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

Ideal Test framework coverage and capabilities:

- Test objectives vary by phase; test cases are leveraged/adapted in later phases
- Test types: ad-hoc, campaign, continuous testing
- Testbed orchestration varies between lab slices and production

Test execution types:

- Ad-hoc testing troubleshoot & verify functionality on demand
- Scheduled/Campaign characterization/benchmark/scale/functional suite of tests
- Continual active monitoring sustained testing for Shift Right, SLA in live production

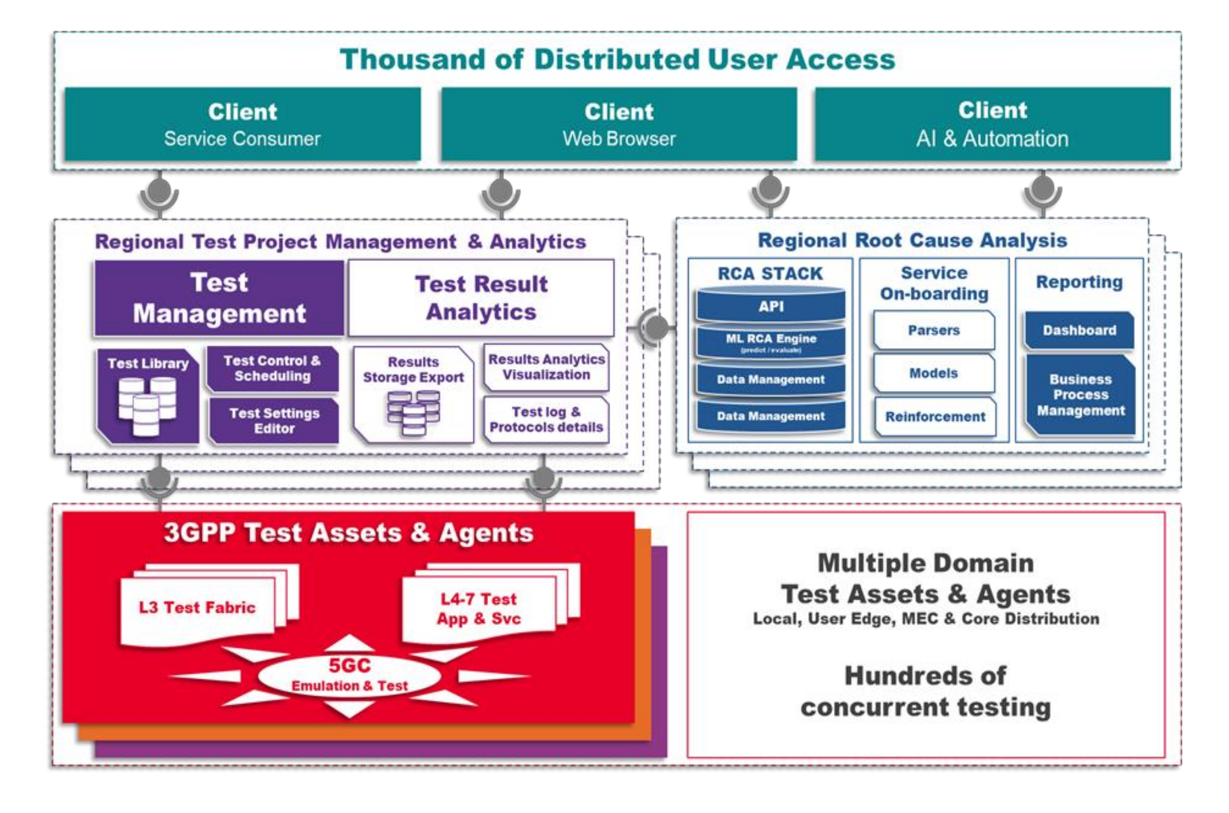

Thousand of Distributed User Access
Client
Service Consumer
Client
Web Browser
Client
AI & Automation
Regional Test Project Management & Analytics
Test Management
Test Result Analytics
Test Library
Test Control & Scheduling
Test Settings Editor
Results Storage Export
Results Analytics Visualization
Test log & Protocols details
Regional Root Cause Analysis
RCA STACK
API
ML RCA Engine
Data Management
Data Management
Service On-boarding
Parsers
Models
Reinforcement
Reporting
Dashboard
Business Process Management
3GPP Test Assets & Agents
L3 Test Fabric
L4-7 Test App & Svc
5GC
Emulation & Test
Multiple Domain Test Assets & Agents
Local, User Edge, MEC & Core Distribution
Hundreds of concurrent testing

Fig 6-17 – Nationwide Distributed Cloud based Network Test Bed Orchestration

Root Cause & Analytic - RCA:

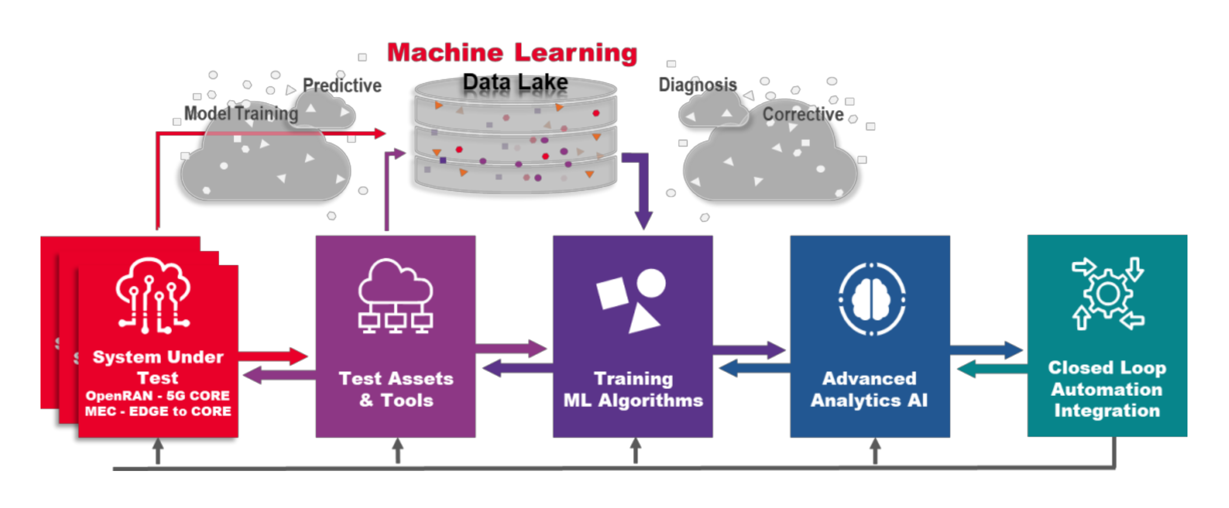


Fig 6-18 – Automated Root-Cause Analysis Topology

Automated RCA and Anomaly Detection Capabilities:

- Cover the entire 5G Core & Open-RAN ecosystem
- Full AI/ML ModelOps, from data and model versioning to deployment

- Enables end-to-end fully-automated CI/CD/CT/CV pipeline

RCA Benefits:

- Fast and more efficient issue resolution, use of SMEs
- Reduced time to operation of complex new technologies
- Higher quality Open-RAN rollout
- Reduced CAPEX and OPEX

6.3 The Test Taxonomy and Requirements from Test Assets, Process Automation to TaaS (Test as a Service)

Distributed & Automated Network Assurance overview:

We explore some of the following use cases:

- Cloud Infrastructure Performance & Capacity Benchmarking
- MEC/Hybrid Cloud Assurance - CI/CD/CT
- O-Cloud OpenRAN
- Service Monitoring
- Triggered Diagnosis & Root Cause Analysis
- Meta Data & Analytics
- Administration & System Health

For the special MEC/Hybrid Cloud Assurance use case - CI/CD/CT, MEC assurance becomes essential for critical edge compute applications and performance and particularly in a multi-cloud environment at the Carrier/Hyperscale gateway.

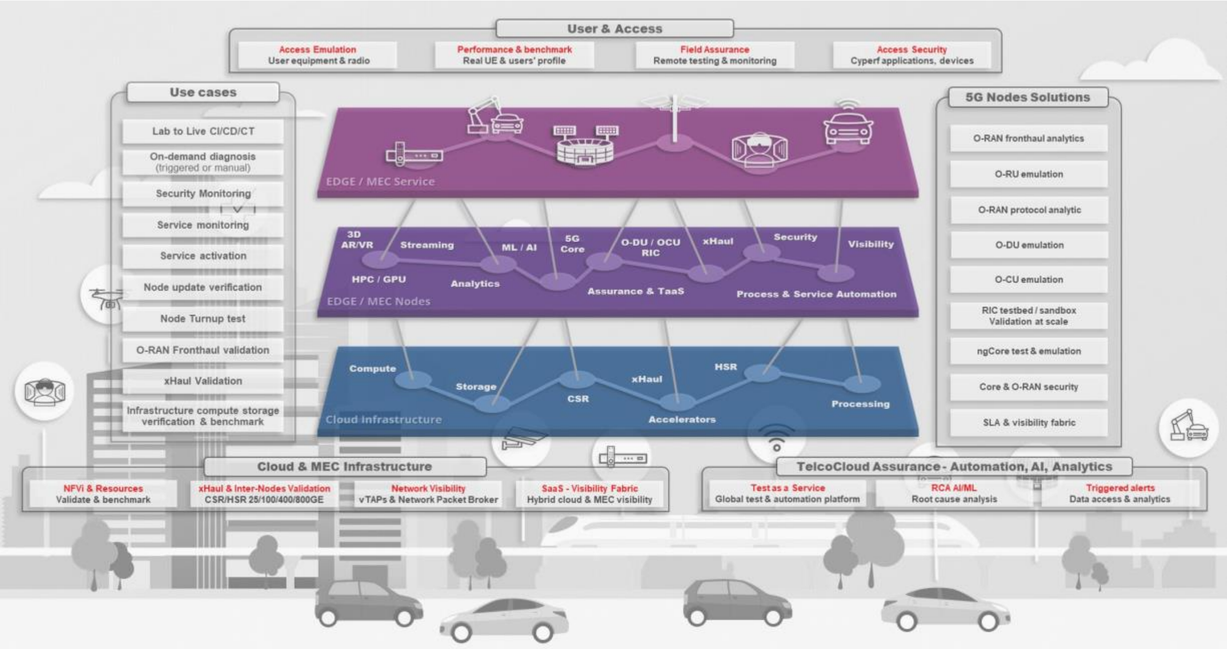


Figure 6-19: Telco Edge Cloud, Next-Gen Service Assurance at Scale

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 Capacity & Performance for Latency, Bandwidth and Resiliency, Benchmarking, Scaling and Secure Access Service Edge (SASE).
Then 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).
And finally the top floor for the MEC vertical Services and 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.

6.4 The Transformation on test process, tools, competencies and organization

All of the above will impact how operators perform test and integration. Vendors will be impacted as well, since they will need to integrate with the operator's pipeline. Testing and integration will be part of the bigger DevSecOps pipeline, described in the next chapter.

7 DEVSECOPS

7.1 Abstract

DevOps is a combination of Development and Operation, which is a collective term for a set of processes, methods and systems used to facilitate communication, collaboration and integration between development (application/software engineering), technical operations and quality assurance (QA) departments. DevSecOps adds security processes to the DevOps principles. It aims at reconciling the need to deliver with the security requirements.
Network virtualization and network disaggregation have brought more supplier equipment combinations and management approaches to operators. The construction and maintenance of telecom network infrastructure and the iteration of communication services/industry applications are increasingly taking on a software-centric cross-organisational collaboration model. To ensure that network quality, customer experience, implementation time, optimisation and maintenance are not negatively affected by technological change, organisational operating models are also required to change to adopt new processes, skills and tools.
It is envisaged that a, DevSecOps organisational design will become a necessary means to comply with the trend of network virtualisation and network disaggregation. This would also extend to cooperation between telecom software suppliers and operators' teams in the future.

7.2 Expectation of benefit - saving potential

By setting up a joint DevSecOps pipeline, rapid (yet secured) upgrade iteration and delivery of software-based network functions and network management systems can be realized, new functions or new business launch cycles can be accelerated, efficiency improved, and costs reduced while maintaining security standards.

7.3 DevOps

7.3.1 Recommendations for Joint DevOps functionality

In order to maximise the move to DevOps with a joint DevOps, pipeline shall provide the following functionalities:

- Automatic delivery: The software from the supplier pipeline to the operator pipeline is automatically delivered to ensure that the operator pipeline can obtain the latest software products in time.

- Acceptance test: The automated tests carried out by the operator's pipeline after receiving the software product to verify whether the software delivered by the supplier meets the operator's expectations. The test can cover trust verification, functional test, performance test, etc.

- Production deployment: Automatically deploy the software that passes the acceptance test to the production environment and provide external services.

- Operation monitoring: Automatically monitor and collect the operational data of supplier software in the operator's production environment for supplier information feedback.

- Information feedback: The operator shall timely feedback the delivery (test), deployment (operation) status and necessary auxiliary information of the newly released software to the supplier for the continuous optimization of the supplier's software.

7.3.2 Recommendations for Joint DevOps implementation

7.3.2.1 Interface

To automate joint DevOps across suppliers and operators (figure 7-1), the following interfaces should be defined:

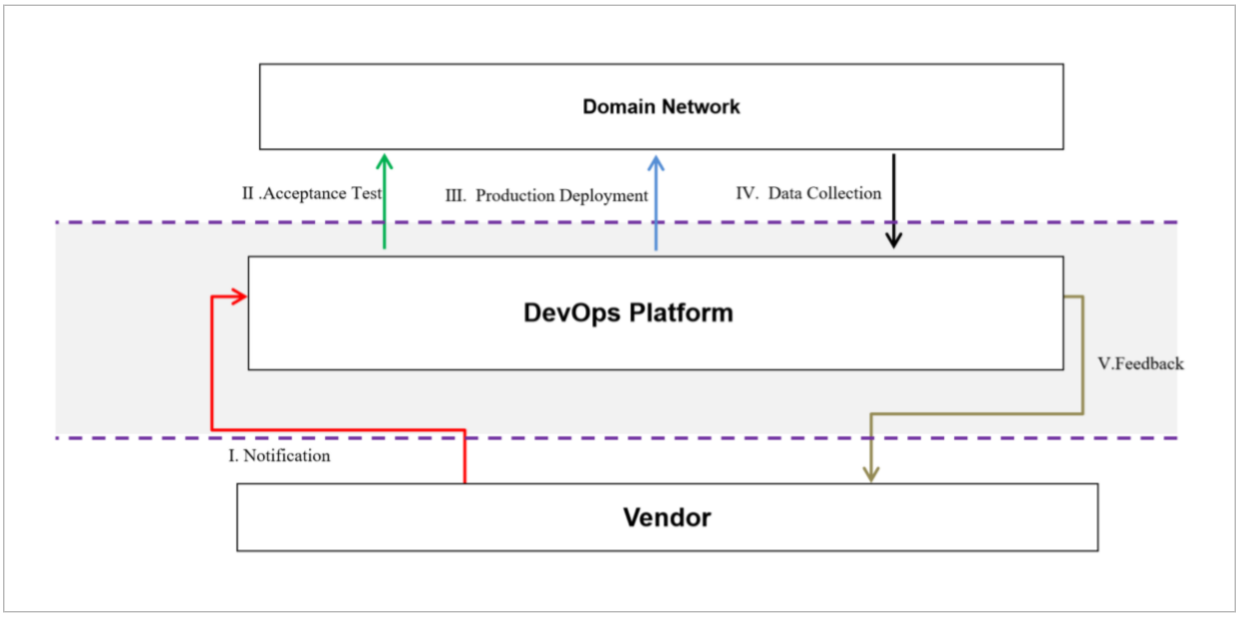


Figure 7-1: Joint DevSecOps

- Interface between DevOps pipeline and suppliers
    - Software synchronization interface: it is used to realize the delivery stage of the supplier's software product release to the operator's pipeline. Through this interface, once the supplier has a software update, it will automatically trigger the subsequent automatic pipeline on the operator's side.
    - Information feedback interface: it is used to realize the information feedback stage from the operator's pipeline information extraction to the supplier's R&D pipeline. This interface is used to form a DevOps iterative closed loop to promote the rapid feedback and upgrade iteration of the supplier's software problems.
- Interface between DevOps pipeline and network management system
    - During the implementation of the DevOps pipeline, it is necessary to coordinate the interface of the network management system to realize the automation process, including:
    - Acceptance test stage
        - Connect to the DevOps server to complete the deployment and configuration of resources and services on demand
        - Connect to DevOps servers to provide network data and analysis services on demand
    - Operation monitoring stage
        - Accept the update notification of the DevOps server, implement the upgrade operation inside the system, and notify the DevOps server after the upgrade is completed
        - Support the collection of operational or environmental data, receive data collection requirements from data handling components, continuously monitor the running status of the software, optionally, with data analysis function
        - When there is a problem with the software operation, support the feedback of relevant operational data, environmental data or analysis results to the data handling component on demand

7.3.3 Recommendations to the Standard

3GPP

- SA5: It is recommended to enhance the following network management functions and open corresponding interfaces to support the DevOps automation process
  - Life cycle management: support automated operations such as test/production environment topology or network element deployment, upgrade, update, and termination
  - Service configuration: Support rapid service configuration and provisioning in the DevOps process
  - Resource verification: used for verification of data and other related resources in DevOps pipeline
  - Performance management/alarm management: Support NF-level performance/alarm data subscription
  - Log management: support subscription or download of system operation logs by NF level
  - Data analysis service: support on-demand subscription of data analysis service to obtain operational data analysis results

ETSI

- NFV TST:
  - Establish a general DevOps system framework for connecting with different network management systems
  - Clarify interface requirements for cross-organization DevOps (including network management system interface requirements, and interface requirements between suppliers and operators)
  - Standardized test case description template to support automated testing
  - Identify the functional requirements for NFV MANO to support cross-organization DevOps and extend existing NFV MANO related standards

7.4 DevSecOps

The Telco domain is facing to a lot of transformation as network softwarization and also the system's disaggregation (split of hardware and software) for gaining flexibility and agility in the network scalability and evolution. However, the disaggregation of network solutions introduces new threats and risks due to the multiplication of the number of interfaces and the need for network openness based on the use of API's and Opensource solutions and tools.

The disaggregation of network solutions coupled with Opensource solutions and tools adoption, requires a new approach in term of security due to the threats and risks increasing with this new approach based on virtualization and cloud native technologies. In addition, the need of networks operations automation implies having an acceptable security level to perform integration and validation tasks as it is very important to prevent attackers to take the control of networks automation tools (like Gitlab CI/CD chain). If security is not factored into this approach, the benefits of CI/CD are simply lost because it is inefficient to factor in security at a later phase. Thus, a DevSecOps approach is a key element to better secure software networks services delivery in the continuous improvement mode. Applying DevSecOps approach to networks solutions disaggregation requires a lot attention on possible supply chain attack vectors regarding hardware failure and also regarding the software used for infrastructure and networks functions.

7.4.1 What does a DevSecOps approach means to network disaggregation?

DevSecOps approach means taking into account of security requirements and best practices in the DevOps mode. DevSecOps is mandatory in the operations automation context and (in the context of) the security of CI/CD chain it becomes more and more essential as a lot of sensitive information manipulated is present in several files which require to be protected. Networks also need to be protected from some vulnerabilities coming from microservices. DevSecOps is a way to integrate and execute automatically and continuously security rules and policies in the CI/CD chain: risks assessment, code analysis (static or dynamic), security tools deployment (System hardening, scan, fuzzing, pentests, certificates lifecycle management, …) answering to a project or context need and objective. In a nutshell, DevSecOps's objective is to automate the security tools in order to industrialise the security checks within the CI/CD chain and also the ability to force security configurations even if they are not initially planned in the backend. DevSecOps approach has also to implement the monitoring of security logs and events as well as in integration and production chains.

8 PROCESSES AND CAPABILITIES FOR NETWORK AUTONOMY

8.1 Measurable goals of operations

An essential goal for the next generation network operations is autonomy of networks in regards of automation, also known as zero-touch operations. Capabilities of management services such as "closed loops" enable network autonomy.

Autonomy of the networks balances out the growing complexity (as mentioned in 3.1), and frees the operator for higher value tasks, such as designing new services. With that, the operator's task moves away from the network operations itself, towards the service design in a DevOps approach (as described in chapter 7). In this way the goal of the CI/CD process becomes the "Autonomous Network Operations".

Network autonomy is enabled by appropriate management systems. The design capabilities need to allow the operator to design new services together with their automation. Looking at standards, this enablement is the primary subject of the ETSI group "ZSM", while many standards contribute to this with various means.

The expected benefits of network disaggregation are identified in chapter 2: Adoption Flexibility, Innovation Acceleration and Expenditure Reduction. Mapping these to concrete operations business metrics, an example may look like this:

- Improved Time to Market for a new service (e.g. less than X months)
- Minimize Down time of critical services (e.g. service being unavailable for less than X minutes per year)
- Reduce time to onboard a new VNF (e.g. less than X weeks)
- Reduced time to migrate a VNF version (e.g. less than X hours)
- Improved time to patch VNFs (e.g. not more than X hours)
- Defined proportion of fully automated problem detection and resolution (e.g. minimum X %)
- Defined Mean Time to Repair for non-automated problem (e.g. resolution in less than X hours)

It is encouraged for an operator to define such goals to really define the improvements expected from disaggregation as well as to clearly measure if goals are met and where optimization is still required.

Disaggregation and cloudification are enablers to achieve such ambitious goals, but it requires the right processes and capabilities, otherwise such goals can never be achieved.

In the picture below (figure 8-1) is shown how the CI/CD process becomes a key element in the Operational Transformation, since CI/CD is the link between the Continuous Automation (which is the process of automation design) and the Autonomous Network Operations at Runtime.

Vendors will contribute their software components into the Continuous Automation process, through an automated pipeline. As a result, it becomes a task of the operator to aggregate the different vendor components for the specific services.

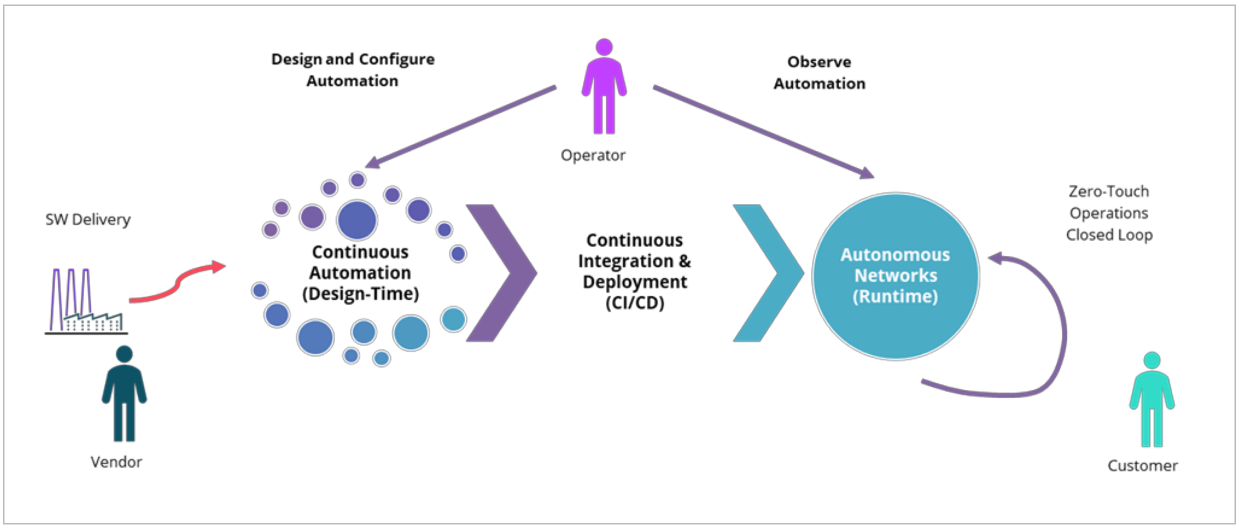

Design and Configure Automation
Operator
Observe Automation
SW Delivery
Continuous Automation (Design-Time)
Continuous Integration & Deployment (CI/CD)
Autonomous Networks (Runtime)
Zero-Touch Operations Closed Loop
Vendor
Customer

Figure 8-1 Operations becomes DevOps

In consequence,

- the processes of operations need to be adapted towards a DevOps approach (Please see Chapter 7 for DevOps).
- the management systems need to provide capabilities to enable autonomy, but also to accelerate and simplify the DevOps process
- finally, 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. Operations need to prepare and plan for that and consider migrations steps to full cloud native networks.

Given an automated business monitoring for the above mentioned metrics is in place, the transition of operations processes and capabilities can be managed for success.
Autonomous service management (enabling autonomous networks) tries to put analysis and 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.

8.2 Operation processes evolution

8.2.1 Operation processes blueprint

Identifying management functions of autonomy, for example looking at 5G as defined by 3GPP for network slicing, we need to address the necessary processes for Design and CI/CD in a blueprint like this (see figure 8-2):

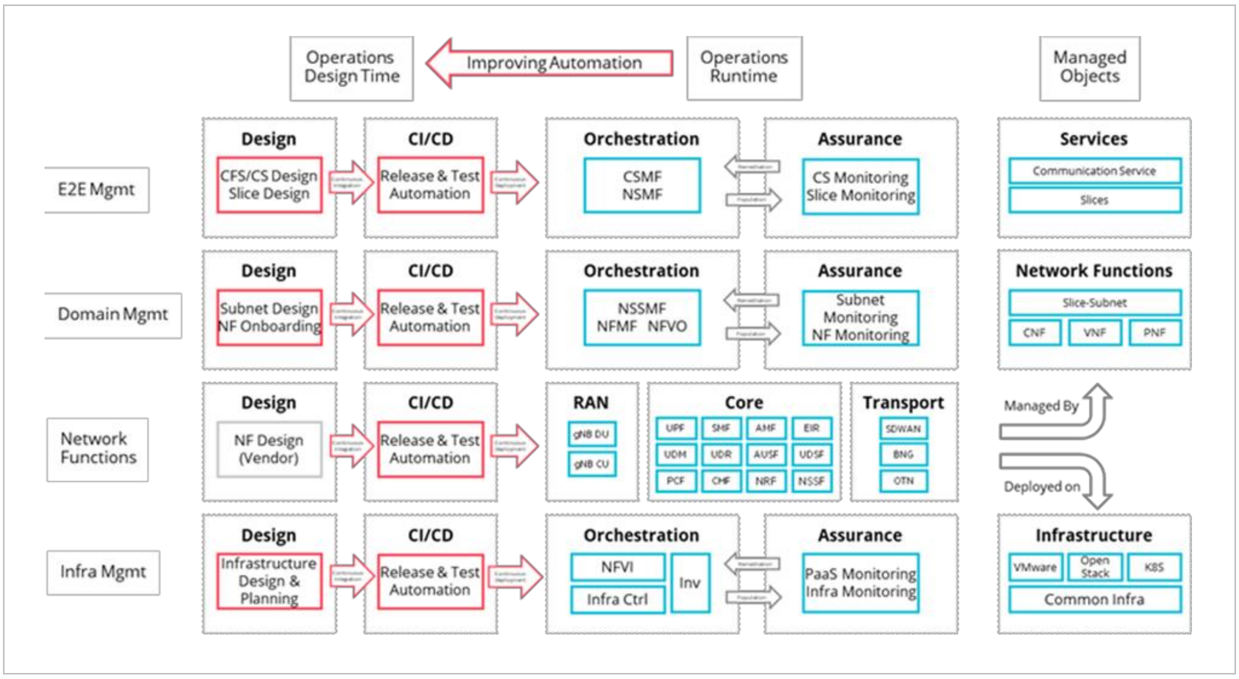


Figure 8-2 Operations Processes from Design to Runtime

Operations focus moves from runtime observations to a continuous automation improvement of the management systems enabling autonomous service and network management.
Each layer may need its own design, for its specific scope, with its specific expertise. A CI/CD environment may use common tools, but different pipelines per target. Vendors will deliver their NF packages in a continuous way into the operators' CI/CD pipelines. Upgrade/Update of NF deployments (day 0), all its configuration (day1/2) to serve the desired services, will be by Operations in a continuous DevOps process.

8.2.2 Operations Use Cases

The above processes are needed to realise the use cases of Design and CI/CD, automating the Runtime use cases of orchestration and assurance. Each use case describes an interaction in a landscape of architectural components of management software and in the CI/CD environment. Ideally the human activity happens at design time, while the runtime shall execute autonomously. The change automation is built on CI/CD pipelines, which integrates and deploys the outcome of the design into the target test- or production runtime environment.

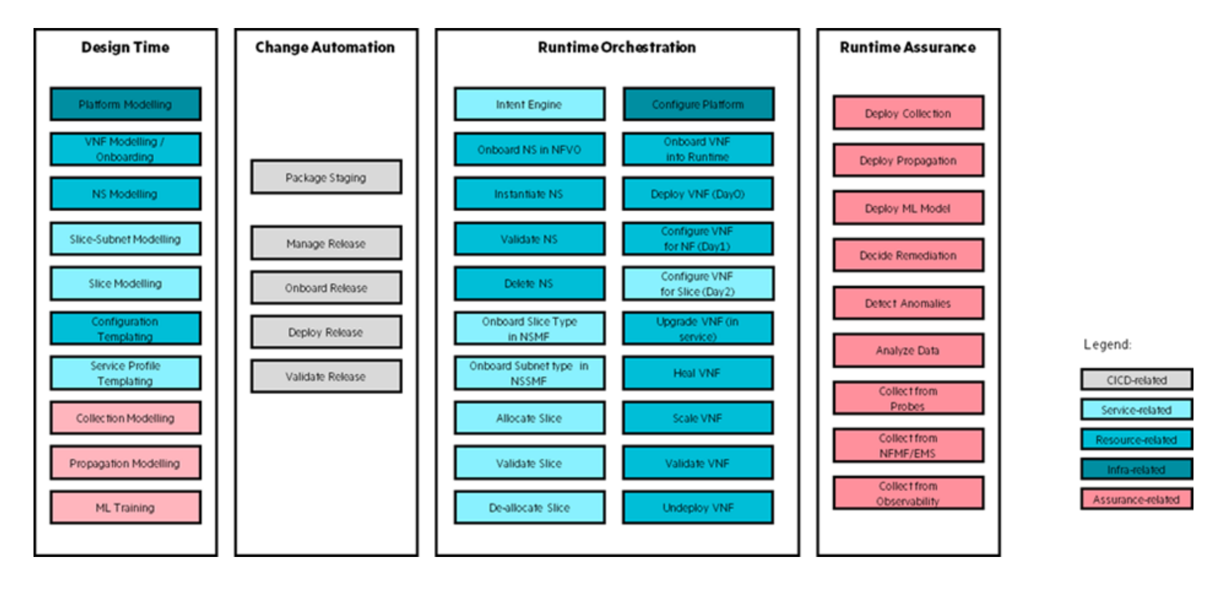


Figure 8-3 Operations use cases

The figure (figure 8-3) shows an example list of typical use cases for each vertical, i.e. Design CI/CD and Runtime. The horizontal layers as well as dependencies of use cases are neglected for simplification.

The software used shall support the use cases to achieve the business goals mentioned above:

- Design goals could be:
    - Time to market for a new service less than a few months
    - Time to onboard a new VNF is less than a few weeks

To achieve the best time to market, the use cases at design time shall allow fast composition of new service and resources. Best case based on models describing dependencies of services and resources together with a behaviour at runtime. It should avoid coding, which is time consuming, and avoids autonomy of situation related decisions.

Introducing a new platform or just a single new VNF remains time consuming, when the software does not support certain standards. Vendors may provide their software in ETSI NFV SOL004 format, including TOSCA together with Helm charts. The MANO orchestration software should allow to translate and integrate the packages in a most efficient way.

Having sufficient data from operations collected, AIOps technologies are used to generate ML models, hence anomalies can be detected (even predicted) automatically by the AI at runtime.

- Possible CI/CD goals are:
  - Time to migrate a VNF version is at maximum X days
  - Time to patch VNFs is at maximum X hour

The CI/CD environment shall allow fully automated integration, deployment and testing of the design outputs. Using the release management, the operator assembles the versions of onboarded software, service models and configurations into a dedicated release. The release is then pushed by a pipeline into a desired target environment for automated testing and finally for production.
The package staging allows vendors to push new or updates of their VNF software into the CI/CD chains – for direct patch deployment or for enhancing the design.

- Runtime goals could be:
  - Down time of services is only X minutes
  - Proportion of fully automated problem detection and resolution is a high amount of percentage (e.g. 80%)
  - Desired Mean Time to Repair for a non-automated problem resolution is less than a few hours (e.g. 2 hours)

All use cases at runtime shall be automated, including a closed loop between assurance and orchestration. Machine learning will increase the automated problem detection over time, the intent engine (like an inference engine) executes deviations from the intent when detected. Together with redundancy mechanisms at different layers, a service-downtime close zero can be achieved.

The intent engine of the orchestration runtime is less a use case to be implemented per service, rather it can be a generic component, able to control the other detailed use cases of the runtime, in the sense of a service composition. An intent-based service orchestration works based on the service models defined at design time, interfering with the as-is status of the network justified by assurance.

In a disaggregated environment the operator takes responsibility for the overall solution since he deals with multiple vendors and can't make a single vendor responsible for the performance of a complex service – since a micro service--based solution is created from independently changing components of multiple contributors.

Hence it becomes paramount that the metrics of such processes (as shown above) get measured automatically to gain efficient control on the operations goals.

8.3 Intent based Service Management

Intent is one element to achieve autonomous operations. Coming to the means of intent i.e. its definition and execution, we need to differentiate the specific goals for operations when using intents.

8.3.1 Goals of intent

While Intent supports autonomy to the highest maturity, we can differentiate more specific goals of intent based.

a) service abstraction – express the need, not the concrete service, allows for autonomy, avoiding service knowledge for the consumer

b) simplify the design – faster time to market, enabling more offerings at lower cost

c) enable intent negotiation – improve buyer-seller relationship, allows more flexible deals

d) enable intent-brokering – find the best producer, allows more competitive offerings

These goals depend on two aspects of Intent to consider:

1. Format of the intent itself – implications for goals A, C and D
2. Execution of the intent – implications for goal B

Looking at the shift from pure network operations towards DevOps the goal to simplify the intent handling has at least same importance, as the service abstraction.

Intent is currently identified and specified by different SDOs as a “formal specification of expectations” given to an intent handler/engine. Intent as such says nothing about the effort to design an intent handling.
For disaggregated networks the execution of an intent means a decomposition into (micro-) services. Depending on the current status of the networks, that decomposition may vary at runtime. It becomes evident, that the operator has the most efficient means to design the intent handling behaviour. Otherwise, the desired time to market will be missed.

8.3.2 Execution of Intent

An intent handler manages the execution of intents. Essentially it controls the closed loop managing and controlling a service instance lifecycle, that is translating the intent into a concrete service, then continuously comparing the as-is state with the to-be state, expressed by the intent. Hence it needs to deal with capabilities to design orchestration and assurance. Those may differ per layer and per domain, while generic capabilities will reduce the need of specific expertise and cost.
In a disaggregated network the Intent handler is a most essential component, since it will not only translate the intent into services, but into micro services delivered by a broad range of vendors.
An intent handler can be an explicit component, on top of orchestration and assurance, or it may be an orchestration able to manage assurance as a service. Orchestration needs to have coded runbooks for actuation the network into the desired status, or it allows generating a runbook based on best knowledge of a current status. Observing and analysing the current status is based on AI/ML, while the ML needs to be trained repeatedly for the right Analysis. Classic approaches with coded workflows fail when it comes to complex and dynamic service and networks; the limited workflows will fail, when it comes to unforeseen situations.
This will also happen, when cloudified applications managed by an autonomous CaaS platform, bring higher dynamics into the observed networks. An intent handling orchestration solution should avoid coding, rather support a service model, defining behaviour of a generic engine. Having service-based networks, together with management services (see also section 5.2) allows a consequent model of dependant services.
The same issue exists for detecting root cause and service impact scenarios. In a disaggregated network this would mean an exponential growth of workflows and detection scenarios. This will become nearly impossible to handle for the operator.

8.3.3 Service orientation to its full extent

As mentioned before and outlined in section 3.1.1, complexity is the essential challenge. A typical way to deal with complexity is disaggregation into smaller (micro) services. Aggregation and composition is also a means to build new (customer facing) service from lower level service and finally logical, virtual and physical resources. Therefore, a consequent method to compose services will allow service design.

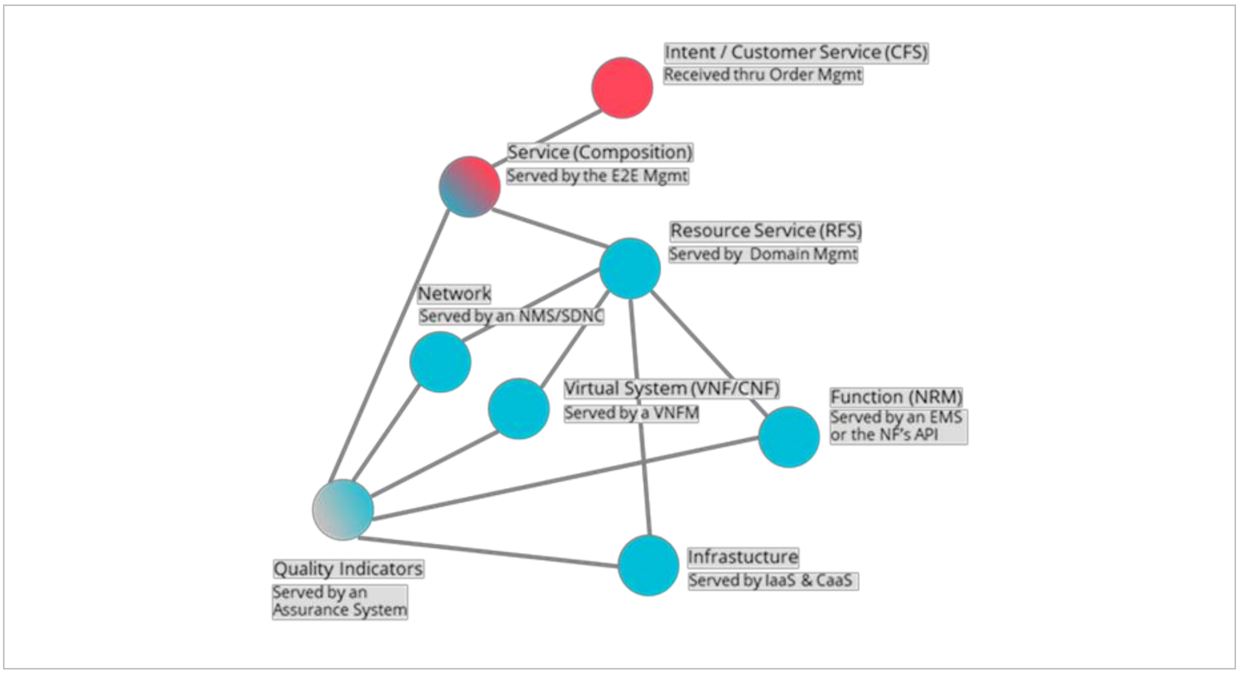


Figure 8-4 Paradigm "Everything is a Service"

At the highest level we see customer facing services (CFS), requested by an order management. If the order does not identify a concrete CFS type, in addition it requests a specific quality (i.e. Latency, reliability etc.), the order is nothing else than an intent. It needs to be translated or decomposed into a more concrete CFS or RFS (internal, Resource Facing Service).

CFS are decomposed from other services and finally from resource facing services. Resources can be e.g. a network, a virtual system (VNF/CNF) or a logical resource provided in an NRM of the NF's API. Finally, the virtual resource depends on a physical resource or infrastructure.

Some services may become manageable by virtualized management systems (e,g. a virtual router may provide management for firewall services). That means virtual resources, provide other services; classic service hierarchies are not sufficient anymore.

Another sort of service is quality indicator, expressing the service quality given with the intent. It can be associated with one of the monitored resources or services. And it is a service of the assurance system. Anyway, all those services, are served by other management systems or their APIs: the E2E Orchestration, the Domain Orchestration, an SDN controller, an EMS, finally the IaaS and CaaS.

Full-service orientation is far more than a design option. In disaggregated networks the APIs of the components become machine readable. The micro services resulting from disaggregation become an integral part of the service model. Hence their integration can be automated into the intent handling. The task of the operator is the definition of the necessary dependency, i.e. the intent based service modelling

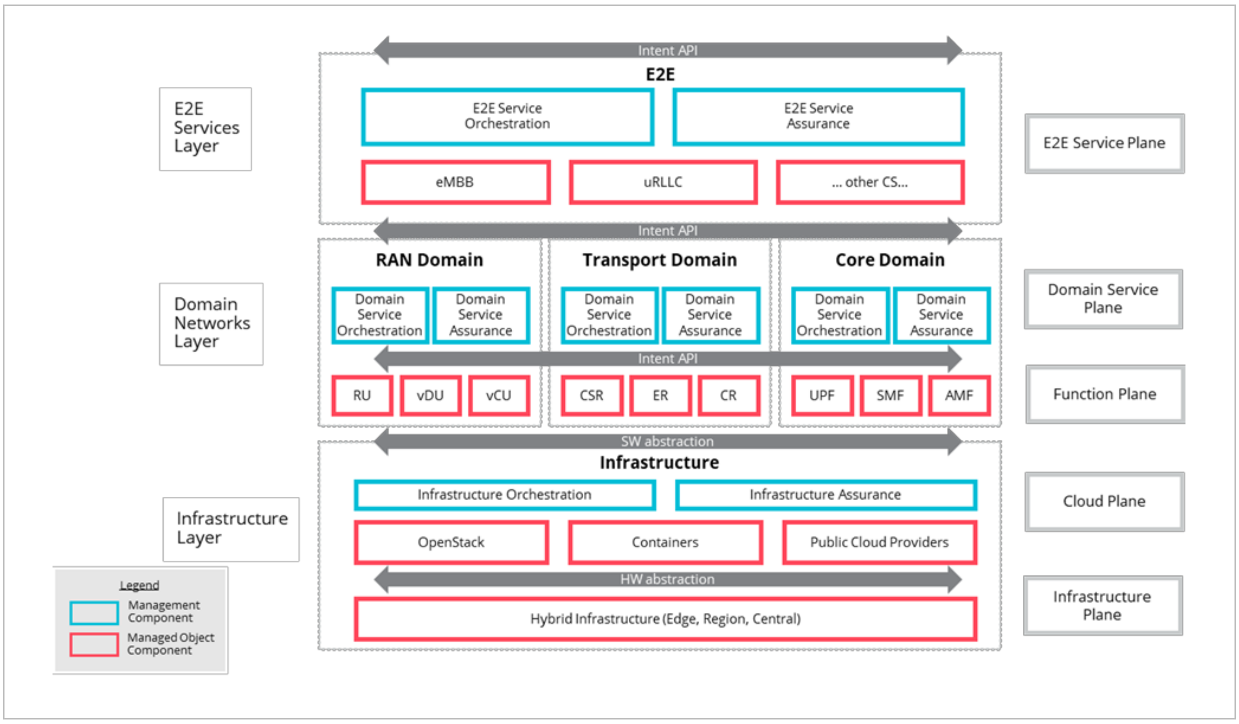


Figure 8-5 Abstraction of layers across domains

Common infrastructure (including clouds) may be shared for different domains and purpose. That allows more efficient infrastructure management, addressing costs and use of “green” technologies see section 4.3.14). Precondition is abstraction, as for all layers.

8.3.4 Intent based Service Orchestration

One way to support service modelling combined with behaviour definition is described in ZSM (ZSM005) for an intent-based service orchestration. Following a goal-based policy evaluation, the engine can decide at runtime, what way to run.

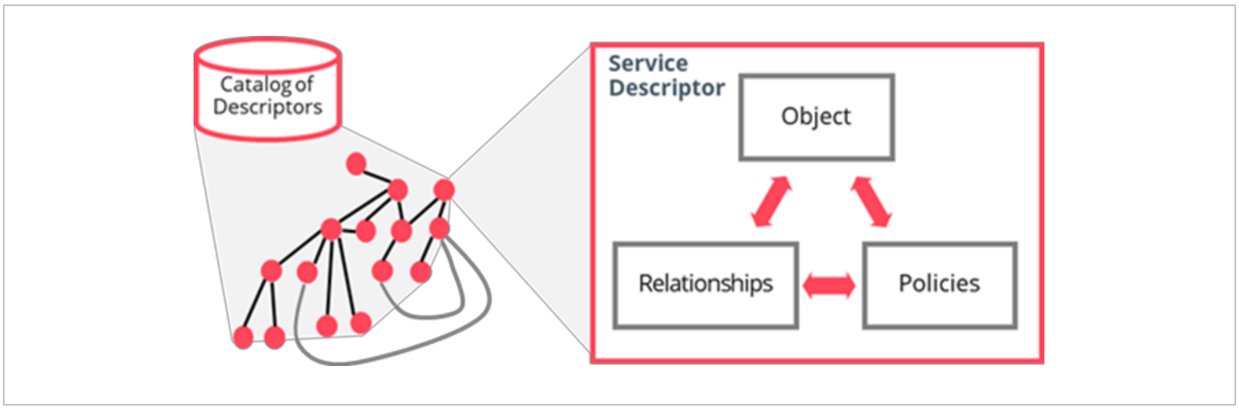


Figure 8-6 Dynamic Service Descriptors

Each service allows to relate in various ways to other services. Goal policies allow decisions at each node in the service graph. The behaviour becomes part of the model what enables a pure generic engine acting at a given as-is situation of the service and network, to achieve the to-be situation desired by intent.

The lower end of the service model is typically the network function, which relies on a resource orchestration.

8.3.5 Intents as knowledge plane

Previous approaches of managing automated networks were concerned about data, management, and control planes. Figure 8-7 shows blocks Actions, Policies and Intents arranged one on top of another. The horizontal axis shows the control surface exposed to the user while the vertical axis shows the functions encompassing a block. Primitive approaches focused on just executing actions, which had the maximum control surface and a lower granularity, most precise function executable on the resource. Then came policies, which helped consumer in automating steps at design time, thus exposing a part of the control surface provided by Actions. Although this restricted the number of functions accessible to the consumer, it did however reduce the complexity of directing actions. Currently, Intents are advocated as the next step, further reducing the complexity, helping the user just focus on the goal or in other words, the complexity of the underlying system is hidden under the façade of an intent specification.

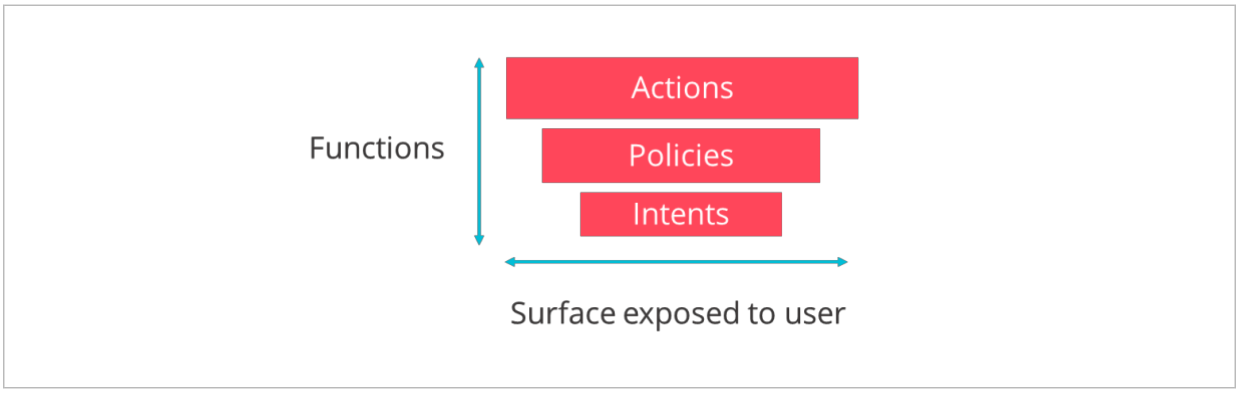


Figure 8-7 Managing Automated Networks through Actions, Policies and Intents

To this end, an intent can be viewed as introducing "knowledge" as the next evolving plane for automating networks.

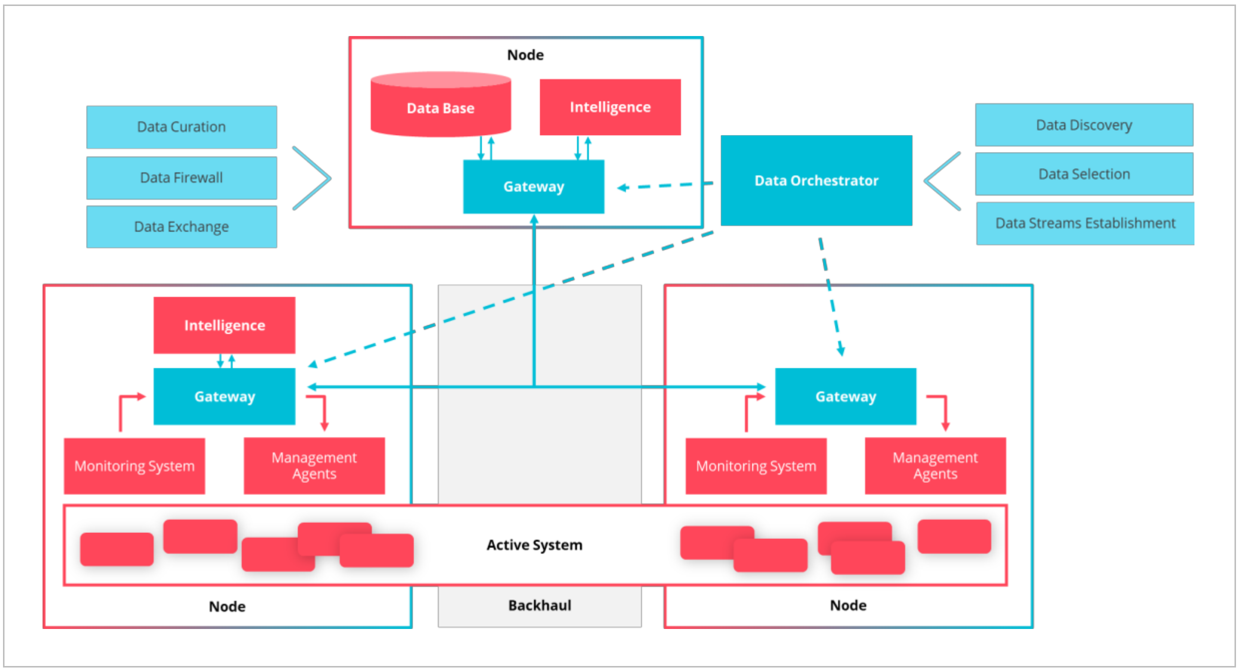


Figure 8-8: Automated Networks: Intents as knowledge plane

As an example, focusing on data exchanges, Figure 8-8 shows two nodes on the lower side, connected through the medium of backhaul network (data plane). The participating processes under the scope of each node is designated as an active system. The example focuses on monitoring the processes through monitoring system and management agents (data and control plane). A central node at the top can holds a collective intelligence and has the capability to direct the gateways of the lower two nodes using the data orchestrator (control and management plane). For an autonomous system, the system needs an additional plane through which an operator or consumer could communicate the goals such the system can leverage the built-in and evolving knowledge of the system, towards taking suitable decisions. The intent-based system is currently under development funded by the project CampusOS (https://campus-os.io/en/home/). A good overview of the control loops under TMF is provided in the [10].

9 CONCLUSIONS

The telecommunications industry has embarked on an exciting journey. One that has started to disrupt the foundations of how networks are planned, designed, built and operated, through their adoption of cloud-native strategies. The rapid adoption of disaggregation capabilities, with all the benefits and challenges identified in the 1st NGMN's ODiN (Phase 1) white paper, still needs a huge amount of work to be properly developed and appreciated. However, what Phase 2 of this work demonstrates is that while the depth and extension of changes are indeed huge, there are broad concepts, initiatives and activities that aim to support and even accelerate the transition. From standardization to alliances, from open proof-of-concept and integration labs to knowledge sharing and transfer, the industry has collectively identified activities across the board, and is supporting operators in making disaggregation a success. In fact, not only does it develop the supporting technologies and solutions, but also it paves the way for other more advanced capabilities such as network autonomy and intelligence, which are fundamental to scale and optimise the networks. With the "toolkit" at hand, we will now tackle the last part of this endeavour: given the opportunities and challenges. Within the two phases of this work so far, a situational analysis of the problem, prospects, challenges and industry direction, as well as some details on how to proceed and conduct network disaggregation, have been outlined. Phase 3 will provide guidance on operating models in a way that fits operators' needs and supports the execution of their strategic goals.

With the completion of the present phase, it is the desire of the team and authors to provide meaningful insight and guidance on the true value of disaggregation and what is needed by and from the operators, industry partners and telecommunications ecosystem players to bring about the benefits of disaggregation. This includes technologies, architectures as well as the activities highlighted in this white paper to mature and bring to fruition the great opportunities outlined.

Network disaggregation sets out the foundations for an agile and flexible future, as the journey of socio-economic transformation and automated industries, with economic and environmental sustainability, demand increasingly diverse use cases with wide range of requirements. This empowers the evolution of cloud-native 5G towards 5G-advanced and beyond, to serve smart societies and industries. The emerging and future paradigms such as integration of intelligence, dedicated smart networks, merger of physical, virtual and digital worlds, with immersive media and digital replicas, or targeting energy and cost efficiencies, all rely on, are enabled by, and leverage the best of network disaggregation and the development of relevant operating models.

LIST OF ABBREVIATIONS

5GC	5G-Core
AF	Application Function
AMF	Access and Mobility Management Function
AN	Access Nework
API	Application Programmable Interface
BBU	BaseBand Unit
BSS	Business Support Systems
CAPEX	Capital Expenditure
CFS	Customer Facing Services
CI/CD	continuous integration continuous deployment
CM	Configuration Management
CNF	Cloud-native Network Function OR Containerised Network Function
COTS	Commercial Of he Shelf
CU	Central Unit
CU-C	CU Control Plane (or CU-CP)
CU-U	CU User Plane (or CU-UP)
cVNF	Cloudified Virtualized Network Function
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DN	Data Network
DoS	Denial of Service
DPDK	Data Plane Development Kit
DU	Distribution Unit
eMBB	enhanced Mobile BroadBand
eCPRI	enhanced Common Public Radio Interface
E-UTRA	Evolved Universal Terrestrial Radio Access
EVPN	Ethernet Virtual Private Network
FM	Fault Management
gNB	Next Generation NodeB
GNBCUCPF	Next Generation NodeB Central Unit Control Plane Function
GNBCUUPF	Next Generation NodeB Central Unit User Plane Function
GNBDUF	Next Generation NodeB Central Distribution Unit Function
GSMA	GSM Association
HCP	Hyperscale Cloud Providers
ICT	Information and Communications Technology
ISP	Internet Service Provider

LBO	Local Breakout
LCM	Lifecycle Management
MAC	Medium Access Control
MANO	Management and Orchestration
MEC	Multi-Access edge Compute
mMCT	massive Machine Type Communication
MNO	Mobile Network Operator
NbR	Name-based Routing
NF	Network Function
NFMF	Network Function Management Function
NFV	Network Function Virtualisation
NRF	Network Repository Function
ng-eNB	Next Generation evolved NodeB
NG-RAN	Next Generation RAN
Non-RT RIC	None Realtime RIC
n-RT RIC	Near-Realtime RIC
NAS	Non-Access Stratum
NSA	Non-Stand-Alone
NSMF	Network Slice Management Function
NSSMF	Network Slice Subnet Management Function
NWDAF	Network Data Analytics Function
NUMA	Non-Uniform Memory Access
O-Cloud	Open Cloud SW
O-CU	Open Central Unit
O-DU	Open Distributed Unit
OPEX	Operational Expenditure
OSS	Operational Support Systems
OTT	Over-the-Top
PaaS	Platform-as-a-Service
PDCP	Packet Data Convergence Protocol
PHY-H	Physical Layer - Higher
PHY-L	Physical Layer - Lower
PM	Performance Management
PNF	Physical Network Function
QoS	Quality of Service
RAN	Radio Access Network
RDMA	Remote Direct Memory Access
RF	Radio Frequency

RFS	Resource Facing Service
RIC	RAN Intelligent Controller
RLC	Radio Link Control
RRH	Remote Radio Head
RU	Radio Unit
SBA	Service Based Architecture
SCP	Service Communication Proxy
SDN	Software-defined Networking
SEN	Service Edge Node
SMO	Service Management and Orchestration
SMF	Session Management Function
SMOF	Service Management and Orchestration Function
SR-IOV	Single-Route Input/Output Virtualization
TCO	Total Cost of Ownership
TEN	Telco Edge Node
TSN	Time Sensitive Networking
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communication
VNF	Virtualized Network Function
vRAN	Virtualized RAN
ASIC	Application-Specific Integrated Circuit
COTS	Commercial Off-The-Shelf
CU	Central Unit
DU	Distributed Unit
FPGA	Field Programmable Gate Array
GPU	Graphics Processing Unit
MNO	Mobile Network Operator used here to represent a provider of connectivity and services
RU	Radio Unit

REFERENCES

[1] NGMN Alliance, 'ODiN – Operating Disaggregated Networks (Phase 1)', October 2021. https://www.ngmn.org/wp-content/uploads/210927_NGMN_ODiN_v1.0.pdf

[2] https://opennetworking.org/news-and-events/blog/5g-transformation-with-open-source-spotlight-wrap-up/

[3] 3GPP, "TS23.501, System architecture for the 5G System (5GS), Release 17", Online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

[4] 3GPP, "Study on UPF enhancement for Exposure And SBA, WI #940076", Online: https://portal.3gpp.org/desktopmodules/WorkItem/WorkItemDetails.aspx?workitemId=940076

[5] NGMN Alliance, 'Green Future Networks: Sustainability Challenges and Initiatives in Mobile Networks', July 2021, https://www.ngmn.org/wp-content/uploads/210719_NGMN_GFN_Sustainability-Challenges-and-Initiatives_v1.0.pdf

[6] NGMN Alliance, 'Green Future Networks: Network Energy Efficiency', December 2021, https://www.ngmn.org/wp-content/uploads/211009-GFN-Network-Energy-Efficiency-1.0.pdf

[7] *REDFISH | DMTF.* (n.d.). https://www.dmtf.org/standards/redfish

[8] Scaphandre. (2021, November 11). GitHub. https://github.com/hubblo-org/scaphandre

[9] NGMN Cloud Native enabling future Telco Platforms V5.2, May 2021, https://www.ngmn.org/wp-content/uploads/NGMN-Cloud-Native-Enabling-Future-Telco-Platforms-v5.2_New.pdf

[10] Gomes, P. H., Buhrgard, M., Harmatos, J., Mohalik, S. K., Roeland, D., & Niemöller, J. (2021). Intent-Driven Closed Loops for Autonomous Networks. Journal of ICT Standardization. doi:10.13052/jicts2245-800x.929