5G PPP Architecture Working Group

The 6G Architecture Landscape

European perspective

Version 1.0, December 2022

Date: 2022-12-08 Status: Release for public consultation

DOI: 10.5281/zenodo.7313232
URL: https://doi.org/10.5281/zenodo.7313232

Table of Contents

Abstract **3**
1 Introduction **4**
1.1 Analysis of current trends in society and technology 4
1.1.1 Societal trends towards 2030 and beyond 5
1.1.2 Economic trends towards 2030 and beyond 5
1.1.3 Regulatory trends towards 2030 and beyond 5
1.1.4 Technological trends towards 2030 and beyond 6
1.2 Use cases and use case families 7
2 Why a new architecture is needed **8**
2.1 E2E architecture 9
2.2 Architectural Principles 12
3 Architectural enablers **14**
3.1 Intelligent network 14
3.1.1 Intelligent network key technological enablers 14
3.2 Flexible network 16
3.2.1 Flexible network key technological enablers 18
3.3 Sustainable network 22
3.3.1 Sustainability targets 24
3.3.2 Sustainable network key technological enablers 27
3.4 Secure network 28
3.4.1 Secure network technological enablers 29
3.4.2 Security architectural components 30
3.5 Versatile radio access network 31
3.5.1 Distributed massive MIMO 32
3.5.2 Cell-free mMIMO 33
3.6 Localization and Sensing 35
3.7 Programmable networks 37
3.7.1 Enabling network programmability 38
3.7.2 Programmability of UEs 41
3.8 Management and Orchestration 42
4 Conclusions and Outlook **51**
5 References **52**
6 Abbreviations **60**
7 List of editors **65**

Abstract

The 5G Architecture Working Group as part of the 5G PPP Initiative is identifying capturing novel trends and key technological enablers for the realization of the 5G and 6G architecture. It also targets at presenting in a harmonized way the architectural concepts developed in various projects and initiatives (not limited to 5G PPP projects only) so as to provide a consolidated view on the technical directions for the architecture design in the 5G/6G era.

The first version of the white paper was released in July 2016, which captured novel trends and key technological enablers for the realization of the 5G architecture vision along with harmonized architectural concepts from 5G PPP Phase 1 projects and initiatives. Capitalizing on the architectural vision and framework set by the first version of the white paper, the Version 2.0 of the white paper was released in January 2018 and Version 3.0 in February 2020, presented the latest findings and analyses of 5G PPP Phase I projects along with the concept evaluations. The last version 4.0 was released in October 2021, presented the outcome of the projects from 5G PPP phase II and III.

The work has continued with the 5G PPP Phase II, III and now Phase IV. Phase IV includes the projects that are defining the architecture for 6G. The results of the Architecture Working Group are now captured in this version of the white paper, which presents the consolidated European view on the 6G architecture design.

1 Introduction

The goal of this white paper is to summarize the findings from the European research landscape on the first version of the 6G architecture. This includes the various technical enablers as well as the first End-to-End system and functional view of the 6G architecture structure. The white paper is organized as follows. The rest of this chapter presents a thorough analysis of different trends e.g., societal, economic, regulatory, and technology toward 2030. The use cases foreseen for the next generation of mobile networks are also described at the end of this chapter. The overall architecture description in Chapter 2 discusses the new stakeholders in the mobile network ecosystem and how the architectural work is taking into account their requirements in all the domains of the network. Specific design principles must take into account for the new architecture are also described. Then, we move to the new findings in the specific network domains, starting from Sub chapter 3.1, which details the enablers for intelligent networks and how the 6G architecture can benefits from automation and artificial intelligence (AI). Sub chapter 3.2 describes the technical enablers for the flexible network such as the non-Triserial network which will be one of the most important parts of the 6G architecture. We move to the discussion of efficiency of the 6G architecture in Sub chapter 3.3. This sub chapter describes solutions for the architecture design such as streamlining and efficient signalling as well as compute as a service in order to make the network more flexible and scalable. Sub chapter 3.4 has the detailed study on the two concepts of "6G for sustainability" and "sustainability for 6G" and presents some practical technical solutions. Sub chapter 3.5 collectively discusses concepts of security and new technology enablers that can be applied to have security as a design concept for the 6G architecture. Sub chapter 3.6 has a deep dive into the radio access technologies such as D-MIMO and Cell-free MIMO that can be a solution for the 6G ultra-dense access network. The localization and sensing concept is presented in Sub chapter 3.7 in detail. Programmability both at the network and user level is one of the uprising concepts for the 6G architecture which is discussed in chapter 3.8. Finally, chapter 3.9 deep dives into the management and orchestration which is required to harmonize the complex structure of 6G architecture. Chapter 4 outlines the future steps and conclude the whitepaper.

1.1 Analysis of current trends in society and technology

Since the invention of mobile communications, wireless network technology has undoubtedly transformed the everyday life of billions of people on the planet, and profoundly impacted and shaped the economy and the evolution of human society to date. Today, the world is facing several unprecedented challenges in parallel: climate change, global pandemics, social inequalities and misinformation are all aspects in today's governmental global economic, societal, and political agendas, which require impacting and sustainable changes of the global economy and the society itself. Infused by emerging and disruptive digital technologies on the horizon, wireless networks are and will be the keystone for enabling such a transformation. The evolution journey will carry on in the year ahead, driving a large scale of adoption of 5G and 5G-Advanced use cases with significantly decreased deployment and operation costs, and enabling new and innovative use-case-driven solutions with higher economic and societal values.

In this context, for guiding the design of human-centered future networks, major societal and economic trends towards 2030 and beyond are analyzed in the following sections. In addition, regulatory and technological trends, which are critical for the design and deployment of future networks, are also discussed, so to ensure that such trends, and the related research work, can consider all the key elements of future network design, a design that is deeply rooted in real needs and can profoundly benefits humanity in the mid-to-long term.

1.1.1 Societal trends towards 2030 and beyond

In 2015, 17 interlinked Sustainable Development Goals (SDGs) were collectively identified and set for "a better and more sustainable future for all" by the General Assembly of the United Nations (UN) [UN15]. Since then, all sectors of society have been called for working towards and delivering on these goals with a timeframe of 2030 and beyond. Information and Communication Technology (ICT) and the wireless network industry have positively contributed to those goals so far. For example, it has been estimated that wireless networks have helped to lift two million people out of extreme poverty in Nigeria during 2010–2016 [GSM20]. Meanwhile, it is worthwhile noticing that the SDG framework extends clearly beyond the climate issues, thus calling for a holistic approach to address all goals, which are very much interconnected. To address the sustainability aspect, it is not sufficient to focus on SDG #13 climate action alone to support all environmental, social or economic goals [RRS+19]. For guiding the design of future networks within the SDG framework, it is also important to take two additional aspects — **trustworthiness and digital inclusion** — into account as well.

1.1.2 Economic trends towards 2030 and beyond

Wireless network technology has long been regarded as an important engine for driving global economic growth. As projected in [Rac20], network technology that encompasses 5G and beyond will potentially trigger $13.2 trillion global sales across ICT industry sectors by 2035, representing 5% of global real GDP, while 6G value chain will be able to generate 22.3 million jobs globally by 2035. This estimation did not even include the impact of connectivity on non-ICT sectors. For enabling economic recovery and (re)-building global growth while building a sustainable future in next decades, digital technologies, in particular wireless technology, have been widely accredited as fundamental tools by global governments and industry. Wireless technology serves and will continue to serve the global economy as critical digital infrastructure for all possible industrial sectors (e.g., automotive, industrial, transportation, agriculture, education, health and entertainment) and inherently enable sustainable growth in all those sectors.

1.1.3 Regulatory trends towards 2030 and beyond

While the telecommunications sector was privatized in the 1990s, sector regulation continues to be important in conjunction with efficient spectrum access rules, aspects of Electromagnetic Field (EMF) Electro Magnetic Compatibility (EMC) and assurance of level playing field with platform and cloud operators beyond telco context. Towards 2030, sector regulation is even getting more impacting on the society and is more than ever needed. For example, spectrum management is at the heart of future networks, any wireless technology development, and governments and regulators will have new opportunities due to a wide variety of spectrum bands in terms of highly distinct deployment characteristics and spectrum access models with different levels and needs of spectrum sharing. Future networks will likely combine a range of radio access network (RAN) technologies from macro cells to small cells with very high-capacity short-range links. This calls for refining regulations to resolve inconsistent local approval processes and frequency band assignments to enable dense small cell deployments. With the emergence of ML/AI technologies across different industry sectors, several regulations have been introduced, e.g., the European AI Act and the US Blueprint for an AI Bill of Rights to regulate AI systems. Towards 2023, it is envisioned that AI to be widely used to enhance future networks' performance and to be provided as a service by the future networks for a wide range of applications. Hence, it is likely that telecommunication sector to be impacted by the AI regulations. Finally it is worth mentioning the need to guarantee the interoperability of numerous solutions developed in different parts of the world: equipment and terminals that can intelligently adapt and smoothly work in all areas of the planet are looked for more than ever.

1.1.4 Technological trends towards 2030 and beyond

The interplay of several technologies is needed to sustain and realize the continue evolution of mobile networks, among which one can mentionnetworks:

- **Localization and Sensing**: Localization was introduced in Release 9 of the 3GPPP specifications and is continuing to evolve. With the use of wider bandwidth signals coupled with high-band spectrum (>100 GHz) as well as the incorporation of Simultaneous Localization and Mapping (SLAM) with communications at lower frequencies, future networks will be designed integrating high-precision localization (with centimeter-level accuracy), sensing (both radar-like and non-radar like) and imaging (at millimeter-level) capabilities. This requires the development of highly novel approaches and algorithms to co-optimize communications, sensing and/or localization.[HEX-D31].
- **Network intelligence:** Artificial Intelligence **(**AI)/Machine Learning (ML) will bring a major disruption to future networks from impacting the design of air interface, data processing, network architecture and management towards computing for achieving superior performance [Nok20], [NOK20b], [Dem20], [HEX-D42]. It will become essential for the end-to-end network automation dealing with the complexity of orchestration across multiple network domains and layers [ZVF+20].
- **Digital Twin (DT):** A DT is a digital replica of a real world entity. The virtual representation reflects all the relevant dynamics, characteristics, critical components and important properties of an original physical object throughout its life cycle. The creation and update of DTs relies on timely and reliable multi-sense wireless sensing (telemetry), while the cyber-physical interaction relies on timely and reliable wireless control [MLC20] over many interaction points where wireless devices are embedded. In future networks, DTs will be used as a valuable tool to create novel and disruptive solutions, especially for vertical industries, that are enabled by a large scale of real-time, robust and seamless interactions among, for example, machines, humans and environments. Particularly, DTs can be scaled up, which enables a large scale of sustainable living with systematic climate mitigation measures, improves the resilience of society in crisis situations by actively monitoring and simulating all possible scenarios and potentially helps transform the whole societal structure that is suitable for 2030 and beyond.
- **Reimagined network architecture**: New network architecture paradigms for the 6G era are driven by a decomposition of the system architecture into platform, functions, orchestration and specialization aspects [ZVF+20]. The future network platform will be associated with an open, scalable, secure, elastic, distributed and agnostic heterogeneous cloud system, which is data flow centric and will include hardware acceleration options. Functionally, the convergence of RAN and Core Networks will help reducing architectural complexity. At the same time, dynamic offloading and flexible instantiation of sub-networks will drive the increased level of specialization of the architecture. Of high relevance for the open provision of services and the monetization of resources will be the transformation of orchestration architecture; cognitive closed loop and automation are likely to become pervasive. All future deployment scenarios will rely on a superior transport network and network fabric that is flexible, scalable, secure and reliable to support demanding use cases and novel deployment options, such as a mixture of distributed RAN and centralized/cloud RAN enabled by AI-powered programmability [Eri20]. The future network architecture shall provide the capability to facilitate all the AI operations in the network.
- **New devices and interfaces:** Future networks will be connected to multitudes of devices and interfaces, enabling novel human-machine and machine-machine communications. New human-machine interfaces created by a collection of multiple local devices will be able to act in unison [Nok20]. In addition, the ubiquity and longevity of IoT devices will be further

enhanced through zero-cost and zero-energy devices where printable, energy harvesting devices can be deployed anywhere.

- **Network of networks:** In order to capture local and specialized network and sub-network needs, 6G network-of-networks will cover multiple scales of – physical and virtual – networks. The evolution of private and 5G non-public network (NPN), such as campus networks, will expand to support many machines and processes with strict requirements on Quality-of-Service (QoS) and connectivity, employing edge processing for further automation. Verticals and enterprises (e.g., energy sector smart grids) will benefit from automated services with guaranteed performance in conjunction with as-a-Service (aaS) business model transformation. Such services will be based on various types of resources, including communication, data and AI processing, and will require tailored network functionality supporting new value chains in a controlled fashion.

1.2 Use cases and use case families

The H2020 EU-funded project called *A flagship for B5G/6Gvision and intelligent fabric of technology enablers connecting human, physical, and digital worlds* (Hexa-X) [HEXA] is the pilot 6G project of the European Commission, chartered with the role of devising the role of 6G in the evolution of society [HEX-D12]. The project proposes six main research challenges, laying the foundation on which relevant use cases for 6G can be forecast, accounting also for the societal and economic trends. Here we identify an initial, non-exhaustive set of use cases as a first baseline to guide the future research directions on 6G, based on the view of the current European research activities on 6G driven through the 5G PPP and 6G-IA initiatives, such as in [HEX-D12], [HEX-D13]. These use cases encompass a wide range of usages, from evolutionary ones, extending and enriching the 5G usages with new capabilities, to more disruptive ones, opening up new horizons where 6G could benefit and transform society. These use cases are clustered into families of use cases, according to the type of usages, as well as the research challenges and values addressed, as summarized in Figure 1.

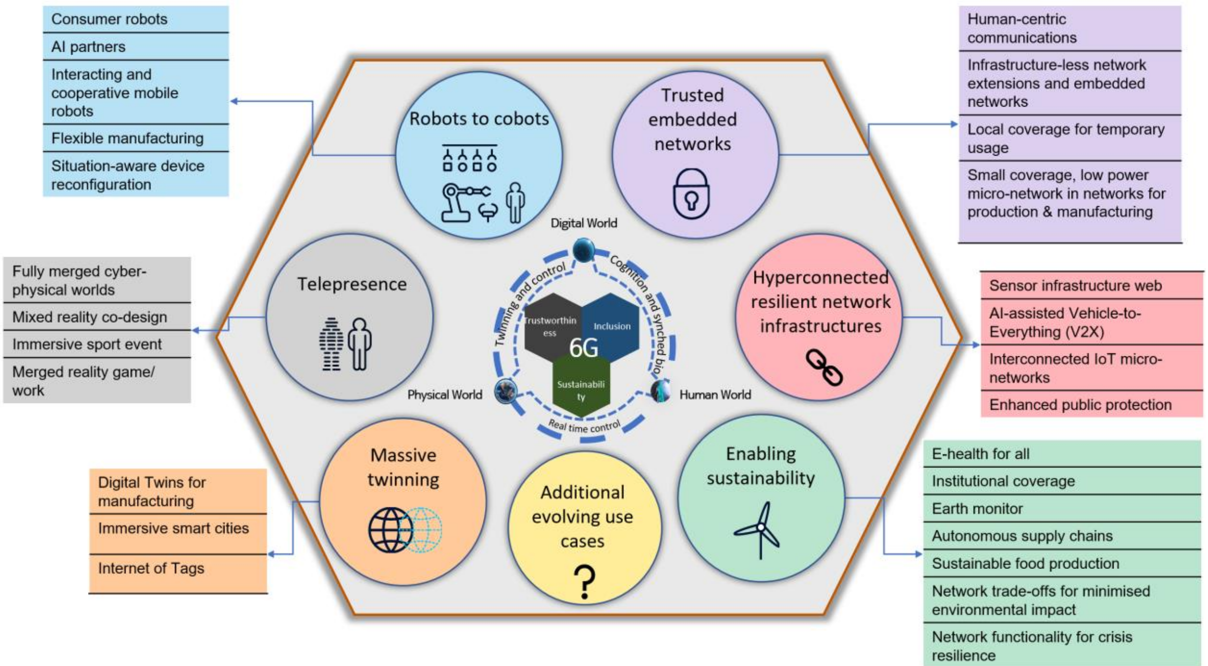

Figure 1: Families of uses cases from [HEX-D13]

2 Why a new architecture is needed

Based on the introduced use cases and their requirements and the technological trends affecting the 6G architecture, this sub-section identifies gaps of currently 3GPP defined 5G architecture and lists several key needed components for the forthcoming 6G architecture:

- **Enabling AI**: Thanks to the enormous development in computational resources, edge- and cloud-computing, as well as due to the ever-increasing amount of available network and application data, AI can now be applied to almost every aspect of mobile networks, enabling automated network operation and user application/service support. However, to be able to harvest from the benefits of AI, 6G systems need to be AI- and computation-pervasive, which calls for the 6G architecture to be data-driven. It is our vision that the 6G network will leverage AI for optimising the 6G air interface (e.g., physical layer configuration; mobility and resource management; QoS assurance) and also to transform a 6G network to a powerful distributed AI platform. Hence, the AI as a Service (AIaaS) concept will be a key 6G enabler.
- **Programmability**: While programmability has been a feature of network devices for a long time, the past decade saw a significant enhancement of programming capability for Network Functions (NFs)NF)spearheaded by the Software-defined networking Designed Network (SDN) paradigm as well as the ongoing trend towards softwarization, edgification, and cloudification. On the one hand, there are now many more APIs and standardized programming interfaces towards NFs than ever before. This allows 3rd party developers to interact with the network in new ways. On the other hand, the capability to program is no longer confined to the Control Plane (CP) but has been introduced into Data Planes (DP) as well using Smart Network Interface Cards (SmartNICs) and switches. A key candidate technology for this is the P4 domain-specific language and the functional abstractions [BDG+14]. The reusability and flexibility through programmability is of particular importance at edge and extreme-edge locations where deployments have a limited footprint (i.e., subject to limited hardware types and models) and therefore need to be flexible to support a wide range of functions and use cases with diverse performance requirements. For 6G, this trend is expected to continue and even accelerate. However, many open questions remain as competing concepts exist, and actual deployments are mostly limited to trials.
- **Cloud native, softwarization and service-based architecture**: 5G Core Network (CN) supports cloud-native implementation of the service-based architecture (SBA). Cloud native means that applications are designed to operate in Cloud compute environments and are built without employing a monolithic software codebase. Further on, 5G employs concepts such as separation of User Plane (UP) and CP functions, network slicing, convergence of fixed and mobile communication (and non-3GPP access), local breakout mechanisms, support for a wide range of frequencies, etc. However, there are some areas of improvements identified here with respect to the current 5G networks, for example, the functional allocation and procedures may prevent full integration of cloud-native NFs across all domains and layers. The current 5G architecture applies the service-based approach in the core network [23.501], [23.502] and defines NFs applying service-based principles, but here the scope is only for the CN omitting RAN and the management system. The service based approach has also been adopted in the management system (SBMA, Service Based Management Architecture), with different management services federated together following service-consumer producer patterns. However, SBMA and SBA - as applied in the CN - differ in the way how SBA in 5G CN is applied: CN builds service discovery around Network Repository Function (NRF) whereas SBMA doesn't have such a service explicitly but multiple options instead. Further, SBMA [28.533] doesn't define NFs but APIs only counter to CN CP. As the cloudification continues within all subsystems (i.e., RAN, CN, and management) the overall architecture should be

revisited to ensure architectural consistency, streamlined introduction of new features and simplicity of customization. Planned improvements include better cross-plane and cross-domain interactions, particularly for data collection for analytics and AI/ML needs. The 6G architecture must be more flexible to accommodate new types of end user devices and access network topologies which calls for dynamic functionality upgrades and function distribution to match changing deployment needs.

- **Continuum Orchestration**: Another reason why a new architecture is necessary is the realisation of the *Continuum Orchestration* concept, which implies the evolution of regular management and orchestration techniques towards the continuum consisting of the joint combination of different orchestration domains: CN, transport network, edge, extreme-edge, and other networks that can be external to the Mobile Network Operator (MNO) (e.g., fixed access networks, private networks or hyperscaler networks). In pre-5G generations, management and orchestration resources were primarily focused on the CN. (5G)5G makes possible the emergence of new architectures enabling the joint management and orchestration services and resources deployed on both: core and edge. However, the concept of "continuum orchestration" for B5G/6G networks takes this a step further by also including other resources as mentioned before.

In addition to the list above, other important aspects are to be considered, among which sustainability, reliability, trustworthiness, cybersecurity, standardization and regulations.

2.1 E2E architecture

Figure 2 depicts a high-level view of the 6G architecture and highlights the key technical enablers. The various building blocks are organized into three layers: Infrastructure, Network Service, and Application.

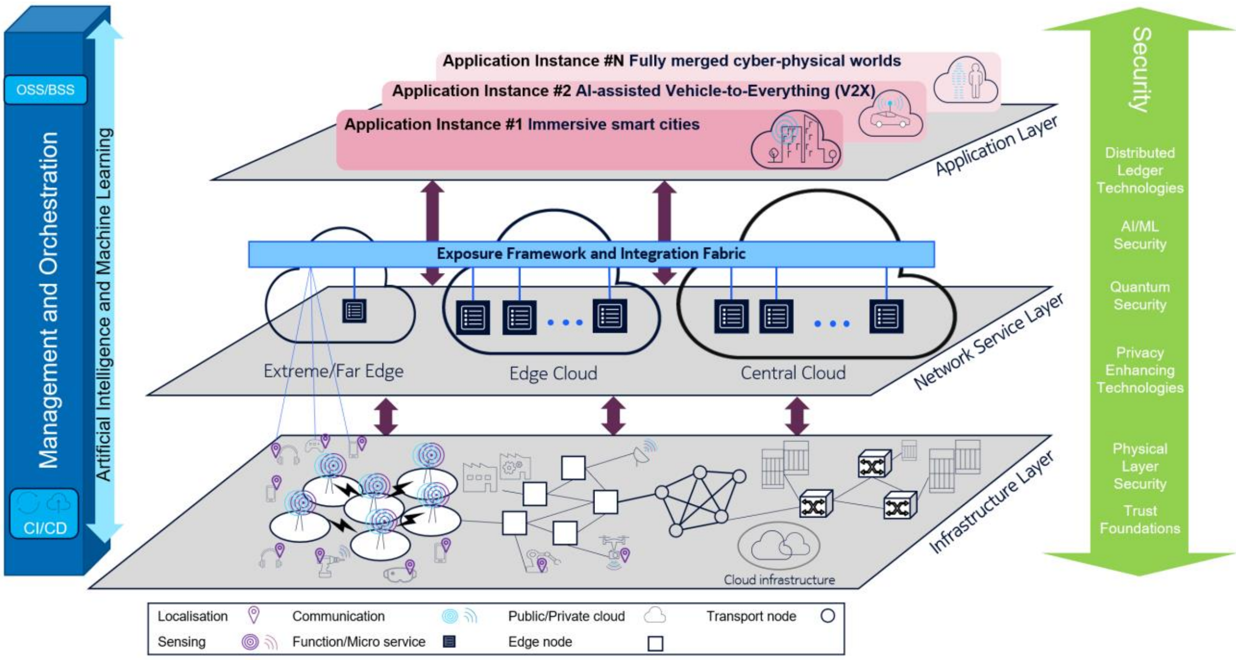

Figure 2: High-level view of the 6G architecture [HEX-D13]

The infrastructure layer is comprised of Network RAN, Network CN, and transport Networks, which contain radio equipment (non-virtualised radio functions like Radio Units (RUs), RU), Distributed Units (DU)), or even classical base stations), switches, routers, communication links, data centres, cloud infrastructure, and so on. The infrastructure layer provides the physical resources to host the network service and application layer elements. Furthermore, due to the introduction of new use cases, e.g., immersive smart city [HEX-D12], the infrastructure layer envisioned for 6G can accommodate new enablers such as localisation and sensing. A thorough gap analysis was conducted on localisation and sensing in deliverable Hexa-X D3.1 [HEX-D31]. The infrastructure layer also contains RAN improvements that enable extremely low latency, high reliability, availability, high data rate, high capacity, affordable coverage, high energy efficiency, accurate localization, and integrated sensing**.** More details on the evolution of RAN technologies in Hexa-X can be found in deliverables D2.1 [HEX-D21] and D2.2 [HEX-D22]. The 6G architecture incorporates different (sub)network solutions into a network of networks. The network of networks can easily and flexibly adapt to new topologies to meet the requirements of both extreme performance and global service coverage, well beyond what 5G is capable of.

The network service layer is envisioned to be cloud and micro-service-based with function and microservices expanded from central cloud to the extreme edge cloud. Extreme edge cloud is referred to all devices beyond the RAN. By having all network functions, operations, and applications implemented as microservices, we can move toward a softwarised, intelligent and efficient 6G architecture. In the following, enablers for an intelligent network describes mechanisms to support AI in 6G and AIaaS, programmability, and network automation. Further on, with a cloud-native approach, the RAN and CN architectures can be streamlined, e.g., reduce some complexity by removing multiple processing points for a certain message and removing duplication of functionalities among functions. This topic is further investigated in the section 3.3 related to enablers for efficient and sustainable networks.

One of the key technology enablers of the network service layer is the introduction of the extreme cloud. Extreme edge cloud covers the part of the network with high heterogeneity of devices with a wide variety of technologies, in terms of both hardware and software. These devices could be personal devices (smartphones, laptops…), and a huge variety of Internet of Things (IoT) devices (wearables, sensor networks, connected cars, industrial devices, connected home appliances, etc.). The concepts of edge and far-edge computing become more and more relevant for the 6G architecture and services. Cloud-native technologies will be required to create cloudlets at the edge of the network, with application-to-application and function-to-function communication capable to satisfy a large number of interconnected assets with flexible mesh topologies. Another important aspect of this layer is the exposure framework and integration fabric. They establish a communication channel that enables seamless interoperation and networking across different domains.

Network management and orchestration are gradually moving toward increasing the levels of automation and fully automated closed-loop control. This is supported by the parallel adoption of advancements in AI/ML technologies. The aim of this shift is to provide a framework to optimally support reliability, flexibility, resilience and, availability through the concept of " continuum orchestration " - i.e., seamless orchestration spanning device-edge-cloud addressing changes in the infrastructure, requirements and failures.

Security and privacy mechanisms are an integral part of the overall architecture, affecting all network layers as well as the management and orchestration domain. Figure 2 highlights the 6G security technology enablers across different layers identified in [HEX-D12].

6G telecommunication networks need to have a fast and efficient way of exchanging information and resources, with minimum possibility of failure, to enhance the QoS they provide. Naturally, the attention has turned towards a new approach to the decentralised framework. One of such a framework is the blockchain-enabled platform, which can be used in several domains (e.g., network slicing, industrial IoT networks). The blockchain-based platform is one of the most prominent technologies to unleash the potential of 6G system.

Privacy-enhancing technologies are important on all layers where sensitive data are gathered or processed, and clearly also in the management domain. Similarly, AI/ML security is relevant for all functions making use of AI/ML, in the sense of specifically protecting this use, but also refers to AI/ML-driven security mechanisms, e.g., in the management domain [UKT22]. Finally, distributed ledger technologies are relevant wherever it is required to establish "distributed trust", i.e., trust that is not anchored in a central trusted authority, as it may be the case in interdomain management, to give an example.

Figure 3 shows the functional view of the 6G reference architecture that we propose. It is hierarchically composed of the set of planes that traditionally build the mobile network architecture and has done so since the earliest releases of the 3GPP standards.

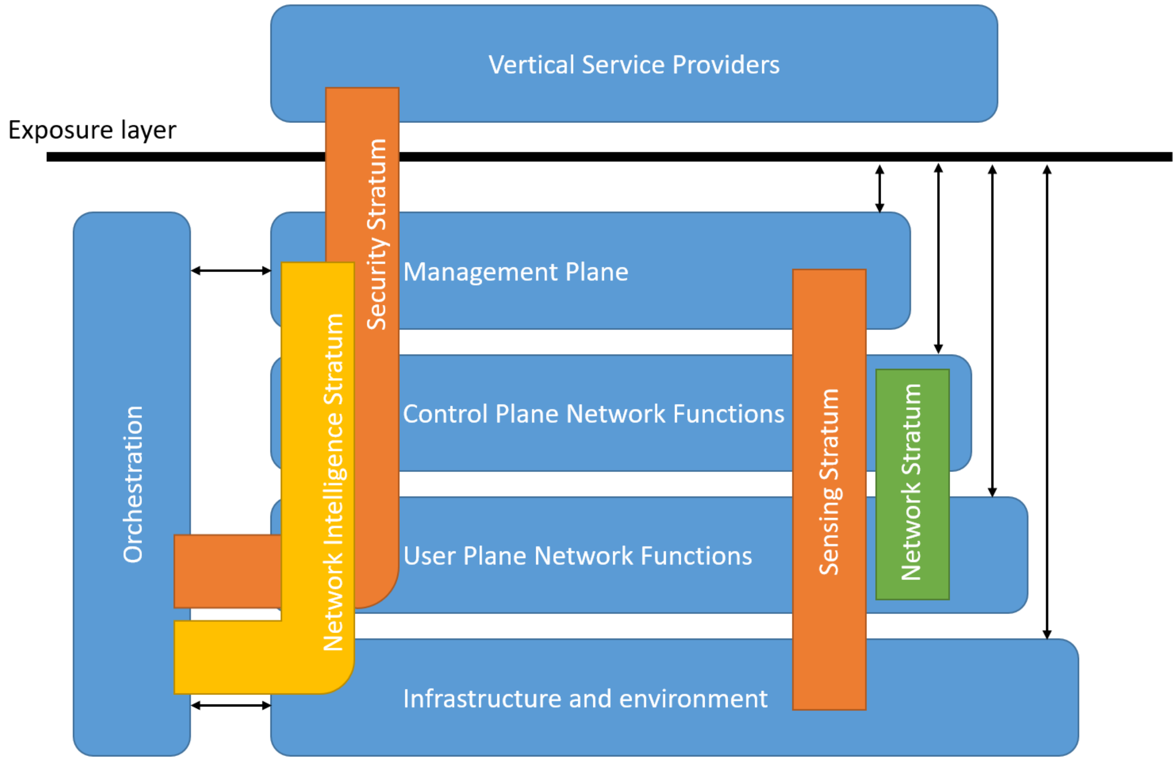

Figure 3: Functional view of the proposed 6G reference architecture

CU/CPP and UP network functions are responsible for delivering the expected QoS, efficiently allowing UEs to exchange data with the network. As previously discussed, these planes entail novel access technologies, which may include also the ones leveraging Terahertz bands and Visible Light Communications; AI-native air interface, arranged in specific ways (e.g., cell free networks [RAB+20], [NAY+17]), and even including Extreme edge functions like the ones that are managing and reconfiguring intelligent metasurfaces. Together, they build the network stratum.

Clearly, this richness in the available NFs, that have to be arranged and properly configured according to the network slices they belong to, poses new challenges to the management plane of the network.

Here we introduce the second stratum of the functional view: the network intelligence stratum. By borrowing and extending the terminology from the 3GPP system, we define a stratum as a set of coordinated functions that are running in different planes (or domains in this case) of the network. Traditionally the non-access stratum included functions from the UE, UP and CP. The network intelligence stratum encompasses and coordinates functions in all the network: ranging from the intelligent operation of network functions to its autonomous management and orchestration. The network intelligence stratum gathers data and analytics also from the infrastructure and environment.

We extend the infrastructure to include environmental aspects (i.e., the environment where the infrastructure is deployed and functions are executed) to allow a tight interaction between the network and the surrounding space. Properly steering beams at very high frequencies or using Unmanned Aerial Vehicle (UAV) to extend the network coverage require a sensing stratum that can efficiently coordinate functions, harvesting data from fixed landmarks or dynamic Light Detection and Ranging (LIDAR) scans, or even use the UP wireless technology as an additional source of sensing, possibly in an energy harvesting fashion.

Finally, the last stratum we discuss in the functional view is the security one, that manages all the cyber security and data privacy aspects in the network. This stratum coordinates functions in all the planes and domains of the network up to the vertical service provider one, that also benefits from the enhanced 6G security and cooperates with it to minimize the attack surface, while allowing the service customers to have full control on the data (including the network one).

This interaction is possible thanks to the enhanced exposure interface between the network and the vertical service providers that, through the use of network applications, can leverage on data, functions, and procedures offered to support and enhance the user experience. Through the exposure interface, the traditional barrier between operators and service provider is removed, allowing a white-box customization of the vertical service.

2.2 Architectural Principles

In [HEX-D51], [EWS+22] eight different architectural principles were defined, meant to serve as guidelines when developing the 6G architecture. A summary of the architectural principles can be found in Figure 4.

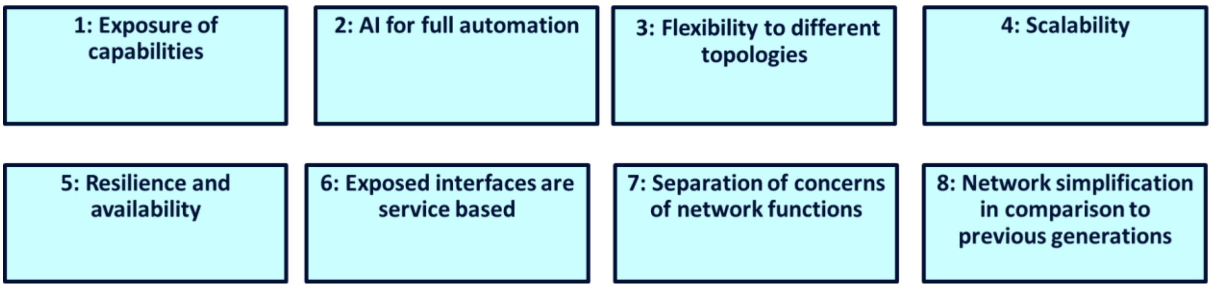

Figure 4: 6G architecture principles from [HEX-D51], guiding the architecture design

Principle 01: Exposure of capabilities

The architecture solution shall expose new and existing network capabilities to E2E applications and management such as predictive orchestration. The analytic information can for example be performance predictions such as latency and throughput, or it can also be localisation and sensing information.

Principle 02: AI for full automation

The architecture should support full automation to manage and optimise the network without human interaction. The closed loop network automation assumes the use of AI/ML.

Principle 03: Flexibility to different topologies

The ability of the network to adapt to various topologies without loss of performance while still enabling easy deployment. This can for example be the ability to adapt to new traffic demands, new spectrum situations, private networks and ad hoc mesh networks.

Principle 04: Scalability

The network architecture needs to be scalable both in terms of supporting very small to very large-scale deployments, by scaling up and down network resources based on needs.

Principle 05: Resilience and availability

The architecture shall be resilient in terms of service and infrastructure provisioning using features such as multi-connectivity and removing single points of failure.

Principle 06: Exposed interfaces are service based

Network interfaces should be designed to be cloud-native, utilising state-of-the-art cloud platforms and IT tools in a coherent and consistent manner.

Principle 07: Separation of concerns of network functions

The network functions have bounded context and all dependencies among services are through their APIs with a minimal dependency with other network functions, so that network functions can be developed, deployed and replaced independently from each other.

Principle 08: Network simplification in comparison to previous generations

Streamline the network architecture to reduce complexity utilising cloud-native upper layer RAN and CN functions with fewer (well-motivated) parameters to configure and fewer external interfaces.

3 Architectural enablers

After having discussed the main novel architectural trends and principles that will vertebrate future 6G network architecture we dig into each specific topic, identifying solutions and technology that we consider relevant for next generation mobile networks. Rather than focusing on specific network sub-domains such as Access, Core, Orchestration only, we structure the discussion along different axes related to 6G features that network should have. Many of them are actually multi-domain, as discussed in Figure 3, such as Intelligence and Security, other are features that shall encompass the design of all 6G components, such as sustainability and programmability. We discuss them next.

3.1 Intelligent network

The ultimate target for the Intelligent Network is to enable autonomous and adaptable networks, with no (or minimal) human intervention, leveraging cognitive, closed-loop control network functions that can be instantiated on an on-demand basis even across network domain boundaries. In this sense, the task of the Intelligent network is to define the underlying mechanisms to support embedded AI for 6G, , and to ensure dynamic adaptability of the network architecture to new use cases while keeping the infrastructure and energy costs at acceptable and sustainable levels. Built-in and integrated AI/ML depend on intelligence distribution and management empowered by distributed data and AI/ML pipelines, automated closed-loop network operations and orchestration to satisfy any E2E service KPIs. Therefore, the constituent network functions need to be adaptable to new environments for which they were not originally planned for. Intelligent Network integrates different software implementations of AI functionality, multiple AI-agent setups and, different learning architectures with AI-driven network orchestration and cross-domain function placement, and built-in data analytics frameworks.

Moreover, such integration of intelligence in the network shall be natively supported by the 6G architecture, introducing specific elements and architecture extensions the following sub sections to build the Network Intelligence Stratum, such as a new Network Intelligent Plane composed of Network Intelligence Function (NIF) and Network Intelligence Service (NIS), an intelligent distribution framework to implement intelligent distribution, and new AI-driven air interface design on RF hardware impairment compensation [FS20], channel estimation [CMWT21] and resource allocations, and development of AI functions to provide AI as a Service (AIaaS) to enable AI training, monitoring and Life Cycle Management (LCM) accounting for the specific tasks and procedures related to the intelligence training, deployment, and monitoring.

3.1.1 Intelligent network key technological enablers

In the following, we detail the key technological enablers for 6G flexible networks.

3.1.1.1 Network automation

Automation of networks aims at replacing tasks undertaken by human operator with processes run by machines or pieces of software. AI-based automation is required in emerging 6G networks to manage the complexity in terms of technology and services and to meet quality, security, and resilience requirements. In practical terms, this translates into reducing human errors in network management and operations, reducing service provisioning time while improving time-to-market, and reducing network and security issues through closed-loop network operations. AI and ML techniques will be key to achieving a high degree of automation in 6G networks, unlocking the potential of data analytics to assist network orchestration and operations.

An example of such network automation is the one leveraging on customized AI/ML techniques that can finally empower such automation vision. As a matter of fact, the loss functions that drive the training process of supervised machine learning models. In the vast majority of cases, loss functions are designed to be generic enough to work well in a wide range of scenarios. However, this approach eventually falls short when dealing with specific network related problem such as capacity forecasting. Therefore, 6G network shall be leverage on especially tailored functions such as the one presented in [CBF22].

3.1.1.2 AI as a Service

To bring AIaaS to 6G open for all, requires several new network functions and corresponding interfaces. [HEX-D52] identifies several relevant AI functions needed to provide AI automation and seamless AI-driven 6G orchestration. The functions are AI repository, training, monitoring, and finally AI agent. A new AI-enabled architecture aims to support distributed AI services, needed for supporting AI as close as possible to the application, AI service chaining (in the sense of assisting with AI traffic flow between AI services in the network) needed to accomplish specific AI tasks, as well as cross-domain AI service consumers and data producers. The in-network AI architecture, as proposed in e.g. [HEX-D51], also aims to support AI-enabled access control considering attributes such as user, data object and environment information, efficient transfer of large amounts of data, network and application-specific analytics, and the sharing of AI models, once available and updated. The new architecture supporting AIaaS will be employed for enabling different learning services, such as Federated Learning (FL) and Explainable AI (XAI). Once a consumer requests the AI service, mechanisms to allocate resources and instantiate the required functions are needed. Based on the service requirements and mobile device's capabilities, the AIaaS-supporting 6G network will be able to decide which functions of the service will be instantiated. On one hand, the mobile device may produce data, receive the global model from the FL server, build local AI models, and make decisions based on it.

Besides being provided as a Service, AI solutions shall be directly taken into account while designing specific part of the network, such as the approach taken in [KHH+21], where deep convolutional networks are directly integrated into the network protocol stack.

3.1.1.3 Dynamic Function Placement

Network Function (NF) migration and placement problem has been studied in a number of previous works, such as [LAG19] and [HJS17]. This work has been extended to 6G architecture to consider Dynamic Function Placement (DFP) to a full fabric of different domains of the architecture, from the end-user domain up to the central cloud to enable continuum orchestration. This implies that DFP needs to operate across domain boundaries of collaborating clouds. The domains need to expose their shared resources and relevant APIs for service discovery.

DFP is responsible for optimal function deployments to provide differentiated services in single domain, multi-domain, and cloud environments [HEX-D51]. For the functions with enabled DFP features, monitoring of the specified cross-layer KPIs must be supported. The monitoring info is used in decision making where the performance of the current functions is evaluated, and a need for changing function instance numbers or locations is determined. Decision-making could be based on the usage of AI/ML techniques, for instance, provided by AI/ML services for Orchestration and Management functionality.

In one sense, DFP could be seen as one of the core functionalities on top of what the orchestration framework's Life-Cycle Management (LCM) provides. The main responsibilities of DFP can be characterised as i) relocation of function instance, and ii) runtime context transfer for the instance relocation, which are closely related to more traditional LCM functionalities like replica management and service scaling up and down. However, the separation of responsibilities and roles between LCM and DFP is not always clear and depends on implementation aspects. For instance, the instance relocation raises some new technical challenges like how to define extractable and hence movable runtime state for any function and how to securely move such state potentially between domains. Additionally, regarding the scope of orchestration and management (incl. DFP) operations, special focus should be put on the notion of the domain, i.e., how to support multi-domain operations.

Figure 5 depicts how DFP is positioned in the E2E architecture and how cross-layer KPIs and metrics are required in the network service layer, which is the focus of the DFP management operations. For different layers in the E2E architecture (i.e., the application layer, the network service layer, and the infrastructure layer) monitoring of layer specific KPIs and Key Value Indicators (KVIs) could be targeted depending on the use case. For instance, for end-user services, the "health" of a service is generally measured in the application layer. Respectively, the infrastructure layer provides resource-specific metrics to be used in operations done in the network service layer. There is a special relationship between the infrastructure and the network service layers visible in definite orchestration and management operations where the existence of special hardware resources in the infrastructure layer governs how the operations can be executed. In other words, functions can only be placed in physical nodes where the required hardware resources are available. In addition, the extreme edge represents the infrastructure layer part with the most limited computing resources and sets new challenges for the cloudification itself.

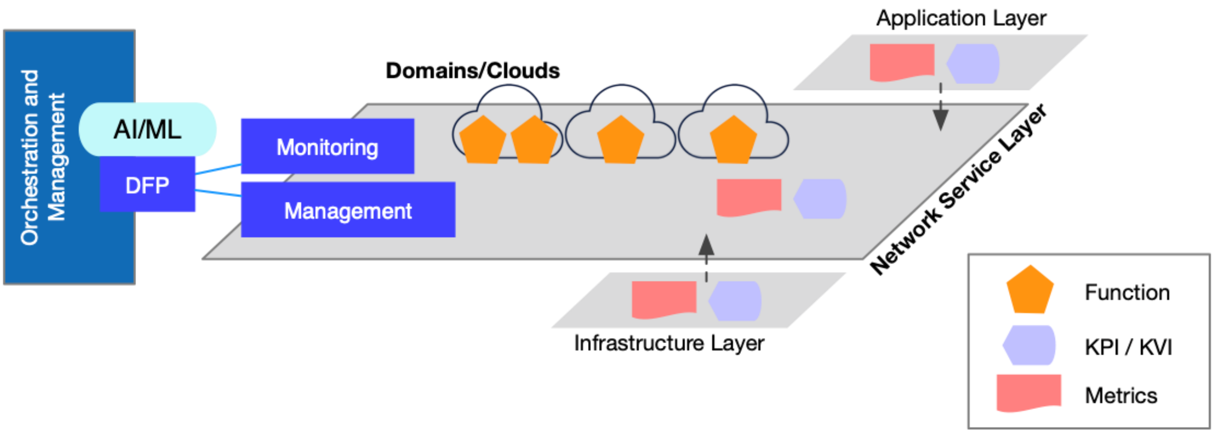

Figure 5: DFP layered view [HEX-D51]

3.2 Flexible network

Flexible networks intend to enable extreme performance and global service coverage. The network functionality and architecture must then be flexible enough so that it can adapt to different topologies. The “Network of Networks” in [HEX-D51] [ECR+21], considers the usage of technologies for supporting flexible topologies to increase the availability and reliability of the connection.

The deployment of mobile networks has become increasingly complex and diverse with every new generation. During the 4G standardisation there were many discussions about so-called Heterogeneous Network (HetNet) solutions, i.e., how networks with both wide-area macro and small-cell pico base stations should cooperate. The extension of the radio spectrum into mmWave in 5G added yet another aspect to flexible deployment. 6G deployments will include nodes using even higher sub-THz spectrum (e.g., in the 100-300 GHz frequency range) with limited coverage as well as nodes at low frequencies with seamless coverage, as illustrated in Figure 6. Furthermore, the number of network solutions for capacity and coverage is also expected to increase in the 6G timeframe. These include solutions such as Distributed MIMO (D-MIMO) networks, Non-Terrestrial Networks (NTN), campus networks, mesh networks, and cloudification of the network elements. Thus, 6G will be a network of networks.

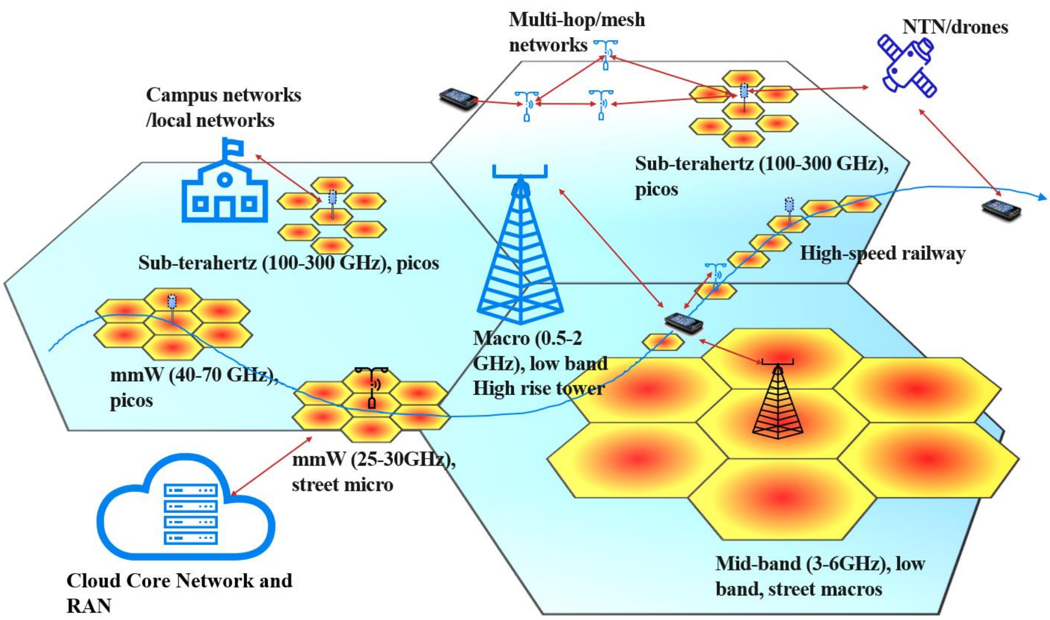

Figure 6: The 6G network of networks [HEX-D51]

As mobile broadband is becoming increasingly critical to society, the architecture of 6G must support reliability and resilience beyond 5G, both in terms of service and infrastructure provisioning, when connecting through any of the diverse connectivity options.

Therefore, it becomes even more important with a 6G Multi-Connectivity (MC) solution with the ability to have efficient spectrum usage and be able to aggregate resources between the current frequency bands and the new sub-THz spectrum bands. This calls for a new improved MC solution. The new 6G MC solution should replace the current DC and CA solutions by combining the best features to be able to handle both extreme reliability and excellent flexibility. The MC solution should support decoupled Downlink (DL) and Uplink (UL) and the ability to quickly add inactive connections. A general disadvantage with the DC solutions for New Radio (NR) is the implementation complexity of the 3GPP specification, for example, the numerous architecture options for DC between LTE and NR and the message exchange over the Xn interface between gNBs [38.331] so care needs to be taken to reduce complexity.

With the combination of Terrestrial Networks (TN) and NTNs it will be possible to achieve 100% global coverage [BFC21]. NTNs can likely provide a lower capacity per km² than terrestrial networks, but at a reasonable cost. Thus, an NTN is suitable for rural areas, including oceans, with low or very low population density. For urban areas, there will always be a need for terrestrial networks. There are two types of architecture options for NTN: Transparent and Regenerative payload architecture. Transparent is the simplest type, where the NTN basically serves as a relay of the signal between the UE and the base station on the ground. The regenerative architecture is equivalent to having the base station (RAN) functions onboard the satellite. The main research question for 6G is how the NTN and terrestrial network mobility will be solved. Since the Low Earth Orbit (LEO) and Medium Earth Orbit (MEO) satellites move, it may be necessary to find solutions that minimize the number of handovers and the signalling needs for mobility robustness. Another important research topic for 6G NTN is the actual architecture solution, e.g., if regenerative or transparent or a hybrid split should be used [HEX-D51, BFC21].

Another possible improvement for 6G is to utilize Device-to-device (D2D) communications in a mesh network. The concept of D2D communications is not new as it has been discussed since 4G networks [DGK+13] to enable devices to communicate directly. D2D communications can also enhance the coverage and capacity of cellular networks through UE relaying. The following architectural challenges are relevant for a new improved mesh D2D communication:

- Defining the trust level for devices participating in the D2D/mesh network.
- Unified modelling of nodes and devices, in terms of network and computational resource characteristics, capabilities and constraints.
- Definition of interfaces to control and interact with devices for resource advertisements, synchronisation, reachability verification, etc.
- Selection of best possible nodes and devices depending on specific parameters (e.g., position, signal quality, battery level, availability, reachability, available computational resources, etc.).
- Integration with network and service orchestration for seamless management, control, and enforcement of D2D/mesh network communications.
- Methods and procedures for discovery of nodes and devices (including synchronisation aspects for capabilities advertisement).

3.2.1 Flexible network key technological enablers

3.2.1.1 Architecture streamlining

A new 6G architecture should support all types of traffic anticipated in 6G. However, this is not enough, 6G should also be streamlining NFs, for the cases where comparisons with previous generations are possible, be more efficient in terms of, e.g., capacity, coverage, signalling overhead, scalability and energy consumption. The assumption is that a cloud native approach can help meet requirements of a future network segments currently associated to CN and RAN.

The number of dependencies and processing points might be reduced by redesigning network functionalities with the aim to perform all relevant processing for a certain network task in a single point. Dependencies between NFs may cause unnecessary complexity and even latency. Based on an analysis and characterization of NF dependencies in [HEX-D52] the following candidate actions can be applied to reduce effects of dependencies:

- Separate subscription, policy handling and UE capabilities for RAN, functions that currently are handled by the Access and Mobility Management Function (AMF) [ECR+21].
- Merge entities responsible for “radio interface” configuration. Splitting CU and DU adds delay while adding complexity for innovation and optimization of radio performance.
- Separate UP control to allow direct signalling between UP nodes. This will reduce latency and provide opportunity for vendor optimizations, e.g., co-implementation.
- Separate UE signalling to enable separate association for UP controls, security, etc.
- Harmonize the service framework, e.g., discovery and security, as well as the context handling procedures, e.g., handover, re-establishment, resume, etc.

One important enabler for 6G architecture is function elasticity [HEX-D52] and in particular 6G-RAN-CN function elasticity, which is achieved by co-locating some of the common 6G-CN NFs with the 6G RAN-CP in the cloud environment, see Figure 7. Signalling procedures that benefit from being in the regional edge cloud comprises 6G mobility management and 6G session management. As a result of placing critical signalling processing together with 6G-RAN-CP in the regional edge cloud, signalling performance is improved thus reducing latency. This approach can be applied for 6G-UE associated services since the 6G-UE context handling would remain within the control of the 6G mobility management without creating new or additional dependencies.

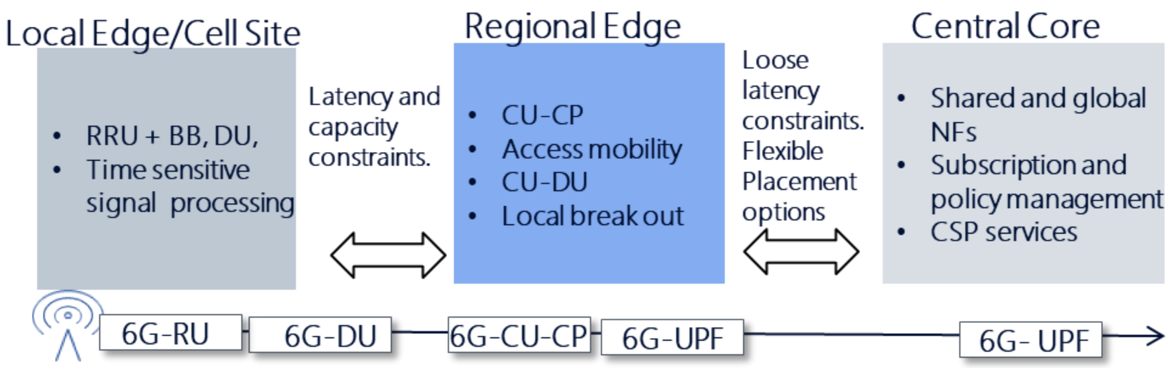

Figure 7: Functionality distribution between RAN and CN clouds [HEX-D52].

Another way to improve the 6G architecture is enhance the possibilities for signaling directly between NFs, i.e., to remove potential bottlenecks. This since many services already today require information transfer from one NG-RAN node to another NG-RAN via the 5GC. In 5GC the information is relayed via the AMF with limited or even no involvement of the AMF [HEX-D52]. To streamline this transfer, introducing Service-Based Interfaces (SBI) would allow this information to be exchanged directly between the NG-RAN NFs without the need to pass through the AMF, see Figure 8. This is also further discussed in section3.2.1.2.

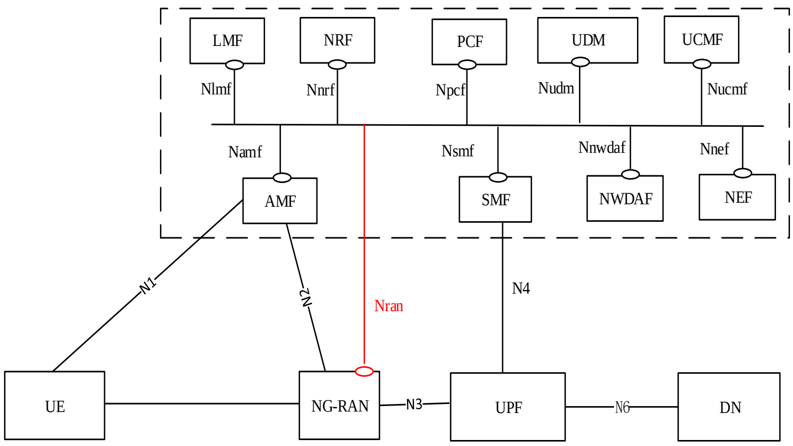

Figure 8: Service-Based Interfaces (SBI) from the RAN to the CN NFs would allow signaling directly between the NG-RAN NFs without the need to pass through the AMF [23.501].

3.2.1.2 Evolved Service-Based Architecture

With the introduction of Service-Based Interfaces (SBI) in 3GPP’s Core Network design, Release 15 has been a ground breaker in the flexibility this change introduced. The resulting Service-Based Architecture for a 5G System is illustrated in Figure 9 and depicts the majority of all 5G Core Network Functions (in green) and the change in interface naming conventions. While in a pre-5G world, naming of interfaces followed the convention of using N combined with an integer number, SBIs named with N followed by the name of the NF that offers a service (called Producer). This reveals a core improvement in the system architecture, i.e., there is no strict enforcement on which NFs can communicate on an interface. This resulting flexibility allows any new functionality of a Producer to be standardised without the necessity to create a new interface name if the requesting entity has changed. Furthermore, Release 16 introduces the Service Communication Proxy (SCP) which routes messages between 5GC NFs, if desired. Note, the SCP is not offering an SBI and therefore does not carry an interface name in the figure below. Also, the SCP is only an optional component and the 5GC can operate in three Models (A through

D), with A and B referred to as "direct communication", as no SCP is in use and Model C and D as indirect communication. For Model C, referred to as "SCP without delegated discovery", any Consumer (the requesting NF) will communicate with the Network Repository Function (NRF) on which Producer (the NF responding to the request) to use and the identifier of the SCP (Fully Qualified Domain Name (FQDN) or IP address). For Model D, referred to as "SCP with delegated discovery", any Consumer has the SCP identifier preconfigured and addresses all requests to this address. The SCP then communicates with the NRF to obtain which NF is supposed to be used.

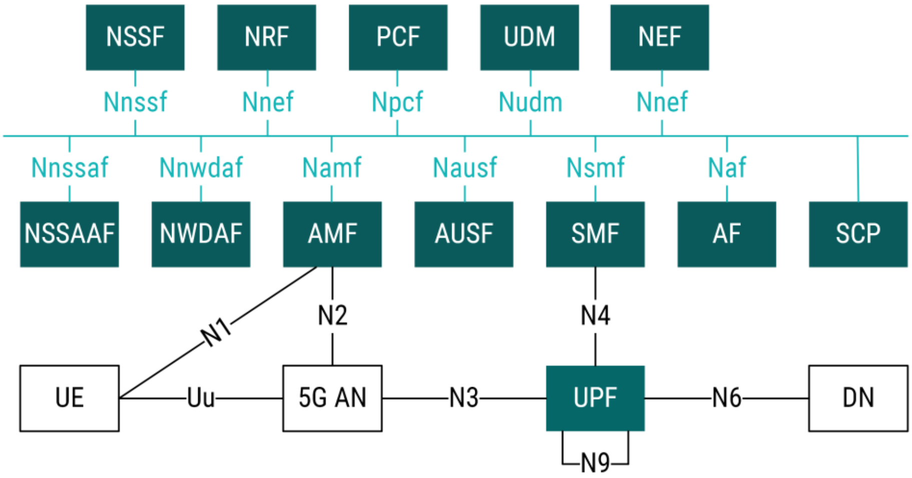

Figure 9: Release 17 5G System Architecture [23.501]

As can be observed in Figure 9, not all 5GC NFs are SBI-enabled, namely the User Plane Function (UPF) resulting in a point-to-point interface between the UPF and the Session Management Function (SMF). Also, the interfaces between RAN and CN, i.e., N1 and N2, are non-SBI-enabled.

Further enhancements are required to be able to, focuses on fully disintegrated private networks and aims to define a unified Service-Based Architecture to improve the operations of a deployed 5G system. The result of this unification is provided in Figure 10 which illustrates a beyond Release 17 5G system architecture with the following improvements:

- The SCP becomes a mandatory component and operates in a new model, Model E, which removes the ability to address the SCP directly and removes the necessity for the SCP to communicate with the NRF. Additionally, the SCP receives resource scheduling capabilities on top of the actual service routing capabilities.
- The N2 and N4 interfaces also use the SCP without any changes to the IP-based protocols they rely on. All endpoints on N2 and N4 are identified through an FQDN, enabling cloud-native orchestration of 5G Cores.
- The NWDAF is split into a Network Monitoring Function (NWMF) and Network Analytics Function (NWAF). While the NWMF is solely responsible for gathering data points, the NWAF offers analytical capabilities based on the data available in the NWMF. The reason for this is to allow different vendors to realise the NWMF and NWAF, given the growing importance of AI/ML.
- The introduction of a new 5G NF, the Who Am I Function (WAIF), which offers the ability to any NF to request information about itself, e.g. the parent domain under which the entire 5GC operates or the NF type it serves. This is mainly to support cloud-native procedures where NFs are packaged as containers or VMs and can be deployed numerous times.
- The last change to the 5G system architecture partially follows 3GPP's Work Item SP-220417 on "Study on UPF enhancement for Exposure And SBA" [23.700-62]. This study introduces an

Nupf interface for monitoring purposes and event notifications. FUDGE-5G is following the key issue on UPF monitoring, indicated by the Nupf interface in Figure 10.

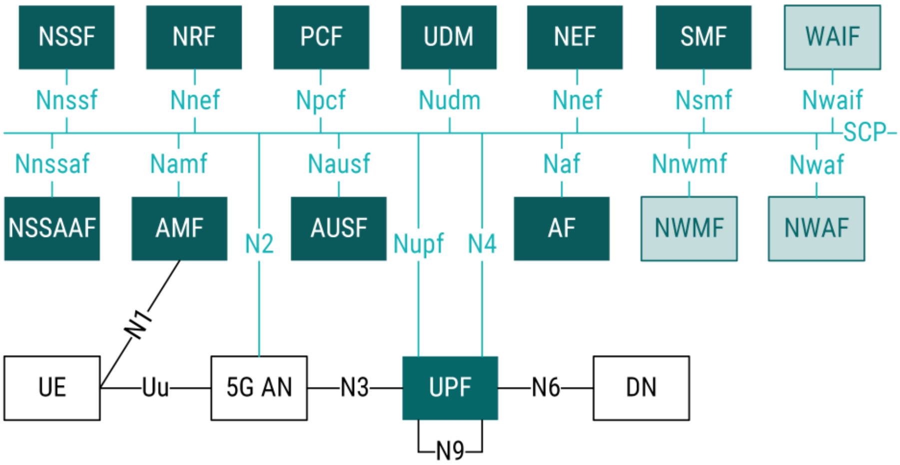

Figure 10: Beyond Release 17 5G System Architecture Implemented by FUDGE-5G [F5G13]

In order to unify the system changes described above, FUDGE-5G introduces a dedicated platform layer between the infrastructure and service layer, where 5GC and vertical applications are categorised as an Enterprise Service interfacing via southbound programmable APIs with the platform. As a result of the unification effort, the 5GC NFs WAIF, NWMF and SCP is located in the platform layer.

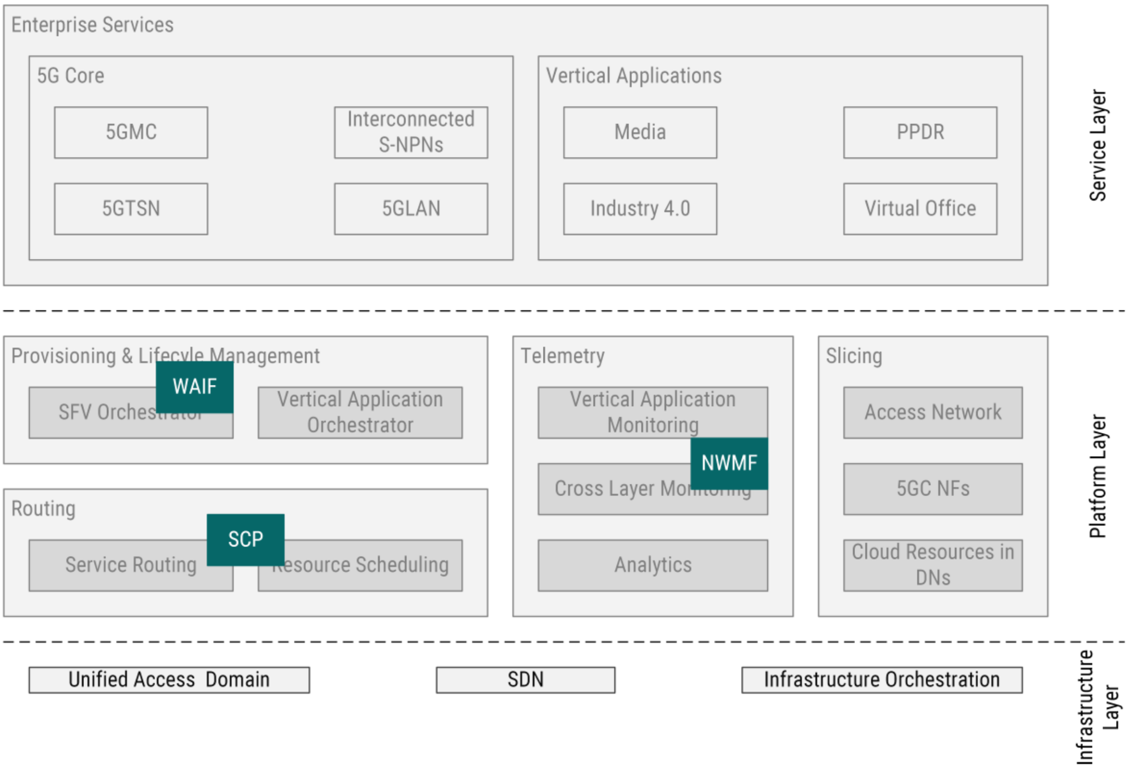

Figure 11: System Overview of FUDGE-5G's SBA Platform [F5G1.3]

3.2.1.3 Compute as a Service

Compute-as-a-Service (CaaS) is a use-case-enabling service approach, as described in [HEX-D12], which is aimed to / shall be used by any device (stationary or mobile, IoT, handheld, etc.) or network infrastructure equipment that chooses to delegate demanding, resource-intensive processing tasks to other parts of the network. The network nodes for workload addressment/execution are chosen as providing more powerful compute nodes, which are also of higher availability at the time of workload generation. These service-offering compute entities can be either devices other than the requesting one, or, for example, integrated in edge cloud servers at the infrastructure side. In the CaaS case, external compute resources can be made available to a specific entity or user device through a well-defined open interface. The basic principles relate to an offload of processing tasks to external compute resources. In this context, some of the needed features to be defined, as part of a 6G network architecture design, are the following [HEX-D51]:

- A general interface providing access to external computational resources.
- Mechanisms for discovery/detection of available compute resources (e.g., via a general register reachable by the CaaS provider).
- A functional entity (e.g., central controller/workload orchestrator) that decides when to offload (fully or partly) a processing workload.

The decisions on whether to offload a processing workload, and, if so, where to delegate the workload, are based on the knowledge of currently available resources of network nodes (or prediction of future availabilities) and taking into account requirements relating to performance (e.g., the delay for producing workload output and dispatching it to the requestor), the energy footprint of the workload delegation and the trustworthiness of the network node(s) offering their compute resources for workload processing. AI capabilities of the network can be exploited to orchestrate the task workload delegations.

3.3 Sustainable network

As mentioned before today´s society faces major challenges, including in particular the pandemic, distrust and global warming, which all need to be addressed while creating innovation-led opportunities for economic prosperity and job creation in a circular, green and digital economy.

Sustainability, both a main research challenge and a core value of 6G, is a holistic concept covering environmental, social and economic aspects, and it is built around meeting the needs of the present without compromising the ability of future generations to meet their own needs. From a 6G perspective, this refers both to the sustainability of 6G itself (***Sustainable 6G***), and the opportunity for 6G to support society and stakeholders across all sectors of the economy in getting more sustainable (***6G for sustainability***).

Focusing first on the direct impact, it encompasses environmental impacts connected to the use of energy and materials, but also social impacts associated with, e.g., transparency, traceability and respect for human rights. From 6G for sustainability perspective, 6G networks need to consider a wide range of environmental, social and economic aspects as outlined by the **UN SDGs** [UNSDG], [SDG] – the main recognized framework for sustainable development. In particular, sustainability mainly relates to SDG11 for sustainable cities and communities and SDG13 for climate action, since high energy efficiency, can be directly translated to lower CO_2 emissions. Apart from the associated KPIs, such as *energy efficiency* and consequently *cost efficiency, sustainability* and *energy consumption* are also main targeted areas of important 6G **Key Value Indicators (KVIs)**, such as the *Ecosystem* and *Innovation* KVIs.

Regarding sustainability, even if the current contribution of the ICT sector to the total carbon footprint of the society is limited (estimated to 1.4% [Itu20], [ML18] of overall global emissions), the increased use of mobile broadband and digital solutions will likely require densification of the network to increase the capacity. It may also require manufacturing of more devices (including IoT devices). This could lead to an increase of overall emissions unless energy efficiency continues to be addressed together with behaviours and the transition to renewable electricity supply. Supporting this, ITU, GSMA, GESI and SBTi have jointly developed trajectories which establish that the ICT sector should reduce its environmental footprint by 50% between 2015 and 2030 to decarbonize in line with a 1.5 °C trajectory in support of the Paris Agreement [Itu20].

Referring to the same sources, it is interesting to note that globally, the energy consumption from using devices represents more than 40% of the ICT power consumption while networks and data centres shared the remaining consumption roughly equally between them. From a carbon emission and life cycle perspective, devices again dominate and represent more than half of the overall emissions, while networks represent around 25%. Overall, the majority of networks and data centre emissions are associated with the use stage, while devices use stage and embodied emissions require as much attention. However, this balance looks different for other impact categories so it is important to consider environmental impacts of the full life cycle also for networks and data centres (including aspects such as life time, recyclability, materials efficiency etc.).

ICT sustainability: The ITU organizes the sustainability of ICT into three orders of effects: i) first order effects that denote the life cycle impacts of goods, networks and services (i.e., its footprint), ii) second order effects that denote the impacts in other sectors due to the use of ICT and iii) other effects which denote higher order effects such as those associated with behavioral changes [Itu14]. In our terminology, the first order effects of 6G are also referred to as Sustainable 6G or footprint, while 6G for Sustainability refers to the second and, to some extent, higher order effects.

To be relevant, an environmental sustainability study on 6G´s first order effects must be *holistic* and take into consideration the entire 6G network (core, transport/aggregation, access, and user equipment/device) during its entire life cycle. To evaluate the environmental footprint of equipment, a network, or a service, Life Cycle Assessment (LCA) provides a comprehensive method for capturing its overall impact. Indeed, LCA covers the entire life cycle of the studied system (from raw materials extraction to end-of-life treatment) and can deliver results for multiple environmental impact indicators (e.g., climate change, abiotic resources depletion, and water consumption). LCA has been standardized for ICT by the ITU [Itu14]. However, application of such standards already during technology development is challenging as the basis for any LCA is the use of resources and release of emissions.

6G will not exist in a vacuum but will instead live along, and in some cases supersede, other mobile and fixed networks. As such, it is important to consider the impact of the ICT sector with and without 6G, as well as the impact of 6G itself. When 6G is deployed, an increase in environmental impact could be expected because of the superposition of 6G with the other mobile network technologies. However, the deployment of newer network technologies makes the decommissioning of older technologies possible. Considering that 6G will be designed to be more sustainable than previous technologies, overall net gains in terms of environmental impact are aimed for.

Regarding the carbon impact of the ICT sector, [ML18a], completed by [ML18], which is one of the most comprehensive and recent studies, estimates the sector to represent 1.4% of overall global Green House Gases (GHG) emissions for 2015, based on a large sample of measured data as reported by companies and estimates that that level will stay quite stable until 2020. This level has also been agreed as a sector baseline for the decarbonation trajectories developed jointly by ITU, GSMA and GESI and applied by SBTi [Itu20]. Of this 1.4%, user devices represent 54% of emissions, networks 25%, and data centers 22% (resulting in 101% overall due to round off effects). From the global perspective, the embodied/use stage emissions ratio is closer to 50/50 for aggregated user devices due to short life spans and less intensive usage, compared to network and data center equipment for which use stage emissions represent most emissions due to longer life spans and as the equipment is used 24/7.There are three major drivers for the future trends in first order emissions of the ICT sector: the decoupling between data traffic and energy consumption, the reduction of ICT energy consumption, and the decarbonation of ICT energy. Let us recall that the L.1470 demands that the sector, to help stay beneath the 1.5°C warming limit, should reduce its emissions by 45% in 2030 and go towards net-zero by 2050 [Itu20] [Itu 21]. For this, the successful decoupling of data traffic and energy consumption of networks will be necessary but not sufficient. Considering the decoupling, the energy usage has been derived as stable 2010–2018 among European Telecommunications Network Operators (ETNO) members, at slightly below 30 kWh/subscription (including overhead), despite substantial data traffic growth (by a factor 12) [LMB+22]. This development sets an example for this decade to follow.

3.3.1 Sustainability targets

In accordance with the UN SDGs, we aim for a threefold sustainability: *societal, economic and environmental*. We now present the three corresponding targets with the associated KPIs, as well as methodological considerations for measuring said KPIs. For each target, we propose technological and societal enablers.

3.3.1.1 KPI1 (Societal target): enable the reduction of emissions of >30% CO_2 eq. in 6G-powered sectors of society

The enablement effect (i.e., a positive second order effect) is commonly associated with solutions or services that could help reduce or avoid GHG emissions [HEX-D13]. Enabling reductions of emissions of >30% CO_2 eq. in 6G-powered sectors of society is targeted. Independent of expected outcome, a common approach for most work in this area is the definition of a baseline scenario without the solution, the definition of a scenario with a solution that reduces GHG emissions applied, and a comparison between the two. Hence the analysis is hypothetical as the two scenarios cannot exist at the same time. In addition, also the direct rebound effects have to be taken into account, i.e., emissions associated with usage of a service which is not associated with modifying the baseline but occurring due to the convenience of the solution. Today, both the baseline and consolidated detailed methods and standards that describe a clear methodology for evaluating the "enablement" impact of ICT on other sectors are lacking [CBH+20]. Work is underway in ITU to provide assessment methods for existing or defined solutions, expected to become available during 2022. As for existing high-level methods, the approach is expected to refer to existing applications with a proven and measurable effect, which is often used as input for different usage scenarios. For future technologies, proven case studies will be lacking, resulting in an inevitable additional level of uncertainty and the need to adapt any existing methodology. Moreover, the overall effect of 6G (the aggregated effect of all potential, future use cases) is beyond reach as the total use of 6G cannot be foreseen. Consequently, the evaluation of 6G can only be scenario-based and refer to specific use cases. The main challenges include the establishment of baselines, estimating impacts of future 6G solutions and their usage, and estimating the induced impact for a future scenario, potentially considering the direct rebound effect (not to mention the difficult extrapolation from case studies to larger populations). To achieve this target, the following items are under study [HEX-D13]:

<u>Baseline</u>: a non 6G powered service compared to a 6G-powered service. The main complexity is the data collection/estimation related to CO_2 impact with and without 6G.

<u>Methodology</u>: applying existing and developing methodologies to provide a transparent and well-founded result is a challenging task associated with significant complexities and uncertainties, especially at this early stage of technology development. Moreover, systematic approaches are required to assess the potential GHG reductions of enablement effects. Knowledge about technology itself is not sufficient to establish usage scenarios; it should be accompanied by considering how strategies and policies may form cultural change and new personal and societal behaviors. In addition to considering the importance of such effects for the assessment, it is currently studied how to consider not only technological aspects, but also the behavioral and cultural ones to identify the core aspects and actions, at both technical and organizational, behavioral, cultural levels that will be key to maximize the enablement effects and thus reach the defined target. Without conducive actions, rebound effects may diminish and even, in some cases, overcompensate the potential advantages. However, it is acknowledged that rebound is a complex area, and some rebound effects may actually amplify reduction effects. [HF15].

Scope: Enablement effects should be defined and evaluated for specific use cases. Such analysis will be performed on a "what-if" basis, outlining the different scenario outcomes should the selected use case(s) be made available and applied with an assumed effect or not. Moreover, in what measure a certain new technology will be adopted and used is also influenced by personal/societal culture, economic factors and behaviors. Importantly, enablement is calculated as a net effect after subtracting the footprint of the solution, unless that is deemed insignificant. This may imply some synergies with KPI2 and KPI3 in terms of modelling.

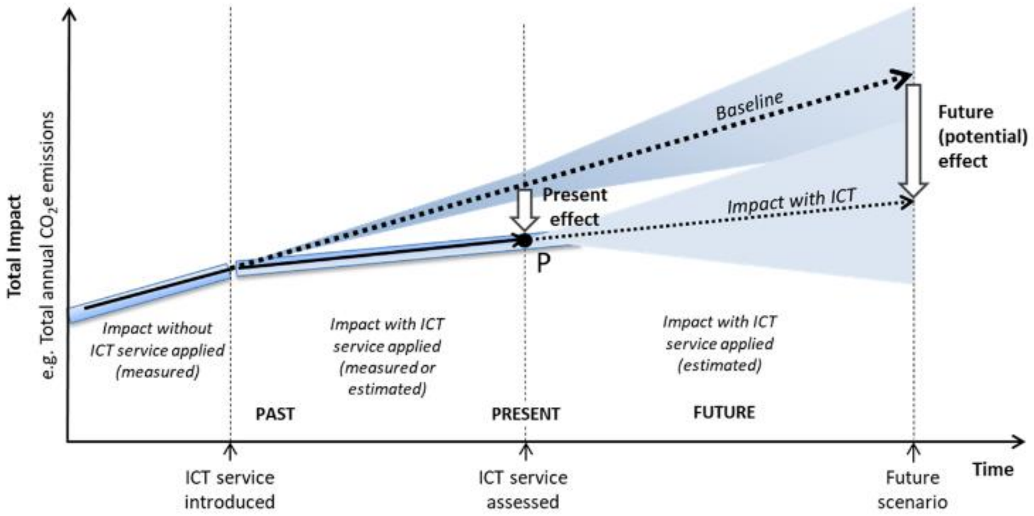

Figure 3.12: Assessing the enablement effect [CBH+20].

To summarize, today, agreed detailed methods that describe a clear methodology for evaluating the "enablement" impact of ICT on other sectors are lacking. It is also concluded that the overall effect of 6G is beyond reach as the total use of 6G with the magnitude of unknown use cases cannot be foreseen. Consequently, the evaluation of 6G can only be scenario based, and refer to specific use cases.

3.3.1.2 KPI2 (Economic target): reduce the Total Cost of Ownership of 6G by >30%

A mobile operator's Total Cost of Ownership (TCO) for the introduction of a brand-new mobile system includes both Capital Expenses (one-time costs) and Operating Expenses (recurring costs), i.e., CapEx and OpEx, respectively [EFA+19]. A reduction of the TCO for 6G by at least 30% is targeted with respect to current networks.

In a typical mobile network today, CapEx is ~30% and OpEx is ~70% of the TCO over a 10-year period, with the Radio Access Network (RAN) being the biggest cost component in both CapEx (~50%) and OpEx (~65%) [Gha20], then followed by transport, core network, energy and other network costs (e.g., people, network management and maintenance, etc.). A breakdown of RAN CapEx shows that the largest cost components are site construction, spectrum and equipment. Similarly, a breakdown of RAN OpEx shows that the largest contributors are power consumption, site rentals and operations.

In order to achieve the economic target a methodology has been developed based on which the 6G TCO evaluation requires a baseline mobile network architecture to be properly identified. Such baseline architecture allows to assess the 6G TCO in relative terms (i.e., *x*% cost savings) with respect to it, by quantifying the potential cost reduction provided by the most promising 6G network enablers when actually deployed, for each of the cost items impacting the TCO. By taking into account that operators are currently deploying 5G networks based on both the new 5G Core network (5GC) and the NR (New

Radio) access technology – i.e., the 5G NR Standalone (5G NR SA) – it is natural to assume the 5G NR SA as the baseline architecture for the 6G TCO evaluation.

For determining the cost structure and the "weight" of each cost component (RAN, transport, etc.) in the overall 5G NR SA TCO, the study provided by the GSMA has been considered [Gsm19]. Such work considers the dynamic interplay of a diverse mix of factors broadly falling into three groups: *cost drivers*, representing the "reasons why" a new (5G) network is needed, e.g., the mobile data traffic growth, the (operator-specific) strategy choices in terms of use cases being exploited for monetization, etc.; *cost accelerators*, that is, factors such as the RAN and the backhaul upgrades, the Edge Computing deployment, etc., which increase the overall cost of owning and operating a (5G) network – and that can be classified as being CapEx or OpEx – as they are needed to cope with the presence of multiple cost drivers; and *cost optimisers* which can serve as a catalyst to accelerate the (5G) network evolution while keeping the TCO at an affordable level from the operator's perspective – typical cost optimisers include new RAN architectural approaches, e.g., virtual RAN (vRAN) instead of legacy distributed RAN (D-RAN), architectural enablers such as automation and Artificial Intelligence (AI) for planning and executing modern mobile network operations, low energy and or CO_2 reduction solutions such as liquid cooling replacing air conditioning for the equipment, etc.

Quantitative analysis and results derived from the above methodology will be provided, where the TCO reduction will be assessed for exemplary use cases each representing an application of a specific deployment strategy among the ones identified by GSMA in their study – after proper identification of the most significant and use case specific architectural enablers allowing to cut costs down.

3.3.1.3 KPI3 (Environmental target): reduce energy transmitted per bit by >90%

Efficiency is expressed as the ratio between energy in kWh and, e.g., data volumes in Gb evaluated during a time period. This is reflected in the MWh/Tb index given in ETSI TS 203-228 which has defined a methodology to evaluate this KPI at the network level.

Several studies have shown that at each transition between two cellular generations, a reduction factor of 10 has been achieved in terms of energy consumption per transmited bit in wireless networks [Arc19], [HEX-D13]. This achievement has largely been obtained thanks to spectral efficiency induced by higher bandwidth combined with the advancements in physical layer techniques (e.g. new modulation and coding, waveforms and multi-antenna transmission schemes), and coupled with a great hardware improvement in terms of integration, miniaturization and processing and also due to a substantial progress in sleep modes management systems.

All the network segments should be addressed including access, transport and core networks. Our ambition is to not consider only networks but also to make the link with services and contents delivery points like cloud and data centers. The 5G NR was selected as a baseline considering different trafic scenario including high or low data rates.

Measurement and assessment methods are now well-known and applied by mobile network operators. The assessment methodology is described in the ETSI 203-228 standard which support operational network. The evaluation method is the measurement of the energy consumed by a radio base station during a time period (generally one hour) and the corresponding total traffic volume delivered by the base station to all the connected users. The trafic volume strongly depends on signal bandwdth and frequency carriers. However, the energy consumption will essentially be related to the hardware capabilities and specifications that can be clustered into the following categories:

Electronic components efficiency. This category considers all the electronic layers that impact the global consumption including the baseband unit (computation part) as well as the radio unit (radio frequency (RF) amplifying part). The computation part is mainly dependent on Moore's law and microchips integration while the RF amplifying part is driven by power amplifiers technology improvements, and materials, e.g., Galium instead of Silicon for its good performance at high frequencies.

Bandwidth and signal characteristics. This lever addresses the signal properties like frequency carriers, aggregation capabilities, bandwidth specification as well as the physical layer features of the signal, e.g., modulation and coding schemes, the waveform type, and precoding, in order to estimate the improvement of spectral efficiency.

Artificial Intelligence and multi-goals optimization. This new lever could bring very promising energy savings and optimizations while maintaining an equivalent quality of service. AI can be introduced to optimize sleeping periods of RF modules for exemple as well as to adapt the needed resources to the user demand. Moreover, AI can also be used to detect energy consumption anomalies and overdimensioned sites that could be reenginereed to adapt the network resources to the targeted quality of service. In addition, AI-empowered receiver can perform signal detection in the presence of power amplifier non-linearities, hence, enabling operation of power amplifier with lower back-off, leading to higher energy efficiency [HEX-D42].

Sleep-modes and network orchestration. Sleep modes have been one of the main levers for decreasing the energy consumption of wireless networks this last decade. Their performance are closely related to the physical and MAC layers design as well as to the signal characteristics. The main improvements have been achieved with the OFDM structure which allow rapid sleep modes generally called micro-DTX. Also, the MIMO configuration now allows to switch off part of the antenna transceivers depending on the trafic demand. 6G PHY/MAC layers design should then consider sleep modes implementation in their DNA to enhance their efficiency. New technics as lean carrier and deep sleep modes could then be implemented without a loss in QoS or user experience.

3.3.2 Sustainable network key technological enablers

6G networks will need to employ a number of key enabling technologies and tools towards achieving sustainable networks. Among them, the disaggregated and virtualized RAN will enable elastic edge computing architectures, which accompanied by energy-efficient End-to-End (E2E) network, compute and storage resource allocation can result in significant network energy efficiency gains. This stems from the fact that 6G networks are expected to be highly heterogenous both in terms of employed technologies as well as resource types (communication, computation and storage resources). Therefore, energy-efficient resource allocation becomes challenging due to the large number of strongly coupled decision variables. In this context, efficient resource allocation strategies should: i) jointly consider all different types of resources, i.e., communication, computational and storage, and access as well as transport technologies, e.g., sub-6GHz, mmWave, optical communications, as well as their constraints, ii) take into account the End-to-End (E2E) network path from the traffic's source to the destined UE to guarantee E2E optimality, iii) induce low computational complexity to enable near real-time decisions, while meeting the E2E delay target, and v) achieve high energy efficiency. Developing energy-efficient solutions serves a twofold goal: a) reducing the Operational Expenditure (OPEX) of the involved stakeholders (e.g., Mobile Network Operators (MNOs), Infrastructure Providers etc.), and b) leading to environmentally friendly solutions by limiting the associated carbon footprint.

The cloudification trend is expected to continue for 6G enabling novel network designs, e.g., cloud-optimised network procedures can be obtained considering NFs capable of accessing any (authorised) network information with limited (or no) nested interactions among NFs. The key challenge is to design a 6G architecture that can fully utilise and interact with the cloud platform with regards to speed of development and reuse of common cloud components, balancing the need to standardise business-critical interfaces with the fast evolution of IT tools, such as DevOps.

Other promising techniques that lay mainly on the device level include wireless power transfer and energy harvesting targeting energy-neutral devices with advanced characteristics. An energy neutral device can be defined as “a passive or active device with a guaranteed continuity of use through a Wireless Power Transfer (WPT) or energy harvesting link that offers sufficient energy” [CBD+22]. The benefits of this type of devices are twofold. First, they can enable the sustainable realization of massive IoT deployments, consisting of a massive number of low-power connected devices, and second, they can limit the excessive number of batteries that is needed for such a realization, which typically contain toxic materials, thus leading to a sustainable environment. A special focus should be also given on the combination of the aforementioned techniques with renewable sources of energy to further boost their sustainability and environmental friendliness.

3.4 Secure network

The evolution towards next-generation networks requires them to be more secure, able to address the additional requirements on trustworthiness associated to the growing number of use cases and the dependability of an increasingly critical infrastructure.

Trustworthiness is one of the six main research challenges in the flagship effort of the Hexa-X project, and security forms a basic foundation for all systematization of trust in connectivity. [HEX-D12].. Security considerations must encompass all aspects of cyber-security: resilience against attacks, preservation of privacy, and ethical, safe application of automation means, especially including AI, to network operations and applications. Security also depends on active management of threat surfaces, including proactive measures such as threat prevention and protection as well as reactive measures such as attack discovery and mitigation. As network services consolidate as essential components in a growing number of application scenarios, their dependability and, equally important, the perception of such dependability as an achievable characteristic, becomes a key feature for network operators, service providers, application developers and, above all, end users.

A realistic approach to this trustworthiness challenge must acknowledge that complete security is not achievable, and that all security measures comes with a cost in other terms (such as usability, agility, or swiftness). Therefore, a balance is required in terms of this cost, the risks to be considered, and the impact of a security breach on the mission objectives being served. The Level of Trust (LoT) of a particular network service in a concrete application scenario is proposed as the essential KVI to be considered in this regard. The characterization of LoT constitutes one of the main goals of the current efforts in analyzing the security features of next-generation networks. This includes identifying both the applicable technologies to domain experts, and respectively analyzing the solutions proposed by these experts in the framework of previous experience and feasible attack patterns.

Moreover, the analysis of network data to improve the security or the performance is not an exception with relevant advances in the past years. However, the usage of data is not exempt of issues, with the privacy of the final users (and the confidentiality of company data) on the focus when data should be shared among different partners. Another similar research issue is the protection of the users against malware and other attacks from the network is possible by monitoring the network traffic.

Though it may seem obvious, it is worth recognizing the imperative to apply this security analysis at all levels: for each individual applicable technology (at any plane and layer in the communications stack and any segment in the network architecture) and from a holistic perspective (addressing network services as a whole including the involved human roles). Therefore, security activities are committed to analyze and drive the evolution of base security technologies, support the analysis of specific solutions at all levels, and assist the security evaluation of the different scenarios contemplated as reference for network evolution.

An initial assessment of these use cases has identified a set of security aspects to be considered:

- Improvement in implementation of general requirements: availability, confidentiality, integrity, and personal data protection.

- Scaling implications related to massive, pervasive deployments of unattended and untrusted devices
- Data provenance and physical-to-logical mappings in digital twin applications
- Real-time data flow protection in new applications such as immersive media or haptic interfaces
- Establishment of trust mechanisms between networks protective of subscriber privacy
- Root-of-trust based approaches to provisioning network gear, including authorizations for virtual network functions that may be deployed on generic hardware.
- Active disruption of network resources to examine the resilience to attacks
- Extension of current network security practices to ad-hoc networking
- AI-specific threats, including threat surface and attack vectors
- Protecting AI data feeds of any nature: raw, pre-processing, normalization and knowledge sharing
- Address the use of AI by attackers
- Security impact of deployment on heterogenous cloud environments

3.4.1 Secure network technological enablers

The ability of supporting data-intensive applications that require the analysis of data under the control of different parties is a priority for 5G/B5G mobile networks [PFN+20]. The considered scenario is typically characterized by a diversity of data sources stored on different nodes, possibly under the control of different parties. Data analysis may then require data exchanges and cooperation between these different parties. In such a context, there are several issues that need to be investigated [VFL+21]. A first problem is related to the fact that data may need to be selectively accessed in a cooperative way for executing certain analysis (queries). This implies the need of exchanging data and of executing collaborative computations that, however, should be controlled to avoid information leakage. For instance, data stored at one node might be released selectively, in restricted form, only to other specific nodes and within specific domains. Several proposals have addressed this problem, but they do not consider the possibility of protecting data through, for example, on-the-fly encryption (e.g., [SKS+19]). There are some solutions under investigation which will instead provide a solution for expressing and enforcing data sharing constraints, considering the cost of operation execution and ensuring their enforcement even in non-trusted environments where data may be possibly encrypted (e.g., [VFJ+17]). Such a solution will include a flexible model for representing, in an easy and effective way, the access privileges to portions of distributed data, supporting different levels of visibility over the data (e.g., plaintext visibility or encrypted visibility). The access privileges will regulate data sharing and flow among providers, also considering the trust assumptions on the parties involved in the data sharing and flow.

A concern related to the storage and collaborative processing of data is the lack of control over the computation and hence the uncertainty about the correctness of the result. This is a well-known problem and the research and industrial communities have devoted many efforts to the development of techniques to assess integrity of the result of computations outsourced to external parties (e.g., [VFJ+16], [ZDW21]). However, the problem of how to use such techniques and of assessing their effectiveness in different application scenarios still need to be further investigated. One possible solution is to focus on probabilistic techniques since they can be applied in contexts where computations are not fixed a priori. In this case, the detection of integrity violations will be based on the combined adoption of approaches such as data replications and markers [KLM+19]. The goal is to define a formal model for assessing the effectiveness and synergy of the probabilistic techniques adopted. The model will allow different parties to tune the amount of control to be enforced (and therefore the security guarantees to enjoy and the performance overhead to pay), considering different contexts or applications. Attention will be also devoted to the design of techniques for distributing different data chunks to different providers for providing better confidentiality guarantees (e.g., sensitive data could be stored within a trusted provider and non-sensitive data and/or an obfuscated version of sensitive data at an untrusted provider).

The usage of ML technologies is becoming pervasive with applications ranging from the diagnosis of cancer [KLM+19] to the selection of advertising online. The analysis of network data to improve the security or the performance [AGG+19] is not an exception with relevant advances in the past years. However, the usage of data is not exempt of issues, with the privacy of the final users (and the confidentiality of company data) on the focus when data should be shared among different partners.

Moreover, delivering a decentralized, blockchain-based platform that supports network slicing transactions via Smart Contracts [LL19], targeting multi-tenant infrastructures for the first time is under study. In this platform, the MNO, MVNOs, and OTT vertical application owners form a Decentralized Autonomous Organization (DAO) which can dynamically negotiate Network Slice contracts, flexibly integrating large and small players without the need for a centralized, trusted entity. Smart Contracts facilitate (and automate) direct contracts among entities that can be dynamically renegotiated based on real-time supply and demand.

Finally, to improve the performance of current signature-based solutions for dealing with zero-day or evolving attacks, hardware accelerated solutions for a decentralized Threat Detection Engine [STG+19] and a centralized Threat Analysis Engine can be provided. ML-based threat detection, that has demonstrated an improved ability to extract complex non-linear relationships in attack data, will be leveraged for the design of Threat Detection Engine (TDE).

3.4.2 Security architectural components

Figure 13 shows the overall architecture, visualising the applicable security and privacy components in all areas, and highlighting the specific 6G security technology enablers introduced in [HEX-D12], further discussed in this section. While the focus lies on the technology enablers as new architectural components, a holistic 6G security architecture must also comprise today's well-proven security mechanisms, as far as they are still relevant in 6G. We briefly summarise them in the following figure, without aspiration of exhaustiveness and depth of detail.

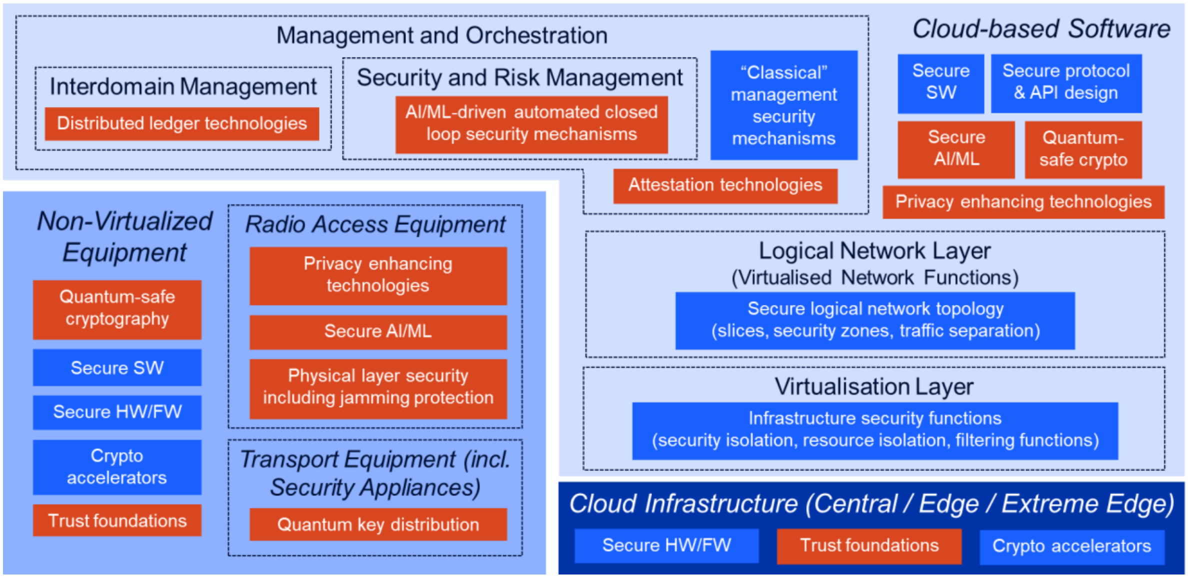

Figure 13: Overview of the essential 6G security architectural components [HEX-D13]

Figure 13 distinguishes among non-virtualised equipment (for radio access and optical transport), the cloud infrastructure, and the software running on it, including the virtualisation layer, the logical network layer, and the management and orchestration functions, including security and risk management and interdomain management. In each part, the figure shows the most relevant security and privacy building blocks or architectural components, with the new 6G security technology enablers highlighted in red, and the more traditional building blocks like for example "Secure SW" in blue.

Many building blocks apply to multiple areas, e.g., "Secure SW" applies to the non-virtualised radio and optical equipment (as far as this equipment comprises software), to the virtualisation layer and to all the software running on it, including management and orchestration functions. As another example, "Trust foundations" apply to all hardware, i.e., the radio and optical equipment as well as the cloud infrastructure. On the other hand, some building blocks appear at dedicated places only, like "Distributed ledger technologies" appearing at interdomain management only, but this does not preclude the potential applicability of the building block in other areas. Also, when a building block appears in an area, this does not imply that the building block is always applicable. For example, certain non-virtualised radio access equipment may not have access to sensitive data, so no privacy enhancing technologies may be required here. As another example, obviously not all transport equipment is required to support quantum key distribution.

The traditional security building blocks may be mostly self-explaining, but note the following:

- "Secure SW" refers to software with a low (close to zero) degree of vulnerability. "Secure HW/FW" has the same meaning for hardware or firmware. An example is the robustness of a processor against leaking information between different processes running on this processor in a (quasi-) parallel manner.
- "Secure protocol and API design" refers to robustness not only against external attackers (which is typically achieved by the use of cryptography), but also against erroneous or malicious behaviour of authorised peers.
- "Classical" management security mechanisms" comprise well established mechanisms such as access control, role-based access, secure logging, isolation of management functions/traffic from all other traffic, etc.

3.5 Versatile radio access network

Network densification (i.e., increasing the number of base stations per unit of space) is one of the main techniques that resulted in improving spectral capacity in 4G and 5G cellular networks [SLL17]. The drawback of this solution is equipment and site costs as well as potentially higher interference that negatively affects performance of cell-edge users [BS19]. Networks of next generations will have to deal with even higher density of infrastructure to provide the expected performance [RAB+20]. This requires re-thinking of the underlying architecture to eliminate the cell boundaries [NAY+17], [BS19].

For instance, in [RAB+20], [NAY+17], a Cell-Free (CF) massive MIMO network is designed, which refers to a network with densely deployed RUs cooperatively serving User Equipment units through coherent joint transmission and reception using the same time-frequency resources. Consequently, the concept of cells is eliminated, motivating the name.

Regarding the network architecture, the intention is to disaggregate the traditional CPU in multiple DUs, in line with 3GPP's 5G architecture [38.401] and propose novel solutions based on fully distributed (aligned with O-RAN Alliance specifications [ORAN4]), data-driven processing and local coordination. The disaggregation is vital for creating scalable versions of cell-free architectures available in SoTA [IFL19], which will unlock the potential of deploying cell-free networking in future 6G networks with massive RU deployments.

Next, another important issue is cluster formation (selection of serving RUs). In contrast with available simplistic distance-based solutions [BAZ+20], it is important to dynamically allocate a sub-set (or cluster) of RUs to each UE based on i) the radio propagation environment; ii) quality of CSI estimates; iii) constraints introduced by computation requirements; iv) fronthaul links capacity, and v) user mobility. Going a step further, innovative ML algorithms could be adopted for optimal cluster formation focusing on real-time operation by using historic data coming from the network, as well as for advanced modulation schemes and/or channel estimation/equalization.

Finally, clustering RUs served by multiple DUs (in contrast to disjoint clusters in [IFL19]), could provide an inter-DU coordination algorithm for decoding the actual signal. Moreover, exploring inter-DU coordination requirements and their effect in the spectral efficiency performance, as well as dynamic adaptability of the coordination levels jointly addressing RU-DU and DU-DU coordination are some of the main research trends in the cell-free MIMO domain.

Extreme high data rate links will be required in some very high-performance applications anticipated in 6G. Mostly those are related to highly advanced on-line imaging including holographic communications as well as providing extreme data rates for high-capacity cells. In those cases, a throughput of 100 Gbit/s or even significantly higher can be required. This means bandwidths of several tens of GHz as anticipated in reports [HEX-D21] and [HEX-D22]. The architecture design, in particular the infrastructure layer, needs to ensure that such data rates can be brought to local small-scale base stations that will serve end-users. From network architecture point of view, this is not only implementing optical, or wireless backhaul connectivity with low latency, but it means a backplane that can support data rates of hundreds of Gbit/s on large scale. This is an expanded requirement for new use cases in 6G.

3.5.1 Distributed massive MIMO

Distributed massive MIMO (D-MIMO) [HEX-D21] [HEX-D22] is a promising technology to address challenges in dense deployments at both low (cmW, lower mmW) and high (upper mmW and (sub-)THz) carrier frequencies. D-MIMO has the potential to

- allow for further densification of Access Points (APs) for increased and consistent area capacity.
- mitigate unreliable links due to shadowing/blockage thanks to macro diversity.
- achieve sufficient link margin despite output power limitations and high pathloss at upper mmW and (sub-)THz frequencies.
- allow for lowering Effective Isotropic Radiated Power (EIRP), simplifying deployment.

As illustrated in Figure 14, D-MIMO UEs can be served by several APs that are controlled by one or several Central Processing Units (CPUs) via fibre-optic or wireless backhaul/fronthaul links.

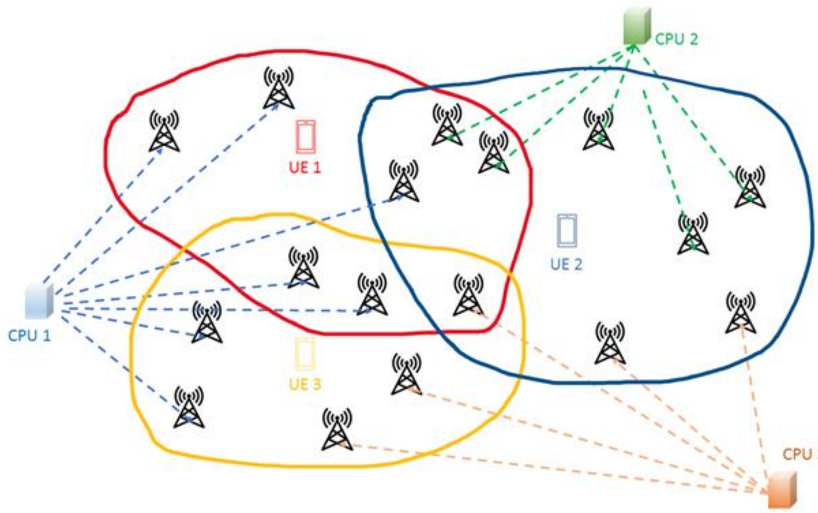

Figure 14 Illustration of distributed massive MIMO [HEX-D22]

Wireless backhaul/fronthaul links can be implemented using dedicated frequency bands or using the same bands as for access, so-called Integrated Access Backhaul (IAB). As such, D-MIMO systems can implement various levels of cooperative MIMO systems ranging from Distributed Antenna Systems

(DAS) to Joint Transmission Coordinated Multi-Point (JT-CoMP), [HEX-D22]. When APs can perform channel estimation and distributed precoding locally, D-MIMO constitutes a scalable way to implement the network MIMO concept using distributed massive MIMO, also denoted as cell-free massive MIMO, [IFL19].

There is basic support available for the implementation of D-MIMO in 3GPP 5G standards (e.g., related to multi-TRP support). However, there are major gaps between theory and practical solutions on real-world deployment of D-MIMO, related to architecture and functional split between CPU(s) and APs, fronthaul/backhaul solutions, scalability, and efficient precoding techniques. Key conclusions from the studies so far is that there are substantially different challenges and opportunities for D-MIMO at lower and upper frequency bands, calling for a scalable approach based on digital and analog solutions. That work also emphasises the need for efficient backhaul/fronthaul by integrating fibre and in-band wireless solutions. Since densification is the key enabler to meet coverage and reliability targets at the higher frequency bands and as it seems there is sufficient spectrum available, low-cost solutions are more important than spectral efficiency (at least in the early roll-out phases) [HEX-D22]. This calls for decentralised solutions at the higher frequency bands. In the lower frequency bands, the need for higher spectral efficiency calls for less distributed more digital approaches for better resource utilisation.

3.5.2 Cell-free mMIMO

A Cell-free (CF) network is a network with many distributed Access Points (APs) cooperatively serving User Equipment units (UEs) through coherent joint transmission and reception using the same time-frequency resources. Combined with the vision of Massive MIMO (mMIMO), distributing a high number of single or multiple antenna elements in a geographic area became popular as CF mMIMO, offering the potential to spectacularly outperform its cellular counterpart. In this context, a novel converged optical-wireless configuration based on the Cell-Free (CF) concept that targets flexible connectivity of a massive number of Radio Units (RUs) and aims to unlock the potential of CF mMIMO deployments in 6G networks.

For the CF mMIMO, the proposed radio network configuration is based on two radio access solutions. The first solution is based on the interconnection of multiple RUs with the DU via a bus configuration (upper right part of Figure 15). This approach aims at addressing the most pressing CF limitations, as well as dealing with the fact that the clustering literature only considers disjoint RU clusters, even when multiple Central Processing Unit (CPU) nodes are assumed; thus, this novel approach will allow CF mMIMO deployment in 6G networks, based on the utilization of dynamic cluster-formation algorithms.

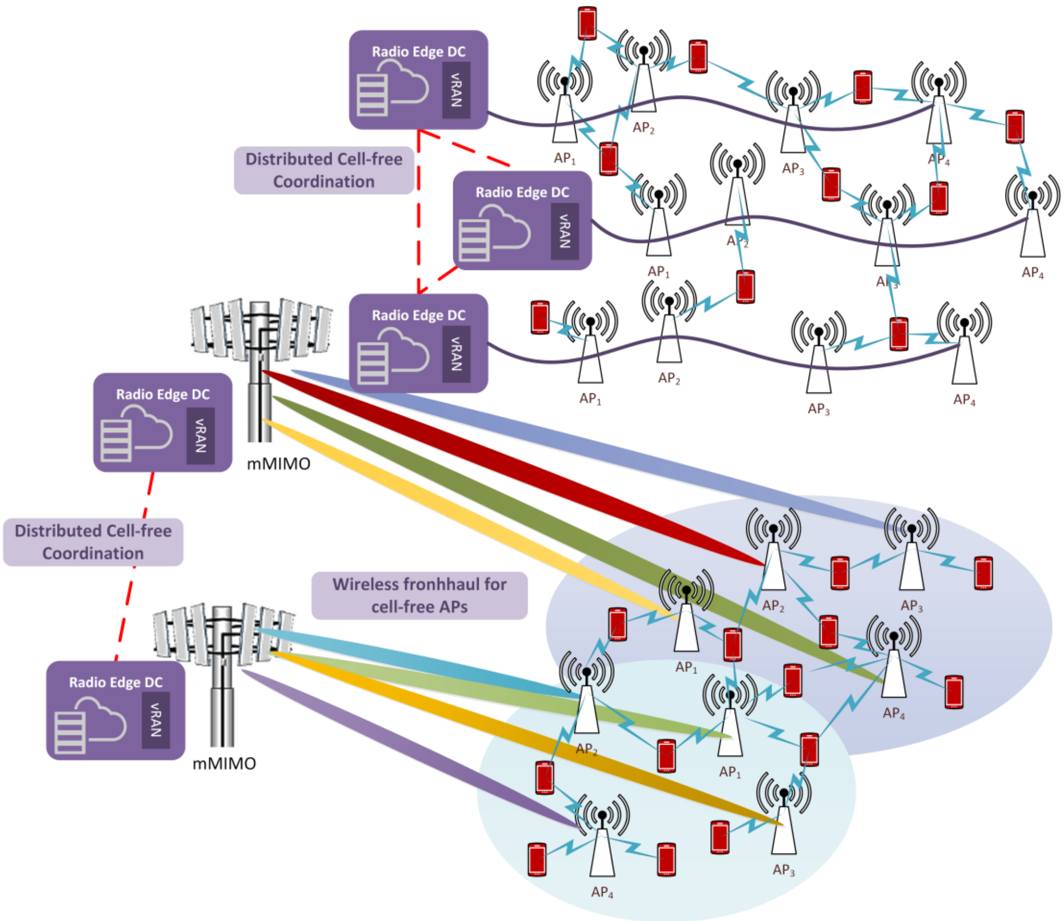

Figure 15: Illustration of Cell-free mMIMO.

The dynamic feature of such RU clustering algorithms is based on the CF mMIMO CPU fragmentation in multiple DUs, a procedure that triggers the support of distributed computation and coordination between RUs and between DUs. Under this networking configuration, clusters of RUs, connected to multiple DUs, jointly address inter-DU and RU-DU coordination for the first time, while also considering the introduced by fronthaul and midhaul constraints. The optimal cooperation levels between RUs and DUs and between DUs can be guaranteed through the application of dynamic adaptability algorithms of the involved entities' coordination levels.

3.5.2.1 Impact on E2E architecture

Related to the 6G architectural principles described in Chapter 2, D-MIMO puts requirements in particular on

Extensibility and flexibility

D-MIMO systems can contribute to 6G systems being able to adapt to various scenarios. In particular, D-MIMO can implement a service to actively shape the propagation environment (cf. passive shaping using Reconfigurable Intelligent Surfaces (RIS)) for rank and multipath control towards programmable propagation environments, which might be very beneficial in certain scenarios. D-MIMO systems can also implement support for services provided by other network functions such as channel sounding for localisation, RF environment mapping, and multi-static sensing (radar) services. Due to the dense deployment, energy efficiency in D-MIMO APs is important. To this end, dynamic activation of AP functionality with short delay should be supported. The delay requirement would be driven by the need of the use case versus the activation/deactivation efficiency gains in the APs.

On the other hand, as input to enable efficient beamforming, shadowing/blocking mitigation and, resource allocation in D-MIMO systems, various context and situational awareness information would be beneficial, such as location, mapping and, dynamic sensing information.

Scalability

One of the key challenges for D-MIMO systems is scalability. Important network architectural enablers would be frequency agility, i.e., support for high (upper mmW) as well as low (cm and mmW) carrier frequencies, and flexible roll-out aspects as described in the following.

In the network architecture, there should be support for heterogeneous nodes (APs, compute & sensing nodes) having specialised functional roles such as supporting low latency communications, uplink RF processing, downlink RF processing, baseband processing, sensing, etc. There should be support for APs having heterogeneous HW capabilities related to transmitting power, carrier frequencies, processing, etc., and also various functionality, e.g., within the control plane (system broadcast, initial access, etc.), and within the user plane (unicast, multicast, targeted flow KPIs, etc.). Furthermore, the network architecture should support a various degree of CPU-AP functional split, and AP cluster sizes.

Dynamic scalability would also be important, such as flexible dynamic use of AP resources, various degree of AP network control capabilities (e.g., broadcast, paging, random access) and UE idle modes (e.g., cell search, idle mode mobility). Various degrees of silence/sleep modes would be needed to maximise energy efficiency under service constraints. Support for pro-active resource allocation for highly mobile users and physical network slicing would further support dynamic scalability.

Resilience and availability

Multi connectivity and separation of CP and UP goes hand in hand with scalable D-MIMO systems. In particular, there should be support for joint multiband transmission/reception. In addition, management and orchestration functionality should operate on a sub-second time scale.

Separation of concerns of network functions

D-MIMO systems can offer capabilities for both communications and localisation and sensing services, and also benefit from localisation and sensing for optimising communications. Thus, a network architecture that supports separations of concerns with clear APIs is important. That would enable scalability, adaptability, support for heterogeneous communications and fusion of localisation and sensing information, and potentially also reuse of various training data (such as reference symbols).

Network simplification in comparison to previous generations

D-MIMO systems would benefit from an architecture that natively supports cloud-RAN.

3.6 Localization and Sensing

Localisation of User Equipment (UE) in mobile communication has been supported from the early stages of 3GPP. With 5G and its target use-cases, localisation is increasingly gaining importance [22.261]. 6G and its visionary scenarios continue this trend and look at localisation that is even more accurate and has even stricter latency requirements [HEX-D31]. Besides localisation, the technologies explored in next generation of mobile network open up the possibility of using mobile communication system itself for sensing. Sensing use cases address for example the detection of landmarks by the network as well as locating humans even though not carrying any device (e.g., UEs). Localisation and sensing can become an inherent feature in next-generation mobile communication, but to meet the challenging performance goals, it must be an integral part of the system architecture.

Industry 4.0 not only requires low-latency, low-jitter and high availability data transmission applications that include closed-loop control on one side and ultra-high data rate communication applications that include video or large sensor data traffic on the other side but also localization accuracy with a precision up to 1 mm that would be an essential enabler for opening up a lot of new applications.

5G localisation systems utilise Received Signal Strength (RSS), Time of Arrival (ToA) and Angle of Arrival (AoA) technologies with sub6GHz, mmWave and OWC for estimating position of User Equipment, whereas 6G Simultaneous Localisation and Mapping (SLAM) systems utilises OFDM, OTFS, OTFS-like or FMCW modulation with THz beam technologies to sense point cloud of its environment by identifying land marks for estimating position of User Equipment.

The localisation accuracy requirement for Automated Guided Vehicles (AGVs) and collaborative Drones is 1cm every 1 second, for Augmented Reality Headsets is 1mm every 100ms, for collaborating mobile robots (cobots) is 1mm with Cycle time of motion control function: 1 ms, synchronicity 10 ns, for motion, temperature and humidity etc. sensors is 10cm every 1 to 10 seconds, whilst all require the provision of localisation with 99.99% reliability [ART21].

In order to achieve these demanding requirements, 6G SLAM will be required that employs multiple access technologies, namely: sub-6GHz, mmWave, sub-THz for RSS, time difference of arrival (TDoA), and angle of arrival (AoA) localisation; combined with sub-6GHz sensing to produce a point cloud for producing a digital twin for updating digital twin for obtaining location from environment landmarks. A Multiaccess Edge Computing cloud is required for producing location with the reliability from all these technologies using Artificial Intelligence / Machine Learning (AI/ML) [COS22].

RadioWeaves technology is being developed to support wireless connectivity for providing ‘real-time’ and ‘real-space’ functionality distributed access architectures. It is a distributed architecture hosting a very large number of antennas offer hyper-diversity that can be exploited well to extract both accurate and precise position information [REI-D11].

Accessing accurate Mobile User (MU) localization measurements using multiple technologies with different measurement sampling times requires the aid of synchronization signals, i.e., time-stamps. A DNN-assisted PF-based (DePF) joint synchronization and localization algorithm, which draws on the CIR to estimate the AoA (using MUSIC algorithm) and to determine the link condition, i.e., LoS or NLoS, using a pre-trained Deep Neural Network (DNN), thereby excluding the erroneous measurements to enable a more precise parameter estimation is developed. It then estimates the joint probability distribution of MU’s clock and position parameters using the Particle Gaussian Mixture (PGM) filter. The dimension of the PGM filter is then reduced by revealing and exploiting the existing linear sub-structures in the measurements, thereby tackling the dimensionality problem [ORD21].

Joint communication and sensing, also known as integrated sensing and communication (ISAC) will be one of the main differentiators of the 6G vision with respect to 5G communication systems. Sensing not only includes positioning but also encompass other novel functionalities that were not present in 5G, such as radar type sensing and non-radar type sensing using communication technologies, which in turn leads to new services such as Sensing as a Service, Landscape Sensing etc. [HEX-D32].

Highly accurate localisation of UEs (Figure 16), as well as highly accurate localisation of assets (Figure 16: B), are examples scenarios. Totally new scenarios that are expected are radar-like sensing scenarios where next-generation mobile communication devices can detect and track objects or humans that do not carry any device (Figure 16: C), and even gesture detection of humans without UEs is conceivable. The double-coloured radio waves in Figure 16 depict the combination of communication and sensing (overlap between blue and purple area): *joint radar, communication, computation, localisation, and sensing (JRC2LS)*. Certainly, pure communication or pure sensing/localisation scenarios must be made possible in the future as well, depending on the application requirements.

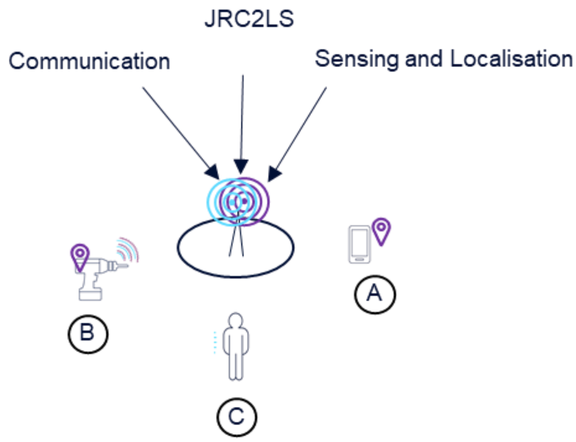

Figure 16 Examples of localisation and sensing scenarios (A: UE localisation, B: asset localisation and C: Detection of assets and humans without UEs via sensing) [HEX-D1.3]

Flexible switching and prioritisation between pure communication, pure sensing/localisation, and a combined JRC2LS service capability should be considered in next generation mobile communication E2E architecture. Note that all three cases are envisioned to share the same hardware.

In the future, localisation and sensing should be designed as base functions or microservices. Accessing information from localisation and sensing services should be possible at different processing stages (e.g., raw sensing data as well as readily calculated position information) via the **exposure framework**. Interfaces for localisation services will need to be extended, e.g., from 3D to 6D (3D position + additional 3D orientation) and, totally new services, protocols and interfaces must be developed for sensing features.

Depending on the (access) rights of service consumers, access to information shall be possible or prohibited. Position and sensing data often are very sensitive data as they can easily be linked to personal information or business/trade secrets which must be protected from misuse. In industrial scenarios, this might even mean that such kind of data must never leave the factory. Localisation and sensing information will be also generated by the mobile communication network**. Securing this information** will be a very important architectural design requirement as the mobile network is not only passing information from application to application through the network but generating sensing information itself. This generated localisation and sensing information must be correct and trustworthy. In order to ensure having a fast and efficient way of exchanging information and resources, the attention has turned towards a new approach to the decentralised framework. Such a framework is the blockchain platform, which can be used in several domains (e.g., network slicing, industrial IoT networks, etc.).

Low latency, which is understood as a short duration between the initialisation of sensing/localisation procedure and acquiring a localisation/sensing estimate, is also a challenge for the E2E architecture. But in general, service consumers must be able to describe applications' functional and non-functional localisation and sensing requirements like latency or reliability towards next generation mobile communication services and must be able to rely on these agreed quality parameters. These parameters are not necessarily static and might change over time which requires **flexible Quality of Service contracts.**

3.7 Programmable networks

While programmability has been a feature of network devices for a long time, the past decade has seen significant enhancement of programming capability for NFs spearheaded by the SDN paradigm as well as the ongoing trend towards softwarization and cloudification. On the one hand, there are now many more APIs and standardized programming interfaces towards NFs than ever before. This allows 3rd party developers to interact with the network in new ways. On the other hand, the capability to program is no longer confined to the CP software but has been introduced into (hardware) data planes as well using Smart Network Interface Cards (SmartNICs) and switches. A key candidate technology for this is P4 domain-specific language and the functional abstractions [BDG+14]. The reusability and flexibility through programmability is of particular importance at edge and extreme-edge locations where deployments have a limited footprint (i.e., subject to limited hardware types and models) and therefore need to be flexible to support a wide range of functions and use cases with diverse performance requirements. For 6G, this trend is expected to continue and even accelerate. However, many open questions remain as competing concepts exist, and actual deployments are mostly limited to trials. Therefore, key research areas in this space include:

- The right structure and level of i) infrastructure abstraction, ii) connectivity specialisation and ii) network enablers engagement, for application developers, especially when direct hardware access is currently the norm.
- Operational practicalities of rolling out functional changes of networking devices (not just configuration) automatically in the field in alignment with CI/CD pipeline methodology.
- Performance and security implications of non-integrated programmable NFs with a larger attack surface due to the exposure of more functionalities via APIs.

3.7.1 Enabling network programmability

With the advent of B5G/6G networks, the number of UEs will be massive in scale, especially if we consider the devices at the extreme-edge domain. In general terms, it is expected a full digitalization of the real world, which translates in a vast amount of data that must be processed. In this context, new design principles and technology enablers have been introduced. They reside i) at service/application provisioning level, ii) at network and resource management level, as well as iii) at network deployment and connectivity level.

At the service/application provisioning level, the exposure of APIs from network core and edge creates new opportunities to third parties for interaction with the network. The work of 3GPP SA6 towards vertical application enablers (VAEs) is a representative paradigm in this field. At the network and management level, there are disruptive changes at any domain of the service provisioning change. Key enablers can be considered the adoption of the cloud-native approach from the CSPs (communication service providers) as well as the recent work from Open RAN alliance towards vendor-agnostic management of radio access components. Finally, at the network deployment and connectivity level (including embedded edge compute capabilities exposed to 3rd party), the deployment of private networks is well specified already, while the concepts of cell-free paradigm and the provisioning of a connectivity mesh topology to end devices are expected to support the vision of a truly flexible access network. In this context, disruptive architectural and service concepts emerge, anticipating multi-connectivity structures (multiple coordinated point-2-point connections), potentially including edge compute and 3rd party service function chains. The service abstractions, programmability features, and an entirely new application to network interaction and negotiation set of capabilities must evolve and be developed accordingly.

The result of the above mentioned continues evolution is expected to be a total transformation of the conventional mobile networks to open service provisioning platforms. The cornerstone of this transformation is the definition of common interfaces and reference points that enable interaction of third parties with the network functions and nodes at each one of the above-mentioned levels. Indeed, already native APIs and interfaces have been standardized for enabling interaction at any level. For instance, 3GPP has defined the service-based architecture (SBA) as a set of functional components, known as interconnected Network Functions (NFs), where each one can use standardized interfaces, or Service-Based Interfaces (SBIs), to access and consume services of other NFs through an API-based internal communication. Already in 5G, critical role is played by the Network Exposure Function (NEF), which provides APIs to third parties enabling an indirect connection with any NF of the SBA. Other native interfaces can be considered the Multi-access Edge Computing (MEC) APIs, APIs that are provided management and orchestration entities, or RAN interfaces[1].

The realization of such interaction is facilitated through various types of interaction-enabling frameworks that on their southbound can securely consume native APIs and access network nodes (e.g., switches, gNBs, and NF of network core) for onboarding new applications or enforcing new policies; while on their northbound they can expose vertical-oriented services to support any kind of network-aware application and services (see Figure 17). Those frameworks shall take advantage of programming languages, such as the protocol-independent packet processors - P4 [P4+14] for data plane programming, as well as common data models, such as the OPC UA information models[2] which refer to vertical specific companion specifications for the industrial/manufacturing nodes.

Overall, the implementation of such frameworks that exploit common/standardized languages, APIs, and data models provides the means for the enforcement of **Programmability** in the next generation networks, a concept that incorporates the capability of a device or a network to accept a new set of instructions that may alter the device or network behaviour [FI+15].

From the business perspective, the above-mentioned Programmability frameworks creates a new business potential around the development of the so-called Network Applications. The Network Applications (or Network Apps) are third party application that interact (through standardized APIs) with the network to provide network or vertical oriented services. Network applications provide network- or vertical- oriented services, meaning that they can assist/enhance either the network operation/management[3] or the vertical application[4]. As third-party apps, the Network Apps should interact with network functions/nodes though open and standardized interfaces/APIs that can reside at any plane (user, control, management) or any domain (core, radio, transport).

[1] In the case of interfacing with RAN nodes, the architecture of Open RAN alliance, includes RAN Intelligent Controller (RIC) where applications developed by third party specialist software providers.

[2] https://opcfoundation.org/developer-tools/specifications-opc-ua-information-models

[3] For instance, in the EVOLVED-5G project a related contribution to 3GPP SA6 work has emerged (3GPP/TSG SA2/eNA_Ph2 Rel.17: Contribution "Support of DN performance analytics by NWDAF" - S2-2101388) under the scope of extending the NWDAF analytics APIs so that network applications can retrieve data from vertical apps, and the NWDAF build performance analytics & predictions by using inputs from network applications.

[4] The ICT-41 projects (5GPPP, phase 3, part 6 projects), work towards providing network applications that fulfil needs and requests from various vertical industries, e.g., automotive (5GIANA, 5GASP), Industry 4.0/manufacturing (5GINDUCE, EVOLVED5G, 5GERA), transport & logistics (VITAL5G, 5GERA), media (5GMediaHub), public protection and disaster relief (5G-EPICENTRE, 5GERA, 5GGASP), healthcare (5GERA).

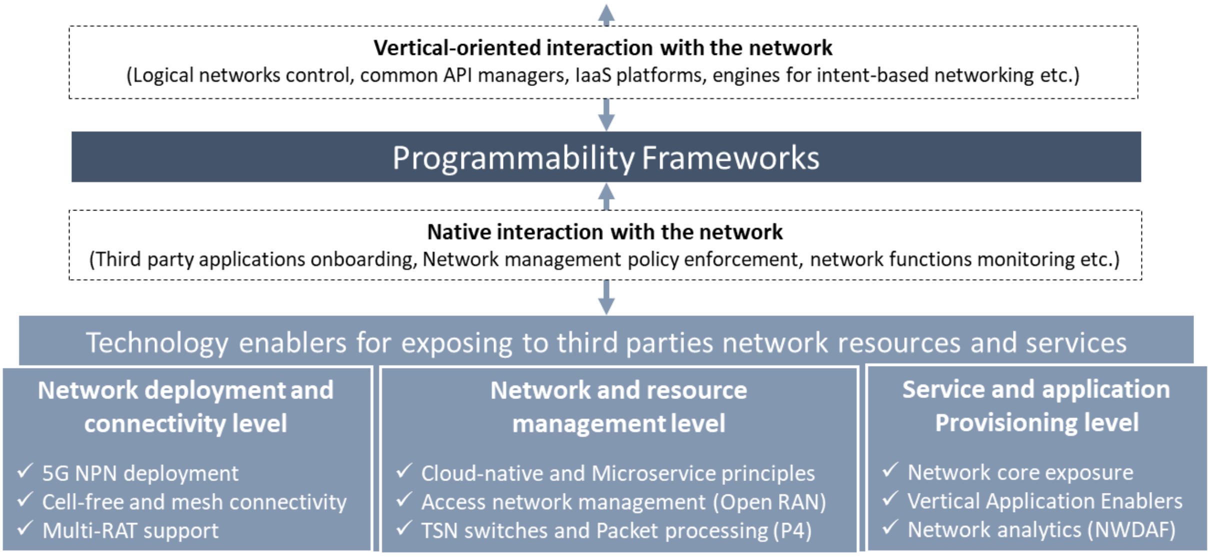

Figure 17 Programmability frameworks take advantage of various technology advancements and enable a rich interaction of verticals with their underlay network, capable to support the network programmability concept.

To better clarify the role of the programmability frameworks in the path towards network programmability, some representative examples are further discussed below.

- **3GPP CAPIF as a secure and interoperable API manager.**

  API-based interaction of third parties with the network is needed for the support of openness at deployment, management and application levels. In this context, the development of a Common API framework (CAPIF)[5] has been coined in 3GPP as an effort to avoid duplication and inconsistency between the various existing API specifications. From the market perspective the need for such management framework is well recognized, while the CAPIF implementation has already emerge [SCT+22].

- **ETSI TerraFlow SDN controller for providing logical networks as a service.**

  The Logical Networks as a Service (LNaaS) concept and service model will become far more extensive, flexible and pervasive as compared with 5G. While 5G is basically offering advanced connectivity service with support of QoS from the UE / Device to a Data Network (identified by a Data Network Name), with 6G we expect that a richer topology of connectivity can be supported, controlled and managed as a service, as an effort to support good or better customer / user experience, while achieving improved overall resource utilization and network performance. ETSI TeraFlow SDN controller[6] is targeted to enable and facilitate LNaaS to (vertical) enterprise customers (VEC) as well as operator internal and inter-NSP connectivity and networking.

- **ETSI VNF Os-Ma-nfvo Reference Point for enabling intent-based networking.**

  OSM provides a unified interface based on NFV SOL005 specifications, which will allow OSS/BSS to control the full operation of Network Services and Network Slices. This interface

[5] https://www.etsi.org/deliver/etsi_ts/123200_123299/123222/17.05.00_60/ts_123222v170500p.pdf

[6] https://www.etsi.org/newsroom/press-releases/2076-2022-05-etsi-launches-a-new-open-source-group-teraflowsdn

can be exploited for creating "intent engines", which acting as an OSS/BSS can leverage AI/ML algorithms to automate service management depending on the end users' intent.

- **O-RAN compliant FlexRIC SDK for enabling E2E programmable data paths.**

  The Flexible RAN Intelligent Controller (FlexRIC) [SIN21] represents a software-defined RAN controller, built through a server library, controller-internal Applications, and optionally a communication interface, all offered by the FlexRIC SDK. The FlexRIC, combined with other software solutions based on Traffic Control (TC), Open vSwitch (OVS) etc. can offer cost-efficient programmable data path capabilities in the kernel of the system, while Smart Network Interface Cards (SmartNICs) such as NetFPGA and Netronome can provide performance boost benefiting from hardware acceleration.

- **P4-based framework for managing programmable Networks**

  Forwarding management and performance monitoring is critical when using programmable networks. This can be achieved using models that can predict the packet forwarding latency when running arbitrary P4 programs on any P4 device as it has been introduced in [P4Cloud+21] [P4-P8+21]. This model makes use of an extensive measurement campaign that identifies the base processing delay of different P4 devices, as well as the marginal delay of executing atomic P4 operations on these devices. Also, to satisfy the requirement of predictable or even deterministic performance, in particular packet processing latency, it is vital to evaluate and model different components of a P4 program, i.e., constructs, on different platforms.

3.7.2 Programmability of UEs

Overall, a programmable network must enable dynamic changes in devices, functionalities, and parameters to be implemented fast, regardless the number of devices. Scalability and sustainability will drive the design of the 6G, while network programmability will stand as a key piece. Network programmability is expected to cover all available resources from extreme edge to CN, enabling a continuum management. It is expected that new types of softwarized functions will rise within the management, user, and data plane. To extend network programmability from the applications layer down to the network functions and to the data plane it will be necessary to expose new APIs on the wireless devices even to the air interface customisation purposes. One step further, the programmability at UE (user equipment) is also essential towards programmable networks.

In the context of UE programmability, the air interface protocols have evolved to be highly configurable with many features for various purposes. However, introducing new features that have an impact on the air interface protocols is time-consuming, as changes should be applied to both UE and gNB via tedious standardization process to achieve consensus between operators, network and device vendors who may all have different priorities. This limitation is even more pressing in dedicated networks, where enterprises call for an integrated networking solution for their operation.

One the one hand, UE programmability may be an enabler to help realise the vision of "fit for purpose" promise of dedicated networks for both legacy and upcoming use cases in 6G. For a truly adaptable network able to introduce new changes, a programmable UE is required in dedicated networks enabling faster time to market, faster innovation, and support of verticals to name just a few. On the other hand, UE programmability will also require improvements in network control.

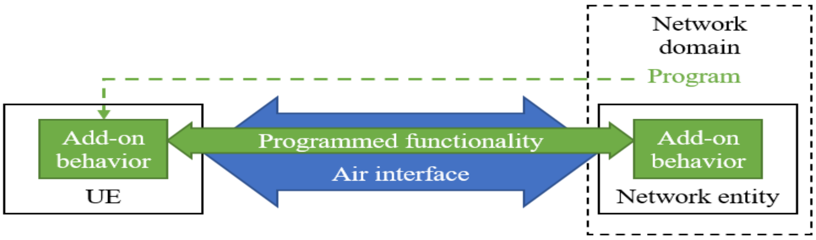

Figure 18 Network and UE programmability [HEX-D13]

Overall, the scope of UE programmability (see Figure 18) should be defined with respect to what is intended to accomplish, with it, which is a research question, to strike a balance between pragmatism and vision which functionality is programmable, and by which means considering the needs and requirements from multiple parties.

3.8 Management and Orchestration

Services Management and Orchestration (M&O) issues the deployment and operation of the network services supplied through the MNO to their customers, preserving all of the contractual aspects associated to those services. It addresses the provision/cessation of services, Quality of Service (QoS)/Quality of Experience (QoE) fulfilment, or fault reporting, among others. In previous generations of the mobile communications systems, the MNO customers have been mainly individuals consuming voice and messaging services. However, the market situation is much more complex now, including new data services and corporate customers, such as vertical industries, digital operators, hyper-scalers, or large-scale content providers, among others. It is anticipated that this trend, in terms of heterogeneity of stakeholders and provided services, could continue and even growth within the coming years.

Common examples of services M&O processes include network services (NS) onboarding, growing/reducing their capacity (scaling), updating their configuration, or processing their termination in an orderly manner. Considering the increased complexity regarding the involved stakeholders and provided services, it is envisaged that in future 6G networks these tasks need to be performed relying on a high diversity of available infrastructure resources, i.e., considering not only the MNO own resources at the core and edge networks, but also other third-party resources in different technical and administrative domains (e.g., extreme-edge resources, or other private or even public cloud resources). In this complex and heterogeneous scenario, the requirements for the services M&O systems increase, asking for higher degree of automation and E2E integration, allowing the deployment and operation of services across a wide variety of network elements which could be distributed on multiple network domains.

To cope with this complexity, it is needed to enable the services M&O systems with the required capabilities to provide the necessary orchestration resources. Specifically, the following main capabilities have been identified for the future 6G M&O systems:

The adoption of the cloud-native principles also in the M&O system. This would be aligned with the E2E architectural concepts in Section 2.2, but from the M&O perspective it would involve three main aspects: (i) the priority on using micro-services, i.e., light-weight self-contained, independent, and reusable components from different suppliers, (ii) the implementation of the *service mesh* concept, regarding the communication among the network components, and (iii) the enabling mechanisms for the NSs to be deployed/updated using "continuous" DevOps-like practices, e.g., implementing continuous integration/delivery (CI/CD) workflows with a high automation degree.

Unified orchestration across the "extreme-edge, edge, core" continuum. Extreme-edge devices (i.e., those beyond the RAN) are taken into consideration not only to collect data from them, but also as an additional set of infrastructure resources for the services deployment. However, the nature of those extreme-edge pool of resources might also require adopting new M&O mechanisms able to address their very specific constraints (e.g., restricted processing/storage resources, asynchronous behaviour in terms of connection/disconnection, error proneness, mobility patterns, etc.).

Unified management and orchestration across multiple domains that could be owned/administered by multiple stakeholders and featured with heterogeneous technology resources. This entails the definition of converging interfaces, the mechanisms to dynamically check and expose the different resources and capabilities from each domain, and the access control procedures for consuming the various primitives and services.

Increased degree of automation to strongly reduce manual interventions regarding the functionalities of service and network planning, design, provisioning, optimisation, and operation/control, leveraging closed-loop and zero-touch responses. The M&O system need to be able to identify, detect or predict potential issues, triggering also automatic reactions. This may be enabled via the programmability of the necessary network resources (see Sec. 3.7).

Adoption of data-driven and AI/ML techniques in the M&O system. AI/ML techniques could cover numerous optimization aspects and lifecycle actions concerning the services M&O, including resource allocation and slice sharing at provisioning time, service composition, scaling, migration, re-configuration, and re-optimization of network services, among others. AI/ML techniques can also be applied on the operational scope (AIOps), and the specific techniques to automatically develop and deploy AI/ML models (MLOps).

Intent-based approaches for service planning and definition. In order to help with the extended complexity, the M&O system would implement automated mechanisms for translating service specifications and commands based on high-level intents, which might be expressed even in natural language (e.g., relying on AI/ML techniques).

To meet these main challenges, the M&O system is seen as a common functionality impacting all layers of the E2E architecture: from the infrastructure up to the applications (blue block at the left-hand side in Figure 2 – High-level view of the 6G architecture). In this regard, in the context of the Hexa-X project, an initial high-level M&O architectural design for the future 6G networks has been produced. This architectural design takes the previous 5G Architectural View from the 5G-PPP Architecture Working Group as a baseline [5gp21][HEX-D62]. Figure 19 represents the structural view of this architecture, with the main building blocks grouped in different layers.

As a whole, what the Figure 19 represents is that NSs and slices at the Service Layer (top) are of course executed on the network elements (physical or virtual) at the Infrastructure Layer (bottom), being "made of" the network functions at the Network Layer (middle). All those elements (network functions, services and slices) are designed and provided from the Design Layer (right). This architectural view is clearly inspired by the 5G baseline architecture in [5gp21], representing an evolutionary step based on it; however, it also includes the following innovations:

Aligned with the OSI management protocol [9595:98] [9596-1:98], there is a clear separation between *M&O resources* (i.e., those in charge of managing, represented within the blue dashed line in Figure 19 – right hand) and the *managed resources* (i.e., what is managed, e.g., network slices or NFs, represented at the left-hand side), which can be commissioned, operated and de-commissioned. *M&O resources* will provide the management capabilities (e.g., provisioning, monitoring, service assurance, etc.) to act on the *managed resources*. A new layer, named as the *Design Layer*, has been included to represent the M&O-related operations involving third-party software providers. This is intended to introduce the well-known DevOps-like practices (e.g., CI/CD) in the telco-grade environment. Also, hyperscalers, private networks, and the extreme-edge domain have been explicitly included as part of the Infrastructure Layer. New control loops have been included: (i) The "DevOps Control Loop", representing the automated continuous iterations (e.g., CI/CD) between the MNO scope (grey colour) and the external Design Layer (light blue colour), and (ii), the "Infrastructure Control Loop", meant to automate the infrastructure discovery processes and the related monitoring methods targeting the extreme-edge assets integration (which can be potentially asynchronous in terms of connection/disconnection of devices, so requiring special processes for their management). As in the baseline architecture in [5gp21], Network Functions are associated in different groups at the Network Layer (e.g., Radio Access Functions, Core Network Functions, M&O Functions, AI/ML Functions, etc.). However, following the cloud-native practices, these functions would be primarily implemented through Containerised NFs (CNFs), although also through Virtualised NFs (VNFs), Physical NFs (PNFs), or other NFs implementation technologies (e.g., to ensure backward compatibility). It should be noticed here that, although some functions work only as managed resources (e.g., CN functions or third-party functions), other are specific M&O resources (e.g., the Monitoring Functions or the Management Functions themselves); however, other functions are *hybrid*: they can support M&O resources (e.g., certain security-related or AI/ML functions) or work as *pure* managed resources (e.g., certain AI as a Service –AIaaS– functions or security functions not in the M&O scope). Functions in the Network Layer are generic, i.e., instead of referring specific functions (e.g., CSMF, MRF, NFVO, etc.) as in [5gp21], just generic blocks are provided. This is intentional, in order to consider the new functions that would be probably defined for the future 6G stack. A new set of AI/ML collaborative components have been distributed across the network covering both: managing and managed scopes. M&O functions can be instantiated in the three different layers (service, infrastructure and network layers), including also specific security-related functions. Finally, and also aligned with the cloud-native approach, a new cross-layer Application Programming Interface (API) Management Exposure block has been included to communicate the different network elements in the different network layers. In short, it mimics the behaviour of the Zero-Touch Service Management (ZSM) *cross-domain integration fabric* [zsm-002], enabling the so-called *capabilities exposure* [5GVIN-D31] of the network of elements in the various architectural layers. It makes possible communicating the various M&O resources within and between administrative domains, although it could be applied more broadly to represent potential federated interactions.

Even considering those innovations, this Hexa-X M&O architecture is considered an evolution built on the same overall principles as the preceding 5G architecture in [5gp21]. One of these most remarkable common principles is the adoption of the Service Based Management Architecture (SBMA) model, already in [28.533] and [zsm-002]. It is considered this model still represents a paradigm shift in the telco stack design, based on shifting from conventional network/service management systems (hard-to-evolve, and with siloed managers connected with point-to-point protocol interfaces) to a cloud-native management system (built out of modular composable management services which might be offered for consumption using HTTP-based RESTful APIs). Based on this SBMA model, it will be feasible to have a collection of management services, each representing a specific management capability and allowing manipulating particular resources (e.g., network slices, CN functions, etc.).

Following the SBMA model, those M&O resources are envisaged as a set of management services, each representing a specific management capability (e.g., provisioning, monitoring, performance assurance, etc.) that allows manipulating the managed resources. Those management services are expected to be produced and consumed through management functions, which might be mappable to vendor "out-of-the-box" solutions. Depending on their scope, management functions can be grouped into two main sets, refereed as *Primary Management Functions* and *Complementary Management Functions*, which are described below.

Primary Management Functions

Pictured as the "Management Functions" box in Figure 19, they represent the collection of Management Functions offering what are considered the basic management capabilities, which are already well-known in the state-of-the-art M&O systems, namely:

Fulfilment capabilities. Those capabilities permitting provisioning instances of managed resources. Following the SBMA model, any provisioning operation over a selected Hexa-X managed resource may be implemented as a CRUD (Create, Read, Update, Delete) primitive over the managed resource. Query parameters are also envisaged to offer advanced features like scoping and filtering multiple resources, or attribute selection [Nok20a].

Assurance capabilities. Those enabling MNOs to constantly monitor and predict probable issues in the network, ensuring services are free of faults (service problem management) and meet the expected behaviour (service quality management). Unlike fulfilment capabilities, which are generally achieved per-request, assurance continues executing in closed-loops. Envisaged management services for assurance in the Hexa-X M&O system may also include performance management systems, fault management services, analytics services, or closed-loop management services, among others.

Artifact management capabilities. Artifacts refer to the set of assets providing operators with assistance in their fulfilment and assurance activities. For their management, MNOs depend upon catalogues and inventories. Catalogues keep the descriptors/templates and software building blocks based on which managed resource instances are created and operated. Of course, since complexity grows as the number of catalogues increases (considering also the ones that would come from specific vendors) Hexa-X recognizes the trouble of getting such a number of catalogues and agrees on the need to find alternative techniques for dealing with them (e.g., the catalogue federation approach). The goal is of course to simplify the catalogues management, addressing one of the main pain points faced in 5G: the need to synchronize catalogues, each keeping up-to-date copies of the Management Information Base (MIBs).

All these management capabilities (fulfilment, assurance and artifact management) are applicable to all managed resources, including those at the infrastructure layer, network layer and service layer resources. This could be achieved by instantiating the necessary functions to provide functionality on each layer (grey M&O blocks in Figure 19).

Complementary Management Functions

As the name suggests, those functions supplement the primary M&O functions by providing additional functions, specifically AI/ML, Security and Monitoring Functions.

AI/ML functions. As it can be seen in Figure 19, the AI/ML Functions block is split into two by the M&O Scope blue dashed line, meaning that certain AI/ML functions could be specifically designed to assist the management functions, whilst others could be deployed for different purposes (e.g., to support other functions, such as RAN functions, CN functions or other third-party functions). As AI/ML functions, these functions are intended to offer the mechanisms to build out the knowledge and the intelligence to take decisions about the actions to be done on the different architectural layers.

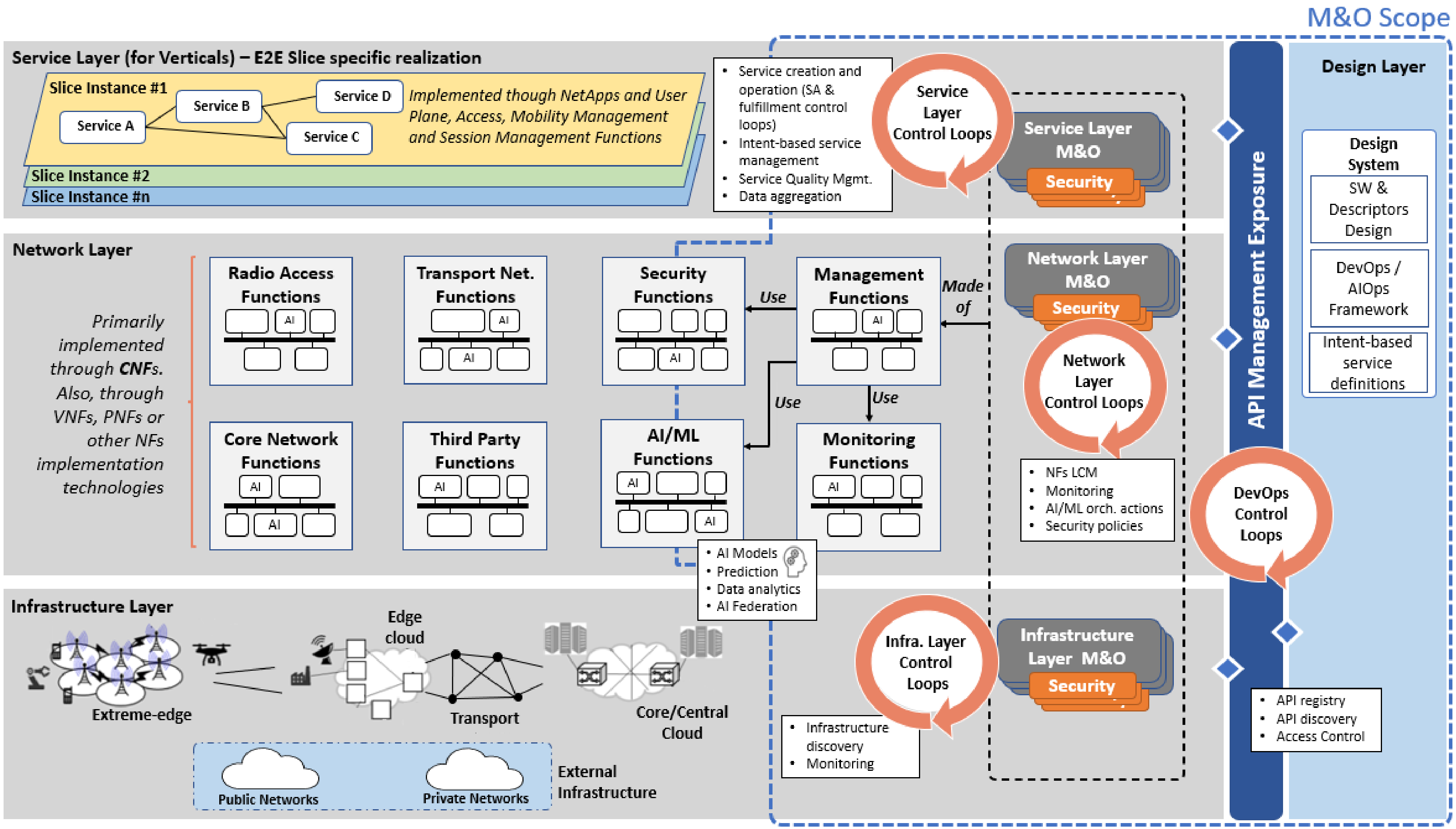

Figure 19: M&O System - Structural View [HEX-D62].

The main reason to use AI/ML capabilities withinside the M&O context is to cope with the complexity envisaged for the future 6G networks regarding the M&O processes themselves. For low-complexity algorithmic problems (i.e., problems requiring dealing with a small number of variables), conventional non-AI methods are generally enough: human programmers can generate algorithms to solve the proposed problem. However, high-complexity issues may require managing a huge number of variables that may be related in a non-obvious way. This could make ordinary algorithmic methods not suitable. For those cases, AI/ML strategies have demonstrated to be a valuable resource, as they provide self-learning capabilities able to manage lots of variables and being capable of extracting non-obvious relationships among them. Specifically for services M&O, the following sources of complexity are in scope:

- Time series: Time evolution of the multiple metrics measuring service KPIs or infrastructure utilization parameters may be processed as time series. AI/ML techniques have demonstrated good performance concerning times series processing [LIM21].
- The extreme-edge integration: As stated before, providing continuum device-edge-cloud management is one of the novel capabilities envisaged for the future 6G networks regarding M&O. To cope with this, integrating the extreme-edge domain is considered of great significance by itself, due to the high quantity and heterogeneity of devices in this environment. In this context, AI/ML may be used to process the large quantity of data coming from the various extreme-edge devices, and trigger orchestration actions based on that. AI/ML has also proven a good performance in this regard [LLF+21].
- Network Operations Management: Application of AI/ML strategies to this context is usually referred as AIOps [MH19][DLH19]. Connected to DevOps, it has to do with automating and enhancing activities within the operations teams by using AI/ML algorithms. Use case examples can be alarms filtering, incident analysis, or gathering and normalizing high volumes of data from operational tools, among others.

Intent-based networking, mainly oriented to non-skilled users, such as end-users or certain vertical customers, to allow them to deploy and set-up their services by simply declaring high-level intents, so preventing them from having to cope with complex lower-level configuration details. AI/ML functions could be used right here to guide the translation of these high-level intents (that might be even in natural language) into the corresponding low level orchestration actions [SZF+18][SZI21].

- More specific examples where AI/ML techniques could be applied in the context of M&O can be the following [5gaiml21]:
- Anomaly detection.
- Closed-loop automation (e.g., by using reinforcement learning techniques [YYY+19]).
- Forecasting network characteristics and events, focused to trigger proactive M&O actions (e.g., scaling, healing or NF migration actions).
- Forecasting security incidents.
- The NFs placement problem (a well-known NP-hard problem) [TCP91][JAS02].
- Autonomous service and slice management, control and orchestration.
- Data processing to support operational teams (e.g., for data validation, anonymisation, data filtering, or classification).

Also, as illustrated in Figure 19, besides the specific AI/ML Functions block described in the preceding paragraphs, there are also other specific AI/ML-related functions which can be distributed throughout the network to assist the M&O processes. They constitute the distributed AI/ML components that might be also managed from the AI/ML Functions block. These components are also described withinside the context of Hexa-X [HEX-D42]. Among other functionalities, they are meant to provide distributed AI/ML-related functionalities (e.g., by means of specific so-called AI-Agents for implementing federated learning techniques). Anyway, although distributed thru the network, dedicated M&O

functions are needed also to coordinate them. In this respect, the AI/ML Functions block will need to have dedicated M&O processes for those distributed AI/ML components.

In the Hexa-X M&O architecture all the AI/ML functions can cooperate and interact among them, and also with the primary M&O functions previously described, following the SBMA communication approach mentioned above. Moreover, they could interact with different sorts of M&O functions, e.g., by ingesting the monitoring information produced by the Monitoring Functions and triggering the Management Functions to trigger the appropriate M&O actions.

Monitoring functions, intended to provide information concerning the operational processes, in the form of trace files, alarms, KPI values, or usage parameters, amongst others. As depicted in Figure 19 Monitoring Functions may be utilized by the Management Functions, which can process the monitoring information to carry out M&O actions. Of course, Monitoring Functions have been already there in one way or another in M&O systems. The SotA telco-grade M&O platforms (e.g., [Osm22], [ONAP]) already offer monitoring capabilities. However, Monitoring Functions have been usually based on providing monitoring for a fixed set of metrics (e.g., CPU consumption, RAM utilization or certain network metrics, amongst others). Beyond this, one of the envisaged requirements for the Hexa-X M&O system [HEX-D62] is to be enabled with a more sophisticated monitoring system, capable to offer monitoring, telemetry, and the handling of data ingestion from all the network segments, permitting to combine data from infrastructure through data and control planes to applications. This calls for higher flexibility in the monitoring system, since it is no longer just about monitoring a fixed set of metrics: having to combine metrics from data and control planes makes it necessary to integrate custom metrics that could be freely defined by verticals or NS suppliers, on the grounds that they are who better understand what metrics may actually be the most relevant for their services. Application-based monitoring makes it possible to carry out more advanced M&O actions in vertical services. But beyond the Monitoring Functions themselves, this means outlining well-designed semantic data aggregators in charge of registering data sources and data consumers formats, data aggregation rules, etc., i.e., a data fabric to manage the pipeline from data collection to data consumption. This will permit the data interchange considering those data could be provided from a variety of sources and with different formats. Although some work has been already carried out on these topics [VARYS] it is considered this should be integrated natively as a core part of the upcoming 6G M&O systems. Also, this requirement on mixing application and infrastructure-based metrics is close related with the AI/ML-related functionalities previously described, and it is considered a primary enabler to provide data-driven orchestration functionalities. What feed AI/ML algorithms are data, so the wider the available dataset, the better (more accurate) AI/ML models may be generated. Enabling the monitoring system to collect (and aggregate) data from the different network layers and domains is considered a key enabler to offer the advanced AI/ML functions needed to implement more intelligent self-adaptation and self-optimization mechanisms, primarily based on correlating rich datasets with heterogeneous data.

In summary, functions in this Monitoring Functions block would be in charge of:

- Collecting raw data from different sources (monitoring probes, system/service logs, etc.) which may be scattered at the different network layers and network elements.
- To offer the necessary APIs to the MNO, verticals, and the service developers, making possible to monitor custom, user-defined metrics (and not just a fixed set of them).
- To act as processing elements (e.g., acting as data filters or data normalisation elements).
- To offer continuous monitoring of data towards the Design Layer, in order to support the CI/CD pipelines.
- To gather and store data for implementing model training on AI/ML systems.
- To provide interfaces to the operational information for both: humans (e.g., by means of real-time monitoring panels, or periodic reports) and other systems (e.g., M&O functions, Security Functions, or AI/ML Functions).

Security functions. The main objective of Security Functions is to protect the confidentiality and integrity of operations and data, and to ensure the continuity of the supplied services. In order to achieve this goal, an effective method consists of complying with reference cyber safety frameworks. Whereas many different cyber security frameworks exist [RKL13] [Anssi21] [Nist18], the overall guidelines are similar through the following main functions:

- Identify the assets to be protected, and the security risks they are exposed to.
- Protect the assets by deploying appropriate tools and functions as countermeasures to reduce risks.
- Monitor and detect any signs of an undergoing attack on the assets.
- Respond to the attack with appropriate actions.
- Recover and learn lessons from the attack.

To perform those security tasks withinside the M&O scope, both security enablers and security management functions are needed. As shown in Figure 19, the security management functions (orange blocks) can be seen as an extension of the primary M&O system, supporting it to ensure the security of the assets under its control. Those orange blocks constitute different instances made of functions in the Security Functions block. Depending on the abstraction layer, different instances of M&O functions (grey blocks) can manage different sorts of assets, that also need to be secured. For example, withinside the Service Layer, the valuable assets would be network services and slices, while on the Network Layer the valuable assets could be NFs. For the Infrastructure Layer, computing, storage and network resources could be the primary assets to be secured. At each layer, the generic M&O functions themselves (grey blocks) could be secured with the aid of the Security Functions (orange blocks). Of course, there can be numerous instances of security functions related to a single M&O functions block, each being devoted to secure a given group of properties managed by the M&O functions. For example, assets may be grouped by security level requirement.

Following this approach, when an entity requests any service associated with a managed object thru the exposed interfaces, the generic M&O blocks could be able to delegate the protection of the service to the associated security functions. This delegation might be transparent for the M&O resources and consumers. For example, on a call for a service such as the provisioning of a network slice, the M&O functions could rely upon the security functions to deal with the security requirements included in the request. When a customer requests a service to be instantiated, the M&O functions could apply LCM actions to instantiate the functions for that service. Based on its internal configuration and on the security requirements expressed for the service, the security functions may proactively suggest/impose extra LCM operations to the M&O functions. These may normally include a change of the configurations of the service functions, an update of these functions, or the addition of new security-specific functions.

The measures to prevent attacks from compromising their targets might also introduce vulnerabilities associated with the presence of unknown bugs or incorrect settings. Adopting a defence-in-depth approach can assist to mitigate those vulnerabilities, which need to include monitoring, detection, and response measures, in addition to preventive protection approaches. As a consequence, during the lifetime of the asset, the security M&O functions shall constantly monitor and detect incoming attacks, both directly, or through the use of the enablers deployed for this purpose and take mitigation and remediation actions if a security incident were confirmed. Besides conventional security tools (such as firewalls or signature-based traffic inspection) enablers to enforce security in future 6G networks may also include AI/ML solutions for analysis and planning, or quantum-based security mechanisms for key distribution. Those AI/ML functions might be deployed as a part of the AI/ML Functions block withinside the M&O system represented in Figure 19.

To perform their work, the security M&O blocks can also use both: services exposed by the primary M&O functions to manage the life cycle of assets, and services exposed through other security M&O

functions to delegate security tasks or report security incidents. The LCM actions that the security M&O functions may have to apply to its security functions might be delegated to the regular M&O functions. Finally, the security M&O functions may also use the services exposed by other functions, which include monitoring services to collect data, and AI/ML services to get predictions and support orchestration actions. These services could contribute to the realisation of automated closed loops a part of the security processes.

4 Conclusions and Outlook

In this White Paper, we discuss the current architectural trends and technologies for future 6G Networks. Motivated by the surge of new requirements stemming from societal trends, use cases, and the availability of new architectural enablers, we draw the high-level trends that are expected to guide the research, development, and standardization trends of next generation mobile network.

We identified trends for the ubiquitous deployment along different network domains of intelligence, sensing, twinning, as well as security solutions deployed all over the network.

Then we deep dive into specific network domains, discussing bleeding edge research trends for aspects such as access networks, intelligence, sustainability, twinning, sensing, security and programmability. Also, we discuss the role of service providers in the networks, through their integration using network applications and intent-based networking.

This discussion allows to have a common consolidated picture of the 5G-PPP projects view on the future 6G Architecture and research directions.

5 References

[22.261] 3GPP TS 22.261, "Service requirements for the 5G system" Release 19, v19.0.0, Sep 2022.

[23.501] 3GPP TS 23.501, "System architecture for the 5G System (5GS)" Release 17, v17.3.0, Dec 2021.

[23.502] 3GPP TS 23.502, "Procedures for the 5G System (5GS); Stage 2," Release 17, v17.3.0, Dec 2021.

[28.533] 3GPP TS 28.533, "Management and Orchestration; Architecture Framework (Release 17)", December 2021.

[38.331] 3GPP TS 38.331 "NR; Radio Resource Control (RRC); Protocol specification," Release 16, v16.7.0, Dec 2021

[38.401] 3GPP, "NG-RAN; Architecture description," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.401, January 2020, version 16.0.0.

[5gaiml21] 5G PPP Technology Board, "AI and ML – Enablers for Beyond 5G Networks", Version 1.0, 2021-05-11, DOI 10.5281/zenodo.4299895, online available at: https://5g-ppp.eu/wp-content/uploads/2021/05/AI-MLforNetworks-v1-0.pdf, [Accessed: 2022-04-03].

[5gp21] 5GPPP, "Architecture Working Group. View on 5G Architecture", Version 4.0, August 2021. [Online] Available at: https://5g-ppp.eu/wp-content/uploads/2021/08/Architecture-WP-v4.0_forPublicConsultation.pdf [Accessed 12 April 2022].

[5GVIN-D31] 5G VINNI D3.1: Specification of services delivered by each of the 5G-VINNI facilities. [Online] Available at: https://zenodo.org/record/3345612 [Accessed 28 March 2022]. June 2019.

[9595:98] ISO/IEC 9595:1998 "Information technology - Open Systems Interconnection - Common management information service", October 1998.

[9596-1:98] ISO/IEC 9596-1:1998 "Information technology - Open Systems Interconnection — Common management information protocol - Part 1: Specification", October 1998.

[AGG+19] J. A. Ayala-Romero, A. Garcia-Saavedra, M., Gramaglia, X., Costa-Perez, A., J. J. Alcaraz, "vrAIn: A deep learning approach tailoring computing and radio resources in virtualized RANs", in 25th Annual International Conference on Mobile Computing and Networking, pp. 1-16, October 2019.

[Anssi21] French Network and Security Agency (ANSSI/Agence nationale de la sécurité des systèmes d'information): Managing Cybersecurity for Industrial Control Systems, June 2021.

[Arc19] Arcep, 2019. Réseaux du futur Note n° 5 L'empreinte carbone du numérique. Available online at: https://www.arcep.fr/uploads/tx_gspublication/reseaux-du-futur-empreinte-carbone-numerique-juillet2019.pdf

[ART21] Alexander Artemenko et al. "Definition and Description of the 6G BRAINS Primary Use Cases and Derivation of User Requirements" 6G BRAINS Deliverable D2.1, 31 July 2021.

[BAZ+20] S. Buzzi, C. D'Andrea, A. Zappone and C. D'Elia, "User-Centric 5G Cellular Networks: Resource Allocation and Comparison With the Cell-Free Massive MIMO Approach," in IEEE Transactions on Wireless Communications, vol. 19, no. 2, pp. 1250-1264, February, 2020.

[BDG+14] P.Bosshart, D.Daly, G.Gibb, et al., "P4: Programming protocol-independent packet processors." ACM SIGCOMM Computer Communication Review 44, no. 3, pp. 87-95, 2014.

[BFC21] R. Bassoli, F. H.P. Fitzek, and E. Calvanese Strinati, "Why Do We Need 6G?" ITU Journal on Future and Evolving Technologies, vol. 2 no. 6, Sep. 2021.

[BS19] E. Björnson and L. Sanguinetti, "Cell-Free versus Cellular Massive MIMO: What Processing is Needed for Cell-Free to Win?," 2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), pp. 1-5, 2019.

[CBD+22] B. Cox, C. Buyle, D. Delabie, L. De Strycker, L. Van der Perre, "Positioning Energy-Neutral Devices: Technological Status and Hybrid RF-Acoustic Experiments", Future Internet 2022, 14, 156. https://doi.org/10.3390/fi14050156.

[CBF22] A. Collet, A. Banchs and M. Fiore, "LossLeaP: Learning to Predict for Intent-Based Networking," IEEE INFOCOM 2022 - IEEE Conference on Computer Communications, 2022, pp. 2138-2147, doi: 10.1109/INFOCOM48880.2022.9796918.

[CBH+20] Coroamă V.C, Bergmark P., Höjer M. and Malmodin J. 2020. A Methodology for Assessing the Environmental Effects Induced by ICT Services – Part I: Single Services. In 7th International Conference on ICT for Sustainability (ICT4S2020), June 21–26, 2020, Bristol, United Kingdom. ACM, New York, NY, USA, 10 pp. 2020.

[CMWT21] Y. Chen, J. Mohammadi, S. Wesemann and T. Wild, "Turbo-AI, Part II: Multi-Dimensional Iterative ML-Based Channel Estimation for B5G," 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), 2021.

[COS22] John Cosmas et al. "Technical Specification of the 3D Location Architecture" 6G BRAINS Deliverable D6.1, 31 January 2022.

[Dem20] N. Demassieux, "6G. Why?", EUCNC 2020, Dubrovnik, Croatia, June, 2020, https://www.eucnc.eu/wp-content/uploads/2020/07/2020-05-29-6G.-Why-Nicolas-Demassieux-EUCNC-VDEF.pdf

[DGK+13] P. Demestichas, A. Georgakopoulos, D. Karvounas, K. Tsagkaris, V. Stavroulaki, J. Lu, C. Xiong, and J. Yao , "5G on the Horizon: Key Challenges for the Radio Access Network," IEEE Vehic. Tech. Mag., vol. 8, no. 3, 2013, pp. 47–53.

[DLH19] Y. Dang, Q. Lin, and P. Huang, "Aiops: real-world challenges and research innovations," 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), IEEE, pp. 4-5, 2019.

[EC20] "A New Industrial Strategy for Europe," COM(2020) 102 final - Brussels, March, 2020, https://ec.europa.eu/info/sites/info/files/communication-eu-industrial-strategy-march-2020_en.pdf

[ECR+21] M. Ericsson; M. Condoluci; P. Rugeland; et. al., "6G Architectural Trends and Enablers", IEEE 4th 5G World Forum, 2021

[EFA+19] Eriksson A.C., Forsman M., Ainen H.R., Willars P., Östberg C., “5G New Radio RAN and transport choices that minimize TCO”, 2019.

[Eri20] Ericsson, “Ever-present intelligent communication,” Whitepaper, 2020, https://www.ericsson.com/en/reports-and-papers/white-papers/a-research-outlook-towards-6g

[EWS+22] M. Ericsson; S. Wänstedt, M. Saimler, et. al., “Setting 6G Architecture in Motion - the Hexa-X Approach”, EUCNC 2022, Grenoble, France, June 6-10, 2022, Online: https://zenodo.org/record/6638245#.Y3dxd0nMIUF

[F5G13] The FUDGE-5G Consortium, “Final Platform Architecture”, Online: https://www.fudge-5g.eu/en/deliverables

[FI+15] M. Boucadair and C. Jacquenet, “Introducing Automation in Service Delivery Procedures: An Overview.,” in Handbook of Research on redesigning the future of internet architectures, Hershey, PA, USA: Information Science Reference, an imprint of IGI Global, 2015.

[FL-RIC+21] Robert Schmidt, Mikel Irazabal, and Navid Nikaein, “FlexRIC: an SDK for next-generation SD-RANS”, Proc. 17th International Conference on Emerging Networking EXperiments and Technologies (CONEXT 2021), 7-10 December 2021, Munich, Germany (Virtual Conference).Traffic Control tc(8), Linux man page, [Online]. Available: https://linux.die.net/man/8/tc.

[FS20] H. Farhadi and M. Sundberg, "Machine learning empowered context-aware receiver for high-band transmission," 2020 IEEE Globecom Workshops (GC Wkshps, 2020.

[Gha20] Ghadialy Z., Understanding the TCO of a Mobile Network, The 3G4G Blog, 2020.

[Gsm19] GSMA, 5G-era Mobile Network Cost Evolution, 2019.

[GSM20] Global System for Mobile Communications (GSMA), “2020 Mobile Industry Impact Report: Sustainable Development Goals,” September, 2020. https://www.gsma.com/betterfuture/2020sdgimpactreport/wp-content/uploads/2020/09/2020-Mobile-Industry-Impact-Report-SDGs.pdf?utm_source=better_future_site&utm_medium=search_engine&utm_campaign=2020_SDG_impact_report

[HEXA] Hexa-X website, https://hexa-x.eu/objectives/.

[HEX-D12] Hexa-X Deliverable D1.2, “Expanded 6G vision, use cases and societal values – including aspects of sustainability, security and spectrum”, Apr. 2021, [Online]. Available: https://hexa-x.eu/wp-content/uploads/2022/04/Hexa-X_D1.2_Edited.pdf.

[HEX-D13] Hexa-X Deliverable D1.3, “Targets and requirements for 6G – initial E2E architecture”, Mar. 2022, [Online]. Available: https://hexa-x.eu/wp-content/uploads/2022/03/Hexa-X_D1.3.pdf.

[HEX-D21] Hexa-X Deliverable D2.1, “Towards Tbps Communications in 6G: Use Cases and Gap Analysis” Jun. 2021, [Online]. Available: https://hexa-x.eu/wp-content/uploads/2021/06/Hexa-X_D2.1.pdf.

[HEX-D22] Hexa-X Deliverable D2.2, "Initial radio models and analysis towards ultra-high data rate links in 6G" Dec 2021, [Online]. Available: https://hexa-x.eu/wp-content/uploads/2022/01/Hexa-X-D2_2.pdf

[HEX-D31] Hexa-X, "Deliverable D3.1: Localisation and sensing use cases and gap analysis", Jan. 2022.

[HEX-D32] Hexa-X, "Deliverable D3.2: Localisation and sensing use cases and gap analysis," Sep. 2022.

[HEX-D42] Hexa-X Deliverable D4.2, "AI-driven communication & computation co-design: initial solutions", Jun. 2022, Online: https://hexa-x.eu/wp-content/uploads/2022/07/Hexa-X_D4.2_v1.0.pdf.

[HEX-D51] Hexa-X Deliverable D5.1, "Initial 6G architectural components and enablers", Dec. 2021, Online: https://hexa-x.eu/wp-content/uploads/2022/03/Hexa-X_D5.1_full_version_v1.1.pdf.

[HEX-D62] Hexa-X Deliverable D6.2, "Design of service management and orchestration functionalities", Apr. 2022, Online: https://hexa-x.eu/wp-content/uploads/2022/05/Hexa-X_D6.2_V1.1.pdf.

[HF15] Håkansson C., Finnveden G., Indirect rebound and reverse rebound effects in the ICT-sector and emissions of CO_2, In the Proceedings of EnviroInfo and ICT for Sustainability 2015. 2015.

[HJS17] H. Hawilo, M. Jammal and A. Shami, "Orchestrating network function virtualization platform: Migration or re-instantiation?" IEEE 6th International Conference on Cloud Networking (CloudNet), pp. 1-6, 2017, available online at:: 10.1109/CloudNet.2017.8071528

[IFL19] G. Interdonato, P. Frenger, and E.G. Larsson, "Scalability Aspects of Cell-Free Massive MIMO," in ICC 2019 IEEE International Conference on Communications (ICC), pp. 1–6, 2019.

[Itu14] [Itu14] Recommendation ITU-T L.1410 (12/14), Methodology for environmental life cycle assessments of information and communication technology goods, networks and services. 2014.

[Itu20] Recommendation ITU L.1470 (01/20). Greenhouse gas emissions trajectories for the information and communication technology sector compatible with the UNFCCC Paris Agreement, 2020.

[JAS02] G. Joya, M. A. Atencia, and F. Sandoval, "Hopfield neural networks for optimization: study of the different dynamics," Neurocomputing vol. 43, no. 1-4, pp. 219-237, 2002.

[KHH+21] D. Korpi, M. Honkala, J. M. J. Huttunen, and V. Starck, "DeepRx MIMO: Convolutional MIMO detection with learned multiplicative transformations," in Proc. IEEE International Conference on Communications (ICC), Jun. 2021. Available: https://arxiv.org/abs/2010.16283

[KLM+19] T. Kohlberger, Y. Liu, M. Moran, P. H. C. Chen, T. Brown, J. Hipp, M. C. Stumpe, "Whole-slide image focus quality: Automatic assessment and impact on AI cancer detection." Journal of pathology informatics, 2019.

[LAG19] A. Laghrissi and T. Taleb, "A Survey on the Placement of Virtual Resources and Virtual Network Functions," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1409-1434, Second quarter 2019, available online at: 10.1109/COMST.2018.2884835.

[LIM21] B. Lim, S. Zohren, "Time-series forecasting with deep learning: a survey," Philosophical Transactions of the Royal Society A, 379, no. 2194, 2021. Available online at: https://www.oxford-man.ox.ac.uk/wp-content/uploads/ 2020/11/Time-Series-Forecasting-With-Deep-Learning_-A-Survey.pdf

[LL19] J. Liu, Z. Liu, "A survey on security verification of blockchain smart contracts". IEEE Access, 7, 77894-77904, 2019.

[LLF+21] Z. Lv, R. Lou, H. Feng, et al., "Novel machine learning for big data analytics in intelligent support information management systems," ACM Transactions on Management Information System (TMIS), vol. 13, no. 1, pp. 1-21, 2021.

[LMB+22] Lundén D, Malmodin J, Bergmark P., Lövehagen N., Electricity Consumption and Operational Carbon Emissions of European Telecom Network Operators, Sustainability, Sustainability 2022, 14(5), 2637.

[ML18] Malmodin J., Lundén D. "The energy and carbon footprint of the global ICT and E&M sectors 2010–2015". Sustainability, 10:3027, 2018.

[ML18a] Malmodin J., Lundén D. Report from the KTH Centre for Sustainable Communications Stockholm; The Electricity Consumption and Operational Carbon Emissions of ICT Network Operators 2010-2015", Technical report, 2018

[MLC20] R. Minerva, G. M. Lee, and N. Crespi, "Digital twin in the IoT context: A survey on technical features, scenarios, and architectural models," Proceedings of the IEEE, vol. 108, no. 10, pp. 1785–1824, 2020. https://ieeexplore.ieee.org/document/9120192

[NAY+17] H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, "Cell-Free Massive MIMO Versus Small Cells," IEEE Transactions on Wireless Communications, vol. 16, no. 3, pp. 1834–1850, 2017.

[Nist18] National Institute of standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity", April 2018.

[Nok20] Nokia Bell Labs, "Communications in the Era of 6G," White Paper, 2020, https://onestore.nokia.com/asset/207766

[Nok20a] Nokia Bell Labs, "The 3GPP-defined Service Based Management Architecture", Technical brief, Document code: SR2007045991EN (July) CID207723, (2020), [Online] Available at: https://nokianews.net/files/ Nokia_Bell_Labs_The_3GPP-defined_Service_Based_Management_ Architecture_White_Paper_EN.pdf

[Nok20b] Nokia, "The AI Opportunity for telecoms," 2020, https://www.nokia.com/networks/research/the-ai-opportunity-for-telecoms/

[ONAP] ONAP. [online] Available at: https://www.onap.org [Accessed 15 November 2022].

[ORAN4] "O-RAN Architecture Description," Technical Specification (TS) O-RAN.WG1.O-RAN-Architecture-Description-v04.00, March 2021.

[ORD21] Jose Ordonez-Lucena "Validation of 5G-CLARITY SDN/NFV Platform, Interface Design with 5G Service Platform, and Initial Evaluation of ML Algorithms" 5G-CLARITY Deliverable D4.2, July 30, 2021

[P4+14] P. Bosshart, D. Daly, G. Gibb, M. Izzard, N. McKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghese, and. Walker, “P4: Programming protocol-independent packet processors,” ACM SIGCOMM Computer Communication Review, vol. 44, no. 3, pp. 87–95, 2014.

[P4Cloud+21] H. Harkous, B. A. Hosn, M. He, M. Jarschel, R. Pries, and W. Kellerer, “Towards performance-aware management of p4-based cloud environments,” in 2021 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV- SDN), 2021, pp. 87–90.

[P4-P8+21] H. Harkous, M. Jarschel, M. He, R. Pries, and W. Kellerer, “P8: P4 with predictable packet processing performance,” IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 2846–2859, 2021.

[PFN+20] Q.V. Pham, F. Fang, V. Nguyen, Md. J. Piran, M. Le, L. B. Le, W.J. Hwang, Z. Ding, “Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art,” in IEEE Access, vol. 8, pp. 116974 – 117017, June 2020.

[RAB+20] N. Rajatheva, et al., “Broadband Connectivity in 6G”, White Paper, arXiv: Signal Processing, 2020. Available at: https://arxiv.org/pdf/2004.14247.pdf.

[Rac20] Racontour, “The economic impact of 5G,” 2020, https://www.raconteur.net/infographics/the-economic-impact-of-5g/

[REI-D11] REINDEER D1.1 ‘Use case-driven specifications and technical requirements and initial channel model’, preliminary version available via https://reindeer-project.eu/results-downloads/

[RKL13] R. Robin, W. ken, T. Lana, "New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)", New Zealand National Cyber Security Centre, 2013.

[RRS+19] J. Randers, J. Rockström, P. Stoknes, U. Goluke, D. Collste, S. Cornell, and J. Donges, “Achieving the 17 Sustainable Development Goals within 9 planetary boundaries,” Global Sustainability, 2, E24. doi:10.1017/sus.2019.22

[SCT+22] A. M. Sanchez, A. S. Charismiadis, D. Tsolkas, D. A. Guillen and J. G. Rodrigo, "Offering the 3GPP Common API Framework as Microservice to Vertical Industries," 2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), 2022, pp. 363-368, doi: 10.1109/EuCNC/6GSummit54941.2022.9815741.

[SDG] https://sdgs.un.org/

[SIN21] Robert Schmidt, Mikel Irazabal, and Navid Nikaein, “FlexRIC: an SDK for next-generation SD-RANS”, Proc. 17th International Conference on Emerging Networking EXperiments and Technologies (CONEXT 2021), 7-10 December 2021, Munich, Germany (Virtual Conference).Traffic Control tc(8), Linux man page, [Online]. Available: https://linux.die.net/man/8/tc.

[SKS+19] G. Salvaneschi, M. Köhler, D. Sokolowski, P. Haller, S. Erdweg, M. Mezini, "Language-Integrated Privacy- aware Distributed Queries", in Proc. of ACM OOPSLA, 2019.

[SLL17] J. Liu, M. Sheng, L. Liu and J. Li, "Network Densification in 5G: From the Short-Range Communications Perspective," in IEEE Communications Magazine, vol. 55, no. 12, pp. 96-102, December 2017.

[STG+19] G. Siracusano, M. Trevisan, R. Gonzalez, R. Bifulco, (2019, November). Poster: on the application of NLP to discover relationships between malicious network entities. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 2641-2643).

[SZF+18] T. Szigeti, D. Zacks, M. Falkner, et al., "Cisco Digital Network Architecture: Intent-based Networking for the Enterprise," Cisco Press, 2018.

[SZI21] P. Szilágyi, "I2bn: Intelligent intent-based networks," Journal of ICT Standardization, pp. 159-200, 2021.

[TCP91] G. A. Tagliarini, J. F., Christ, and E. W. Page, "Optimization using neural networks," IEEE transactions on computers, vol. 40, no. 12, pp. 1347-1358, 1991.

[UKT22] E. Ustundag Soykan, L. Karaçay, F. Karakoç and E. Tomur, "A Survey and Guideline on Privacy Enhancing Technologies for Collaborative Machine Learning," in IEEE Access, vol. 10, pp. 97495-97519, 2022, doi: 10.1109/ACCESS.2022.3204037.

[UN15] United Nations, "Transforming our world: the 2030 Agenda for Sustainable Development," Resolution adopted by the General Assembly, September, 2015, https://upload.wikimedia.org/wikipedia/commons/d/d5/N1529189.pdf

[UNSDG] http://www.un.org/sustainabledevelopment/sustainable-development-goals/

[VARYS] Next Generation Platform as a Service (NGPaaS). 2019. VARYS: Multi-tier Technology-agnostic Monitoring as a Service solution for Cloud systems. [Online] Available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform/13777;isExactMatch=false;advancedFilters=1;projectId=761557 [Accessed 30 March 2022].

[VFJ+16] S. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, P. Samarati, "Efficient Integrity Checks for Join Queries in the Cloud, " JCS, vol. 24, no. 3, 2016, pp. 347–378.

[VFJ+17] S. Vimercati, S. Foresti, S. Jajodia, G. Livraga, S. Paraboschi, P. Samarati, "An Authorization Model for Multi-Provider Queries," in Proc. of the VLDB Endowment, vol. 11, n. 3, November 2017.

[VFL+21] S. Vimercati, S. Foresti, G. Livraga, P. Samarati, "Data Security and Privacy in Smart Cities," in Smart Cities Policies and Financing Handbook, Morgan Kaufmann, 2021.

[YYY+19] Q. Yang, Y. Liu, Y. Cheng, et al., "Federated learning. Synthesis Lectures on Artificial Intelligence and Machine Learning," vol. 13, no. 3, pp. 1-207, 2019.

[ZDW21] B. Zhang, B. Dong, W. H. Wang, "CorrectMR: Authentication of Distributed SQL Execution on MapReduce," IEEE TKDE, vol. 33, no. 3, pp. 897 – 908, March 2021.

[ZVF+20] V. Ziegler, H. Viswanathan, H. Flinck, M. Hoffmann, V. Räisänen and K. Hätönen, "6G Architecture to Connect the Worlds," in IEEE Access, vol. 8, pp. 173508-173520, 2020, doi: 10.1109/ACCESS.2020.3025032., 2020.

6 Abbreviations

3GPP	3rd Generation Partnership Project
5G PPP	5G Public Private Partnership
5GC	5G Core (network)
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
AIaaS	AI as a Service
AIOps	AI-assisted Operations
AMF	Access and Mobility Management Function
AoA	Angle of Arrival
API	Application Programming Interface
B5G	Beyond 5G
BSS	Business Support System
CA	Carrier Aggregation
CAPIF	Common API Framework
CF	Cell-Free
CFS	Customer Facing Service
CI/CD	Continuous Integration/Continuous Deployment
CIR	Channel Impulse Response
CN	Core Network
CNF	Containerised Network Function
CP	Control Plane
CPU	Central Processing Unit
CRUD	Create, Read, Update, Delete
CSI	Channel Status Information
CSMF	Communication Service Management Function
CSP	Communication Service Provider
CU	Centralised Unit
DAO	Decentralised Autonomous Organisation
DAS	Distributed Antenna System
DC	Dual Connectivity
DC	Data-Centre
DePF	DNN-assisted Particle Filter
DFP	Dynamic Function Placement

DL	Down-Link
D-MIMO	Distributed MIMO
DNN	Deep Neural Network
DP	Dynamic Programming
DT	Digital Twin
DU	Distributed Unit
EC	European Commission
EIRP	Effective Isotropic Radiated Power
EMF	Electric and Magnetic Field
EP	Embedding Propagation
ETSI	European Telecommunications Standards Institute
EU	European Union
FL	Federated Learning
FPGA	Field Programmable Gate Array
FQDN	Fully Qualified Domain Name
GDP	Gross Domestic Product
GESI	Global Enabling Sustainability Initiative
gNB	Next generation NodeB
GSMA	GSM Association
GST	Generalised Slice Template
HTTP	Hyper-Text Transfer Protocol
HW	Hardware
IAB	Integrated Access and Backhaul
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronics Engineers
IM	Information Model
ISAC	Integrated sensing and Communication
IT	Information Technology
ITU	International Telecommunication Union
JRC2LS	Joint Radar, Communication, Computation, Localisation, and Sensing
JT-CoMP	Joint Transmission Coordinated Multi-Point
KPI	Key Performance Indicator
KVI	Key value Indicator
LADN	Local Area Data Network

LCM	Lice-Cycle Management
LEO	Low Earth Orbit
LIDAR	[Laser|Light] Imaging, Detection and Ranging
LNaaS	Logical Network as a Service
LTE	Long Term Evolution (4G)
MANO	Management and Orchestration
MC	Multi Connectivity
MDT	Minimisation of Drive Tests
ME	Mobile Edge
MEC	Multi-access Edge Computing
MEO	Medium Earth Orbit
MIB	Management Information Base
MIMO	Multiple-Input and Multiple-Output
ML	Machine Learning
MLOps	Machine Learning Operations (lifecycle management of ML mechanisms)
mMIMO	Massive MIMO
MNO	Mobile Network Operator
MRF	Media Resource Function
MU	Mobile User
MVNO	Mobile Virtual Network Operator
NF	Network Function
NFV	Network Function Virtualisation
NFVI	Network Function Virtualisation Infrastructure
NFVO	NFV Orchestrator
NIC	Network Interface Card
NIF	Network Intelligence Function
NIS	Network Intelligence Service
NPN	Non-Public Network
NR	New Radio (5G)
NRF	Network Repository Function
NS	Network Service
NSA	Non-Standalone
NSD	Network Service Descriptor
NSS	Network Slice Subsystem

NTN	Non-Terrestrial Network
NWAF	Network Analytics Function
NWDAF	Network Data Analytics Function
NWMF	Network Monitoring Function
OFDM	Orthogonal Frequency-Division Multiplexing
ONAP	Open Network Automation Platform
OPC	Open Platform Communications
OPC-UA	OPC Unified Architecture
OPEX	Operational Expenditure
OSI	Open Systems Interconnection (ISO standard series)
OSM	Open Source MANO
OSS	Operations Support system
OTFS	Orthogonal Time Frequency Space
OTT	Over-The-Top
OVS	Open vSwitch
OWC	Optical Wireless Communication
PGM	Particle Gaussian Mixture
PNF	Physical Network Function
QoE	Quality of Experience
QoS	Quality of Service
RAM	Random Access Memory
RAN	Radio Access Network
REST	Representational State Transfer
RF	Radio Frequency
RFS	Resource Facing Service
RIC	RAN Intelligent Controller
RIS	Reconfigurable Intelligent Surface
RSS	Received Signal Strength
RU	Remote Unit
SBA	Service-Based Architecture
SBI	Service-Based Interface
SBMA	Service-Based Management Architecture
SBTi	Science Based Targets initiative
SCP	Service Communication Proxy

SDG	Sustainable Development Goal
SDK	Software Development Kit
SDN	Software-Defined Networking
SDO	Standards Developing Organisation
SID	Shared Information/Data Model (TMForum)
SLA	Service Level Agreement
SLAM	Simultaneous Localization and Mapping
SMF	Session Management Function
SOTA	State-Of-The-Art
SW	Software
TC	Traffic Control
TDE	Thread Detection Engine
TDoA	Time Difference of Arrival
TN	Transport Network
TRP	Transmit/Receive Point
UAV	Unmanned Aerial Vehicle
UE	User Equipment
UL	Up-Link
UN	United Nations
UP	User Plane
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communication
VAE	Vertical Application Enabler
VEC	Vertical enterprise Customer
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
WAIF	Who Am I Function
WPT	Wireless Power Transfer
XAI	Explainable AI
ZSM	Zero-Touch Service Management

7 List of editors

Name	Company / Institute / University	Country
Boldi, Mauro	Telecom Italia	Italy
Bulakci, Ömer	Nokia	Germany
Cosmas, John	Brunel University	U.K.
Ericson, Mårten	Ericsson	Sweden
Gavras, Anastasius	Eurescom	Germany
Ghoraishi, Mir	Gigasys Solutions	U.K.
Gramaglia, Marco	University Charles III of Madrid	Spain
Kostopoulos, Alexandros	Hellenic Telecommunications Organisation (OTE)	Greece
Li, Xi	NEC Laboratories Europe	Germany
Masood Khorsandi, Bahare	Nokia	Germany
Mesodiakaki, Agapi	Aristotle University of Thessaloniki	Greece
Rahman, Arifur	IS Wireless	Poland
Rugeland, Patrik	Ericsson	Sweden
Tsolkas, Dimitris	Fogus Innovations & Services	Greece
Uusitalo, Mikko	Nokia	Finland

The list of contributing projects can be obtained from the 5G PPP website at https://5g-ppp.eu/5g-ppp-phase-3-projects/. In particular this document reflects the joint opinion of the the latest generation of projects as listed for parts 4, 5 and 6 of phase 3 of the 5G PPP programme.

- 5G PPP Phase 3, Part 4: 5G Long Term Evolution
- 5G PPP Phase 3, Part 5: 5G Core Technologies innovation and 5G for Connected and Automated Mobility (CAM)
- 5G PPP Phase 3, Part 6: 5G innovations for verticals with third party services & Smart Connectivity beyond 5G