Autonomous Private Mobile Networks: State of the Art and Future Challenges

Arturo Bellin, Marco Centenaro, Nicola di Pietro, Arif Ishaq, Daniele Munaretto, Daniele Ronzani, Andrea Spinato, Stefano Tomasin, and Fabrizio Granelli

***Abstract*—As mobile systems for private use are gaining momentum, the area of network management automation is bound to attract renewed attention from standardization organizations and vendors. Prominent examples of tasks that would benefit from network automation tools are provisioning, diagnosing, and healing. Nevertheless, due to the various network and service providers as well as stakeholders involved in the deployment of a non-public mobile system, the success of such automation heavily depends on a smooth and effective interoperability among the components of the overall system. In this paper, we review the state of the art of network operations, administration, and management in the context of non-public mobile systems, highlighting the differences with respect to traditional public networks. In order to emulate the evolution of such mobile network architectures implemented with heterogeneous software, we provide preliminary results on automated provisioning based on a research testbed under continuous integration. Finally, we propose a list of future challenges in this research area.**

***Index Terms*—5G and beyond, non-public networks, private mobile networks, open ecosystem, 3GPP, ETSI, NFV, MEC, management and orchestration.**

Introduction

RECENTLY, mobile communication networks for private use [1] – also called Non-Public Networks (NPNs) for the fifth-Generation (5G) of the networks standardized by the 3rd Generation Partnership Project (3GPP) [2], [3, §5.30] – are attracting attention in both the academic and industrial research communities. NPNs aim at providing the technologies developed for public networks (such as 5G) to private entities or network tenants by restricting network access only to authorized terminals. For such reason they are expected to support a variety of *vertical industries*, e.g., Industry 4.0, smart grids, and public safety, with a combination of (dedicated) services, including (edge) cloud computing, mission-critical communication, Internet of Things (IoT), indoor communication and positioning. Among the key enablers for a widespread adoption of NPNs, it is possible to mention i) the utilization of commodity hardware to host virtual mobile network functions and ii) open and standard interfaces to prevent vendor lock-in, thus opening up the market to new players, foster interoperability, and ease network management and orchestration. The former approach has been a trend over the last decade (with the advent of Software Defined Networking and Network Function Virtualization), representing the corner stone of NPNs. The latter entails the concept of *openness* in different aspects and forms:

1) *Inter-subnetwork openness* – It ensures interoperability across domains, e.g., the radio access network and the core network.
2) *Intra-subnetwork openness* – The segmentation between control-plane network functions (NFs) and user-plane NFs as well as radio access network (RAN) protocol stack split enable interworking among (software) infrastructure providers.
3) *Security openness* – Thanks to the standardization of user equipment (UE) profiles and their authentication means, NPNs enable a private tenant to apply thorough access control policies.
4) *End-to-end system orchestration openness* – The widespread adoption of network deployment approaches based on commodity hardware allows to focus on the management and orchestration of virtual NFs via standard interfaces.

The 3GPP and the European Telecommunications Standards Institute (ETSI) have been playing a key role to foster the creation of such an open ecosystem thanks to their standards related to 5G. This paper specifically focuses on the last openness factor, i.e., the overall orchestration of a non-public mobile system. Since most of the envisioned private users are not experts in mobile technologies, it is reasonable to assume that the network automation means will need to evolve to incorporate the principles of zero-touch network and service management, so to build *autonomous NPNs*, needing (almost) no intervention from human operators. This objective can be achieved with the collaboration of all the involved vendors and stakeholders, especially the new ones that are entering the market of mobile network equipment for private entities – typically referred to as *private mobile networks*, without an explicit label on the intended use of the network. In the following, we aim at identifying the standardization framework for building an autonomous NPN, while highlighting the possible risk factors which may prevent to achieve this target.

The rest of the paper is organized as follows. We first provide an overview of the state of the art of the standardization process, highlighting how NPNs differ from traditional public land mobile networks (PLMNs) in terms of requirements, system architectures, and governance. Then, we introduce

A. Bellin and F. Granelli are with the Department of Information Engineering and Computer Science (DISI), University of Trento, 38150 Trento, Italy. A. Bellin is the corresponding author.

M. Centenaro, N. di Pietro, A. Ishaq, D. Munaretto, D. Ronzani, and A. Spinato are with the Research & Innovation Department, Athonet S.r.l., 36050 Bolzano Vicentino, Italy.

S. Tomasin is with the Department of Information Engineering (DEI), University of Padova, 35131 Padova, Italy.

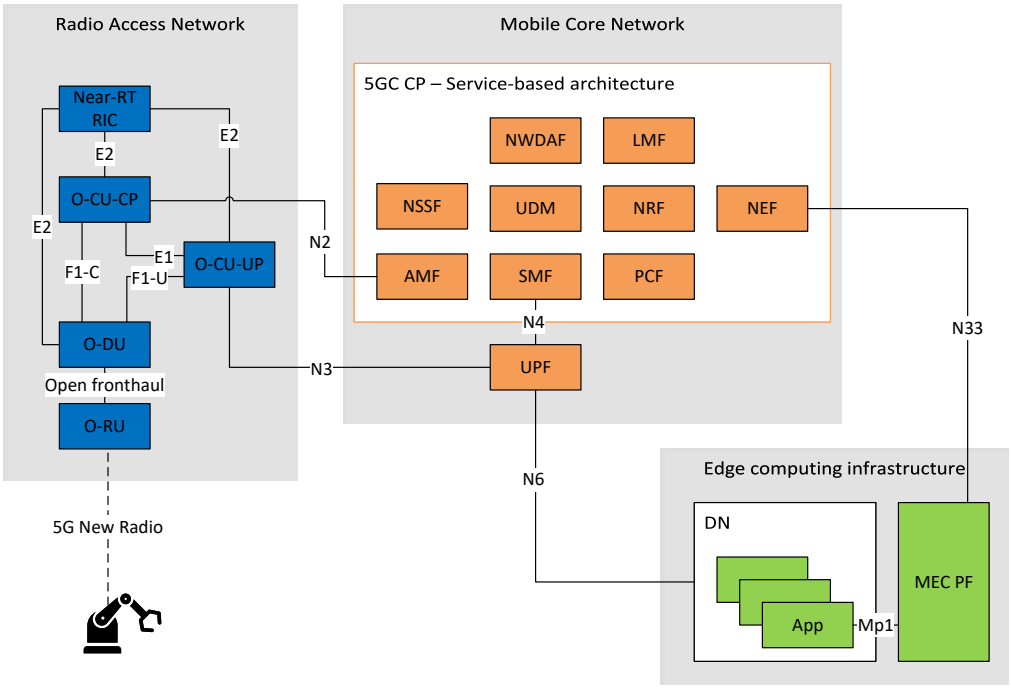

Fig. 1. E2E communication architecture for a generic 5G NPN. NF acronyms and reference points are those defined by the respective standards.

our research testbed, integrating both proprietary and open-source tools as well as designing features for management and orchestration of private mobile networks. Finally, we identify the future challenges for a widespread adoption of fully autonomous NPNs.

State of the Art

In this section, we describe the concept of 5G NPNs from the standardization perspective.

NPN Communication Architecture

Since Industry 4.0 is one of the prominent use cases of NPNs [4], Fig. 1 shows the end-to-end (E2E) communication architecture of a 5G NPN for this purpose. Such architecture can be consider as an embodiment of a 3GPP 5G system (5GS) [3] integrated with an edge computing infrastructure. It comprises three domains accounting for i) RAN, ii) the 5G core network (5GC), and iii) the ETSI multi-access edge computing (MEC) infrastructure.

From the figure, we can identify two degrees of openness out of the four abovementioned ones. About the inter-subnetwork openness, notice that the N2/N3 reference points ensure the interworking between the RAN and the 5GC domains regardless the adopted network equipment [3]; the same holds for N6/N33 for the interworking between the 5GC and the MEC system [5]. On the intra-subnetwork openness, each of the three domains utilizes standard interfaces among blocks of the same color. At 5GC level, this type of openness is significantly simplified in its implementation by the use of a service-based architecture among control-plane (CP) NFs. At RAN level, important steps forward have been taken with respect to the past. Despite it was traditionally the most closed domain, because of the historical (and natural) binding between hardware and software in radio equipment, the contribution by the O-RAN Alliance has been yielding a progressive decoupling between the radio software from the hardware. Novel RAN protocol stack split options across (open) remote units (O-RU), distributed units (O-DU), and centralized units (O-CU) have been introduced, decomposing the monolithic radio equipment into multiple modules that can effectively interwork with one another [6]. Finally, at MEC level the Mp1 reference point allows MEC applications to discover, advertise, consume and offer MEC services from/to the MEC platform.

NPN Management Architecture

Considering the NPN communication architecture for an Industry 4.0 scenario, Fig. 2 shows a (simplified) overview of its E2E operations, administration, and management (OAM) architecture. Each of the three domains in the figure features a dedicated OAM system specified by the respective standard development organization, namely the 3GPP for the RAN and the 5GC [7] and the ETSI MEC industry-specification group for the MEC system [8]. In particular, it is worth observing that the O-RAN Alliance specifies its service management and orchestration framework (SMO) by extending the 3GPP RAN OAM system with several features, including the non-real time RAN intelligent controller (non-RT RIC).

Note that three further domains, which are specific of the management architecture, are also introduced in Fig. 2, namely the operations/business support system (OSS/BSS), the

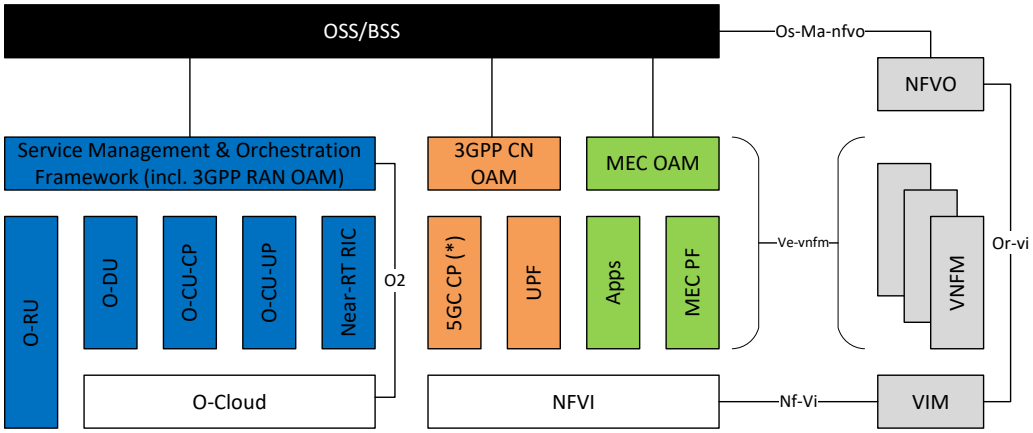

Fig. 2. E2E OAM architecture for the 5G NPN drawn in Fig. 1. Note that not all management entities are shown in this simplified representation. (*): the entire 5GC CP is shown as a unique software instance for graphical constraints only.

hardware infrastructure and the associated transport subnetwork, and the NFV management and orchestration (MANO) framework (in black, white, and grey, respectively). OSS/BSS provide means to the NPN operator (NPN-Op) to manage the overall network by leveraging the OAM systems of the various domains. To this end, OSS/BSS leverages the NFV MANO framework specified by ETSI for the lifecycle management of the virtual network functions (VNFs). In fact, while the fault, configuration, accounting, performance, and security (FCAPS) of each VNF is performed by the respective element manager (or domain OAM), the NFV MANO is responsible for, e.g., provisioning, diagnosing, and healing the virtual instances of network functions, let them be virtual machines or containers. Finally, all VNFs need to rely on an underlying physical infrastructure, consisting of hardware for computing, e.g., servers, and for the transport network, e.g., switches, routers, and firewalls. These elements are referred to as network function virtualization infrastructure (NFVI) in ETSI NFV and 3GPP, while O-RAN has introduced the concept of O-Cloud. In this respect, it is worth mentioning that, despite the O-Cloud is inspired to a NFVI [9], the two virtualization platforms may not be fully aligned because, e.g., of specific hardware requirements in terms of hardware acceleration needed by the RAN. As a consequence, interfaces between the orchestrator and the virtual infrastructure in O-RAN and ETSI NFV do not coincide in general.

An open framework in terms of management architecture enables not only the interoperability among different network equipment vendors, but also the seamless exchange of the NFV orchestration infrastructure, let it be proprietary (e.g., VMware telco cloud automation [10]) or open-source, as Open Source MANO (OSM) and Open Networking Automation Platform (ONAP) [11]. Moreover, we observe that an autonomous NPN relies on the interworking of all of these domain OAM systems. In this respect, the ETSI on zero-touch network and service management (ZSM) industry specification group is working to accelerate the definition of the required end-to-end architecture and solutions.

Important Remarks

The presented architectures refer to an implementation of a 5G NPN for the Industry 4.0 vertical, thus they do not include several configurations typical of a mobile network for private use. For example, the IP Multimedia System (IMS) and Mission-Critical Push-to-talk (MCPTT), which are crucial for, e.g., indoor voice communications and public safety, are not shown in Fig. 1. Moreover, the means to integrate the NPN private network with legacy network technologies for private use, like Wi-Fi or Ethernet [2] are missing.

Similarly, also Fig. 2 does not comprise several NPN setups. For example, for NPNs isolated from other systems or dedicated to public safety, dynamic management and orchestration might not be of primary importance. Nevertheless, the standard OAM framework turns out to be quite complex, as each domain features independent management and orchestration functionalities, which eventually need to interwork together in order to build an effectively autonomous NPN. Moreover, the picture does not include the possibility that each domain is managed by a different entity, thus exacerbating the problem. In the next section, we will highlight how these shortfalls jeopardize the effectiveness of a smooth E2E OAM of NPNs, also considering the new stakeholders introduced by the private mobile networks paradigm.

A Comparison Between NPNs and PLMNs

Although NPNs have been clearly identified and defined recently in the 5G network context, they could be obtained more than a decade ago leveraging fourth-generation (4G) mobile systems. As a matter of fact, almost all current deployments worldwide leverage the 4G technology, including, e.g., the systems operating in the USA on the Citizen Broadcast Radio System (CBRS) frequencies and following the specifications of the OnGo Alliance. Even some vertical markets can be still efficiently and reliably served by 4G systems for private use. This applies in particular to those related to critical communications for public safety, which traditionally require a very much stable and dependable system, and have been

considering this technology to replace the legacy Terrestrial Trunked Radio (TETRA) in the recent years. In other cases, instead, the Long Term Evolution (LTE) technology cannot meet new application requirements. For example, when considering a network connecting control systems and physical actuators, latency and reliability requirements become very stringent. In this context, the ultra-reliable low-latency communications (URLLC), which significantly benefit from the new 5G air interface (the so-called New Radio) design as well as leverage the enhanced 5GC uptime, are necessary. A huge expectation for 5G NPNs thus comes from the smart industry sector [4], [12], where URLLC can be combined with the security ensured by a NPN in terms of access control and user equipment authentication.

Pushed by the market, the 3GPP specified two standard ways of supporting NPNs in 5G, namely the Standalone Non-Public Network (SNPN) and the Public Network Integrated NPN (PNI-NPN) [3, §5.30]. Both deployment options present different advantages, challenges, and use cases.

Standalone NPN

A SNPN is a 5GS for private use which leverages a novel approach for identifying such network, that is, via the combination of a PLMN identifier and a network identifier (NID). Such (combined) ID is broadcast by the RAN infrastructure to enable authorized UEs to discover the SNPN, thus starting the secured attach procedure which makes the difference between a NPN and a PLMN. Indeed, it holds a separated subscriber list, thus a UE that aiming at connecting to the network and accessing its functionalities must be subscribed to the SNPN.

Typically, the SNPN is managed and operated entirely by a NPN-Op that can be the enterprise customer itself or a delegated third-party company. As a matter of fact, in general a SNPN does not share any functionality with the PLMN; the RAN is the only infrastructure element that may be in common, although it may be also dedicated. In the latter case, the NPN-Op utilizes a separate portion of the spectrum, which can be licensed from the PLMN Operator (PLMN-Op), obtained from the Regulatory Authorities or, if available, be part of unlicensed frequency bands. A further characteristic defining an SNPN is the confined radio coverage, as it is limited to the geographical area of interest to the enterprise customer. To guarantee connectivity outside the premises, the UE needs two subscriber identity modules (SIMs), having a separate subscription to a PLMN or a roaming plan that enables the mobility between networks.

A SNPN type of deployment provides a valid solution for an enterprise or organization that require a fully customized configuration and a tight control over the mobile network: these needs also justify the additional overhead of setting up and manage an independent 5GS infrastructure. Another advantage in using SNPN is its stronger protection of sensitive and proprietary data, which are handled locally accordingly to the company security policies.

Public Network Integrated NPN

In many use cases a certain degree of integration between the NPN and the PLMN can be desirable, especially when the private entity does not shoulder the burden of the entire NPN management. Two ways to support a NPN within the network of a PLMN-Op:

1) via configuration of closed access groups (CAG) at access stratum level;
2) via deployment of dedicated network slices for non-public use or dedicated Data Network Names (DNN).

We observe that, in both cases,

- the spectrum is owned by the PLMN-Op, and can be shared or reserved across the networks;
- the non-public users need to subscribe to the same PLMN ID as public users – it is up to the network to enforce user segregation in a correct fashion;
- the maximum level of integration is achieved when all physical infrastructures are shared among both networks, so that the NPN is entirely hosted by the PLMN. Nevertheless, it is reasonable to assume that the a dedicated user plane function may be deployed close to the serving RAN, i.e., at the so-called edge cloud.

It is also worth mentioning that additional authentication means are provided to the private network tenants of a PNI-NPN, based on the tenant's own authentication servers, in order to ensure the enforcement of user access control policies by the PLMN-Op.

The Emerging Role of Hyperscalers

Unlike traditional mobile systems for PLMNs, 5G NPNs aim at reaching many independent customers, which are typically much more than the amount of existing PLMN-Op. However, as opposed to a traditional PLMN-Op, the NPN-Op are not technology experts in most cases: this is why new actors come into play. For example, the Regulatory Authorities now play an instrumental role by reserving spectrum portions for direct lease by private entities instead of allocating it to a handful of national operators. Especially in countries where the spectrum can be leased for private use, the traditional role of the PLMN-Op is challenged by independent system integrators and, lately, by *hyperscalers* such as, e.g., Amazon Web Services (AWS) and Microsoft, that are companies that provide cloud, networking, and Internet services at on a very large scale by offering organizations access to infrastructure as a service (IaaS).

As a matter of fact, (both public and private) cloud-based environments can be used for hosting the instances of virtual mobile core networks for SNPN deployments. In particular, as public cloud providers, the hyperscalers typically provide the private entities with a hybrid cloud environment, whereby a SNPN can be split between a remote site featuring non-critical NFs and an edge apparatus comprising the critical NFs.

The role of hyperscalers is yet to be fully unleashed, though they have already entered the mobile network market.[1] Specifically, their experience in the automation field (though not related to mobile networks) gives them an advantage, possibly pushing their proprietary solutions as *de facto* standards.

[1]See, e.g., https://aws.amazon.com/it/private5g/. Last visited: January 31, 2022.

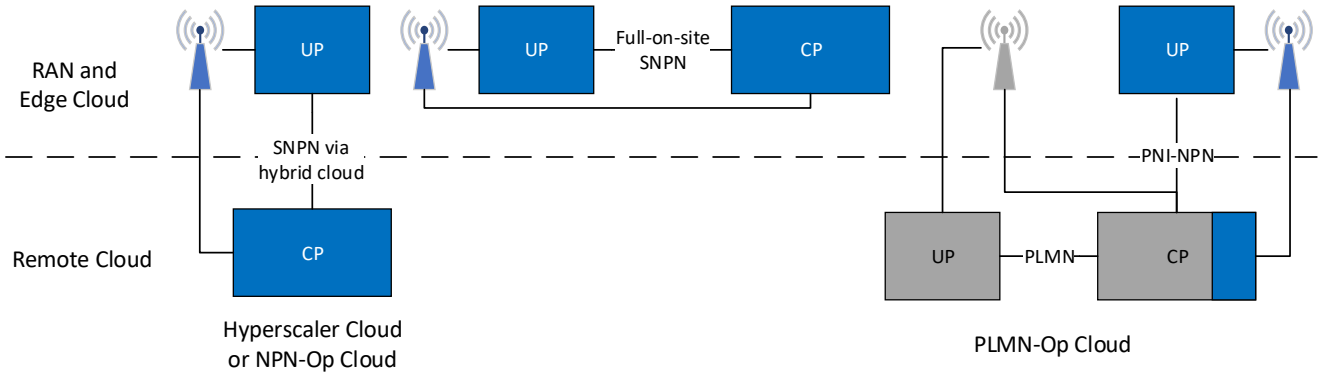

Fig. 3. 5G NPN deployment options. The left-most solution is the SNPN solution powered by the hybrid cloud. The one in the center is the full-on-site SNPN, where the entire SNPN is deployed at the edge cloud, in proximity of the RAN. Finally, the right-most solution is a PNI-NPN where the grey blocks represent the PLMN domain and the blue ones a private network slice comprising the central PLMN CP as well as dedicated user plane function at the edge.

Similarly to the case of PNI-NPNs, the private entity can leverage SNPN powered by hyperscalers to offload part of the network management. This comes at the price of sharing part of the 5G NFs with other tenants.

Summary and Observations

An overview of previously mentioned NPN configurations is provided in Fig. 3 and Table I. In particular, in the table we summarize each NPN configuration feature along with its degree of customizability and the management effort required from the point of view of the NPN-Op. A SNPN deployment provides a much higher level of customizability of the network that can be easily tailored to the needs of the customer and the constraints of the specific use case. As a trade-off, the NPN-Op is required to actively partake in the management of the infrastructure by establishing and maintain personalized configurations, network services and traffic policies. This burden can be partially taken by an hyperscaler. In contrast, by using pre-existing public infrastructures, a PNI-NPN deployment offers a lower operating expenditure (OPEX) and capital expenditure (CAPEX) solution as well as catering to private entities that do not have the expertise and technical know-hows. It is the PLMN-Op that maintains most of the management responsibilities and customization options, with only a small set of capabilities that might be exposed to the private network tenant using specific APIs. In fact, a PLMN-Op is not likely to accept anyone else to orchestrate their infrastructure or accessing their proprietary management services with the risk of compromising nation-wide and mission-critical systems [2].

Testbed Setup

In order to emulate the evolution of NPN architectures and their management means towards zero-touch principles, we have been designing and implementing a research testbed, which is continuously integrated. In this section, we present the current testbed architecture as well as some preliminary testing results on 5G SNPN automated provisioning.

Testbed Architecture

The testbed is implemented at Athonet premises, and is inspired to the work done in [13]. At the time of writing, it comprises two physical machines:

- a Dell PowerEdge R640 server based on two Intel(R) Xeon(R) Silver 4210R CP @ 2.40 GHz and 64 GB of memory, and
- a commodity Desktop PC equipped with an Intel(R) Core(TM) i7-2600 @ 3.40 GHz and 16 GB of memory running Ubuntu 20.04.

The testbed aims at emulating a real world scenario wherein a NPN may be deployed, in small. In particular, the server node simulates a remote cloud datacenter, while the PC node simulates a constrained edge server deployed on the premises of the private entity or network tenant.

The infrastructure is fully virtualized as per ETSI NFV specifications. In particular, OpenStack[2] is utilized as the NFV Infrastructure (NFVI) and the Virtual Infrastructure Manager (VIM). The NFVI is composed of the physical hardware resources, including storage, computing and networking, and by the virtualization layer which abstracts the underlying hardware and provides the virtual resources and environment wherein the VNFs carry out their lifecycle. The VIM is responsible for the management of the virtual resources, their allocation and usage by the VNFs.

For the VNF managers and NFV orchestrator (NFVO), Open Source MANO (OSM) is employed. OSM is an open source and community-led ETSI-hosted project that provides a NFV MANO software stack aligned to the latest ETSI NFV information model and architecture. OSM Release TEN was chosen, since it provides all the required features and bring significant improvements compared to previous releases, mainly in the scaling functionalities and in the operational dashboard. OSM is based on three main modules.

1) The Resource Orchestrator (RO) is responsible for managing the resources across multiple VIMs by using a set of plug-ins specific to different underlying VIMs.

[2]https://www.openstack.org/software/. Last visited: January 31, 2022.

TABLE I
NPN CONFIGURATION OPTIONS AND THEIR IMPACT ON MANAGEMENT AND ORCHESTRATION.

Deployment Option	RAN	Core Network	MEC Platform	Customizability	Management effort (NPN-Op side)
SNPN	Shared or dedicated	Dedicated (on site or via hybrid cloud)	Dedicated (on site)	Medium/High: NPN-Op can obtain customized network configurations based on its needs	Medium/High: SNPN owner needs to take care of network management (medium if assisted by hyperscaler)
PNI-NPN	Shared (w/ or w/o CAG)	Shared (network slice or dedicated DNN)	Shared or dedicated (on site)	Low: most of the network is physically shared and partially logically shared, thus has feature constraints	Low: most of the network is centrally managed by the PLMN-Op

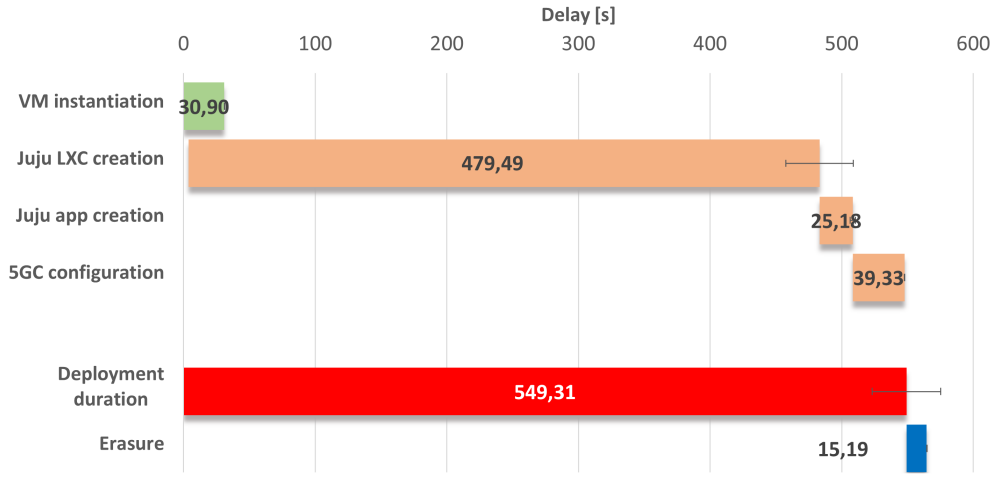

Fig. 4. Time delays associated with the 5GC deployment and erasure.

2) The VNF Configuration and Abstraction (VCA) is an abstraction of a generic VNF Manager. By default the framework used is called Juju and is implemented through a set of scripts called charms.
3) The Lightweight Lifecycle Manager (LCM) is responsible for the lifecycle of NFs, including: instantiation, scaling, updating, and decommissioning. It is also responsible for the interconnection of multiple VNFs to create end-to-end Network Services (NS).

Recently, OSM was successfully tested for zero-touch automation purposes, being capable to support MEC and O-RAN use cases.[3]

Results

In such an environment, we have been emulating the NPN architectures presented in the previous sections. Both SNPN and PNI-NPN deployment models have been tested on the infrastructure and their deployment automated using OSM descriptors. As for the SNPN model, the entirety of the CN functionalities are deployed on the edge node. As for the PNI-NPN model, the NPN is served as a network slice of a PLMN deployed on the remote cloud, with which it shares all the control plane functionalities. Instead, the user plane functionalities of the NPN are not shared and are deployed independently on the edge cloud in order to preserve the advantages of a MEC architecture. Both proprietary and open-source 5GC implementations have been tested.

In Fig. 4, we show the average time delays for 10 consecutive 5GC deployments and erasures – extending the similar results obtained for 4G system in [14]. The total deployment duration (in red) is the sum of the VM instantiation time (in green) and the configuration time of the VNF Managers and the VNFs themselves (in orange). The configuration delay is the time necessary for Juju to create a Linux container (LXC) in which to install and run the charm responsible for the 5GC configuration. Before executing the charm, several time-consuming steps are carried out. The first and most demanding one is the download of the LXC's cloud image followed by the update and upgrade of the installed packages. This time delay is an acknowledged limitation of OSM and, though mitigation strategies exist, they shall not be used in production environments.[4]

ENVISIONED FUTURE CHALLENGES

A smooth OAM for 5G NPNs represent the key challenge for the effectiveness of mobile systems for private use. To face

[3]See https://www.etsi.org/newsroom/press-releases/1863-2020-12-open-source-mano-release-nine-fulfils-etsi-s-zero-touch-automation-vision-ready-for-mec-and-o-ran-use-cases. Last visited on January 31, 2022.

[4]https://osm.etsi.org/docs/vnf-onboarding-guidelines/08-advanced-charms.html. Last visited: January 31, 2022.

this challenge, NPNs need to embrace automation in network and service management and orchestration, so to be seamlessly integrated with the incumbent infrastructure of the NPN-Op as well as to implement extensive zero-touch management approaches. A few crucial challenges need to be faced in the coming years in this regard.

- *Automation easiness* – From the point of view of a NPN-Op, which is likely to be non expert of mobile telecommunications, the setup of a E2E OAM may non be trivial. Many heterogeneous stakeholders such as the network infrastructure suppliers, the cloud providers, the NFV MANO providers, need to collaborate to build an holistic vision towards a solution of this problem.
- *Normative work by SDOs* – On the other hand, the OAM standards need to be harmonized in the scope of NPNs. In particular, the segregation of duties between 3GPP OAM and ETSI NFV MANO as well as the simplification of ETSI MEC OAM deserves attention from the involved SDOs. The 3GPP will be in the forefront of this challenge, looking at the study item activity carried out in Rel-17 [15].
- *New technological challenges* – The compatibility between public and private cloud infrastructure providers and the associated orchestration tools will be a key factor to preserve the openness of the NPN framework.

REFERENCES

[1] M. Wen *et al.*, "Private 5G Networks: Concepts, Architectures, and Research Landscape," *IEEE J. Sel. Topics Signal Process.*, pp. 1–1, 2021.

[2] J. Prados-Garzon *et al.*, "5G Non-Public Networks: Standardization, Architectures and Challenges," *IEEE Access*, vol. 9, pp. 153 893–153 908, 2021.

[3] *System architecture for the 5G System (5GS)*, 3GPP Tech. Spec. 23.501, Rev. 16.11.0, Dec. 2021.

[4] J. Ordonez-Lucena *et al.*, "The use of 5G Non-Public Networks to support Industry 4.0 scenarios," in *Proc. of 2019 IEEE Conf. on Standards for Commun. and Networking (CSCN)*, 2019, pp. 1–7.

[5] S. Kekki *et al.*, "MEC in 5G Networks," ETSI MEC ISG, Whitepaper, Jun. 2018. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

[6] A. Garcia-Saavedra and X. Costa-Perez, "O-RAN: Disrupting the Virtualized RAN Ecosystem," *IEEE Commun. Standards Mag.*, pp. 1–8, 2021.

[7] *Management and orchestration; Architecture framework (Release 16)*, 3GPP Tech. Spec. 28.533, Rev. 16.4.0, Jun. 2020.

[8] *Mobile Edge Management; Part 1: System, host and platform management*, ETSI Group Spec. 010-1, Rev. 1.1.1, Oct. 2017.

[9] "O-RAN Use Cases and Deployment Scenarios," O-RAN Alliance, Whitepaper, Feb. 2020.

[10] VMware Inc., "VMware Telco Cloud Automation; Operational agility through unified orchestration and automation for the Telco Cloud." [Online]. Available: https://telco.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmw-telco-cloud-automation.pdf

[11] G. M. Yilma *et al.*, "Benchmarking open source NFV MANO systems: OSM and ONAP," *Computer Communications*, vol. 161, pp. 86–98, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366420305946

[12] A. Aijaz, "Private 5G: The Future of Industrial Wireless," *IEEE Ind. Electron. Mag.*, vol. 14, no. 4, pp. 136–145, 2020.

[13] B. Nogales *et al.*, "Design and deployment of an open management and orchestration platform for multi-site NFV experimentation," *IEEE Commun. Mag.*, vol. 57, no. 1, pp. 20–27, 2019.

[14] F. Asquini *et al.*, "An ETSI NFV Implementation for Automatic Deployment and Configuration of a Virtualized Mobile Core Network," in *Proc. of 2021 17th Int. Conf. on Wireless and Mobile Computing, Networking and Commun. (WiMob)*, Bologna, Italy, 2021, pp. 357–362.

[15] *Study on management of Non-Public Networks (NPN); (Release 17)*, 3GPP Tech. Rep. 28.807, Rev. 17.0.0, Dec. 2020.