IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 5, 2021, accepted July 13, 2021, date of publication July 26, 2021, date of current version August 5, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3100120

Multi-Domain Solutions for the Deployment of Private 5G Networks

XI LI[1], CARLOS GUIMARÃES[2], GIADA LANDI[3], JUAN BRENES[3], JOSEP MANGUES-BAFALLUY[4], JORGE BARANDA[4], (Senior Member, IEEE), DANIEL CORUJO[5], (Senior Member, IEEE), VITOR CUNHA[5], JOÃO FONSECA[5], JOÃO ALEGRIA[5], AITOR ZABALA ORIVE[6], JOSE ORDONEZ-LUCENA[7], PAOLA IOVANNA[8], CARLOS J. BERNARDOS[2], ALAIN MOURAD[9], AND XAVIER COSTA-PÉREZ[1,10,11], (Senior Member, IEEE)

[1]NEC Laboratories Europe, 69115 Heidelberg, Germany
[2]Department of Telematic Engineering, Universidad Carlos III de Madrid (UC3M), 28911 Leganés, Spain
[3]Nextworks, 56122 Pisa, Italy
[4]Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), 08860 Castelldefels, Spain
[5]Instituto de Telecomunicações and Universidade de Aveiro, 3810-193 Aveiro, Portugal
[6]Telcaria Ideas S.L., 28911 Leganés, Spain
[7]Telefónica I+D, 28050 Madrid, Spain
[8]Ericsson, 56124 Pisa, Italy
[9]InterDigital, London EC2A 3QR, U.K.
[10]i2cat, 08034 Barcelona, Spain
[11]ICREA, 08010 Barcelona, Spain

Corresponding author: Xi Li (xi.li@neclab.eu)

This work was supported in part by the European Commission (EC) H2020 5GPPP 5Growth Project under Grant 856709, and in part by the H2020 5G European Validation platform for Extensive trials (5G EVE) Project under Grant 815074.

ABSTRACT Private 5G networks have become a popular choice of various vertical industries to build dedicated and secure wireless networks in industry environments to deploy their services with enhanced service flexibility and device connectivity to foster industry digitalization. This article proposes multiple *multi-domain* solutions to deploy *private 5G networks for vertical industries* across their *local premises* and interconnecting them with the *public networks*. Such scenarios open up a new market segment for various stakeholders, and break the current operators' business and service provisioning models. This, in turn, demands new interactions among the different stakeholders across their administrative domains. To this aim, three distinct levels of multi-domain solutions for deploying vertical's 5G private networks are proposed in this work, which can support interactions at different layers among various stakeholders, allowing for distinct levels of service exposure and control. Building on a set of industry verticals (comprising *Industry 4.0, Transportation and Energy*), different deployment models are analyzed and the proposed multi-domain solutions are applied. These solutions are implemented and validated through two proof-of-concept prototypes integrating a 5G private network platform (*5Growth* platform) with public ones. These solutions are being implemented in three vertical pilots conducted with real industry verticals. The obtained results demonstrated the feasibility of the proposed multi-domain solutions applied at the three layers of the system enabling various levels of interactions among the different stakeholders. The achieved end-to-end service instantiation time across multiple domains is in the range of minutes, where the delay impact caused by the resultant multi-domain interactions is considerably low. The proposed multi-domain approaches offer generic solutions and standard interfaces to support the different private network deployment models.

INDEX TERMS Non-public networks, multi-domain, 5G and beyond systems, vertical services.

I. INTRODUCTION

The 5G and beyond systems are rapidly gaining recognition as an all-inclusive service platform for industry digitization. The standardization of 3GPP Rel-16 and Rel-17 features provides the necessary capabilities for the support of mission-critical services, enhanced mobile broadband services (eMBB), massive machine type communications (mMTC), and ultra-reliable low-latency communications (URLLC). This digital transformation enables

The associate editor coordinating the review of this manuscript and approving it for publication was Anandakumar Haldorai.

service innovation, opening up new use cases from a wide variety of industry verticals, including manufacturing, transportation, or energy sectors, utilities, public infrastructures (e.g., airport, railway, seaport), public safety agencies, and others.

Although 5G built-in capabilities provide the enhanced bandwidth, increased reliability, and lower latency that various industry verticals demand, fulfilling these requirements is not always feasible with the sole use of public networks, also known as Public Land Mobile Networks (PLMNs). On the one hand, the PLMN coverage is limited to the mobile network operator's (MNO's) administrative domain, which typically excludes vertical premises where vertical devices operate (e.g., industrial factories, campus, transportation hubs). On the other hand, the archetypal design of PLMNs is traditionally used to deliver broadband mobile communication for public users and services, and it may not support the dedicated and critical wireless communication requirements that some verticals require, especially in terms of performance (e.g., latency, reliability, availability) and functionality (e.g., standalone management of private devices with respect to mobility and subscription data, separated from the management of public subscribers).

The limited MNO's service footprint, together with the exclusive need of verticals of demanding dedicated and secure 5G network capabilities, make private 5G networks an attractive choice to support industry use cases. These private 5G networks [1], [2], referred to as Non-Public Networks (NPNs) in 3GPP terminology, are the most preferred way of delivering wireless connectivity for the vertical industries. Today, different deployment scenarios have been defined for NPNs, with different pros/cons each. However, it is up to each industry vertical to decide on the most appropriate scenario for their individual use cases, analyzing: *(i)* the functional and non-functional requirements of individual use cases; *(ii)* what costs and resources the vertical is willing to invest to build and run an NPN infrastructure; and *(iii)* how much control the vertical wants to take over of the NPN at operation time, e.g., from simple access to monitoring data to retaining full management of the NPN.

According to 3GPP Rel-16 specifications [3], NPN can be of two of types: *(i)* standalone NPN (SNPN), i.e., a NPN deployed as an isolated and standalone network which does not rely on PLMN provided network functions; and *(ii)* Public Network Integrated NPN (PNI-NPN), i.e., a NPN deployed in conjunction with a PLMN, which requires certain level of integration and infrastructure sharing with the PLMN. In the latter cases, proper solutions are required to implement the PNI-NPN at the data-plane and control plane as well as at the management plane. Although 3GPP defines some basic means to deploy a PNI-NPN, implementing End-to-End (E2E) solutions in the real 5G systems is still a big challenge. Some early initiatives already started investigating potential solutions for implementing a PNI-NPN, mainly following three different approaches. First, by setting up dedicated network slice(s) to serve the NPN (e.g., [4] and 5G-VINNI [5]). Second, by integrating the NPN as a non-3GPP access network (such as, Wi-Fi and LiFi) to deploy private 5G networks (e.g., 5G-CLARITY [6]). And third, by setting up a dedicated Access Point Name (APN) or Packet Data Network (PDN) to serve NPN customers by subscriber provisioning (e.g., SIM cards) or roaming provided by the MNOs. Complementary to this, several research projects under the EU Horizon 2020 5G PPP program, are working on developing envisaged solutions that leverage NPN deployments for several use cases, such as the ones listed below.

1) 5GZORRO [7] is focused on the design of a security and trust framework, integrated with 5G service management platforms, to demonstrate Zero Trust principles in distributed multi-stakeholder environments and automated security management to ensure trusted and secure execution of offloaded workloads across domains in 5G networks.
2) 5G-RECORDS [8] is focused on embracing some of the most challenging scenarios in the context of professional content production environments, where the use of NPNs in the form of network slicing to guarantee Quality of Service (QoS) is complemented with synchronization and timing parameters.
3) FUDGE-5G [9] is focused on highly customized cloud-native deployment of NPNs for realizing highly significant five vertical use cases featuring diverse range of network and radio requirements, deployment, and configurations options, representing a very high innovation and business impact for the private 5G network market.

Finally, quite a number of industry use cases proposed in the scope of 5G-INDUCE [10], 5G-TOURS [11], [12], 5G-VICTORY [13] and 5G-SMART [14] projects are being considered to take good advantage of NPN capabilities for e.g., accommodating more stringent security and privacy requirements, providing highly customizable networks, etc.

So far, most of the current research activities are focused on enhancing the 5G capabilities on network slicing solutions and introducing additional functionalities to improve security, automation, performance isolation and assurance, device and data management, fog/edge deployments for industrial applications, etc., to support NPNs. However, the real deployment of the NPNs still face many open challenges, especially in the cases of PNI-NPN, where there are not yet specific and standard interfaces defined to connect the NPNs with the PLMNs. This depends on the roles of all the involved stakeholders from both the NPN and PLMN sides, and the information that each side will expose to exchange/share with other entities, and the level of trust and business relationships along with the Service Level Agreements (SLAs) between the NPN owner (e.g., verticals) and the MNOs. In particular, the PNI-NPN opens a new market segment where private enterprise and industrial networks can have a bigger role [15]. New stakeholders (such as, third-parties NPN service provider, network slice provider, NPN operator and integrator) can enter in this new market segment and take part in the revenue stream.

This is disrupting the current business and service provisioning models of MNOs (which are mainly on the network services level) and, therefore, requires new levels of interactions and new interfaces among the different stakeholders and their owned domains. In turn, new multi-domain solutions are needed to enable such new interactions required at different layers of the system among various stakeholders, incorporating the new interfaces supporting different levels of service exposure and control.

To address this specific challenge, this paper proposes three different levels of multi-domain interactions and the corresponding interfaces to implement the PNI-NPNs. The proposed solutions focus on the management plane functions and on the development of standard interfaces for each multi-domain interaction. They are aligned with the architecture design of the 3GPP and ETSI NFV. These solutions are implemented in the 5Growth service platform [16] (being developed under the EU 5Growth project[1]), which provides a SDN/NFV-based 5G Mobile Transport and Computing Platform and offers service and network slicing functionalities that can be mapped to the role of different stakeholders. For the aim of validation, the proposed multi-domain solutions are implemented and experimentally evaluated through two proof-of-concept (PoC) prototypes, where the 5Growth platform is used to manage the NPN domain and also interacts with external 5G platforms to deploy vertical services across the NPN and PLMN domains. The external 5G platforms used in the PoCs, serving as the management platform of the MNOs belonging to the PLMN, are based on *(i)* 5G EVE platform [17], which offers a 5G end-to-end facility for performing experimental testing and validation of 5G technologies; and *(ii)* a network slicing platform developed for the scope of this work, which is based on ETSI Open Source MANO (OSM)[2] and provides network slicing services.

In summary, the contributions of this paper consist of:

1) An overview of different NPN deployment scenarios set as baselines by the MNOs and relevant industry for a, given in Section II. Some possible variants for specific implementation are also identified.
2) Proposals of three different levels of multi-domain solutions – including corresponding interfaces offers – for the PNI-NPN integration, presented in Section III.
3) An experimental validation – based on two Proof-of-Concept (PoC) prototypes – of our proposed multi-domain solutions developed in the 5Growth platform, to implement two different NPN deployment scenarios. The PoCs and experimental results are described in Section IV. The experiments results focus on the E2E service instantiation and termination times across NPN and PLMN domains, including a detailed time profiling of the different steps of the service instantiation workflow, and further analyzing the resultant service performance and overheads.
4) An analysis, by taking examples in Section V, of three real vertical pilots and associated use cases across Industry 4.0, Transportation, and Energy verticals, discussing their need for a specific NPN deployment model. These pilots select the most suitable multi-domain solution(s) for their chosen NPN deployments to support their specific service use cases and requirements.

[1] http://www.5growth.eu/
[2] https://osm.etsi.org/

II. NPN DEPLOYMENT SCENARIOS

A NPN is a private 5G network deployed for the sole use of a given business-to-business (B2B) customer such as a vertical. NPNs can be deployed in a wide variety of forms, depending on the vertical use cases to be supported as well as the regulatory issues in place [18]. In a bid to simplify this casuistry, the 5G Alliance for Connected Industries and Automation (5G-ACIA) has defined a set of baseline deployment scenarios for NPNs [19]. These scenarios have become *de-facto* in the telco industry, and have been used as reference for discussion in other works. In [20], the authors provide a comparative analysis of these scenarios when applied in Industry 4.0 environments, discussing their pros and cons using different criteria, including QoS customization, security, service continuity and entry barriers, among others. Reference [1] discusses these scenarios from a management view, relating them with plausible operational and business models. Finally, [5] depicts provisioning mechanisms for PNI-NPN, clarifying what NPN components should be provided by the PLMN and how network slicing can be applied on them.

The GSM Association (GSMA), which is a telco industry association representing the interests of MNOs worldwide, has recently published a white paper on 5G industry campus networks [21]. Leveraging the state-of-the-art work mentioned above, together with the guidelines from the MNO perspective (e.g., standardization readiness, case studies, and lessons learned), this GSMA white paper lays out the key factors that may influence the NPN deployment choices.

In this section, we take the guidelines from operator roll-out strategies captured in the GSMA white paper [21] as well as the recommendations from relevant industry fora (e.g., 5G-ACIA) to identify and elaborate on representative, future-proof deployment scenarios for NPNs. It is important to note that they only represent a set of baseline scenarios recommended for the deployment (which however cannot be standardized, neither in 3GPP nor other standard development organizations, as the deployment is highly dependent on the vertical customer and related use cases) and are open for different variations, as discussed at the end of this section. Following up this criterium, a total of four scenarios have been selected, all captured in Figure 1: (a) and (b), belonging to the SNPN category, and (c) and (d), belonging the PNI-NPN category. For all these deployment scenarios, we assume an archetypal NPN architecture, with the NPN formed by the following functional components:

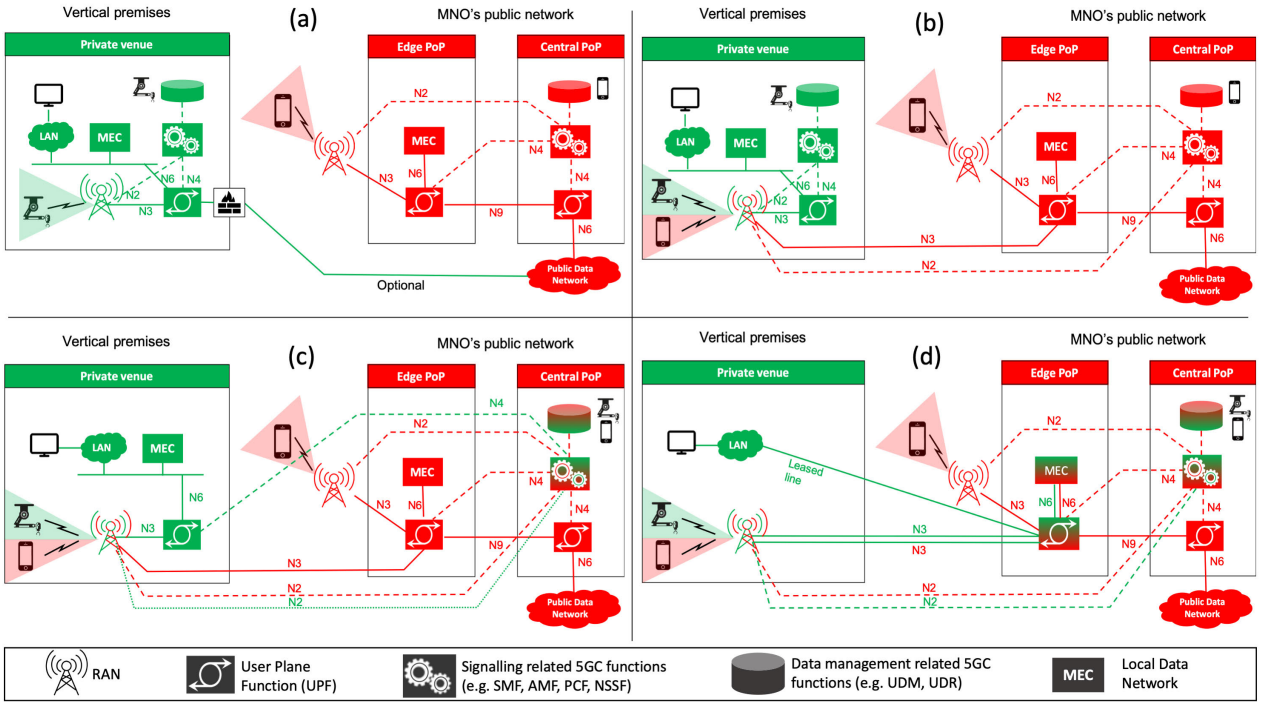


FIGURE 1. NPN deployment scenarios: (a) SNPN without RAN sharing; (b) SNPN with RAN sharing; (c) PNI-NPN with RAN and 5GC control plane sharing; (d) PNI-NPN with full sharing.

- 3GPP 5G radio access network (RAN), deployed with one or more Next Generation Node Bs (gNBs). A gNB is a 5G base station providing New Radio (NR) based connectivity towards the end devices.
- 3GPP 5G core network (5GC) [3], relying on the principle of control-user plane separation. On the one hand, the 5GC user plane consists of one or more instances of the User Plane Function (UPF). On the other hand, the 5GC control plane is formed of cloud-native network functions providing both signalling and data management functionality. Examples of signalling related 5GC functions are Session Management Function (SMF), Access and Mobility Function (AMF), Policy Control Function (PCF) and Network Slice Selection Function (NSSF). Examples of data management related 5GC functions include Unified Data Management (UDM) and Unified Data Repository (UDR).
- A local data network, providing a Multi-Access Edge Computing (MEC) hosted execution environment for vertical service applications.

In the following, we provide an overview of the scenarios represented in Figure 1. The discussion will focus on the deployment aspects, leaving out any further insights on the operational aspects (i.e., which stakeholder is in charge of managing individual components). For more information on these operational aspects, see [1] and 3GPP TS 28.557 [22].

In the **SNPN without RAN sharing scenario** (Figure 1 (a)), all the NPN components are deployed within the vertical premises, resulting in a E2E, in-house 5G network. The complete separation between the NPN and the PLMN is manifested in two facets. First, the assignment of dedicated spectrum to the NPN, either private (i.e. obtained from the local regulator) or licensed (i.e. leased from the MNO). Secondly, the lack of presence of PLMN provided components along the entire NPN, from access to the local data network; indeed, all the NPN components are owned by the vertical.

In the **SNPN with RAN sharing scenario** (Figure 1 (b)) the on-premise gNB is made available for RAN sharing, with the vertical playing the role of neutral host. The neutral host represents a role whereby the site owner invests in on-premise network infrastructure, which is used for its own purposes, and also leased to different MNOs. In this scenario, the leasing can include cell site infrastructure sharing, i.e. passive RAN sharing, and Multiple Operator Core Network (MOCN), i.e. active RAN sharing. The neutral hosting model is beneficial for both the vertical and the MNOs. On the one hand, the vertical (neutral host) monetizes the in-house infrastructure by selling mobile coverage solutions to the different hosted MNOs. On the other hand, the MNO can increase its coverage area without the need to invest in on-premise equipment, thus expanding its service footprint at a much more reduced cost. The reason why this NPN deployment scenario is a SNPN is because the gNB, which is used to serve both vertical devices and UEs from hosted MNOs, is owned by the vertical and used independently from MNO's gNBs.

Unlike the two above-referred scenarios, in the PNI-NPN category it is assumed that some NPN components are

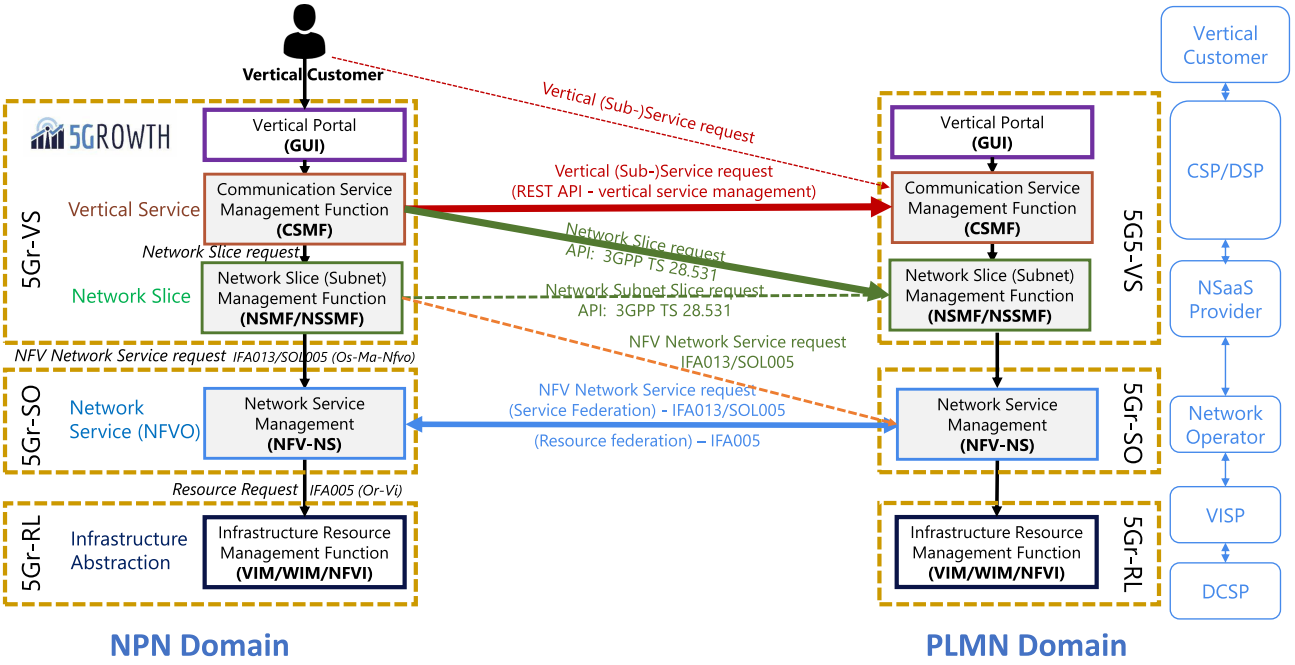


FIGURE 2. Multi-domain solutions for NPN and PLMN integration (PNI-NPN).

provided by the PLMN. In the **PNI-NPN with RAN and 5GC control plane sharing scenario** (Figure 1 (c)), these NPN components are the 5GC control plane, which is entirely hosted by the MNO's infrastructure. This means that subscription data and signaling traffic from vertical devices is transferred to the PLMN, thereby leaving the vertical premises. The **PNI-NPN with full sharing scenario** (Figure 1 (d)) goes a step further, keeping UPF and MEC out of the vertical premises as well. This means that all NPN components are shared with the PLMN. With this setup, user plane flows are also forwarded externally to the PLMN, raising some concerns about the delay budget (latency can be a major problem, depending on the distance between the premises and the MNO's edge node). In these two PNI-NPN scenarios, the MNO leverages network slicing and/or Data Network Name (DNN)-based solutions [3] for the provision of PLMN provided components to the NPN.

The vertical pilots presented in this paper (see Section V) leverage on the four deployment scenarios described above. The selection of one or another NPN deployment scenario will not only characterize the performance of individual use cases, but also the level of interaction between the industry vertical and the MNO. It is worth noting that for the PNI-NPN scenarios, in this work we also go beyond the state-of-the-art, proposing deployment variants that are relevant for some use cases. Examples of these variants is transport network sharing (the transport substrate connecting the vertical premises with MNO's edge site is shared between NPN and PLMN). While for most of the realizations of scenario (c) it is assumed that the transport network is dedicated, based on the use of leased lines or hard-slicing solutions (e.g., dedicated wavelength), there are also possibilities to share the transport network in the quest of a much more cost-efficient solution. This sharing guarantees traffic isolation between public and private subscribers, while exploiting multiplexing gains at the same time. One of the 5Growth vertical pilots presented in this paper proposes this variant and has developed a shared transport network solution to support the needs of their vertical use cases (see Section V).

III. MULTI-DOMAIN OPTIONS FOR PUBLIC-PRIVATE NETWORK INTEGRATION

This section presents our proposed multi-domain solutions to be supported on top of the 5Growth platform for the integration of a NPN with PLMNs, motivated by the business needs of different verticals and by new or extended roles of different stakeholders. We start with a high level introduction of the architecture of the 5Growth platform and then we explain in detail the multi-domain solutions.

A. 5GROWTH SERVICE PLATFORM ARCHITECTURE

This section presents the high level architecture of the 5Growth service platform [16], [23], its baseline leveraging from the 5G-TRANSFORMER (5GT) platform [24]. On top of it, different multi-domain solutions for public-private network integration are developed. The architecture, as shown in Figure 2, consists of the following three fundamental layers.

Vertical Slicer (5Gr-VS), acting as one-stop shop entry point for verticals to request custom network slice(s)

tailored to their needs. At its northbound, the Vertical Slicer provides a vertical portal for all the verticals to request the provisioning and management of vertical services through a simplified and vertical-oriented interface. It provides a catalogue of Vertical Service Blueprints (VSB), as service templates to specify service logic with composed vertical applications and the requirements of vertical services. The vertical can select the required service from this catalogue and customize it by defining a Vertical Service Descriptor (VSD) with additional service-level details (e.g., dimensioning of the service, required level of isolation and security, its target coverage area, IP addresses for management systems, etc). Based on that, the 5Gr-VS then builds customized network slices. In our system, the definition of network slices is aligned with the model from 3GPP [25]. To manage them, the 5Gr-VS implements the network slice management functionalities to identify the kind of network slice(s) required to provision the requested vertical service and to manage the lifecycle of the network slices and their network slice subnets, in case of composed network slices. These functionalities can be mapped into the Communication Service Management Function (CSMF), Network Slice Management Function (NSMF) and Network Slice Subnet Management Function (NSSMF) defined by 3GPP [26], and it includes the procedures to instantiate new network slice (or subnet) instances, modify or terminate them, according to the directives received by the vertical service management logic. In this sense, the 5Gr-VS is able to handle different kinds of mapping between vertical services and network slices.

Service Orchestrator (5Gr-SO) provides both network service and resource orchestration capabilities of a NFV orchestrator (NFVO) to instantiate and manage network slices, which are deployed as NFV-defined Network Services (NFV-NS), over shared resources across single or multiple administrative domains. More specifically, it is in charge of *(i)* E2E orchestration of NFV-NSs and management of their service lifecycle operations; and *(ii)* deciding the optimum placement of the VNFs and assign corresponding virtual resources across multiple domains, based on service requirements, the service catalogue and the resource availability offered by each of the domains. Additionally, the 5Gr-SO provides multi-domain network service orchestration through federation. In this direction, the 5Gr-SO interacts with 5Gr-SOs of other administrative domains through its eastbound-westbound interface on the E2E deployment of the network services. This interface is mostly based on ETSI NFV specifications, such as ETSI IFA013 [27], developed with an extension to coordinate the interconnection of VNFs of the same NFV-NS deployed in multiple administrative domains, as described in [28].

Resource Layer (5Gr-RL) is responsible for managing the infrastructure at the vertical sites and the required transport resources to interconnect them. The 5Gr-RL layer hosts all the compute, storage and networking physical and virtual resources where network slices and E2E services are executed. It manages all the infrastructures as a Single Logic Point of Contact (SLPOC), providing a unified abstraction view of the managed resources to the 5Gr-SO. The SLPOC is connected to different plugins: the transport WAN Infrastructure Manager (WIM) plugins, the Virtual Infrastructure Manager (VIM) plugin, and the MEC plugin, the RAN plugins. These plugins expose abstracted resources view to the SLPOC and also handle the configuration of the underlying resources.

The three layers and their internal functional entities can be owned and operated by different stakeholders. The mapping of the building blocks to different stakeholders is shown in Figure 2, which is also aligned with the view of the 3GPP [26]. The CSMF function inside the 5Gr-VS can be managed by a Communication Service Provider (CSP) or a Digital Service Provider (DSP), while NSMF/NSSMF function can be run by a Network Slice provider (NSP), who offers a network slice along with the services that it may support and configure. The service orchestration layer is usually managed by network operators (NOPs), while the resource layer is under the control of different infrastructure owners, namely Virtualisation Infrastructure Service Provider (VISP) and Data Centre Service Provider (DCSP).

B. MULTI-DOMAIN SOLUTIONS

The proposed solutions address three different levels of multi-domain interaction, including: (*i*) *Communication Service Level*; (*ii*) *Network Slice Level*; and (*iii*) *Network Service Level*, as shown in Figure 2. In all of these approaches, we apply the same mapping of the building block functions to different stakeholders as described above, i.e., the CSMF function will be managed by a CSP, while NSMF function will be provided by a NSP and the service orchestration function (i.e., NFVO) are offered by private or public network operators (NOPs). Depending on the business cases, one or multiple of these functions can be included at each NPN and PLMN domain. For instance, the verticals can have contracts with a third party CSP or NSP to compose service requests to the PLMN, or a NPN operator can manage the whole NPN for a vertical customer. Moreover, the proposed solutions assume the network connectivity has been pre-provisioned between the infrastructure of NPN and the PLMN. There is currently on-going work, such as the presented in [7] [29], which aims to tackle this limitation by automatically provisioning network connectivity between the different parts of the service using SDN based technologies. It is important to mention that our proposed models are generic and flexible to adapt to the different cases.

1) COMMUNICATION SERVICE LEVEL

A communication service, or more in general a vertical service, can be deployed across multiple domains. In this case, the vertical service is composed of elements that can be considered as sub-services, possible to be instantiated in domains controlled by different CSPs. The provisioning of this kind of service needs to be coordinated across multiple target domains in order to deliver the whole E2E service.

This includes the proper interconnection of all its component across the targeted domains and configured in a consistent manner.

In the following, we consider a scenario with two target domains, including a NPN domain and a PLMN domain. As shown in Figure 3, this coordination can be performed either by the Communication Service Consumer (CSC) such as a vertical customer (option (a)), or managed by one of the two CSPs which directly offer a part of the service (option (b)). In the former case, the CSC needs SLAs to be established with both CSPs and needs to implement suitable procedures to handle the composition of the service decomposed in several sub-services deployed by various CSPs. In the latter case, the CSC has an established SLA with a single CSP, which offers the single access point to request the entire service and hides the details of the service composition. Thus, SLAs between both CSPs are transparent to the CSC, and CSPs may select peering CSPs based on internal policies, business considerations or restrictions explicitly declared by CSC.

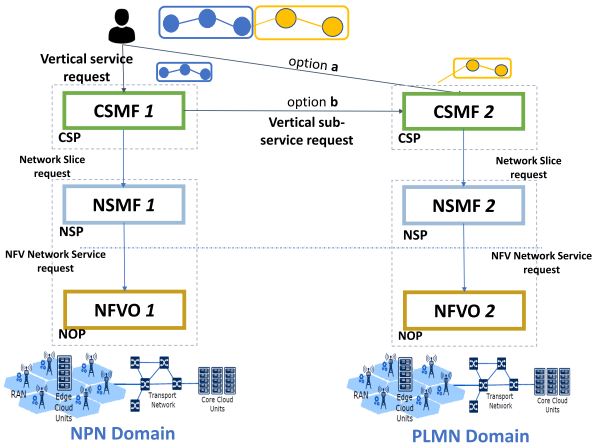


FIGURE 3. Communication service level.

At the architectural level, the interaction between two CSPs is handled through an East-Westbound Interface between the CSMF of the Vertical Slicers owned and controlled by each CSP, resulting in a peer-to-peer communication. This interaction is shown by the red straight line in Figure 2.

The decomposition of the vertical service in multiple sub-services is defined in the vertical service template, namely the Vertical Service Blueprint (VSB), where the service components are declared as atomic functions or sub-services. Currently the vertical service decomposition is performed during the service design phase by the service designer. Future work may address this decomposition in a dynamic and online manner through developing algorithms and policies to translate the particular service request into a set of vertical sub-service and domains. The CSMF receiving the initial request for the composite vertical service (the CSMF client, CSMF-C) needs to identify which sub-services can be deployed in the local domain and which ones can be requested to peer CSPs. The requests will be then issued to the associated CSMFs, which will act as CSMF provider (CSMF-P). The decision on the target CSPs is driven by the CSMF-C internal policies and it depends on the SLAs established with the CSP's customers (who may have restrictions on using services or resources from external providers) and with the peer CSPs.

The CSMF-C coordinates the procedures to instantiate and manage the lifecycle of the composite vertical service. This includes also the management of the interaction with the CSMF-P to request the instantiation and termination of the vertical sub-services. In this case, CSMF-P (located in the PLMN domain) is responsible for the management of the network slices corresponding to the vertical sub-service deployed in its domain, while CSMF-C (located in the NPN domain) manages the network slices corresponding to the locally deployed services. The interface between the two CSMFs should enable the following actions:

- Advertisement of VSBs related to the vertical sub-services that can be offered by the CSMF-P to the CSMF-C. This can be implemented through queries performed on the CSMF-P's VSB catalogue, using the VSB information model and the VSB catalogue query messages [30];
- Creation of VSDs with the service-level configuration requested by the CSMF-C to the CSMF-P, using the VSD information model and the VSD onboarding messages [30];
- Instantiation, termination and queries of vertical sub-services requested by the CSMF-C to the CSMF-P. This is enabled by the vertical service oriented lifecycle management API [30].

2) NETWORK SLICE LEVEL

The previous model is based on the assumption of two peer domains both of them offering vertical services. However, some administrative domains may not implement the CSMF component at their Vertical Slicer, but only the NSMF. In this case, the second domain is controlled by a Network Slice as a Service (NSaaS) Provider that offers network slices instead of vertical services, as shown in Figure 4.

In this scenario, the CSMF-C needs to identify the network slices associated to the vertical sub-services whose resources must be allocated into the external domain and to request their instantiation to the NSMF located there. The interaction between the two domains becomes a hierarchical one (the green straight line in Figure 2) and the CSMF-C acts as client for both the local and the remote NSMFs. In this case the CSMF-C (located in the NPN domain) is responsible for coordinating the lifecycle management of all the network slices. The mapping between the vertical sub-services and their associated Network Slice Templates (NSTs) must be handled in the VSB catalogue of the CSMF-C, while each NSMF is responsible of advertising their own set of NSTs. This allows the CSMF-C to select a target NSMF able to deliver the required network slice. The interface between

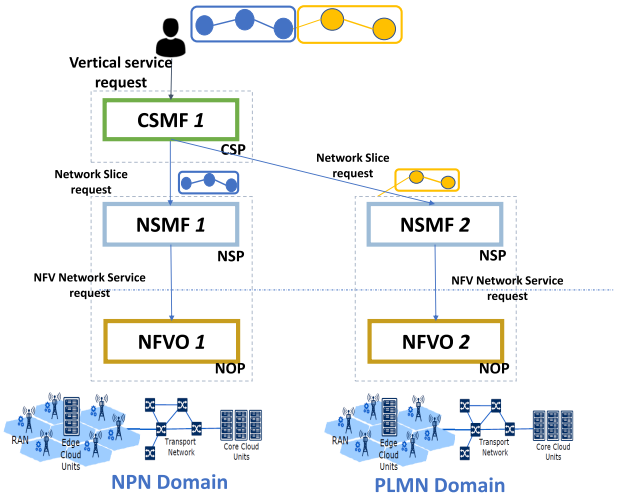


FIGURE 4. Network slice level.

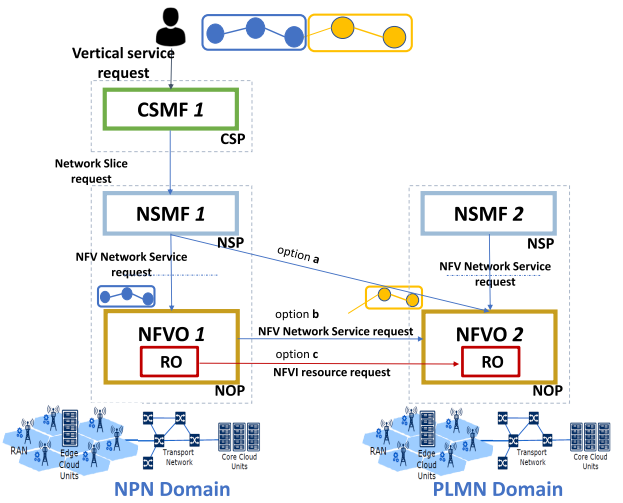


FIGURE 5. Network service level.

the CSMF-C and external NSMF should enable the following actions:

- Advertisement of NSTs that can be offered by the external NSMF to the CSMF-C. This can be implemented through queries performed on the NSMF's NST catalogue, based on NSMF APIs (3GPP TS 28.531 [31]) and the network slice resource model (3GPP TS 28.541 [25]);
- Instantiation, termination and queries of network slices requested by the CSMF-C to the NSMF on the NST basis, using the network slice life-cycle management API (3GPP TS 28.531 [31]).

It should be noted that this kind of CSMF-to-NSMF interaction implies that the vertical service can be decomposed in sub-services, where each of them can be delivered through a network slice instance. In particular, network slices offered by each domain are assumed to be independent on each other, without any composition of network slice subnets from multiple domains into an E2E multi-domain network slice. In fact, the composition of network slice subnets into a single E2E network slice would require a different kind of interaction, managed from the NSMF of the originating Vertical Slicer that would request the instantiation of network slice subnets to the peer NSMF (the green horizontal dotted line in Figure 2).

3) NETWORK SERVICE LEVEL

The NFV Network Service (NFV-NS) decomposition allows creating a single Network Slice that spans across different domains, provided that a suitable interconnection between all ends of the slice is established. This interaction refers to the option (a) shown in Figure 5, corresponding to the orange dotted line in Figure 2. In this case, the NSMF of the client side composes the E2E network slice as multiple NFV-NSs and requests their deployment to multiple NFVOs belonging to different NOP domains. This form of inter-domain Network Slice allows greater NSP agility, as it may ease the requirements over a single NOP and diminishes the need for prior agreements between the NSP and the NOPs to reserve larger resource pools to fulfill greater demands. The NSP could contract any NOPs that can deliver the requested decomposed network service, potentially benefiting from NOP's spot pricing while fulfilling the service requirements, and thus increasing competition and allowing for cost optimization. However, this approach and business benefit to the NSP comes at the cost of increased operational complexity.

The interaction between multiple domains can also be done between peering service orchestrators through their East-Westbound interface, i.e., the option (b) and (c) as shown in Figure 5, and in Figure 2 (blue straight arrow). In this case, the NFVO of the client side composes an E2E network service interacting with other peering NFVOs in other NOP domains. This is a federation relationship in which services or resources of peering domains are advertised and used together with the local ones, namely *(i)* NFV-NS federation; and *(ii)* resource federation, as described below.

The case of NFV-NS federation refers to option (b) in Figure 5. In this model, the vertical is assumed to focus on the vertical service logic and fully delegates service deployment to the 5Growth platform as long as the SLAs are respected. Therefore, the vertical slicer gathers the requirements and vertical service topology from the vertical and maps them into a network slice, which will eventually translate into an NFV-NS request towards the service orchestrator. The service orchestrator acts as an NFVO and, as such, comprises service and resource orchestration functionalities. In this option, the NFV-NS request may come in the form of a composite network service and the service orchestrator deploys each nested NFV-NS in one provider domain by interacting with their peering service orchestrator. The federation process is completely transparent to the higher layers and also the verticals. The interface to request nested NFV-NSs follows the same information model based on ETSI IFA013 [27] as that between the vertical slicer and the

underlying service orchestrator with modifications for federation support and its main functionalities are:

- Lifecycle management of nested network services deployed in provider domains;
- Resource management to enable coherent stitching of E2E network services. For instance, this includes the exchange of resource IDs between domains (e.g., IP address pools to avoid conflicts or VLAN IDs to allow the underlying resources to configure the inter-nested link in their respective transport infrastructures). That is, after all nested NFV-NSs are deployed, the client service orchestrator (that receiving the vertical service request) is in charge of coordinating their stitching into a composite E2E NFV-NS. It is worth to mention that this is the only optimum way for stitching an E2E service since the 5Gr-SO in each domain has both the view of network service requirements and the knowledge of the underlying infrastructure resources.

Within the 5Growth project (and its predecessor 5G-TRANSFORMER), several static and dynamic federation mechanisms have already been proposed, validated and evaluated in [28], [32]–[35].

The case of resource federation is the option (c) in Figure 5, to request the NFVI resources from the peering domains. In this case, there is an initial phase during which client domains advertise/discover resource availability (computing, storage, network) of peering domains. Based on this information, the client domain decides what resources from what provider domains to use and generates the corresponding NFVIaaS (NFVI as a Service) service requests. After completion of the corresponding resource allocation procedure, the control of provider-domain resources is fully delegated to the client domain, which handles them as if they were client domain resources. Therefore, any network function or network path could be deployed in the provider domain in the same way it is deployed in the client domain.

In 5Growth, resource federation is handled at the 5Gr-SO level, i.e. with an interaction between the resource orchestration (RO) functions of peering service orchestrators, as shown in Figure 5 option (c). The East-Westbound interface for resource federation among peering service orchestrators offers the following functionality:

- Resource availability request: resource orchestrators in each domain request resource availability information from the local resource layer and this information is stored in the NFVI resource repository of the service orchestrator;
- Resource exposure: each service orchestrator applies the resource abstraction procedures to the resource information it plans to offer to other domains of the federation. In this way, it selects the appropriate exposure level according to domain policies;
- Resource allocation request: the client domain selects the resources from the domains it wants to use and requests them in the form of an NFVIaaS request. This request is handled by the provider domain, abstracted and sent to the local resource layer to allocate the resources;
- Control delegation: the resource federation will migrate the management and control of the selected resources to the client domain so that these resources can be fully handled from the client domain while the resource federation agreement is in place.

As a result, when a service request is received in the client domain, the RO function of the service orchestrator handles federated resources in the same way as local ones. Therefore, these resources are also provided to the placement algorithm, which can place VNFs there to be connected with VNFs located in client-domain resources.

In the following section, the aforementioned levels of multi-domain solutions will be validated and evaluated through experimental results of two proof-of-concepts.

IV. EXPERIMENTAL EVALUATION

This section reports on the experimental results of two proof-of-concepts (PoCs) implemented to validate the proposed multi-domain solutions of the 5Growth platform, as described in Section III, for different PNI-NPN deployments. In both PoCs, the 5Growth platform, embodying the 5G service platform to manage private 5G networks at the vertical premises (i.e., NPN), interacts with external 5G EVE and OSM-based platforms, embodying the management platform of one or more MNOs in the PLMN. Their integration and validation are performed under 5G-enabled testbeds available at 5TONIC lab[3] (which includes the 5G EVE Spanish site), and 5Growth Aveiro pilot infrastructure. Each experiment presented in this section is repeated 10 times.

A. PROOF-OF-CONCEPT IMPLEMENTATIONS

The required extensions to support the interaction between 5Growth and both 5G EVE and OSM-based platforms have been implemented under the 5Growth project. These are described in the following, highlighting the main implementation details of both PoCs.

1) PoC #1: COMMUNICATION SERVICE LEVEL AND NETWORK SERVICE LEVEL

This PoC implemented both solutions through the integration of 5Growth and 5G EVE platforms, as depicted in Figure 6. The scenario envisioned by this PoC implements the SNPN with RAN sharing deployment model, as described in Section II. In this scenario, the vertical requests for the 5G service offered by the PLMN, to deploy vertical applications at the edge cloud provided at the vertical premises, while an on-premise gNB is used to connect the vertical devices.

In this setup, the 5Gr-VS interacts with an external PLMN domain managed through the 5G EVE platform [36], [37] to implement the multi-domain communication model based on peer CSMFs (i.e., communication service level). 5G EVE offers a Portal to request the experimentation of

[3]https://www.5tonic.org/

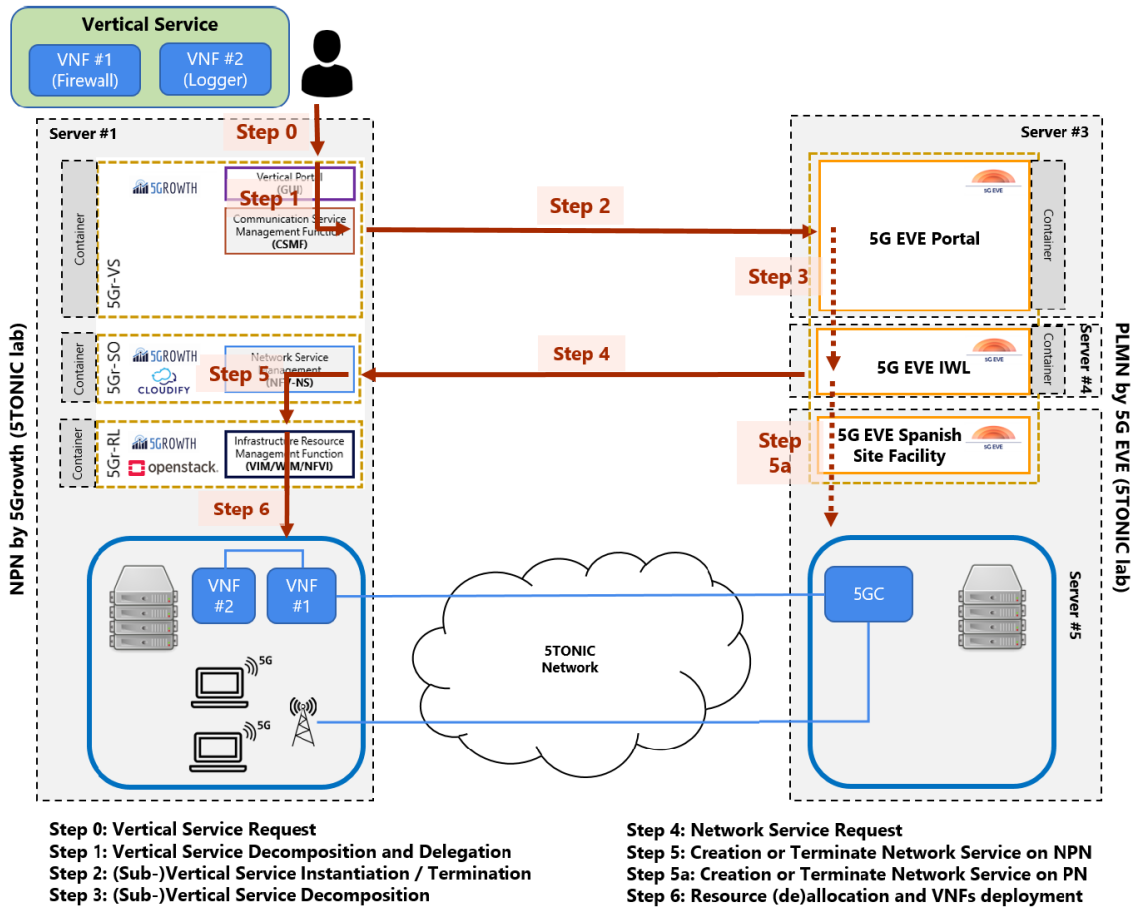


FIGURE 6. Evaluation scenario of PoC #1 comprising the integration of 5Growth and 5G EVE platforms (SNPN with RAN sharing deployment).

vertical services in configurable 5G environments, hosted in multiple 5G-enabled facilities across different European countries. In this sense, the 5G EVE Portal can be considered as the CSMF-P of the peer CSP. The interaction between the 5Gr-VS and the 5G EVE Portal is based on a dedicated driver that acts as client of the 5G EVE Portal. This driver translates between the information models of 5Growth vertical services and 5G EVE experiments, adapts the 5Growth vertical service lifecycle procedures to the ones regulating the declaration, instantiation and execution of 5G EVE experiments, and implements the client side of the REST-based communication with the 5G EVE Portal.

The network service level interaction is implemented between the 5G EVE Interworking Layer (IWL), an adaption layer in charge of abstracting the on-boarding and lifecycle management capabilities from multiple NFV Orchestrators, and the 5Gr-SO. As such, additional extensions are implemented in the form of two different drivers that enable the interaction between both platforms. First, since the 5G EVE IWL exposes to its upper layers an ETSI SOL005 [38] interface while 5Gr-SO exposes an ETSI IFA013 [27] interface, the 5G EVE IWL is extended with the support of a translation driver between both interfaces. Second, 5Growth and 5G EVE use different information models to describe the NSDs and VNFDs. While 5G EVE leverages on TOSCA-based models, 5Growth adopts ETSI IFA014 [39] and IFA011 [40] for NSDs and VNFDs. Thus, the second translation driver is responsible for mapping both information models.

In terms of the data plane, the 5G network (available at 5TONIC lab) implements 5G NSA access (BB630 baseband and Advance Antenna System AIR 6488) and devices are connected via Ethernet to a 5G CPE that, in turn, provides connectivity towards the 5G network. Finally, since both 5Growth and 5G EVE domains are deployed in the 5TONIC lab datacenter, the data plane connectivity consists of a set of static route configurations. Such approach to connect both domains is opted as a simplification for this PoC. However, more secure interconnection approaches should be carefully taken into consideration, such as VPNs or secure tunnels.

Additional information regarding the 5Growth stack deployment is that the 5Gr-SO uses Cloudify software as Core MANO platform to deploy the NFV-NS in collaboration with the 5Gr-RL. The 5Gr-RL controls an instance

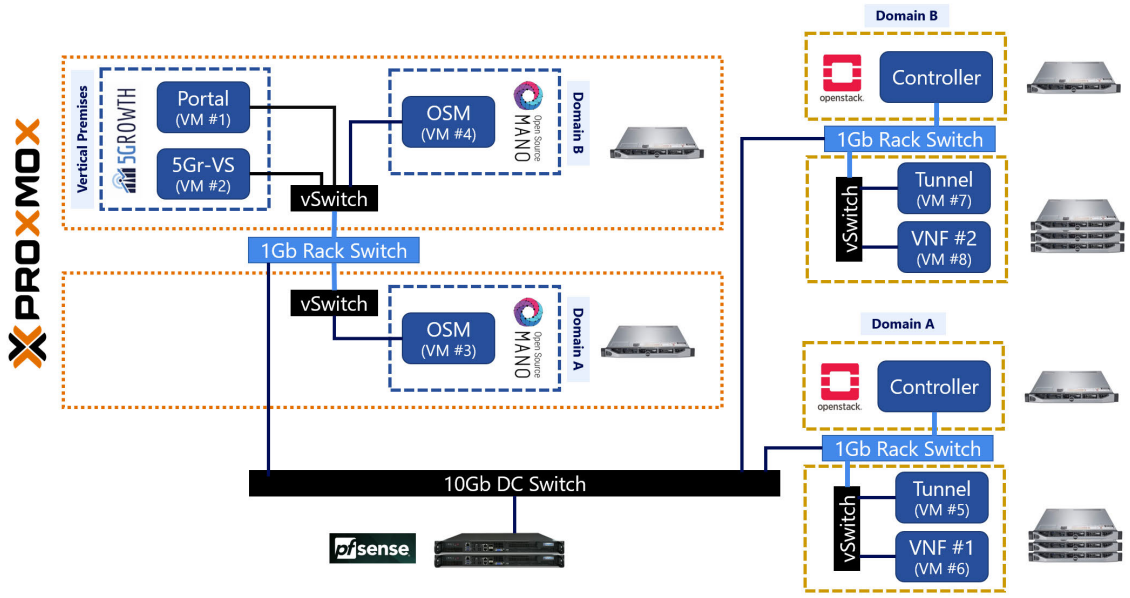


FIGURE 7. A detailed overview of the infrastructure used for the evaluation scenario of PoC #2.

of OpenStack (Rocky Release) to instantiate the VNFs of the NFV-NS as virtual machines. Finally, 5Growth solution is installed as a guest KVM with 40 vCPUs, 140GB of RAM and nested virtualization, in a host with the following specifications: CPU Intel(R) Xeon(R) CPU E5-2609 v3 @ 1.90GHz, 192GB(12 × 16) DDR4 2133 MHz of RAM, and 1TB HDD (raid 1) + 400GB SSD.

2) PoC #2: NETWORK SLICE LEVEL

This solution is implemented through the integration of 5Growth and OSM-based platforms. The scenario envisioned by this PoC implements the PNI-NPN with full sharing deployment model, as described in Section II. In this case, the vertical requests for an E2E network slice deployment across two PLMN network domains (Domain A and B in Figure 7), each domain provides a sub-slice, which is inter-connected with each other.

The prototype for the inter-domain E2E vertical slice is implemented according to CSMF-to-NSMF multi-domain communication model. The CSMF-C of the 5Gr-VS is extended with procedures to request multiple network slices to multiple NSMFs, either local (i.e., managed by the 5Gr-VS) or remote ones. The interaction with the NSMFs is handled through a software component that offers the CSMF-C a unified interface inspired by the 3GPP standards related to the NSMF APIs (3GPP TS 28.531 [31]) and the network slice resource model (3GPP TS 28.541 [25]). Internally, the NSMF-specific drivers translate the CSMF-C's requests in the format supported in each external domain and either map the respective NSTs or decompose the slice request into the respective network services. ETSI OSM is used as each domain's service orchestrator. Therefore, an OSM adapter translates the messages for instantiation, termination, and queries of network slices from/to TS 28.531 format and the decomposition to suitable network services controllable through the OSM REST API.

Because these inter-domain communications go through a public network, we must make additional security considerations to ensure proper operation in the above management interfaces (i.e., integrity, confidentiality, and availability). Furthermore, the E2E inter-domain forwarding plane used by the vertical services' must also be protected. Therefore, we have previously researched secure and reliable network slicing [41] and adopted three approaches to tackle some of the challenges: (1) we have used an Moving Target Defense (MTD) mechanism [42] to protect the inter-domain management interfaces against unknown types of attacks (e.g., 0-days); (2) we assure reliability in the forwarding-plane through performance isolation and QoS using SDN and a mixed Openflow/P4 data-path; and, (3) we have an AI/ML-assisted anomaly detection mechanism.

However, our previous forwarding plane assurances focused chiefly on performance isolation and required controlling all network switches in that path, which is an extreme assumption within this PNI-NPN scenario. Thus, we complement our previous research by introducing secure tunnels between the domains to allow for greater flexibility. We may have to sacrifice some of the performance guarantees but will still retain the integrity and confidentiality in the public transport network. Our design contemplates separate secure tunnels for the management and each of the vertical service's forwarding planes. We take a deeper look into the latter later in the article.

Figure 7 shows the infrastructure used for the evaluation scenario of PoC #2. Each of the rack-mountable server units represents a Dell PowerEdge R430 server equipped with 2xIntel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz. The most significant difference between the different servers is the amount of RAM installed and the type of storage used. The compute cluster of Domain A's Openstack uses a Ceph based storage that spans across the local disks installed in each compute node. In turn, the compute cluster of Domain B's Openstack and the Proxmox cluster use the same centralized Dell SCv2020 DC storage unit with 24x 1.2TB SAS 10k 12Gbps 2.5'' hard drives in RAID 6. The Openstack controller of the Domain A is containerized and virtualized within that hardware node, having 6GB of RAM allocated. Domain's B controller runs directly on the hardware and has 256GB of RAM installed to perform a large block chache of the centralized storage. Each of the VMs in this deployment was dimensioned for the PoC, using monitoring data gathered during early runs. The portal and 5Gr-VS VMs each had 2 vCPUs and 8GB of RAM. The OSM VMs were given up-to 8 vCPUs and 32GB of RAM depending on the current usage. Each of the service VMs instantiated in the respective domain's Openstack had 4 vCPUs and 4GB of RAM.

The simulated IXP/ISP environment used for the inter-domain communications consists of different 1 Gbps copper networks within a data center. Each network is local to the switch of the respective compute cluster that runs the 5Growth software and each of the VIM domains. Each of the domains under evaluation is placed in physically distinct compute nodes. The local networks are then routed centrally by the data center's firewall, a redundant pfSense system with 10 Gbps fiber links to the switches. The dataplane of the E2E slice is achieved using secure tunnels (Wireguard) that carry the packets across domains, being those tunnels overlaid atop the simulated IXP/ISP environment. We will provide further details about the tunneling solution in the respective evaluation subsection.

B. RESULTS OF COMMUNICATION SERVICE LEVEL AND NETWORK SERVICE LEVEL SOLUTIONS (PoC #1)

Figure 6 depicts the evaluation scenario for the Communication Service Level and Network Service Level Solutions, where the vertical service under evaluation consists of a simple service composed by two different VNFs (i.e., *Firewall* and *Logger*). Although more complex vertical services can be devised (e.g., composite and/or multi-site services) that reflect the real needs of the previous vertical industries, the following validation aims at providing a baseline reference for deeper and more complex analysis. The experimental results cover both instantiation and termination lifecycle management operations, being reported the time profiling of the various steps. These steps are also represented in Figure 6 and are described as follows:

- **Step 0:** Vertical requests the vertical service instantiation or termination at the 5Gr-VS Portal. This step sets the initial time for the experiments.
- **Step 1:** 5Gr-VS decomposes the vertical service into multiple sub-services and delegates their provisioning and management to an external 5G EVE domain, including translation and mapping of all the required requests. This step takes an average of 5.918 ± 0.081 s and 1.324 ± 0.074 s for, respectively, instantiation and termination operations.
- **Step 2:** 5Gr-VS issues vertical service instantiation or termination requests towards the 5G EVE Portal (through a programmable REST API), as well as monitors their execution status. This step takes an average of 49.416 ± 0.049 s and 87.783 ± 13.492 s for, respectively, instantiation and termination operations. However, it is important to highlight that the 5Gr-VS follows a pooling approach to check the status of the operations towards 5G EVE portal, resulting on the high values witnessed for this step.
- **Step 3:** 5G EVE manages the decomposition of the vertical service and issues NFV network service requests towards the 5Gr-SO and/or service orchestrator of other site facilities. This step is omitted from the analysis since 5G EVE requires a manual validation procedure to accept and schedule new vertical services.
- **Step 4:** 5G EVE IWL processes requests related to the interaction with the 5Gr-SO, including translation between ETSI SOL005 and ETSI IFA013 data models and polling (each 10s) the status of operations. This step takes an average of 5.274 ± 2.687 s and 3.530 ± 3.606 s for, respectively, instantiation and termination operations.
- **Step 5:** 5Gr-SO processes incoming requests, including creation or elimination of NSs, verification of available resources at the 5Gr-RL, and update of existing databases. This step takes an average of 235 ± 42 ms and 84 ± 6 ms for, respectively, instantiation and termination operations.
- **Step 6:** 5Gr-RL (de)allocates the required resources (intra-PoP network) where to deploy the VNFs, including their instantiation or termination. This step takes an average of 2.09 ± 0.05 min and 0.99 ± 0.03 min for, respectively, instantiation and termination operations.

The time profiling corresponding to each one the aforementioned steps is presented in Figure 8 and Table 1. The total time of the instantiation and termination operations is about 3.10 min and 2.55 min, respectively. When comparing to a fully local 5Growth deployment (i.e., without using the 5G EVE), this represents an average increase of 34s and 53s for the instantiation and termination operations. This increase is mainly due to the polling periods between 5Growth and 5G EVE components. Finally, due to a 60s polling period, the 5Gr-VS only detects the vertical service in the execution state $\approx$ 53 s after its instantiation. Results show that the most time-consuming operation during the vertical service instantiation is related to the creation and instantiation of the VNFs and the creation of the virtual links and networks (step 6), which represent about 63% of the total time.

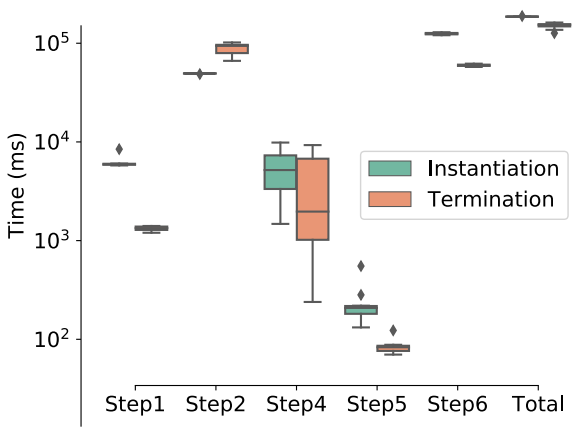


FIGURE 8. Service instantiation and termination time profiling (PoC #1) (the values of 20th-tile, min. mean, max. and 80th-tile are shown in Table 1).

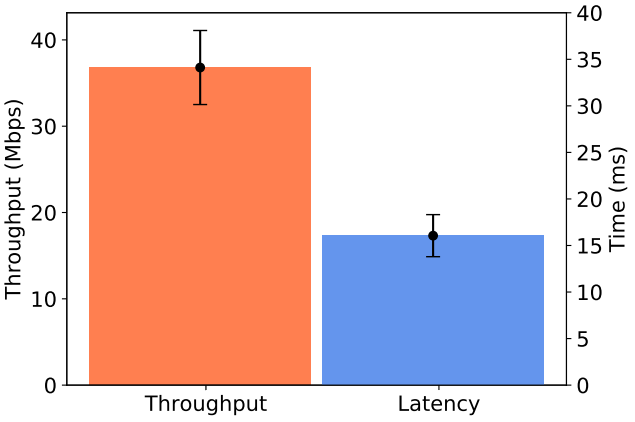


FIGURE 9. Impact on E2E communication (PoC #1) (plots the average values with min-max lines. Uses the central limit theorem to analyze the population within 2σ. That is, $\approx$ 95% confidence interval).

TABLE 1. Service instantiation and termination percentile analysis (PoC #1).

	20th-tile	Min.	Mean	Max.	80th-tile
Instantiation					
Step 1	5.861 s	5.778 s	6.171 s	8.446 s	6.035 s
Step 2	49.326 s	48.697 s	49.344 s	49.492 s	49.442 s
Step 3	—	—	—	—	—
Step 4	2.573 s	1.477 s	5.274 s	9.851 s	7.884 s
Step 5	0.163 s	0.132 s	0.235 s	0.552 s	0.269 s
Step 6	122.552 s	120.557 s	125.143 s	129.233 s	127.804 s
Termination					
Step 1	1.229 s	1.201 s	1.324 s	1.407 s	1.403 s
Step 2	68.795 s	66.294 s	87.783 s	93.983 s	100.391 s
Step 3	—	—	—	—	—
Step 4	0.557 s	0.239 s	3.530 s	9.286 s	8.369 s
Step 5	0.073 s	0.070 s	0.084 s	0.123 s	0.087 s
Step 6	57.876 s	57.518 s	59.482 s	62.083 s	61.608 s

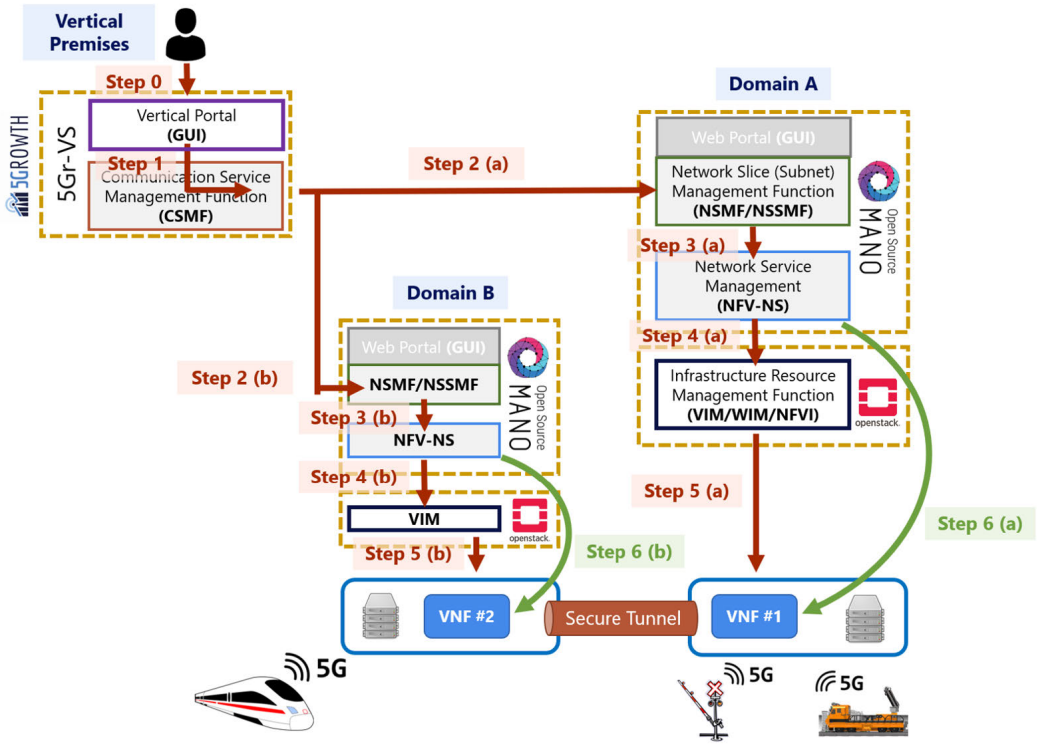
Analogously, the termination and clean-up of the previous aspects (step 6) are also accounting the greater time-consumption, representing about 40% of the total time.

In addition, the performance of the 5G data plane is measured, namely in terms of the E2E throughput and E2E latency between both 5G devices. Results are depicted in Figure 9, showcasing the correct operation of the vertical service when deployed across the 5Growth and 5G EVE domains. However, it is important to highlight that a secure interconnection between both domains (e.g., through the implementation of a secure tunnel) is not considered in this PoC. The selected network tunneling protocol to establish such interconnection impacts the security level and performance of the logical link, thus the additional packet processing will result in a throughput decrease and a latency increase. Their impact on the data plane performance is out of the scope of this PoC.

C. RESULTS OF NETWORK SLICE LEVEL SOLUTION (PoC #2)

Figure 10 depicts the evaluation scenario for the Network Slice Level Solution. It implements the network slice multi-domain solution, where the vertical service under evaluation consists of a simple service composed of two instances of a probing VNF. The probing VNF aggregates local sensorial data (e.g., train and track informational telemetry) in closer proximity with the provider where it is instantiated. The probing VNF collects forwarding-plane performance data (throughput and latency) and evaluates if the E2E slice complies with the KPIs specification. The instantiation of the E2E vertical slice requires an additional VNF to handle the secure tunneling (i.e., Wireguard) that interconnects the two sub-slices. The 5Gr-VS instantiates the secure tunnel VNF, an internal component of the 5Growth inter-domain solution, and seamlessly manages it without the vertical's intervention. The experiment results cover the most significant interactions required to instantiate the inter-domain slice across domains A and B, profiling the various steps' delays. Each of these steps is represented in Figure 10 and further described as follows:

- **Step 0:** A vertical's human operator enters the pilot's 5Gr-VS Portal. He will then select the vertical service that will result in a multi-domain E2E vertical slice with the two probing VNF instances and request its instantiation. The delays resulting from the human operator are omitted. In doing so, it is just measured the loading time required to show the instantiation page, fully rendered with all the dynamically acquired information about available templates, resources, and other system states. The page load took on average 238.32 ± 5.96 ms.
- **Step 1:** The pilot's 5Gr-VS Portal maps the vertical service request into the appropriate templates/descriptors and translates the user request into a compliant request to the 5Gr-VS CSMF. This step considers the elapsed time between pressing the action button in the instantiation form and triggering action in the 5Gr-VS CSMF. This step takes an average of 9.95 ± 1.54 ms.
- **Step 2:** The 5Gr-VS CSMF decomposes the E2E vertical slice into separate sub-slices. It requests their provisioning and management to the respective domain's



Step 0: Load service catalogs and generate page
Step 1: Map Services into the Instantiation Request
Step 2 *(a/b)*: (Sub-)Slice decomposition and Request to the respective domain(s)
Step 3 *(a/b)*: (Sub-)Service decomposition of the (sub-) slice request
Step 4 *(a/b)*: Find suitable VIM and begin the LCM (instantiating the Service)
Step 5 *(a/b)*: Allocated virtual resources and instantiate VDUs
Step 6: Service provisioning after instantiation

FIGURE 10. Evaluation scenario of PoC #2 comprising the Integration of 5Growth platform and Two OSM-based domains (PNI-NPN with full sharing deployment).

5Gr-VS NSMF, parallelizing the requests to separate domains (e.g., *a* or *b* in Figure 10). The 5Gr-VS CSMF also requests the instantiation of the secure tunnel VNF in each sub-slice and instructs the 5Gr-VS NSMF that the tunnel VNF must be configured through the respective primitive with endpoint information that arises from the resolved addresses after VDU instantiation. The step takes an average of 216.69 ± 26.67 ms.

- **Step 3:** The 5Gr-VS NSMF translates the sub-slice request into the appropriate artifacts of the domain's NFV-NS (i.e., using network slice templates or composition of network service descriptors). The 5Gr-VS NSMF will then request, in parallel, that each SO instantiates all components required to build the sub-slice. The NFV-NS Life-Cycle Management (LCM) is now delegated to the respective SO. The parallel requests took an average of 4.09 ± 0.70 ms in domain A and 3.50 ± 0.52 ms in domain B.
- **Step 4:** The SO determines which VIM is more suitable to fulfill the request and starts the LCM of the requested components, deploying the service-specific managers and support for service primitives (if the component requires them). In particular, the secure tunnel VNF crucial for the inter-domain connectivity requires a mix of day-1 and day-2 primitives to configure the tunnel endpoints with the resolved VDU information. Step 4 and 5 take 62.90 ± 6.74 s in domain A and 50.94 ± 8.60 s in domain B.
- **Step 5:** The VIM receives the instantiation requests and delivers the virtual resources from its shared resource pool if the resources to fulfill that request are available within the set constraints. Upon instantiation of each VDU, the VIM makes available the resolved endpoint address information. Steps 4 and 5 combined take 62.90 ± 6.74 s in domain A and 50.94 ± 8.60 s in domain B.
- **Step 6:** Upon delivery of the virtual resource, the LCM within the NFV-NS will start provisioning the slice/network services accordingly to the vertical requirements and the computed configurations during the network slice decomposition process of the upper layers of the stack. This facility will also enable the on-demand configuration of the vertical's services if those primitives exist. The step takes

421.93 ± 67.26 s in domain A and 160.39 ± 13.73 s in domain B.

The total instantiation time of the E2E vertical slice was 8.16 ± 1.07 min, with the critical path determined by the slowest domain (A). The fastest domain (B) completes the instantiation in 3.61 ± 0.27 min and is closer to the same services' instantiation times without the inter-domain connectivity (3.20 ± 0.37 min).

The time measured at each step's is plotted in Figure 11 and provided in Table 2 to ease analyzing the results and facilitate the discussion. The time of steps 0-2 does not change when using the inter-domain solution. The time required for the data acquisition to render the vertical portal's page (step 0), the translation that happens after submitting the request to the CSMF (step 1), and the decomposition into the instantiable artifacts that realize the vertical service (step 2) depends mostly on the number of available services and locations, rather than the actual placement where each of the instantiations will happen. Regardless of the service being instantiated in a single domain or across domains A and B, the delay caused by these steps is the same provided the same number of options is available. Furthermore, the 5Growth stack design uses the same running systems for steps 0-2. Therefore the same performance is expected for a very similar workload (i.e., the only difference is the variable(s) that hold the placement). Note that while, conceptually, step 2 shifts into an element (NSMF) specific to the contacting domain (as in Figure 10), in reality, the NSMF instance runs inside the 5Gr-VS stack.

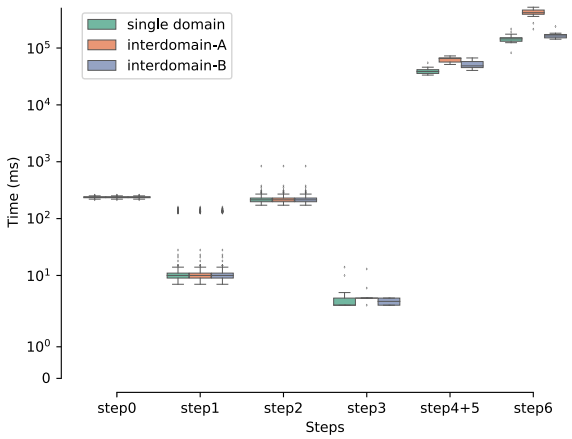


FIGURE 11. Instantiation time profiling of the E2E vertical slice (PoC #2) (the values of 20th-tile, min. mean, max. and 80th-tile are shown in Table 2).

Starting with step 3, other systems under the control of a different domain are contacted. The evaluation domains (A and B) are in different hardware and different loads caused by other customers. Domain A was reproducibly slower than domain B. Therefore, domain B is used to collect the baseline results using a single domain. Figure 11 shows that the partial instantiation using the inter-domain solution was slower than the baseline. The inter-domain solution requires the instantiation and configuration of the additional secure tunnel VNF, thus already expected to add overhead. The experimental results show that the translation overhead in step 3 was ≈ 6% over the baseline (a few milliseconds). While that overhead exists and is experimentally reproducible, it is not an impactful increase. The delay caused by the VIM interaction and the artifacts' actual instantiation was closer to ≈ 30% over the baseline. This interaction has a more noticeable delay, but the added flexibility that arises from the inter-domain capabilities more than warrant the added ≈ 12 s of instantiation time. Lastly, the measured overhead for step 6 with the inter-domain solution was ≈ 10% over the baseline (i.e., ≈ 15 extra seconds). The total sum of the overheads and their effects over the vertical service instantiation time is not significant compared to the inter-domain solution's benefits. Furthermore, the overheads are only in effect when the vertical service is instantiated across multiple domains. That is, there is no penalty for offering the functionality but opting not to use it.

TABLE 2. Service instantiation percentile analysis (PoC #2).

	20th-tile	Min.	Mean	Max.	80th-tile
Single Domain					
Step 0	233.00 ms	225.00 ms	238.33 ms	251.00 ms	243.00 ms
Step 1	9.00 ms	7.00 ms	9.95 ms	28.00 ms	11.00 ms
Step 2	194.80 ms	172.00 ms	216.69 ms	314.00 ms	232.20 ms
Step 3	3.00 ms	3.00 ms	3.30 ms	5.00 ms	4.00 ms
Step 4+5	35.59 s	33.44 s	38.69 s	46.02 s	42.20 s
Step 6	128.72 s	124.21 s	145.78 s	193.46 s	155.85 s
Interdomain A					
Step 0	233.00 ms	225.00 ms	238.33 ms	251.00 ms	243.00 ms
Step 1	9.00 ms	7.00 ms	9.95 ms	28.00 ms	11.00 ms
Step 2	194.80 ms	172.00 ms	216.69 ms	314.00 ms	232.20 ms
Step 3	4.00 ms	3.00 ms	4.09 ms	6.00 ms	4.00 ms
Step 4+5	56.20 s	51.40 s	62.90 s	72.63 s	68.04 s
Step 6	368.40 s	272.51 s	421.93 s	521.84 s	471.75 s
Interdomain B					
Step 0	233.00 ms	225.00 ms	238.33 ms	251.00 ms	243.00 ms
Step 1	9.00 ms	7.00 ms	9.95 ms	28.00 ms	11.00 ms
Step 2	194.80 ms	172.00 ms	216.69 ms	314.00 ms	232.20 ms
Step 3	3.00 ms	3.00 ms	3.50 ms	4.00 ms	4.00 ms
Step 4+5	42.97 s	40.39 s	50.94 s	66.91 s	59.66 s
Step 6	146.18 s	143.01 s	160.39 s	182.28 s	173.42 s

After evaluating the control overheads caused by the inter-domain solution during the vertical service instantiation, the behavior in the slice's forwarding-plane is evaluated. This includes an assessment on if the inter-domain solution can comply with the slice KPIs and determine the interconnection overheads of stitching the two sub-slices into a single E2E vertical slice. Two crucial KPIs are selected for this evaluation: throughput and latency. A control baseline is established in order to show the network performance between the two domains, which is measured using a E2E slice between the two vertical VNF instances, placed each in a separate domain. The measured forwarding plane performance is shown in Figure 12, highlighting that the limiting factor is the secure tunnel that inter-connects the different domains (i.e., a Wireguard tunnel). That tunnel accounts for a drop of nearly 30% in the measured throughput, going from ≈ 936 Mbps of the direct connection to ≈ 620 Mbps of the vertical slice. Despite the secure tunnel's expressive

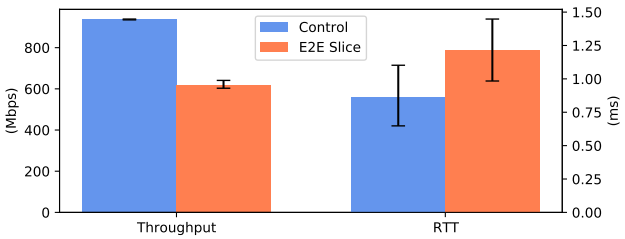


FIGURE 12. Impact on E2E communication (PoC #2) (plots the average values with min-max lines. Uses the central limit theorem to analyze the population within 2σ. That is, ≈ 95% confidence interval).

overhead, this loss must be critically evaluated in the context of the benefits to the E2E network slice and the compliance with the KPIs. The throughput values through the tunnel are reliable, much like the domains' direct interconnection values. Therefore, the inter-domain solution crucially delivers its benefits while still obeying the high throughput KPI (up to the ≈ 620 Mbps of ≈ 1 Gbps) as long as the domain's underlying interconnection remains compliant with its SLA. As for the measured Round-Trip-Time (RTT), because the direct connection already had such a low baseline (≈ 0.86 ms), the E2E slice results in an increase of nearly 40% of RTT (to ≈ 1.21 ms). Despite the large percentage, the absolute value does not invalidate its usage for most vertical applications. Therefore, the inter-domain solution obeys the low latency KPI (up to ≈ 1.21 ms) as long as the underlying connection between the domains remains compliant with its SLA.

V. 5GROWTH VERTICAL PILOTS AND USE CASES

This section analyses three different vertical industries being addressed in the scope of 5Growth project, and how their business needs are translated into different NPN deployments. These are centered in Industry 4.0, transportation and energy sectors, comprising a set of use cases with distinct business and technical requirements. These are briefly described as follows:

A. INDUSTRY 4.0

With the upcoming Industry 4.0, the industrial sector is shifting its business processes towards increasingly connected and smart processes. Building upon on its digitalization, industrial environments are enhanced in different key pillars: modular and cable-free infrastructures, mobility-features and seamless service experience, remote operation and telemetry functionalities, smart and predictive maintenance, and cybersecurity. In this work, a subset of the envisioned use cases are considered:

- *Digital Twin (I4.0-DT):* a virtual representation of something that exists in the real world, such as physical assets, people, places, systems and devices connected in real-time thanks to a continuous data stream.
- *Connected Worker for Remote Operation (I4.0-CMM):* Coordinate-Measuring Machine (CMM), a quality control equipment, is controlled, configured and calibrated by specialised personnel remotely from different geographic locations.
- *Telemetry (I4.0-Tel):* an extensive sensor deployment is in place to monitor and prevent failures of machinery and equipment through massive data collection (e.g., vibration, pressure and temperature).
- *Augmented ZDM Decision Support System (I4.0-ZDM):* Autonomous Guided Vehicles (AGVs) and a CMM coordinate their processes in order to automate the different stages of the quality control process by preemptively triggering the CMM measuring program to be dynamically loaded.
- *Digital Tutorial and Remote Support (I4.0-RS):* technicians and maintenance staff are provided with digital tutorials and remote support by means of high definition videos and live connections to remote technical offices.

The best deployment approach must be selected on a case-by-case basis, since it depends on several factors that might not be common to all industrial environments. For example, the level of QoS customization and control required, autonomy towards the MNO, security, and isolation of their internal processes, support of mobility when outside the factory premises. Moreover, the know-how and specialized personnel to manage the NPN, which might be out of the knowledge domain of these industries, and the costs of deployments influence the choice of a specific NPN deployment approach. The critical nature of the selected use cases require their processes to be executed in a secure and isolate way, while guaranteeing a full privacy of the generated data. Moreover, depending on the size of the Industry 4.0 players and/or the relation with its customers, these use cases might range from a single geographical location up to multiple facilities spanning across different locations. Finally, the strict technical requirements of these use cases require data plane functions (e.g., the UPF) to be instantiated in the vertical premises.

B. ENERGY

Electrical secondary substations interconnect medium and low voltage electrical distribution and are geographically widely spread. Maintenance and security aspects require that monitoring (e.g., sensors) and video footage data are provided to remote operators in centralized control centers, but also to mobile maintenance crews, in order to prevent and recover from failures and prevent electrical grid downtime costs. This is something that is realizable already today, but requires several different access technologies, impacting costs and flexibility. The following use cases are considered:

- *Advanced Monitoring and Maintenance Support for Secondary Substation MV/LV distribution substation (Energy-AMM):* a 5G link operates as the single technology, but able to support performance, security and isolation requirements for the service and information running therein.
- *Advanced Critical Signal and Data Exchange across wide smart metering and measurement infrastructures*

TABLE 3. 5Growth use cases mapping to NPN deployment scenarios and multi-domain interactions.

Vertical	5Growth Use Cases	NPN deployment scenario	5Growth Multi-Domain Interaction
Industry 4.0	*I4.0-DT* *I4.0-Tel*	**SNPN without RAN sharing and/or SNPN with RAN sharing**: Meets the tight and controlled latency and data rate requirements as well as supports massive connectivity for the sensors and different machinery. Increased security and isolation, protected against external malfunctions as e.g., in the PLMN. However, hinders the interaction of NPN with PLMN, hampering an inter-site deployment of the use cases.	None
	I4.0-CMM *I4.0-ZDM*	**PNI-NPN with RAN and 5GC control plane sharing**: Meets the tight and controlled latency and bandwidth requirements and increased security and isolation of the internal data traffic, guaranteed through dedicated 5G base stations (gNBs) and UPF at the vertical premises. Eases mobility and inter-site deployments, when services span across facilities in different locations. Reduces the costs and need for know-how. However, operation and subscription information of the internal devices are exposed to the PLMN.	It can be achieved in two ways: *(i)* at the communication service level; or *(ii)* through a combination of both communication service and network service levels. In the former, the CSMF of the vertical domain requests additional vertical (sub-)services towards the CSMFs of the MNO (and other premises domains), managing internally the vertical (sub-)services to be deployed on its own domain. In the latter, the whole vertical service is forwarded to the CSMF of the MNO, which in turn is responsible for federating the different NFV-NSs across the MNO and other premises domains.
	I4.0-RS	**PNI-NPN with RAN, 5GC control plane and transport network sharing:** The use of a shared network instead of private infrastructure , allows to reduce Total Cost of Ownership (TCO) and unlock Industry 4.0 use cases to small and medium enterprises that can leverage on infrastructure managed by MNO. Moreover it enables the capability to requires on demand new services or modify the existing ones according the actual needs. The shared network has to guarantee the same performances, such as latency and isolation of the private ones.	As previous case, it can be reached in two ways: (i) at the communication service level; or (ii) through a combination of both communication service and network service levels. In the former, the CSMF of the vertical domain requests additional vertical (sub)services towards the CSMFs of the MNO (and other premises domains), managing internally the vertical (sub-)services to be deployed on its own domain. In the latter, the whole vertical service is forwarded to the CSMF of the MNO, which in turn is responsible for federating the different NFV-NSs across other premises domains.
Energy	*Energy-AMM* *Energy-ACS*	**PNI-NPN with full sharing**: As electrical distribution substations are available in very large numbers and widespread geographically, public deployments are required, albeit able to provide isolated communications due to reliability and security requirements. Performance is also of a major concern due to scenario heterogeneity, where broadband traffic required for live-streaming Ultra-HD surveillance footage in substations meets ultra-low latency last-gasp intelligent electrical devices fault readouts.	In these scenarios, the widespread geographical dispersion of communicating devices provides no motivation for the vertical to hold its own private infrastructure. Therefore, communications are delegated towards the offerings of available network service providers. Here, the multi-domain aspect addresses the need for involving several MNO's in order for the vertical to achieve full reachability towards it's communication assets, for coverage or reliability reasons. This provides a very ample setting, where a network service can be provided or mediated by a MNO that interacts with other MNO's at the CSMF or Network service levels, or a combination of both. However, the 5Growth Service Platform provides the unique ability to allow the vertical itself to hold control of the Vertical and Network Slice logic, and directly interface with the Vertical Slicer entities existing in MNO's, for it to tailor its network services through the stitching of multi-domain network slices.
Transportation	*Transport-SCC* *Transport-NSCC*	**PNI-NPN with full sharing:** The widespread geographical distribution of the railway crossings, rain-detection sensors, along with the trains and maintenance crews, requires a large network coverage to interconnect these different entities. A dedicated private infrastructure will be extremely costly to provide such coverage while fulfilling reliability, safety and performance requirements. A wide-coverage public offering, coupled with isolation capabilities, is required for this case.	

(Energy-ACS): explores the low-latency capability of the 5G link to provide last-gasp messaging, allowing the last information to be sent to control centers, upon electrical distribution device failure.

The high geographical distribution of electrical secondary substations, along with the reliability and safety requirements of the exchanged telemetry, pose complex communication logistics, preventing any reliance on dedicated private infrastructure owned by the energy providers. Therefore, current solutions impose restrictions on the telemetry capabilities, which are coupled to the capabilities of the underlying used access technologies, and their coverage.

C. TRANSPORTATION

Train-approach detection for closing barriers in railway crossings have been requiring cable-based communications and protocols, imposing high deployment costs. 5G will be used to provide a reliable wireless solution to ensure railway safety communications for the following use cases:

- *Safety Critical Communications (Transport-SCC):* the connectivity between the train-approaching detectors in the railroad tracks and the level crossing controller that operates the barrier is provided through a 5G link.
- *Non-Safety Critical Communications (Transport-NSCC)* a 5G link is also shared to provides real-time

surveillance video from the level crossing, towards incoming trains and to maintenance crews.

Radio solutions for these scenarios are able to increase flexibility and usage capability (e.g., by adding the capability for video). However, they must still ensure that information between train-detection sensors and railway crossings is exchanged in a reliable and protected way, with sufficient performance capability. Additionally, similar to the Energy pilots, the constituents of this pilot can be geographically widespread and in great numbers, which prevent the deployment of dedicated private networks as the means to provide absolutely secure highly-available communications.

Building on previous pilots and their use cases, the motivation for the selection of a specific NPN deployment approach as well as the mapping to the multi-domain interactions is summarized in Table 3.

VI. SUMMARY AND CONCLUSION

This paper proposes a generic architectural solution for integrating 5G non-public networks (NPNs) with public networks (PLMNs), i.e., to implement a PNI-NPN. This done is through the design of three distinct levels of multi-domain solutions, namely at the *Communication Service Level*, the *Network Slice Level*, and the *Network Service Level*, to support various interactions among the different stakeholders. The proposed solutions are built upon the three main building blocks of the 5Growth platform, namely a *vertical slicer*, a *service orchestrator* and a *resource layer*. The *vertical slicer* provides an entry point to the industry verticals to express their service requests and requirements. Those are next mapped onto customized network services orchestrated E2E and across one or multiple domains by the *service orchestrator*. Then, the network services are deployed in various physical and virtual resources composing the *resource layer* which manages all the compute, storage and networking infrastructures.

The PNI-NPN multi-domain solutions have been experimentally validated. We presented the results from two proof-of-concept prototypes showcasing two different NPN deployments. In both validations, the 5Growth platform (playing the role of the NPN) has been integrated with external E2E 5G testing platforms (playing the role of the PLMN), namely 5G EVE platform and an OSM-based platform. The obtained results demonstrated both the feasibility and benefits of the proposed architecture. Finally, three real vertical pilots have been conducted, comprising Industry 4.0, railway transport and energy industry verticals, leveraging on the proposed multi-domain options to support their service use cases and NPN deployments. As such, this work also analyzes which NPN deployment scenarios are better suited to meet the vertical use case requirements.

REFERENCES

[1] A. Rostami, "Private 5G networks for vertical industries: Deployment and operation models," in *Proc. IEEE 2nd 5G World Forum (5GWF)*, Sep. 2019, pp. 433–439.
[2] A. Aijaz, "Private 5G: The future of industrial wireless," *IEEE Ind. Electron. Mag.*, vol. 14, no. 4, pp. 136–145, Dec. 2020.
[3] *System Architecture for the 5G System (5GS)* Standard 3GPP TS 23.501, 2018.
[4] H. C. C. de Resende, J. P. de Brito Gonçalves, C. B. Both, and J. M. Marquez-Barja, "Enabling QoS-secured enhanced non-public network slices for health environments," in *Proc. 6th EAI Int. Conf. Smart Objects Technol. Social Good*, Sep. 2020, pp. 18–23, doi: 10.1145/3411170.3411244.
[5] W. Y. Poe, J. Ordonez-Lucena, and K. Mahmood, "Provisioning private 5G networks by means of network slicing: Architectures and challenges," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6.
[6] D. Camps-Mur, M. Ghoraishi, J. Gu. Terán, J. Ordonez-Lucena, T. Cogalan, H. Haas, A. G. Gómez, V. Sark, E. Aumayr, S. van der Meer, and S. Yan, "5G-CLARITY: Integrating 5GNR, WiFi and LiFi in private 5G networks with slicing support," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2020, pp. 1–2.
[7] G. Carrozzo, M. S. Siddiqui, A. Betzler, J. Bonnet, G. M. Perez, A. Ramos, and T. Subramanya, "AI-driven zero-touch operations, security and trust in multi-operator 5G networks: A conceptual architecture," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*. Dubrovnik, Croatia: IEEE, 2020, pp. 254–258.
[8] *Deliverable D2.1: Use Cases, Requirements and KPIs*, document 5G-RECORDS, May 2021.
[9] *Deliverable D1.1: Technical Blueprint for Vertical Use Cases and Validation Framework*, document FUDGE-5G, Mar. 2021.
[10] *5G-INDUCE Project*. Accessed: May 13, 2021. [Online]. Available: https://www.5g-induce.eu/
[11] L. Vignaroli, M. Gramaglia, M. Fuentes, A. Casella, R. Odarchenko, L. Natale, B. Altman, and F. D'Andria, "The touristic sector in the 5G technology era: The 5G-TOURS project approach," in *Proc. IEEE Globecom Workshops (GC Wkshps*, Dec. 2020, pp. 1–6.
[12] *Deliverable D2.1: Use Cases, Deployment and Techno-Economic Requirements—High Level Description*, document 5G-TOURS, Jun. 2019.
[13] *Deliverable D2.1: 5G VICTORI Use Case and Requirements Definition and Reference Architecture for Vertical Services*, document 5G-VICTORY, Mar. 2020.
[14] *Deliverable D1.1: Forward Looking Smart Manufacturing Use Cases, Requirements and KPIs*, document 5G-SMART, Jun. 2020.
[15] G. Soós, D. Ficzere, T. Seres, S. Veress, and I. Németh, "Business opportunities and evaluation of non-public 5G cellular networks—A survey," *Infocommun. J.*, vol. 12, no. 3, pp. 31–38, 2020.
[16] X. Li, A. Garcia-Saavedra, X. Costa-Perez, C. J. Bernardos, C. Guimaraes, K. Antevski, J. Mangues-Bafalluy, J. Baranda, E. Zeydan, D. Corujo, P. Iovanna, G. Landi, J. Alonso, P. Paixao, H. Martins, M. Lorenzo, J. Ordonez-Lucena, and D. R. Lopez, "5Growth: An end-to-end service platform for automated deployment and management of vertical services over 5G networks," *IEEE Commun. Mag.*, vol. 59, no. 3, pp. 84–90, Mar. 2021.
[17] M. Gupta, R. Legouable, M. M. Rosello, M. Cecchi, J. R. Alonso, M. Lorenzo, E. Kosmatos, M. R. Boldi, and G. Carrozzo, "The 5G EVE end-to-end 5G facility for extensive trials," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–5.
[18] *5G IoT Private & Dedicated Networks for Industry 4.0—A Guide to Private and Dedicated 5G Networks for Manufacturing, Production and Supply Chains*, GSMA, London, U.K., Oct. 2020.
[19] *5G Non-Public Networks for Industrial Scenarios (White Paper)*, 5G-ACIA—5G Alliance for Connected Industries and Automation, Frankfurt, Germany, Jul. 2019.
[20] J. Ordonez-Lucena, J. Folgueira Chavarria, L. M. Contreras, and A. Pastor, "The use of 5G non-public networks to support industry 4.0 scenarios," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2019, pp. 1–6.
[21] *5G Industry Campus Network Deployment Guideline, NG. 123, V1.0*, GSMA, London, U.K., Nov. 2020.
[22] *Management and Orchestration; Management of Non-Public Networks (NPN); Stage 1 and Stage 2*, Standard 3GPP TS 28.557, 2018.
[23] C. Papagianni, J. Mangues-Bafalluy, P. Bermudez, S. Barmpounakis, D. De Vleeschauwer, J. Brenes, E. Zeydan, C. Casetti, C. Guimaraes, P. Murillo, A. Garcia-Saavedra, D. Corujo, and T. Pepe, "5Growth: AI-driven 5G for automation in vertical industries," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2020, pp. 17–22.
[24] X. Li, T. Deiss, J. Mangues-Bafalluy, J. Baranda, X. Costa-Perez, G. Landi, C. J. Bernardos, P. Iovanna, A. Zurita, and P. Bertin, "Automating vertical services deployments over the 5GT platform," *IEEE Commun. Mag.*, vol. 58, no. 7, pp. 44–50, Jul. 2020.

[25] *Management and Orchestration; 5G Network Resource Model (NRM)*, Standard TS 28.541, V16.3.0, 3GPP, Dec. 2019.
[26] *Study on Management and Orchestration of Network Slicing for Next Generation Network*, Standard TR 28.801, V. 15.1.0, 3GPP, Jan. 2018.
[27] *ETSI, Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Os-Ma-Nfvo Reference Point—Interface and Information Model Specification*, Standard ETSI GS NFV-IFA 013 V2.3.1, Aug. 2017.
[28] J. Baranda, J. Mangues-Bafalluy, R. Martinez, L. Vettori, K. Antevski, C. J. Bernardos, and X. Li, "5G-TRANSFORMER meets network service federation: Design, implementation and evaluation," in *Proc. 6th IEEE Conf. Netw. Softwarization (NetSoft)*, Jun. 2020, pp. 175–179.
[29] P. Shantharama, A. Thyagaturu, N. Karakoc, L. Ferrari, M. Reisslein, and A. Scaglione, "LayBack: SDN management of multi-access edge computing (MEC) for network access services and radio resource sharing," *IEEE Access*, vol. 6, pp. 57545–57561, 2018.
[30] *Deliverable D3.1: Definition of Vertical Service Descriptors and SO NBI*, document 5G-TRANSFORMER, Mar. 2018.
[31] *Management and Orchestration; Provisioning*, Standard TS 28.531, V15.4.0, 3GPP, Sep. 2019.
[32] K. Antevski, J. Martin-Perez, A. Garcia-Saavedra, C. J. Bernardos, X. Li, J. Baranda, J. Mangues-Bafalluy, R. Martnez, and L. Vettori, "A Q-learning strategy for federation of 5G services," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.
[33] J. Baranda, J. Mangues-Bafalluy, L. Vettori, R. Martinez, K. Antevski, L. Girletti, C. J. Bernardos, K. Tomakh, D. Kucherenko, G. Landi, J. Brenes, X. Li, X. Costa-Perez, F. Ubaldi, G. Imbarlina, and M. Gharbaoui, "NFV service federation: Enabling multi-provider eHealth emergency services," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 1322–1323.
[34] K. Antevski and C. J. Bernardos, "Federation of 5G services using distributed ledger technologies," *Internet Technol. Lett.*, vol. 3, no. 6, p. e193, Nov. 2020, doi: 10.1002/itl2.193.
[35] J. Baranda, J. Mangues, R. Martínez, L. Vettori, K. Antevski, C. Bernardos, and X. Li, "Realising the network service federation vision," *IEEE Vehicular Technol. Mag., Future Netw. Initiative Special Issue 5G Technol. Appl.*, vol. 15, no. 2, pp. 48–57, Jun. 2020.
[36] J. Garcia-Reinoso, M. Gupta, M. M. Rosello, E. Kosmatos, G. Landi, G. Bernini, R. Legouable, L. M. Contreras, M. Lorenzo, and K. Trichias, "The 5G EVE multi-site experimental architecture and experimentation workflow," in *Proc. IEEE 2nd 5G World Forum (5GWF)*, Sep. 2019, pp. 335–340.
[37] W. Nakimuli, G. Landi, R. Perez, M. Pergolesi, M. Molla, C. Ntogkas, G. Garcia-Aviles, J. Garcia-Reinoso, M. Femminella, P. Serrano, F. Lombardo, J. Rodriguez, G. Reali, and S. Salsano, "Automatic deployment, execution and analysis of 5G experiments using the 5G EVE platform," in *Proc. IEEE 3rd 5G World Forum (5GWF)*, Sep. 2020, pp. 372–377.
[38] *Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; RESTful Protocols Specification for the Os-Ma-Nfvo Reference Point*, Standard ETSI GS NFV-SOL 005 v2.7.1, ETSI, Jan. 2020.
[39] *Management and Orchestration; Network Service Templates Specification*, Standard ETSI GS NFV-IFA 014 V2.4.1, ETSI, Feb. 2018.
[40] *Network Functions Virtualisation (NFV); Management and Orchestration; VNF Packaging Specification*, Standard ETSI GS NFV-IFA 011 v2.1.1, ETSI, Oct. 2016.
[41] V. A. Cunha *et al.*, "5growth: Secure and reliable network slicing for verticals," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit), Netw. Softwarisation (NET) (EuCNC & 6G Summit—NET)*, Porto, Portugal, Jun. 2021, pp. 1–6.
[42] V. A. Cunha, D. Corujo, J. P. Barraca, and R. L. Aguiar, "TOTP moving target defense for sensitive network services," *Pervas. Mobile Comput.*, vol. 74, Jul. 2021, Art. no. 101412.

XI LI received the M.Sc. degree, in 2002, and the Ph.D. degree, in 2009. She is currently a Senior Researcher on 5G networks research and development at NEC Laboratories Europe, focused on research of 5G and beyond networks. She is the Technical Manager of 5GPPP Project 5Growth and has led work packages on the orchestration of 5G mobile networks in the 5GPPP Projects 5G-Crosshaul and 5G-TRANSFORMER.

CARLOS GUIMARÃES received the M.Sc. degree, in 2011, and the Ph.D. degree, in 2019. He is currently a Postdoctoral Researcher with the Universidad Carlos III de Madrid (UC3M), where he is pursuing research activities in 5G technologies and main enablers as well as in the application of AI/ML into computer networks.

GIADA LANDI received the M.Sc. degree, in 2005. She is currently the Research and Development Leader of architectures and network design at Nextworks. She has participated in many industrial and European research projects. She holds more than ten years experiences in telecommunication networks, with focus on control plane architectures and protocols and consultancies on PCE, SDN, and NFV topics.

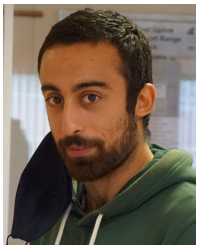
JUAN BRENES received the master's degree in telematics from the Universidad Carlos III de Madrid (UC3M), Madrid, Spain, in 2015. He is currently a Research and Development Engineer of architectures and network design at Nextworks. For the last five years, he has been working as a researcher and a consultant in the areas of NFV, SDN, and 5G technologies for different companies and participating in several EU funded projects.

JOSEP MANGUES-BAFALLUY received the Ph.D. degree, in 2003. He is currently a Senior Researcher and the Head of the Communication Networks Division, CTTC. He has participated in various roles, including leadership in several public funded and industrial research projects, such as 5GPPP 5Growth or 5G-REFINE. He was the Vice-Chair of IEEE WCNC 2018, Barcelona.

JORGE BARANDA (Senior Member, IEEE) received the M.Sc. degree, in 2008. He is currently a Senior Researcher with the Communication Networks Division, CTTC. He has participated in several European, national, and industrial projects related with SDN/NFV-based orchestration of mobile networks, efficient routing for mobile backhauling, and novel wireless communication systems.

DANIEL CORUJO (Senior Member, IEEE) received the Ph.D. degree, in 2013. He is currently an Assistant Professor with the University of Aveiro and a Researcher at the Instituto de Telecomunicações.

VITOR CUNHA received the M.Sc. degree, in 2015. He is currently pursuing the Ph.D. degree with the University of Aveiro. He is a Researcher at the Instituto de Telecomunicações. He is working on dynamic security mechanisms for softwarized and virtualized networks. His interests include network security, SDN, NFV, and pervasive computing.



JOÃO FONSECA is currently pursuing the M.Sc. degree with the University of Aveiro. He is a Researcher at the Instituto de Telecomunicações. He is also an active proponent of software freedom and an advocate for the Linux kernel and disseminates, a broad set of skills in managing and developing for this operating system through GLUA.

JOÃO ALEGRIA received the B.Sc. degree, in 2019. He is currently pursuing the M.Sc. degree with the University of Aveiro. He is a Researcher at the Instituto de Telecomunicações. He is working on creation and instantiation of softwarized and virtualized networks and services, as well as multidomain support for those networks and services.

AITOR ZABALA ORIVE received the M.Sc. degree, in 2020. He is the Chief Technical Officer at Telcaria Ideas S.L., Spain. He is an experienced developer in SDN, NFV, and SD-WAN. His current research interests include open RAN and 5G campus-networks.

JOSE ORDONEZ-LUCENA received the M.Sc. degree, in 2017. He is currently a Technology Analyst and a 3GPP SA5 & ETSI ZSM Standards Delegate at Telefónica I+D. His current research interests include network slicing, private 5G networks, and SD-WAN.

PAOLA IOVANNA received the M.Sc. degree, in 1996. She is currently a Principal Researcher at Ericsson, leading a research team on networking and automation (SDN/NFV) solutions for 5G networks. She is the author of more than 70 patents and 80 publications in either international scientific journals or conferences.

CARLOS J. BERNARDOS received the Ph.D. degree in telematics from UC3M, Spain. He currently works as an Associate Professor with UC3M. He is an Active Contributor to IETF. His current research interests include network virtualization and wireless networks.

ALAIN MOURAD is currently the Director of engineering research and development at InterDigital Labs, London, U.K., leading research on 5G and beyond. Prior to InterDigital, he was a Principal Engineer at Samsung Electronics Research and Development and a Senior Engineer at Mitsubishi Electric R&D Centre Europe, where he was active in the specification of wireless standards (3GPP, IEEE802, DVB, and ATSC).

XAVIER COSTA-PÉREZ (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in telecommunications from the Polytechnic University of Catalonia. He is currently a Professor at ICREA, the Director at i2cat, and the Head of 6G research and development at NEC Labs Europe.