
ZSM PoC Report

1 PoC Project Details

1.1 PoC Project Review

PoC Number:	5
PoC Project Name:	On-demand Non-Public Networks (NPNs) for industry 4.0: zero-touch provisioning practices in public-private network environments.
PoC Project Host:	Telefónica S.A.
Short Description:	This PoC showcases the ability to provision a tailored 5G private network for an industry 4.0 service, upon request (on demand), with no human intervention (zero-touch). In particular, the PoC demonstrates the automation in the provisioning of a Public Network Integrated Non-Public Network (PNI-NPN) to enable Autonomous Guide Vehicle (AGV) navigation in a factory for intralogistics services. The private network segment, deployed within the factory premises, includes three network domains: access domain (5G NR+Wi-Fi6 technologies combined with the use of ATSSS functionality), transport domain (L2 Ethernet network), core domain (5GC). The public network segment includes a pre-trained obstacle detection application to assist AGV trajectory. This application function corresponds to the data network, hosted in a PLMN operator's telco edge node. The ETSI ISG ZSM PoC#5 has been developed using the network and service management solutions developed in two European Commission (EC) funded projects, under the 5G PPP/H2020 programme: 5G-CLARITY [1] and 5GZORRO [2]. The implementation of these solutions complies with the ZSM standards. More specifically, the design architecture of the use case follows ZSM 002 (ZSM framework), and the workflows governing interactions across the different ZSM services follow the recommendations captured in ZSM 003 (end-to-end slicing) and ZSM 008 (cross-domain orchestration).
PoC Project Status : (Ongoing/Completed)	Completed

1.2 PoC Team Members Review

	Organisation name	ISG ZSM participant (yes/no)	Contact (Email)	PoC Point of Contact (*)	Role (**)	PoC Components
1	Telefónica	Yes	Jose Ordóñez-Lucena joseantonio.ordonezlucena@telefonica.com Diego R. López diego.r.lopez@telefonica.com	X	Network/ service provider	• Use case specification • PoC architecture definition • Sponsor of 5TONIC testbed
2	Fundació i2CAT	No	Daniel Camps daniel.camps@i2cat.net Adriana Fernández-Fernández adriana.fernandez@i2cat.net Ferrán Cañellas Cruz ferran.canellas@i2cat.net		Supplier; test labs	• 5G-CLARITY components (see list in Section 2.2.2) • Setup and maintenance of i2CAT lab (infra and NFs)
3	NextWorks	Yes	Giacomo Bernini g.bernini@nextworks.it Juan Brenes j.brenes@nextworks.it Michael de Angelis m.deangelis@nextworks.it Pietro G. Giardina p.giardina@nextworks.it		Supplier	• 5G-ZORRO components (see list in Section 2.2.2) • Lead integration with 5G-CLARITY
4	Interdigital	No	Tezcan Cogalan Tezcan.cogalan@interdigital.com Sebastian Robitzsch Sebastian.Robitzsch@interdigital.com		Solution integrator	Obstacle detection function: implementation, training and onboarding.
5	Universidad Carlos III de Madrid	No	Borja Nogales bdorado@pa.uc3m.es Francisco Valera fvalera@it.uc3m.es Iván Vidal ividal@it.uc3m.es		University; test labs	• Setup and maintenance of 5TONIC lab. • Layer 2 inter-site communication mechanism.
(*) Identify the PoC Point of Contact with an X. (**) The Role will be network/service provider, supplier, or other (universities, research centers, test labs, Open Source projects, integrators, etc...).						

All the PoC Team members listed above declare that the information in this report is conformant to their activities during the PoC Project.

1.3 PoC Project Scope Review

1.3.1 PoC Topics

Report the status of all the PoC Topics and Expected Contributions anticipated in the PoC Proposal.

PoC Topic Code	PoC Topic Description	Related WI	Submitted Contribution link	Date	Status (*)
2	Automation in Multi-Stakeholder Ecosystem	ZSM 001, ZSM 003	The PoC showcased at the EuCNC & 6G event (see section 1.5) and the report in this	May-June 2022	Completed

			document captures the contributions which had been anticipated in the proposal. For further information, see NOTE 1 and NOTE 2.		
4	Cross-domain user-driven E2E services	ZSM 002, ZSM 008	The PoC showcased at the EuCNC & 6G event (see section 1.5) and the report in this document captures the contributions which had been anticipated in the proposal. For further information, see NOTE 3 and NOTE 4.	May-June 2022	Completed
(*) Planned, On-going, Completed, delayed (new target date), Abandoned					

NOTE 1: The contributions in scope of topic 2 that have been covered by this PoC include:

- Usage of network slicing models and solution sets for the provisioning of a public-private 5G network, i.e. PNI-NPN, following the recommendations captured in ZSM 003 [4].
- Showcasing a PNI-NPN deployed across two administrative domains (on-premises infrastructure and PLMN infrastructure). In the PoC, there exist three stakeholders: vertical customer (ZSM consumer), CSP's B2B unit (ZSM operator #1) and CSP's MNO unit (ZSM operator #2).
- Usage of solutions from different research and innovation projects, developed by different parties. These solutions include vendor (commercial) and open-source products.

NOTE 2: No direct contributions have been submitted to ZSM 001 [3] and ZSM 003 [4], since both specifications are frozen.

NOTE 3: The contributions in scope of topic 2 that have been covered by this PoC include:

- Showcasing the end-to-end nature of the PNI-NPN, with all network domains covered: 3GPP (5G NR) and non-3GPP (Wi-Fi 6) access, transport network (L2 Ethernet), 3GPP core network (5GC) and data network (application server).
- Implementing ZSM management and data services providing fulfilment capabilities with management functions. The specific ZSM services used in this PoC are aligned with the ones captured in ZSM 002. Further details on this are specified in Section 2
- Integrating the management functions into individual management domains and the E2E service management domain.
- Demonstrating cross-domain workflows across the management functions, according to the governance captured in ZSM-008.

NOTE 4: No direct contributions have been submitted to ZSM 002 [5] and ZSM 008 [6], since both specifications are frozen.

1.3.2 Other topics in scope

Report the status of all the additional PoC Topics and Contributions anticipated in the PoC Proposal.

PoC Topic Code	PoC Topic Description	Related WI	Submitted Contribution link	Date	Status (*)
(*) Planned, On-going, Completed, delayed (new target date), Abandoned					

"Automation in Multi-Stakeholder Ecosystem" was the only PoC topic which was active during the PoC lifetime.

1.4 PoC Project Milestones Review

PoC Milestone	Milestone description	Target Date	Additional Info	Completion Date
P.S,	PoC Project Start	Feb 2022		14/02/2022
P.P.1	PoC Proposal submission	March 2022	Submission to ZSM PoC Management Team for approval.	15/03/2022
P.P.2	PoC Proposal Announce	April 2022	Public Web announced in 5G-CLARITY and 5G-ZORRO media (web, twitter, etc.).	04/04/2022
P.M1	PoC internal milestone 1: inter-site connectivity up and running	March 2022	L2 connectivity over VPN set up between facilities.	10/04/2022
P.M2	PoC internal milestone 2: user story detailed	March 2022	Detailing workflows across different PoC components, to comply with the user story (see Table 1).	15/03/2022
P.M3	PoC internal milestone 3: test campaign	April 2022	Specification of testing plan, with the collection of test cases to be conducted for PoC evaluation	10/05/2022
P.M4	PoC internal milestone 4: PoC execution	May 2022	PoC components integrated and ready for evaluation. Test campaign execution.	01/06/2022
P.D1	PoC demo	June 2022	Showcasing PoC results at 2022 EuCNC & 6G Summit (EuCNC'22). Coordinates: 7-10 June 2022, Grenoble (France).	08/06/2022
P.C1	Contribution on lessons learned	June 2022	Collect feedback about the lessons learnt about the PoC, to make improvements when executing the PoC in production factory networks	October 2022 (ZSM#20)

1.5 Confirmation of PoC Event Occurrence

The PoC was presented in a F2F event, whose details are captured below:

- **Event Name:** EuCNC & 6G Submit 2022 (<https://www.eucnc.eu>).
- **Event Occurrence:** Grenoble, France, 7-10 June 2022.
- **Event description:** This event builds on putting together two successful conferences in the area of telecommunications: EuCNC (European Conference on Network and Communications), supported by the European Commission, and the 6G Summit, originated from the 6G Flagship programme in Finland, one of the very first in its area. The conference is sponsored by the IEEE Communications Society and by the European Association for Signal Processing, and focuses on all aspects of telecommunications ranging from 5G deployment and mobile IoT to 6G exploration and future communications systems and networks, including experimentation and testbeds, and applications and services.
- **Event statistics:** It brings together cutting-edge research and world-renown industries and businesses, globally attracting in the last years more than 1,300 delegates from more than 40 countries all over the world, to present and discuss the latest results, and an exhibition with more than 70 exhibitors, for demonstrating the technology developed in the area, namely within research projects from EU R&I programmes

For the PoC showcasing, the PoC team:

- **printed two posters** (see Figure 1), each sponsored by the participant projects: 5G-CLARITY (left-side poster) and 5G-ZORRO (right-side poster). These posters were available for public consultation at the two project booths during the full event.

- displayed a pre-recorded video (see Figure 2). The video was continuously reproduced at the 5G-CLARITY and 5GZORRO project booths during the full event.

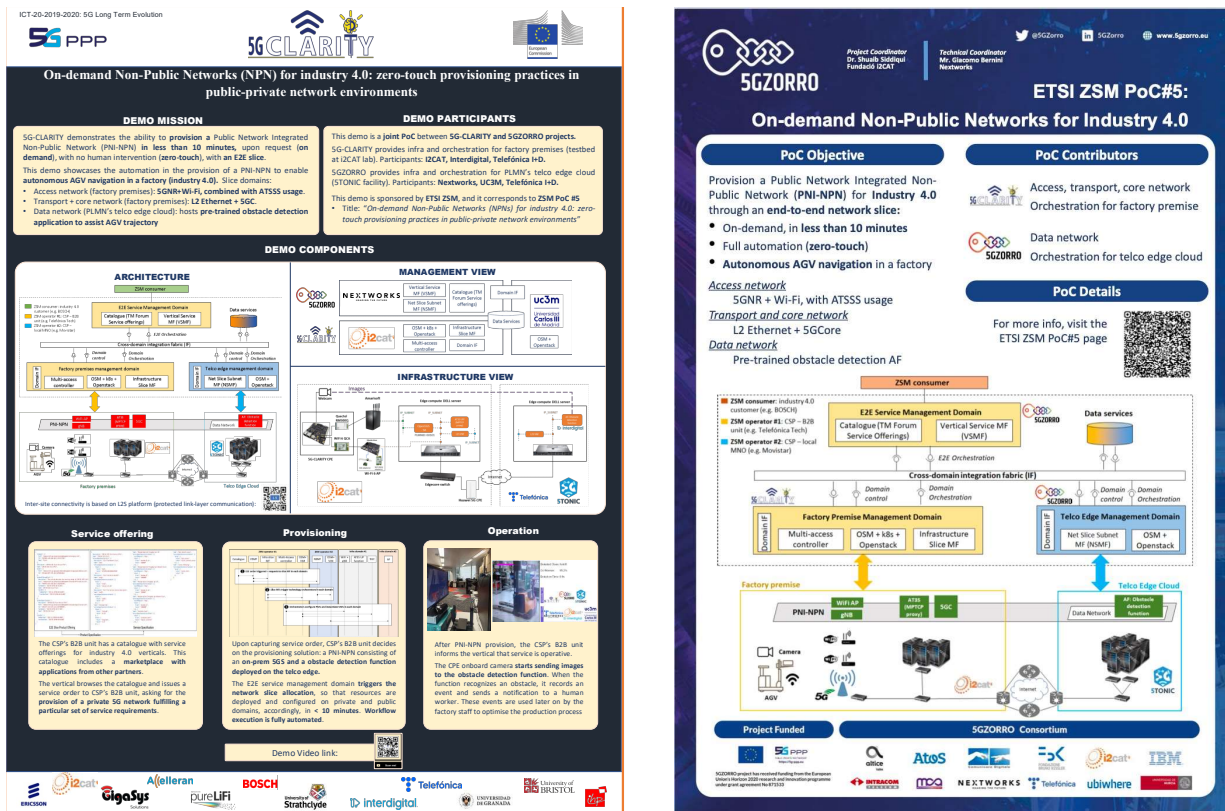


Figure 1: Posters promoting ETSI ISG ZSM PoC#5. The right-side poster was hanging at 5G-CLARITY project booth, whereas the left-side one was distributed as a leaflet at the 5G-ZORRO project booth.

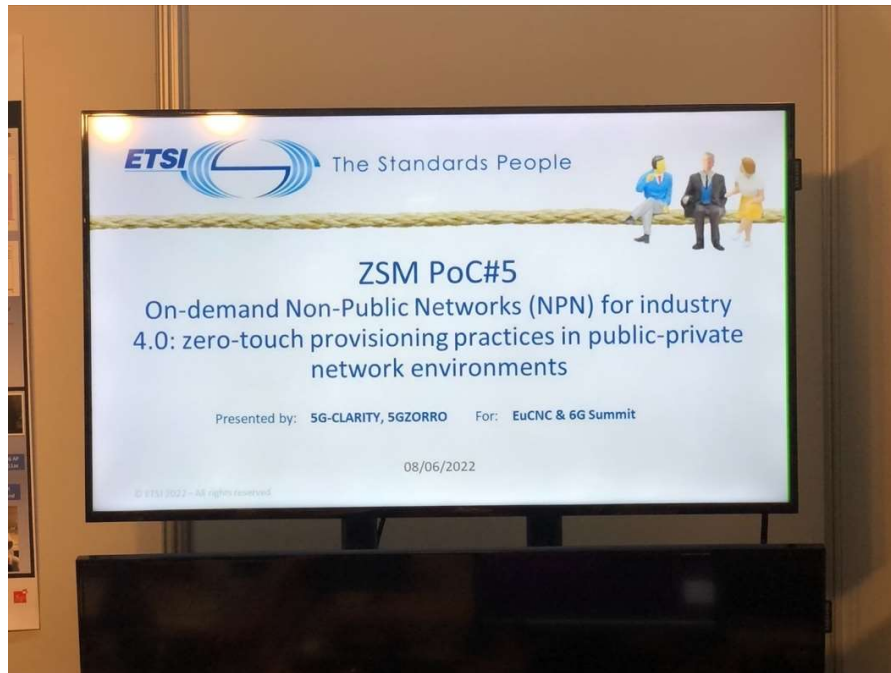


Figure 2: PoC execution video. This video is available at the YouTube channels of participant projects: 5G-CLARITY [7] and 5GZORRO [8].

Figure 3 shows the PoC team members who physically attended the EuCNC & 6G Summit 2022 event. All these members participated in the activities inherent to the PoC showcasing, explaining the golden nuggets to the audience that approached the booths and disseminating ZSM topics in scope of PoC execution.

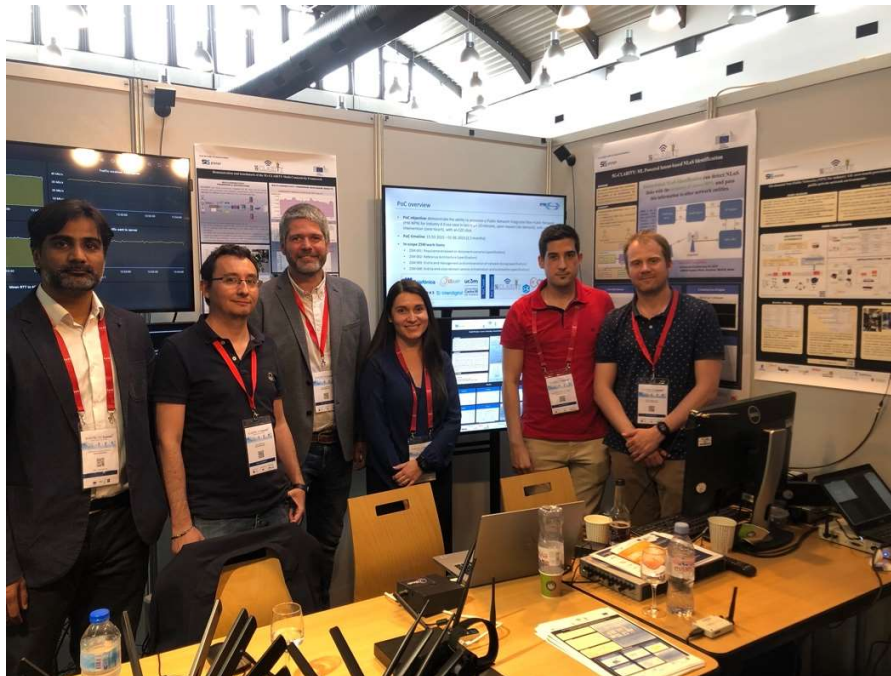


Figure 3: PoC team members who physically attended the event.

1.6 Other dissemination activities

To reach a wider audience, the ISG ZSM PoC#5 will be presented at the NetworkX trade fair (see Figure 4), which will be taking place in-person 18-20 October in Amsterdam, the Netherlands. The conference program combines three top-tier events (5G World, Broadband World Forum, and the newly launched Telco Cloud) under one roof, as well as overarching telco super themes. With over 350 expert speakers and 300 exhibitors, this trade fair constitutes an ideal dissemination venue for PoC#5, which may get much more visibility and thus contribute to increase ZSM awareness among telco and tech giants, start-ups and innovators.

The PoC#5 will be presented at the Expo Stage Theatre in the 5G World event. The specific session will be a 45-minute slot at 12:00 CEST on 20th October.



Figure 4: NextworkX website: <https://networkxevent.com>

2 ZSM PoC Technical Report

2.1 Setting the scene

This section details the rationale and motivation behind PoC#5.

2.1.1 Problem statement

The use of Autonomous Guided Vehicles (AGVs) in factories and warehouses, for example in the transportation of goods, can mitigate the impact of human errors which then leads to improvements in safety, efficiency, quality and productivity of the intralogistics processes. After interviews with real-world industry 4.0 verticals, PoC participants have identified the “as-is” (current) and “to-be” (desired) scenarios in relation to AGV related use cases.

- **As-is scenario:** AGVs have predefined routes for their movement through the factory floor, but the status of the route is ignored.
 - Only the origin and destination are known. With this information, the vertical can carefully plan AGV trajectories, programming the AGV speed, acceleration and deceleration, as well as the specified points where goods are picked up or dropped.
 - However, the vertical does not have visibility on the trajectory in between. This means that any incident causing AGV deviation from the planned route (be it inaccurate speed, sudden acceleration/braking, or unplanned stops) cannot be detected and thus be acted upon by the vertical.

- **To-be scenario:** AGVs have predefined routes for their movement through the factory, and the status of the route is known.
 - The vertical can detect in near real-time whether any incident occurs along the AGV routes, and if so, get valuable information about such an incident, such as its position (coordinates) and root cause (e.g., what has caused the disturbance of AGV planned route?).
 - The vertical can use the above information to gain business intelligence and optimize AGV trajectories accordingly.

2.1.2 Use case description

The shift from as-is to to-be scenarios requires the usage of 5G capabilities. In this regard, it is proposed to develop and showcase a private 5G solution that enhances autonomous navigation of the AGV in the shop floor of a factory, allowing a remote worker to keep track of the AGV trajectory and alert/him on unexpected incidents that cause deviation from the planned route. In the present demo, the incident is the presence of an obstacle on the AGV route.

The use case logic is as follows: when the unexpected incident happens, the AGV slows down or stops, captures a photo on what is in front of it with the on-board camera, and sends the photo to a pre-trained obstacle detection function. This application identifies that the root cause of the incident is an obstacle, and notifies the Operational Technology (OT) operator accordingly, with the coordinates where the obstacle is, together with the photo taken.

2.2 PoC description

2.2.1 PoC objectives

PoC#5 aims at provisioning a private 5G network for this AGV use case. The PoC objectives are all related to the actual provisioning, linking it to the following requirements:

- **FUNC-REQ-1:** the private 5G network shall build on i) 3GPP Rel-15&16 system features, including combined use of 5G NR and Wi-Fi with ATSSS, to provide the necessary performance (e.g., throughput and latency) and functional capabilities (e.g., multi-access technology support); ii) pre-trained obstacle detection application, to assist AGV trajectory.
- **FUNC-REQ-2:** the private 5G network shall be deployed as a Public Network Integrated Non-Public Network (PNI-NPN), with all service components executed on the factory premises (private 5G infrastructure), except for the application function, which runs on the telco edge node (public 5G infrastructure). The PNI-NPN is the 3GPP jargon used for referring to hybrid 5G (public-private) deployments.
- **FUNC-REQ-3:** the private 5G network will be commissioned and configured using an end-to-end network slice. According to the recommendations captured in 3GPP TS 23.501 [9], the usage of network slicing is key to make an agile yet efficient provisioning of an PNI-NPN.
- **FUNC-REQ-4:** the private 5G network shall be provisioned on-demand, upon customer request.
- **FUNC-REQ-5:** the private 5G network shall be provisioned with full automation (no human intervention).
- **NON-FUNC-REQ-1:** the private 5G network shall be provisioned in less than 10 minutes.

To achieve the above-listed requirements (five functional requirements and one non-functional requirement), the PoC #5 makes use of the ZSM framework assets, which includes ZSM management and data services.

2.2.2 PoC architecture

For the PoC #5, the network slice realizing the PNI-NPN is end-to-end, covering the following network domains:

- Access network. This network domain includes two physical nodes: i) one small-cell gNB, providing 5G NR protocol stack; and ii) one Wi-Fi access point, providing IEEE 802.11ax protocol stack. This network domain also includes one Multi-Path TCP (MPTCP) proxy, which terminates MPTCP connections coming from the mobile CPE and that are linked to access traffic steering, switching and splitting (ATSSS) functionality. ATSSS is a 3GPP Rel-16 feature that allows making a combined use of both 5G NR and Wi-Fi 6 technologies at the same time.
- Core Network. It is implemented using Open5GS [10]. This 5GC solution suite is right-sized for use in private 5G networks, and can be deployed fully virtualized.

- **Transport Network.** It corresponds to Ethernet fabric consisting of Layer-2 (L2) switches.
- **Data Network.** This domain hosts the obstacle detection application, developed by Interdigital and pre-trained with obstacles from a real-world factory. This application function is deployed after the UPF, at the 3GPP N6 interface.

Figure 5 shows the PoC architecture.

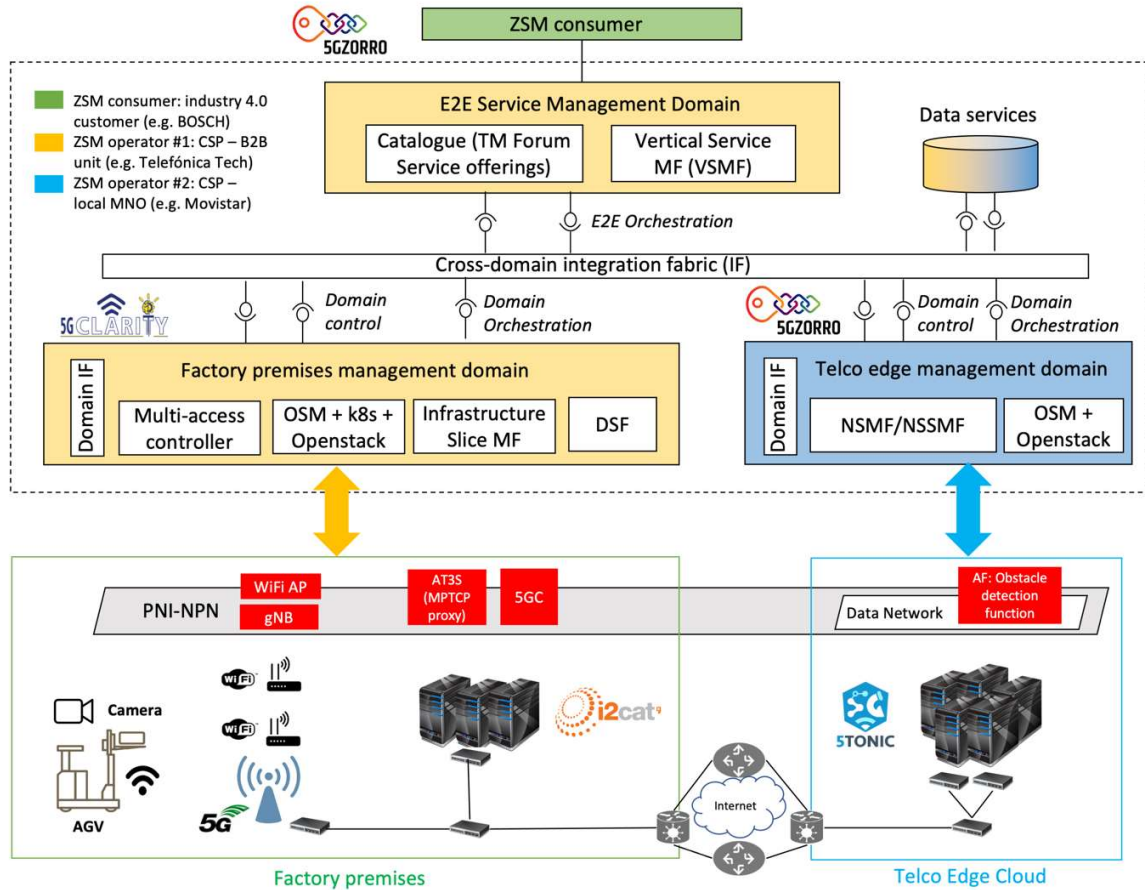


Figure 5: PoC architecture.

The lower side of Figure 5 illustrates **the infrastructure view of the architecture**, shedding light on how the different network domains span across the public-private network infrastructure. As shown in the picture, all the slice components are deployed within the factory boundaries, except for the application function, hosted in the telco edge node; in other words, all 3GPP managed functions are executed atop the on-prem infrastructure. As it was not possible to validate the PoC in productive environment, a testbed was used instead (for further details, see [11]). In this testbed:

- the i2CAT lab facility [12] provides the environment that mimics the factory premises
- 5TONIC lab facility [13] represents the telco edge node
- the AGV is replaced with a multi-connectivity CPE with the camera on board. The CPE takes photos and sends them to the application function for obstacle detection.
- the i2CAT and 5TONIC facility sites are connected using link-layer connectivity over L3VPN, as reported in [14].

The upper side of Figure 5 illustrates **the management viewpoint of the architecture**. This view has two different dimensions under consideration.

- On the one hand, the different roles that take part in ZSM resource operation:
 - The on-prem resources (and functions running atop) are operated by ZSM operator #1. This role is played by the B2B unit of a CSP, who is the service provider (business contact) of the industry 4.0 vertical. This vertical, as owner of the in-factory infrastructure, plays the role of the ZSM consumer and hands the management activities over to the ZSM operator #1.

- The telco edge cloud resources (and application function running atop) are within the administrative domain of the ZSM operator #2. This role is played by the local MNO, with which ZSM operator #1 has a business agreement with.
 - The typical scenario is where ZSM operator #1 and #2 are played by different units of the same CSP company. This is the assumption made for the present PoC.
- On the other hand, the mapping of management and orchestration stack to the ZSM reference framework [5]. One can notice that not all the ZSM service categories specified in [5] are planned to be used in the PoC implementation. This is because the PoC focuses on the fulfilment activities, so only orchestration and control services are strictly required; the rest of ZSM services (e.g., intelligence, data collection, analytics, etc.) are more relevant to the assurance activities. The table below provides a list of the components that constitute the PoC, and their mapping with ZSM services.

Management domain	Component	Provided ZSM services
ZSM operator #1 – E2E MD	Catalogue ¹	• E2E orchestration • E2E data services
	Vertical Service Management Function (VSMF) ¹	• E2E orchestration • E2E data services • Domain integration fabric • Supporting services (policy mgmt)
ZSM operator #1 – MD's	Multi-access controller ²	• (AN) Domain orchestration • (AN) Domain control • Supporting services (policy mgmt) • (AN) Domain data services
	Infrastructure Slice Management Function ²	• (NSS) Domain orchestration • (NSS) Domain control • (NSS) Domain data services
	MANO stack ² : NFVO (Open Source MANO) + VIM (Openstack) + CISM (k8s)	• (Cloud+CN) Domain orchestration • (Cloud+CN) Domain control • (Cloud+CN) Domain integration fabric • Supporting services (policy mgmt) • (Cloud+CN) Domain data services
	Data Semantics Fabric (DSF) ²	• (TN) Domain orchestration • (TN) Domain control • (TN) Domain data services
ZSM operator #2 – MD's	Network Slice [Subnet] Management Function (NSMF/NSSMF) ¹	• (NSS) Domain orchestration • (NSS) Domain control • (NSS) Domain data services
	MANO stack ¹ : NFVO (Open Source MANO) + VIM (Openstack)	• (Cloud+DN) Domain orchestration • (Cloud+DN) Domain control • (Cloud+DN) Domain integration fabric • (Cloud+DN) Supporting services (policy mgmt) • (Cloud+DN) Domain data services
NOTE 1: The components marked with (1) are provided by the 5GZORRO project. The components marked with (2) are provided by the 5G-CLARITY project. NOTE 2: Multi-access controller deals with 5G NR and Wi-Fi6, together with MPTCP proxy (ATSSS functionality) allowing for their combined use.		

According to the above table, it is worth to mention that the solutions available in the management domains owned by ZSM operator #1 and #2 are different, despite having similar functionality. For example, the solutions providing network slice management functionality are based on different implementations. This is realistic in real-world scenarios, where different units of the same CSP work with different vendors and therefore different telco stacks, since their targeted services and customers are not the same.

2.2.3 PoC user story

The table below details the user story of the PoC.

User story	Description
Pre-conditions	• ZSM operator #1 (CSP's B2B unit) has a marketplace with industry 4.0 partners. These partners include vendors, solution integrators and application developers, among others. • ZSM operator #1 (CSP's B2B unit) is the partner service provider for ZSM consumer (industry vertical). There exists a provider-customer relationship between ZSM operator #1 and ZSM consumer. • ZSM operator #2 (CSP's MNO unit) administrates PLMN assets, scale infrastructure nodes and spectrum. • ZSM operator #1 and ZSM operator #2 are units from the same CSP company. For the provision of services for B2B customers that require the use of PLMN assets, ZSM operator #1 has agreements with ZSM operator #2. • There exists WAN connection between ZSM operator #1 and ZSM operator #2 facilities. This connection is based on a link-layer connectivity over L3VPN, as reported in [14]. • There is a pre-existing private 5G network, on premises, that is already managed by the ZSM operator #1. This network is a Standalone NPN (SNPN). • Obstacle detection application is onboarded by ZSM consumer into ZSM operator #1. This application is pre-trained.
Begins when	• ZSM consumer issues a service order to ZSM operator #1, asking for the provision of a private 5G network fulfilling a particular set of service requirements. These requirements are captured in an SLA. • Upon capturing service order, the ZSM operator #1 realizes that the SNPN is not enough, since it cannot host the obstacle detection function. Therefore, the ZSM operator #1 decides on the provisioning solution: a PNI-NPN consisting of an on-prem advanced 5G system, with the obstacle detection application deployed on the telco edge node. • The PNI-NPN resources are to be allocated into an end-to-end network slice.
Steps	A number of workflows are executed. These workflows include request-response and notify-subscription messages across the PoC architecture components, and that are detailed in Section 2.3.
Post-conditions	• All the managed functions building up the PNI-NPN are successfully instantiated and configured. • ZSM operator #1 (CSP's B2B unit) informs ZSM consumer (vertical) that the private 5G network is set up and running. • From this moment on, the use case is operative. This means that the CPE can start taking photos and sending them over to the obstacle detection function. The function will identify the obstacle with a high confidence level.

2.2.4 PoC setup

Figure 6 shows the implementation details of the PoC.

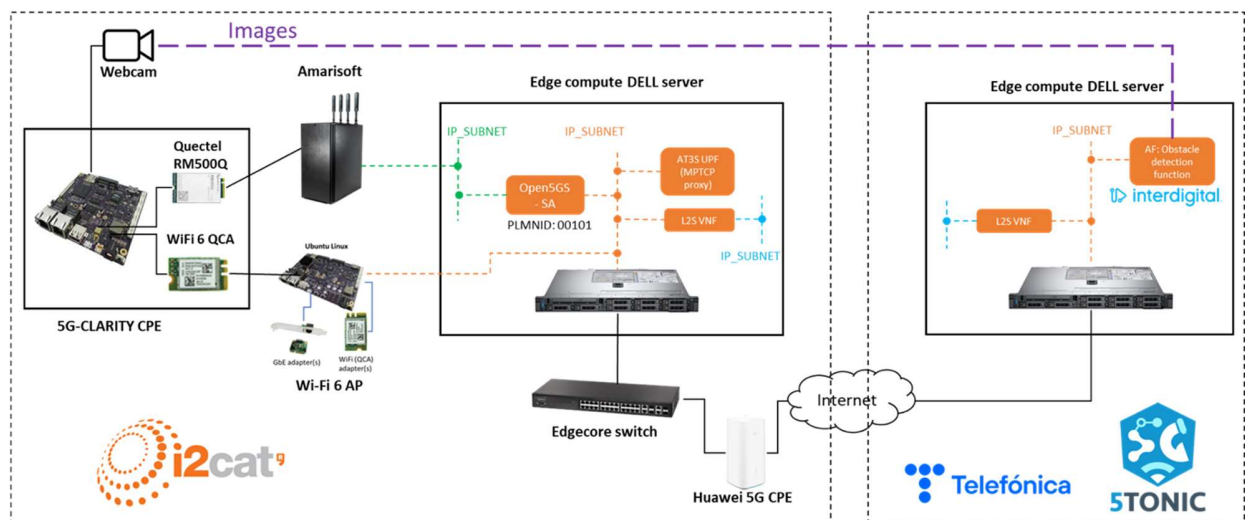


Figure 6: PoC setup.

Figure 7 and Figure 8 show further details of the actual facilities which were used in the PoC.

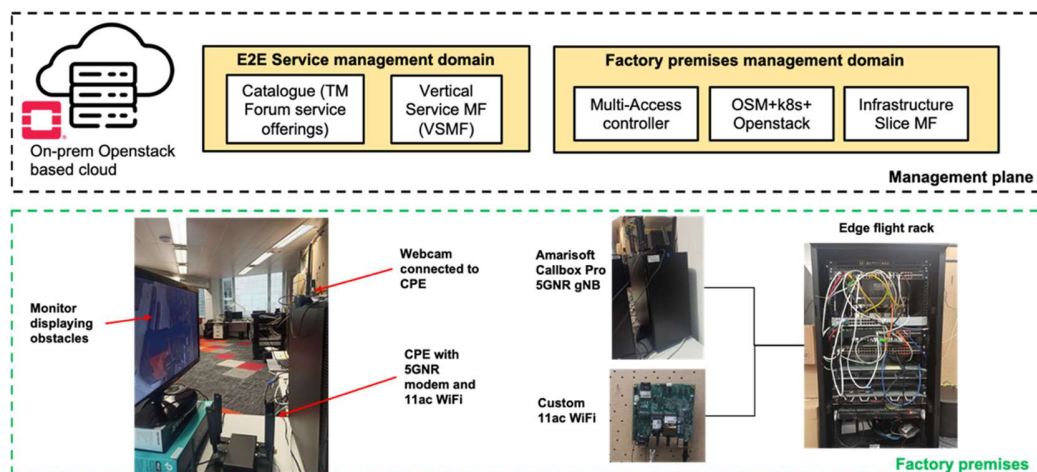


Figure 7: i2CAT lab facility (acting as factory premises).

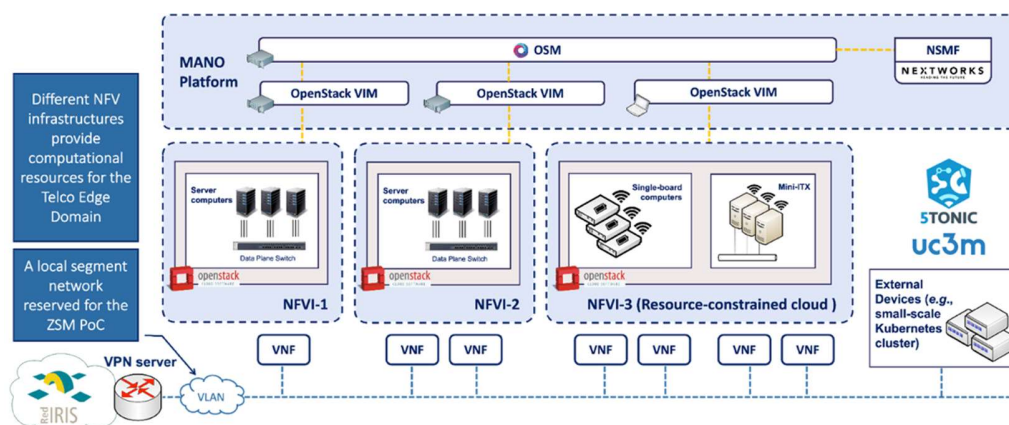


Figure 8: 5TONIC lab facility (acting as public network).

2.3 PoC showcasing

This section provides a tutorial-style description of workflow execution for this PoC.

2.3.1 PoC initial stage: the E2E slice is not yet provisioned

2.3.1.1 Scenario #1: Onboarding descriptors into the NFV stacks

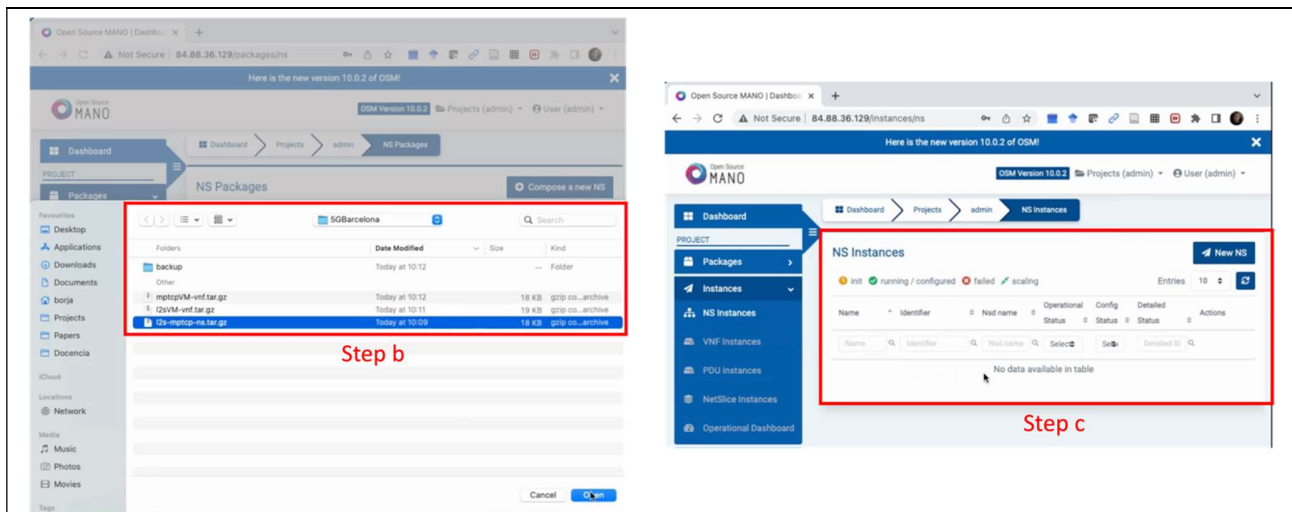
Goal	To make all the NFV artifacts, including VNF Packages and NSDs, available into the OSM stack of individual management domains: ZSM operator #1 (@i2CAT) and ZSM operator #2 (@5TONIC) .
Pre-conditions	• All the requirements captured in Error! Reference source not found., row “pre-conditions”. • No VNF Package / NSD is onboarded into OSM (@i2CAT) • No VNF Package / NSD subnet is onboarded into OSM (@5TONIC)
Post-conditions	• The VNF Package / NSD associated to the virtualized workloads to be deployed at the factory premises are available into the OSM’s (@i2CAT) catalogue. • The VNF Package / NSD associated to the virtualized workloads to be deployed at the factory premises are available into the OSM’s (@5TONIC) catalogue.
Sequence flow	Includes steps a-e described below.

Step a -> OSM (@i2CAT), OSM (@5TONIC): ZSM operators #1 and #2 sign in to start sessions in the NFVO’s belonging to their administrative domains.

The image displays two side-by-side screenshots of the Open Source MANO (OSM) dashboards. The left screenshot is for the @i2CAT domain, showing the 'Projects' view with a sidebar menu and a main area displaying 'No Instances Available' and a 'Failed Instances' section. The right screenshot is for the @5TONIC domain, showing the 'VNF Packages' view with a sidebar menu and a main area displaying 'Just drag and drop files or click here to upload files' and a table with 'No data available in table'.

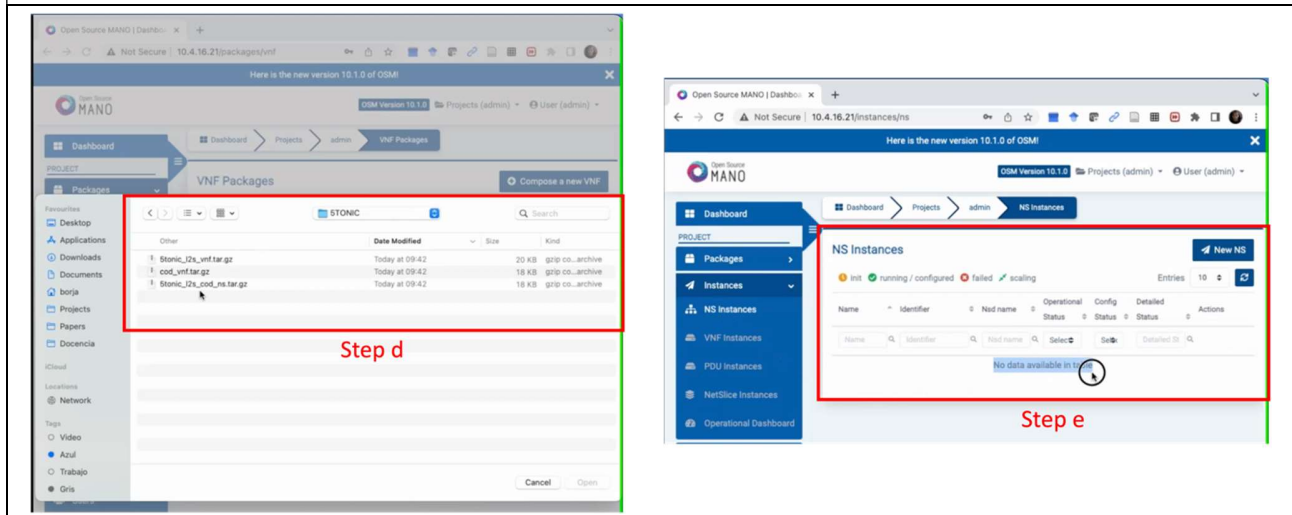
Step b -> OSM (@i2CAT): ZSM operator #1 onboards VNF Packages and NSDs into the OSM’s catalogue.

Step c -> OSM (@i2CAT): ZSM operator #1 gains access to OSM’s inventory, and validates that no NFV instances are created yet.



Step d-> OSM (@5TONIC): ZSM operator #2 onboards VNF Packages and NSDs into the OSM catalogue.

Step e-> OSM (@5TONIC): ZSM operator #2 gain access to OSM's inventory, and validates that no NFV instances are created yet.



2.3.1.2 Scenario #2: 5G-CLARITY CPE connectivity status

Goal	To validate status of available 5G and WiFi networks before deploying the E2E network slice (PNI-NPN).
Pre-conditions	CPE equipped with 5G and WiFi connectivity
Post-conditions	No suitable WiFi or 5G networks are found after scanning because the E2E network slice has not been provisioned yet.
Sequence flow	Includes steps a-c described below.
Step a -> CPE (@I2CAT): ZSM operator #1 shows the list of interfaces available at the CPE. The Wpl4s0 is the WiFi interface and wwan0 is the 5GNN interface.	

```

root@5gclarity-cpe:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp1s0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0d:b9:50:f2:24 brd ff:ff:ff:ff:ff:ff
3: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0d:b9:50:f2:25 brd ff:ff:ff:ff:ff:ff
    inet 192.168.40.66/24 brd 192.168.40.255 scope global dynamic enp2s0
        valid_lft 6692sec preferred_lft 6692sec
    inet6 fe80::20d:b9ff:fe50:f225/64 scope link
        valid_lft forever preferred_lft forever
4: enp3s0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0d:b9:50:f2:26 brd ff:ff:ff:ff:ff:ff
5: wlp4s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 50:e0:85:87:6a:f4 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::52e0:85ff:fe87:6af4/64 scope link
        valid_lft forever preferred_lft forever
7: wwan0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether f6:42:86:67:e7:49 brd ff:ff:ff:ff:ff:ff
root@5gclarity-cpe:~# iw wlp4s0 scan | grep -i etsiPoc
root@5gclarity-cpe:~#
(reverse-i-search)`minic': minicom -D /dev/ttyUSB2

```

Wi-Fi

5G NR

Step b -> CPE (@i2CAT): ZSM operator #1 scans for Wi-Fi Access Points (APs) named “etsiPoC” in the CPE. As noted below, no APs are found.

```

root@5gclarity-cpe:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp1s0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0d:b9:50:f2:24 brd ff:ff:ff:ff:ff:ff
3: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0d:b9:50:f2:25 brd ff:ff:ff:ff:ff:ff
    inet 192.168.40.66/24 brd 192.168.40.255 scope global dynamic enp2s0
        valid_lft 6692sec preferred_lft 6692sec
    inet6 fe80::20d:b9ff:fe50:f225/64 scope link
        valid_lft forever preferred_lft forever
4: enp3s0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0d:b9:50:f2:26 brd ff:ff:ff:ff:ff:ff
5: wlp4s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 50:e0:85:87:6a:f4 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::52e0:85ff:fe87:6af4/64 scope link
        valid_lft forever preferred_lft forever
7: wwan0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether f6:42:86:67:e7:49 brd ff:ff:ff:ff:ff:ff
root@5gclarity-cpe:~# iw wlp4s0 scan | grep -i etsiPoc
root@5gclarity-cpe:~#
(reverse-i-search)`minic': minicom -D /dev/ttyUSB2

```

Step c -> CPE (@i2CAT): ZSM operator #1 scans for availability of 5G networks. As seen, only one 5G network is found, which corresponds to the public network of a Tier-1 in Spain.

```

Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on Dec 23 2019, 02:06:26.
Port /dev/ttyUSB2, 10:40:44

Press CTRL-A Z for help on special keys

at+qscan=2
+QSCAN: "NR5G",214,03,640704,428,-,-,-,1

OK

```

2.3.2 PoC execution: workflow sequence

This section details the core part of the PoC, with all the workflows associated to the on-demand slice provisioning and activation. For the sake of clarify, these workflows have been grouped into three scenarios, as shown in the figure below.

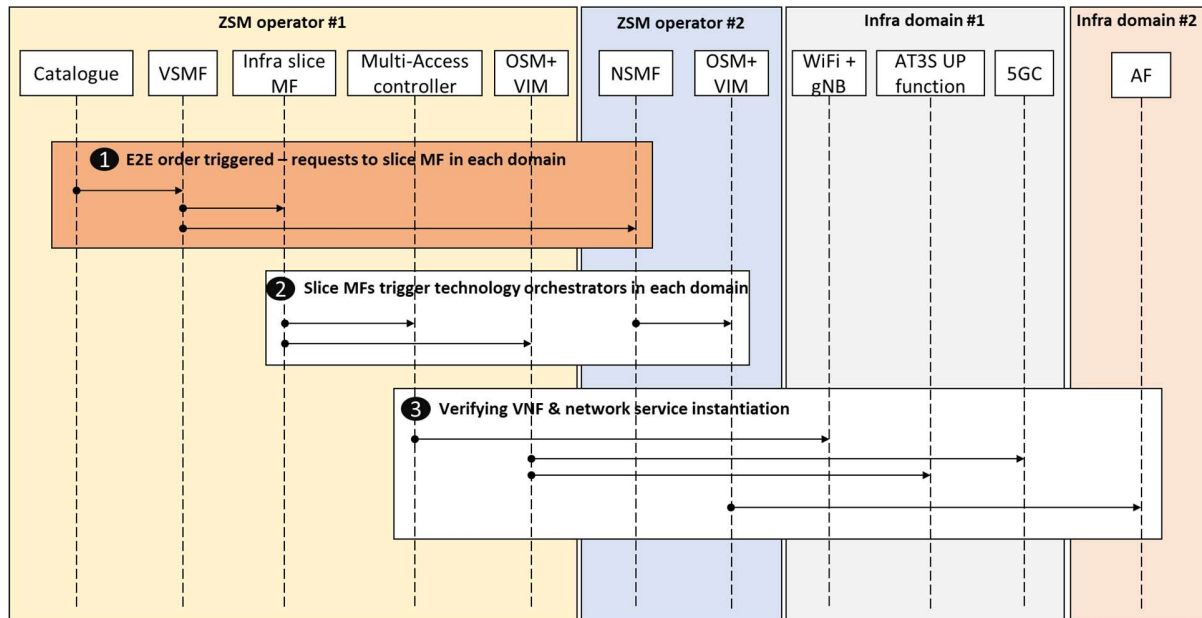
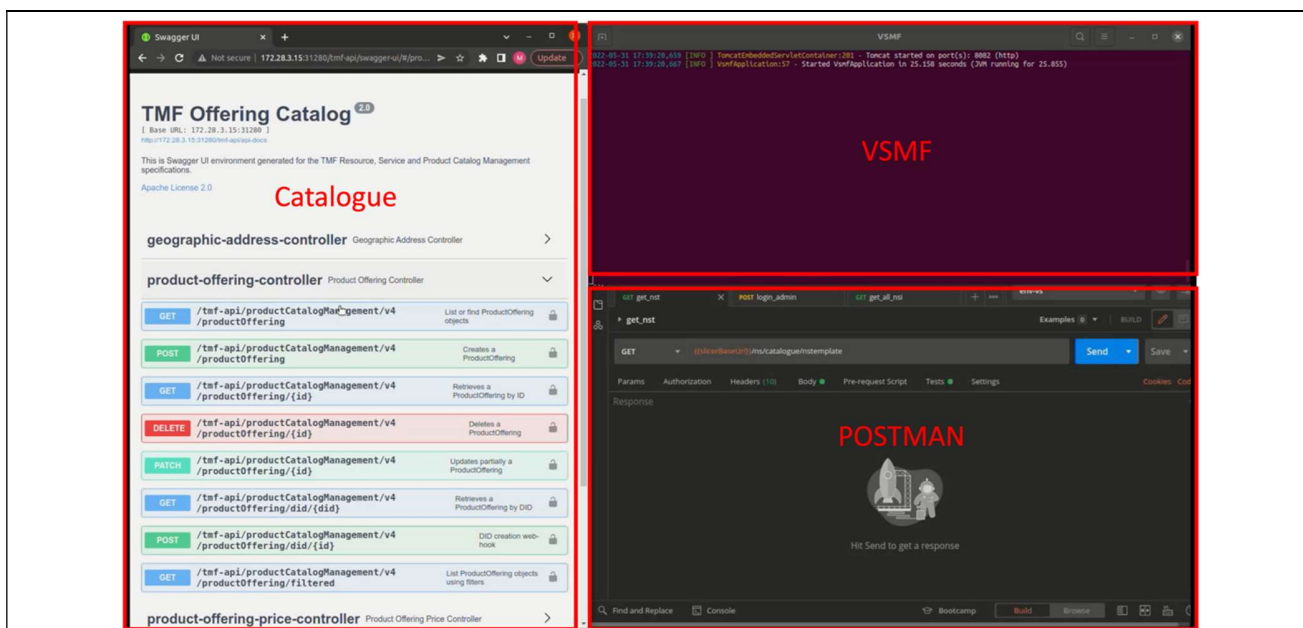


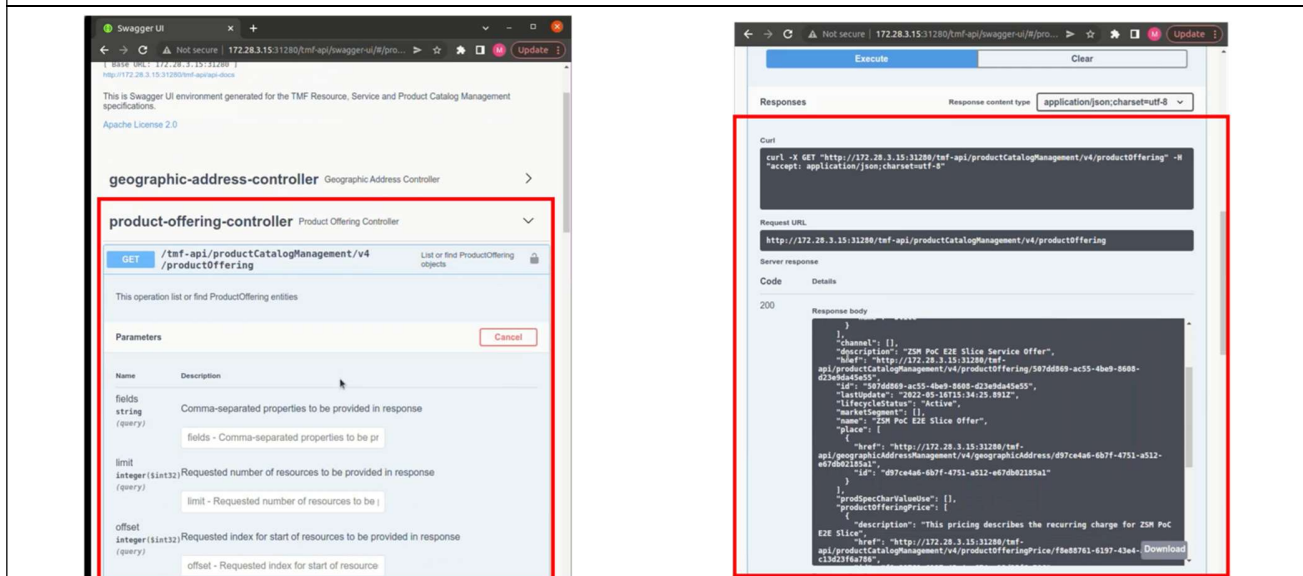
Figure 9: Workflow sequence.

2.3.2.1 Scenario #1: E2E order triggered – request to slice MF in each domain

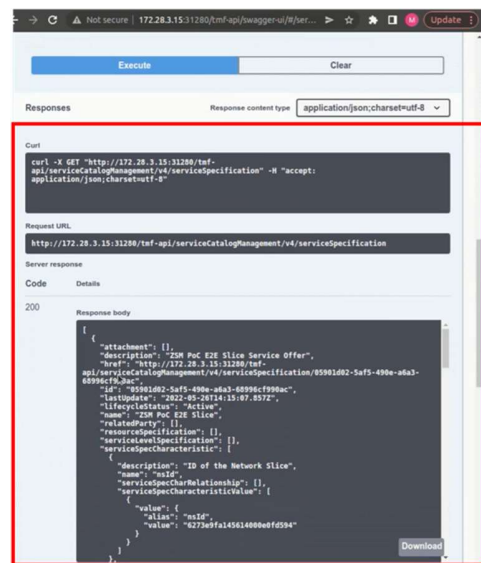
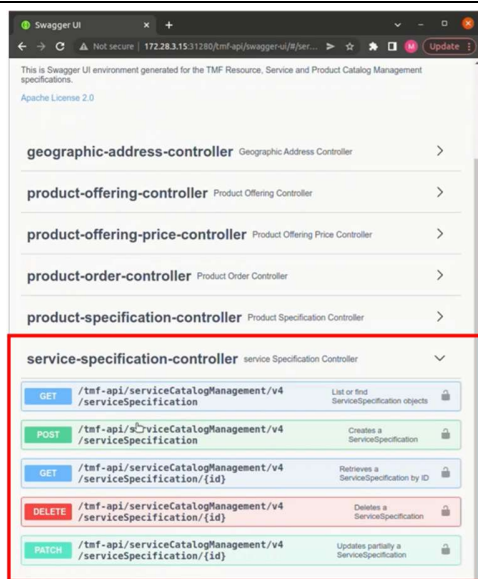
Goal	To enable the ZSM Consumer query the available TMF Service Offerings from the Catalogue, and ask for the deployment of the E2E network slice. This service order will automatically trigger orchestration workflows involving ZSM Operator #1 (@i2CAT) and ZSM operator #2 (@STONIC).
Pre-conditions	- The E2E network slice service offering (compliant with the TMF Product Offer data model) is onboarded in the E2E Service Management domain's Catalogue. - The E2E network slice template (aligned with 3GPP Network Resource Model) is onboarded in the VSMF. - No end-to-end Network Slice instances are currently provisioned and managed by the VSMF
Post-conditions	- The Infrastructure Slice MF (@i2CAT) is invoked by the VSMF to trigger the instantiation of factory premise subnet slice in the ZSM Operator #1 domain. - The NSMF/NSSMF (@STONIC) is invoked by the VSMF to trigger the instantiation of the obstacle detection subnet slice in the ZSM Operator #2 domain.
Sequence flow	Includes steps a-f described below.
Step a -> Catalogue (@i2CAT), VSMF (@i2CAT): ZSM consumer can access the Catalogue User Interface to issue API calls for managing E2E network slice offerings. Similarly, the ZSM operator #1 can access the VSMF (through a Postman User Interface) to issue API calls for managing E2E network slice templates and instances (e.g., for monitoring/observing purposes).	



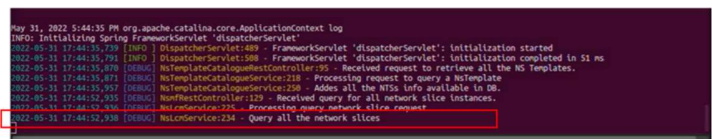
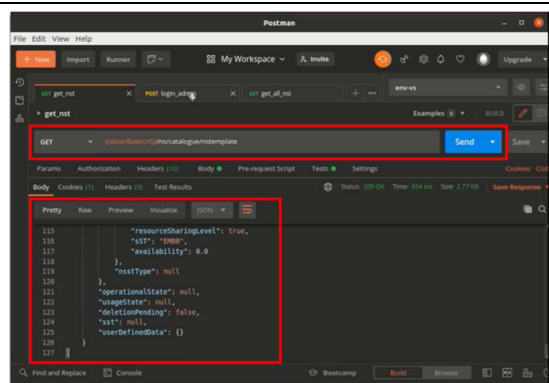
Step b -> Catalogue (@i2CAT): The ZSM Consumer can retrieve the E2E network slice offering as a TMF compliant Product Offer, by accessing the Catalogue User Interface.



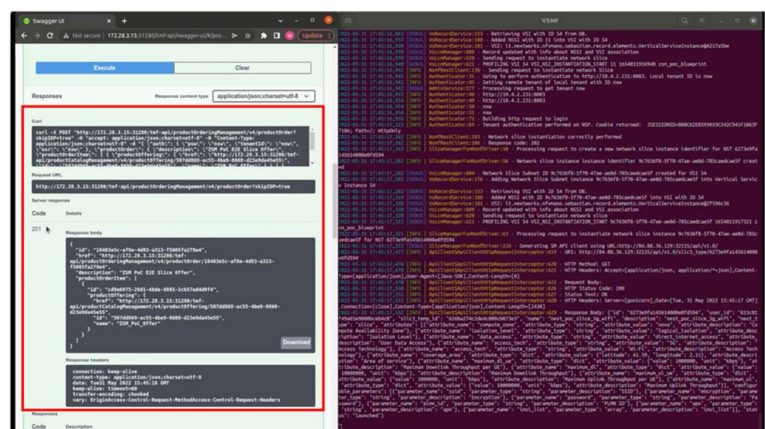
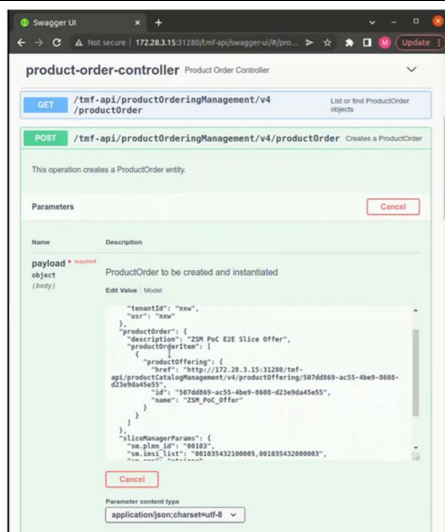
Step c -> Catalogue (@i2CAT): The ZSM Consumer can also browse the specific slice offering specification through the Catalogue (@i2CAT) User Interface by issuing a dedicated API call, which returns the network slice features and requirements.



Step d -> VSMF (@i2CAT): The ZSM Operator #1 can fetch the 3GPP aligned Network Slice Template (with the slice subnets) from the VSMF through the VSMF User Interface (based on Postman). This allows to retrieve the low-level technical requirements of the E2E network slice.



Step e -> Catalogue (@i2CAT): Now, the ZSM consumer can order the Network slice directly from the Catalogue User Interface.



Step f -> VSMF (@i2CAT): The VSMF processes the request and proceeds (in parallel) with requesting the activation of the factory premise subnet slice (RAN + 5GC + ATSSS) through the Infrastructure Slice MF (@i2CAT), and the obstacle detection subnet slice in the public network through the NSMF/NSSMF (@5TONIC).

The screenshot shows a Swagger UI interface for a REST API. The URL is `http://172.28.3.15:31280/tnf-api/productOrderingManagement/v4/productOrder?skipIP=true`. The response is a JSON object with the following structure:

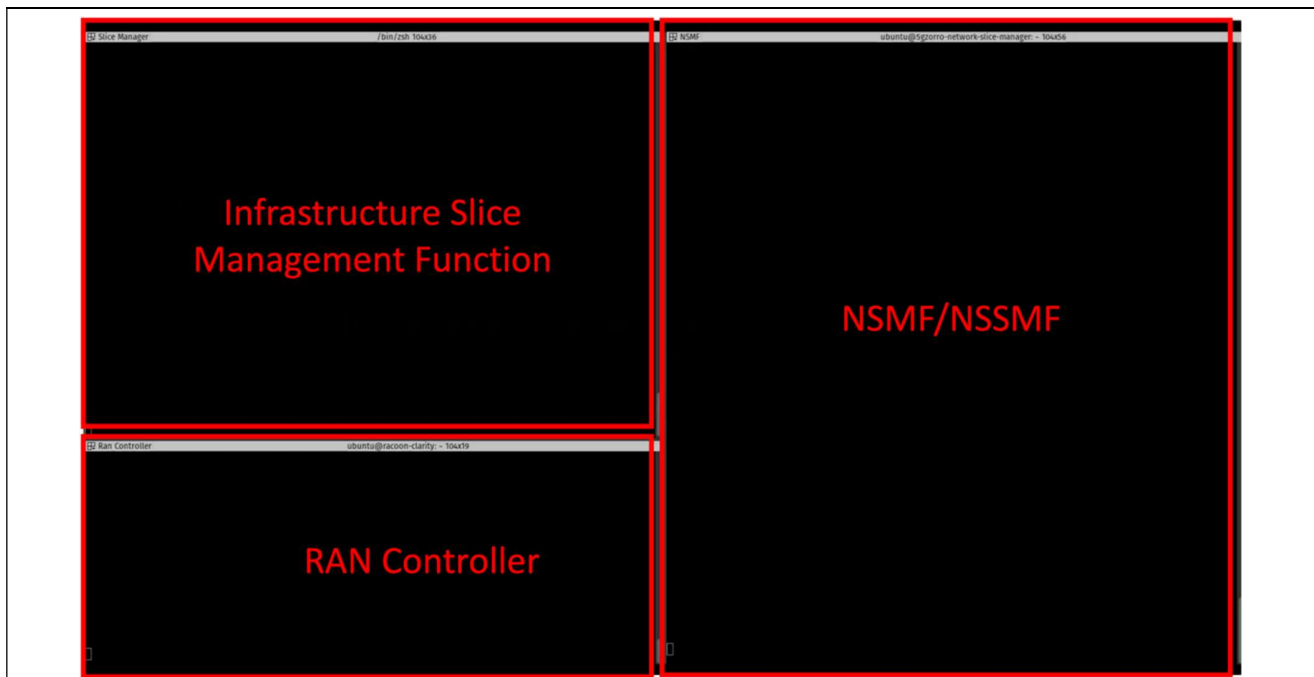
```

{
  "id": "18403e5c-af8e-4d33-a313-f5065fa278e4",
  "href": "http://172.28.3.15:31280/tnf-api/productOrderingManagement/v4/productOrder/18403e5c-af8e-4d33-a313-f5065fa278e4",
  "description": "ZSM PoE E2E Slice Offer",
  "productOrderItem": [
    {
      "id": "cd9ae973-28d1-48de-8885-2cb57e4d49f4",
      "productOffering": {
        "href": "http://172.28.3.15:31280/tnf-api/productCatalogManagement/v4/productOffering/507d0869-ac55-4be9-8608-d23edda5e55",
        "description": "507d0869-ac55-4be9-8608-d23edda5e55",
        "name": "ZSM PoE Offer"
      }
    }
  ]
}

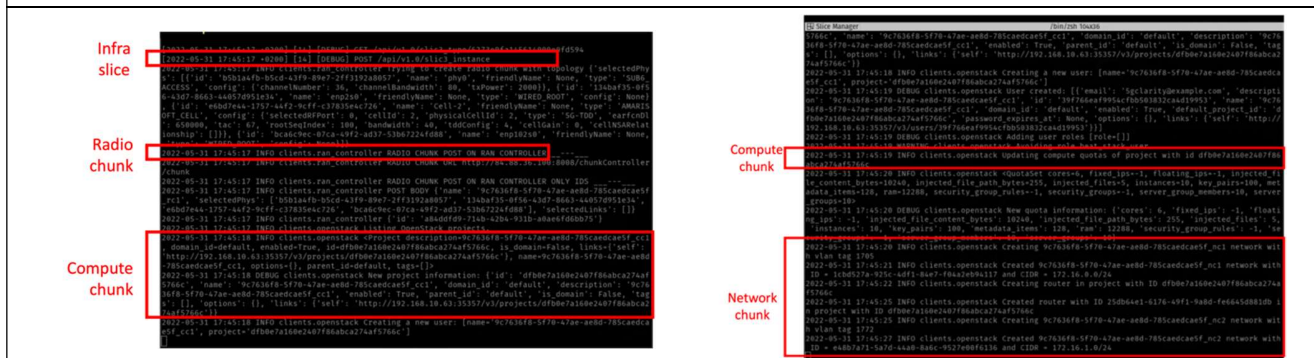
```

2.3.2.2 Scenario #2: Slice MFs trigger technology orchestrators in each management domain

Goal	Instantiate and configure the VNFs and PNFs in the two infrastructure domain: private (infrastructure domain #1) and public (infrastructure domain #2). The mission is to provision the PNI-NPN as as an E2E slice.
Pre-conditions	- VNFs are on-boarded into the NFVO of private and public domains. - Physical network functions (Wi-Fi APs and 5GNNR gNB) are registered in the multi-access controller (@i2CAT). - E2E slice provisioning triggered from VSMF.
Post-conditions	- VNF with obstacle detection function instantiated in the public domain. - Dedicated 5GC, DHCP server, ATSSS user plane function and L2VPN function deployed on the on-prem edge compute node (see Figure 6 and Figure 7). - Wi-Fi AP and 5GNNR gNB are configured to advertise dedicated SSID and PLMNID for the PNI-NPN.
Sequence flow	Includes steps a-h described below.
Step a -> Infrastructure slice MF (@i2CAT), RAN controller (@i2CAT), NSMF/NSSMF (@5TONIC): ZSM operators #1 and #2 gain access to these components.	



Step a -> Infrastructure Slice MF (@12CAT): creation of the slice, composed of radio, compute and network chunks of infrastructure resources.



Step b -> NSMF/NSSMF (@5TONIC): receives the obstacle detection function subnet slice instantiation request, process it by retrieving the related NFV NSD and issues and instantiation request to the 5TONIC OSM.

Instantiation request
issues to 5TONIC
OSM.

Step c -> Infrastructure Slice MF (@I2CAT): launching of the mobile core and DHCP server to enable the user connectivity.

```

er@chunuk/a84ddf9-714b-42ba-931b-a0ae6fdbb75/service /bin/zhsh 10x3s
2022-05-31 17:45:28 INFO business.radio_service Trying to deploy open5gs core network
2022-05-31 17:45:29 INFO clients.openstack Creating Mobile Core instance in 9c7636f8-5f70-47ae-aed8-785cdae5cf_nc1
2022-05-31 17:45:30 INFO clients.openstack Waiting for Mobile Core core_9c7636f8-5f70-47ae-aed8-785cae5cf_nc1 to configure interfaces properly
2022-05-31 17:45:45 INFO clients.openstack Interfaces on Mobile Core core_9c7636f8-5f70-47ae-aed8-785cae5cf_nc1 successfully configured ['9c7636f8-5f70-47ae-aed8-785cae5cf_nc1': ['172.16.0.17'], '9c7636f8-5f70-47ae-aed8-785cae5cf_nc2': ['172.16.1.49'], 'acceleran-access-net-1701': ['192.168.100.14']]
2022-05-31 17:45:45 INFO clients.openstack Created Mobile Core instance 9c7636f8-5f70-47ae-aed8-785cae5cf_nc1
2022-05-31 17:45:45 INFO clients.openstack Disabling port security on port 02eab478-2cdc-4728-839a-5653bc16f950
2022-05-31 17:45:45 INFO clients.openstack Disabling port security successfully on interface 02eab478-2cdc-4-4728-839a-5653bc16f950
2022-05-31 17:45:45 INFO clients.openstack Disabling port security on port 16679421-9ea3-423a-9168-f2802a9deeba
2022-05-31 17:45:46 INFO clients.openstack Disabling port security successfully on interface 16679421-9ea3-423a-9168-f2802a9deeba
2022-05-31 17:45:46 INFO clients.openstack Disabled port security successfully on interface 16679421-9ea3-423a-9168-f2802a9deeba
2022-05-31 17:45:46 INFO clients.openstack Disabled port security successfully on interface 16679421-9ea3-423a-9168-f2802a9deeba
2022-05-31 17:45:46 INFO clients.openstack Allocating Floating IP from network 1193bd5b-b714-40e5-a64e-14b0fd55ee8c to Project dfb0e7a160e2407f86abc274af5766c
2022-05-31 17:45:48 INFO clients.openstack Allocated Floating IP 192.168.40.178 successfully to Project dfb0e7a160e2407f86abc274af5766c
2022-05-31 17:45:48 INFO clients.openstack Attaching Floating IP 192.168.40.178 to server core_9c7636f8-5f70-47ae-aed8-785cae5cf_nc1
2022-05-31 17:45:51 INFO clients.openstack Attached Floating IP 192.168.40.178 successfully to server core_9c7636f8-5f70-47ae-aed8-785cae5cf_nc1 nating in server's IP 172.16.0.17
2022-05-31 17:45:52 INFO business.radio_service Extra DHCP server is attached to 1cbd527a-925c-4df1-84e7-fc04a2eb9417
2022-05-31 17:45:52 INFO clients.openstack Creating DHCP server...
2022-05-31 17:45:53 INFO clients.openstack DHCP server instance created!

```

Step d -> Infrastructure Slice MF (@I2CAT): call towards the RAN controller for the configuration of the radio service.

Step e -> RAN Controller (@I2CAT):

- Creation of a virtual Wi-Fi interface for the slice
- Configuration of the Wi-Fi Access Point on top of the virtual interface
- Creation and configuration of the 5G NR cell. Multi-Operator Core Network (MOCN) is used to connect the cell to the dedicated 5GC.
- Creation of the VLAN interfaces to connect the access points to the slice.

```
2022-05-31 17:46:02 INFO clients.ran_controller RADIO SERVICE POST ON RAN CONTROLLER ---
2022-05-31 17:46:02 INFO clients.ran_controller RADIO SERVICE URL http://84.88.36.100:8008/chunkController/chunk/a84ddf9-714b-42b4-931b-a0ae6df6bb75/service
2022-05-31 17:46:02 INFO clients.ran_controller POST BODY {'selectedPhys': ['b5b1a4fb-b5cd-43f9-89e7-2ff3192a8057', '134ba6f35-0f56-43d7-8663-44057d951e34', 'e6b7de44-1757-44f2-9cff-c37835e4c726', 'bca6c9ec-0c3a-49f2-ad37-53b67224f88'], 'vlanId': 1795, 'serviceConfig': {'cellularConfig': {'plmnId': '00103', 'amariSoftConfig': {'coreIpAddress': '172.16.1.49', 'corePort': 38412, 'vlanCore': 1772}, 'wirelessConfig': {'ssid': 'etsiPoC', 'encryption': 'WPA', 'password': 'etsiPoC22'}}}}
```

Step f -> Infrastructure Slice MF (@I2CAT): instantiation of the services on top of the slice. Services include ATSSS user plane function (for a combine use of 5G NR and Wi-Fi) and L2VPN service (to connect to 5TONIC site).

[illegible]

```

2022-05-31 17:47:00 -> 2020-01-01 [INFO] GET /api/v1.0/network_service_instance/6296384651188a000de6a5a
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:03 INFO business.network_service_instance Allowed DNS traffic in compute chunk '9c7636f
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:03 INFO business.network_service_instance Allowed DNS traffic in compute chunk '9c7636f
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:03 INFO business.network_service_instance Allowed ICMP traffic in compute chunk '9c763
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:03 INFO [GET] /api/v1.0/s1ic_instance/6296384651188a000de6a5a
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:03 INFO clients.opentaskBadRequest adding security rule icmp:1
2022-05-31 17:47:03 INFO business.network_service_instance Allowed ICMP traffic in compute chunk '9c7636f
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:03 INFO business.network_service_instance Allowed SSH traffic in compute chunk '9c7636f
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:03 INFO clients.opentaskBadRequest adding security rule tcp:22
2022-05-31 17:47:03 INFO business.network_service_instance Allowed SSH traffic in compute chunk '9c7636f
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:03 INFO business.network_service_instance Allowed DNS traffic in compute chunk '9c7636f
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:04 -> 2020-01-01 [INFO] GET /api/v1.0/network_service_instance/6296384651188a000de6a5a
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:04 INFO clients.opentaskBadRequest adding security rule tcp:53
2022-05-31 17:47:04 INFO clients.opentaskBadRequest adding security rule udp:53
2022-05-31 17:47:04 INFO business.network_service_instance Allowed DNS traffic in compute chunk '9c7636f
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:04 INFO business.network_service_instance Allowed ICMP traffic in compute chunk '9c763
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:05 INFO clients.opentaskBadRequest adding security rule icmp:1
2022-05-31 17:47:05 INFO business.network_service_instance Allowed ICMP traffic in compute chunk '9c7636f
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:05 INFO business.network_service_instance Allowed SSH traffic in compute chunk '9c7636f
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:05 INFO clients.opentaskBadRequest adding security rule tcp:22
2022-05-31 17:47:05 INFO business.network_service_instance Allowed SSH traffic in compute chunk '9c7636f
18-5f70-47ae-aed-785caedca5ef_csl'
2022-05-31 17:47:08 INFO clients.opm 'short-name'

```

Step g -> NSMF/NSSMF (@5TONIC): OSM (@5TONIC) instantiates a single-VNF network services for the obstacle detection function, and notifies the NSMF/NSSMF accordingly. The NSMF/NSSMF in turn notifies the VSMF (@i2CAT) about the successful creation of the network slice subnet

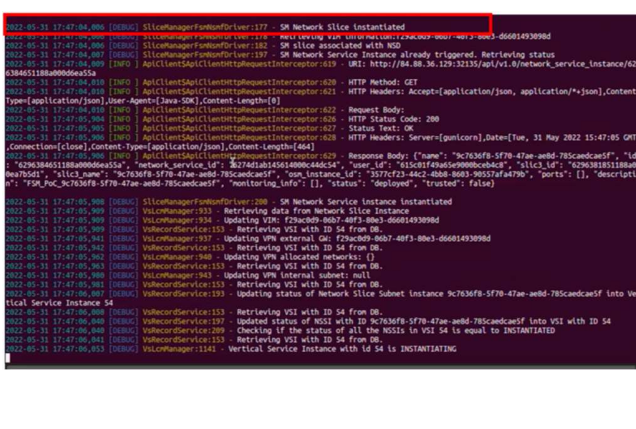
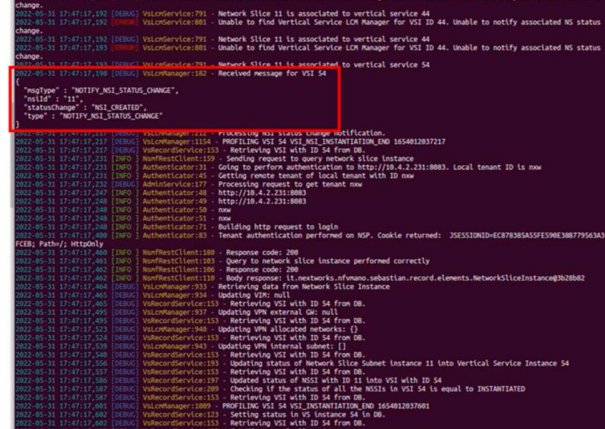
[illegible]

```

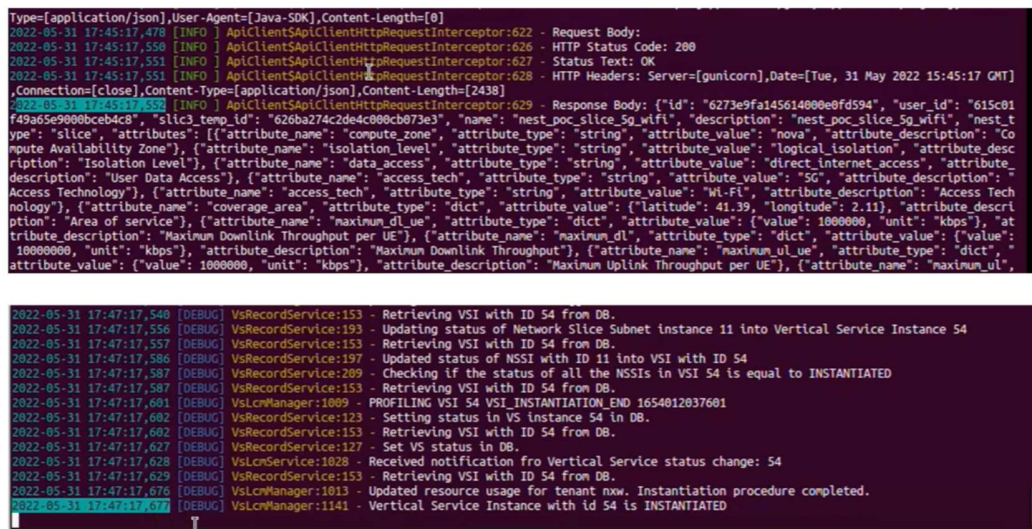
2022-05-31 17:47:16,735 DEBUG NSKRecordService:125 - Retrieving NSI associated to NFV Network Service with ID 2797c7ca-88e5-49b1-9131-c82cf4ad9e1 from DB
2022-05-31 17:47:16,735 DEBUG NSKRecordService:125 - Retrieved NSI 2797c7ca-88e5-49b1-9131-c82cf4ad9e1 is associated to network slice 11
2022-05-31 17:47:16,783 DEBUG NFVnlcmOperationManager:119 - Notification sent
2022-05-31 17:47:16,781 DEBUG NFVnlcmOperationManager:119 - Operation 0962d64d-c774-4f8a-820e-e26dbf3cee removed from the list of VNM operations to be polled
2022-05-31 17:47:16,782 DEBUG NFVnlcmOperationManager:119 - Operation 0962d64d-c774-4f8a-820e-e26dbf3cee removed from polling processing.
2022-05-31 17:47:16,782 DEBUG NSKManager:168 - Received message for NSI 11
2022-05-31 17:47:16,782 DEBUG NSKManager:168 - Received message for NSI 11
{"msgType": "NOTIFY_NSI_NSI_STATUS_CHANGE",
"infoFields": {"2797c7ca-88e5-49b1-9131-c82cf4ad9e1": {"statusChange": "NS_CREATED", "successful": true, "type": "NOTIFY_NSI_NSI_STATUS_CHANGE"}},
2022-05-31 17:47:16,785 DEBUG NSKManager:187 - Processing NFV NSI status change notification.
2022-05-31 17:47:16,785 DEBUG NSKManager:187 - Successful instantiation of NFV NS 2797c7ca-88e5-49b1-9131-c82cf4ad9e1 and network slice 11
2022-05-31 17:47:16,829 DEBUG NSKController:264 - Building terminate NS request in SOL 005 format
2022-05-31 17:47:16,812 DEBUG NSKManager:496 - Retrieving NSsi tree for NSI:nsnt_vpn_al_image_recognit on Instance 1011 nstnsid=1011
2022-05-31 17:47:16,812 DEBUG NSKService:198 - Adding slice subnets into parent slice 11 in DB.
2022-05-31 17:47:16,813 DEBUG NSKService:220 - Retrieving NSI with ID 11 from DB.
2022-05-31 17:47:16,813 DEBUG NSKService:286 - Subscribed to NSI 11
2022-05-31 17:47:16,829 DEBUG NSKService:290 - received request to register a NS LCM for:11 nstnsid=nsnt_vpn_al_image_recognition tenant=ns
2022-05-31 17:47:16,829 DEBUG NSKService:386 - Already registered, IGNORING
2022-05-31 17:47:16,829 DEBUG NSKService:220 - Retrieving NSI with ID 11 from DB.
2022-05-31 17:47:16,839 DEBUG NSKService:141 - Setting status INSTANTIATED for network slice 11 in DB.
2022-05-31 17:47:16,839 DEBUG NSKService:220 - Retrieving NSI with ID 11 from DB.
2022-05-31 17:47:16,856 DEBUG NSKManager:438 - Status set for network slice 11
2022-05-31 17:47:16,856 DEBUG NSKManager:438 - Sending notification to engine.
2022-05-31 17:47:16,860 DEBUG VnmRestClient:59 - Sending notification about NSI status change
2022-05-31 17:47:16,860 DEBUG VnmRestClient:59 - Sending notification about NSI status change http://172.28.3.15:8122. Local tenant ID is ns
2022-05-31 17:47:16,861 DEBUG Authenticator:45 - Getting remote tenant of local tenant with ID ns
2022-05-31 17:47:16,861 DEBUG Authenticator:377 - Processing request to get tenant name
2022-05-31 17:47:16,868 INFO Authenticator:48 - http://172.28.3.15:81092
2022-05-31 17:47:16,868 INFO Authenticator:49 - http://172.28.3.15:81092
2022-05-31 17:47:16,869 INFO Authenticator:59 - ns
2022-05-31 17:47:16,869 INFO Authenticator:59 - ns
2022-05-31 17:47:16,869 INFO Authenticator:71 - Building http request to login
2022-05-31 17:47:17,107 INFO Authenticator:83 - Tenant authentication performed on NSP. Cookie returned
2022-05-31 17:47:17,107 DEBUG VnmRestClient:76 - Sending HTTP request to NSP
2022-05-31 17:47:17,107 DEBUG VnmRestClient:72 - Sending HTTP message to notify network slice status change.
2022-05-31 17:47:17,285 DEBUG VnmRestClient:76 - Response code: 200
2022-05-31 17:47:17,286 DEBUG VnmRestClient:80 - Notification correctly dispatched.
2022-05-31 17:47:17,428 DEBUG VnmRestController:96 - Received query for network slice instance with ID 11
2022-05-31 17:47:17,429 DEBUG NSKService:225 - Processing query network slice request
2022-05-31 17:47:17,429 DEBUG NSKService:225 - Retrieving NSI with ID 11 from DB.

```

Step h -> VSMF (@I2CAT): when the VSMF receives notifications of successful subnet slice instantiation, the end-to-end slice instance is ready (status: INSTANTIATED).

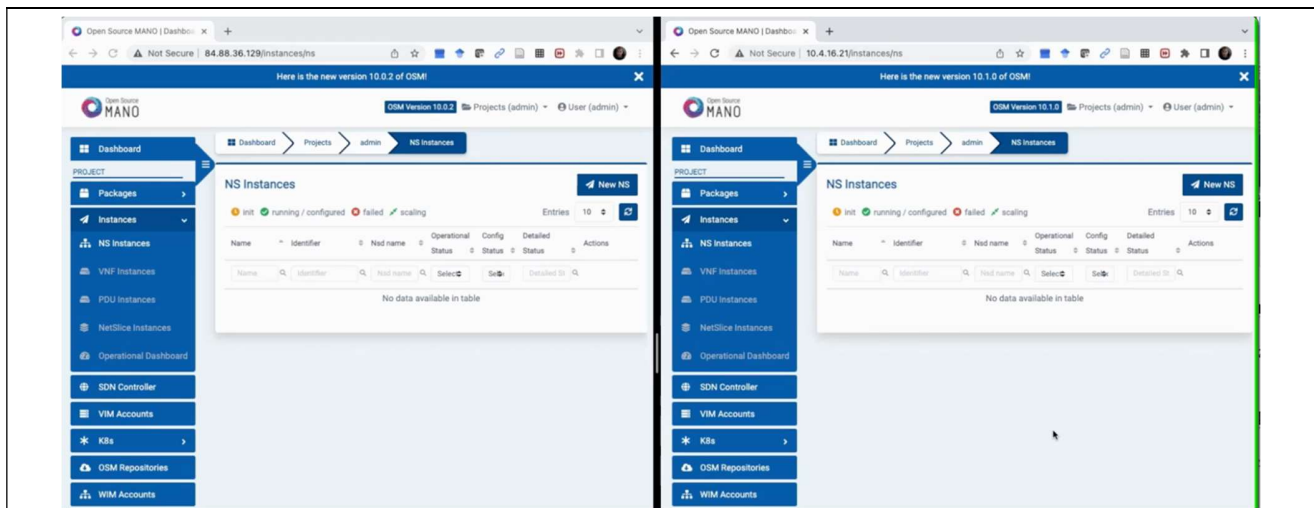
	
---	--

Step i -> VSMF (@i2CAT): the VSMF logs show a total provisioning time of 120 seconds.

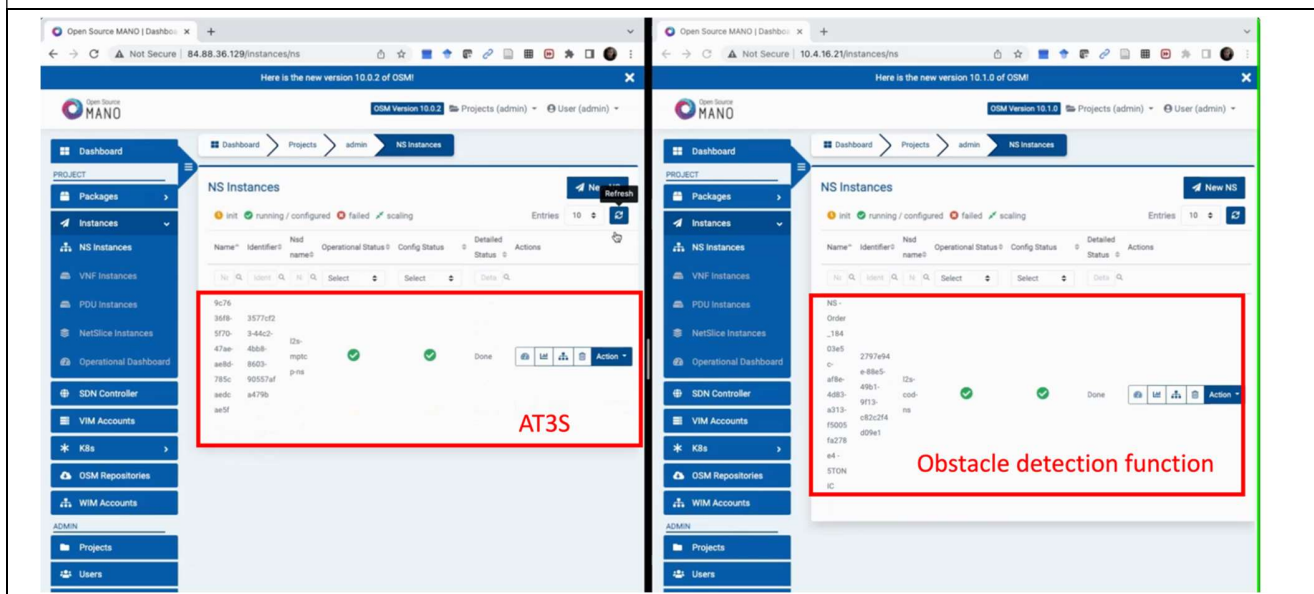
Provisioning start time Provisioning end time	
---	---

2.3.2.3 Scenario #3: Verifying VNF & network service instantiation.

Goal Pre-conditions Post-conditions Sequence flow	This scenario is to simply verify the automated deployment of network services that were executed in the scenarios #2, steps g and h. Instead of Infrastructure slice and NSMF/NSSMF, the viewpoint is now the OSM instances at the two operator domains. - VNF Package and NSD for ATSSS Network Service onboarded into OSM (@i2CAT). - VNF Package and NSD for Obstacle Detection Function Network Service onboarded into OSM (@5TONIC) - Infrastructure Slice MF (@i2CAT) and NSMF/NSSMF (@5TONIC) are processing their slice subnet provisioning actions upon VSMF (@i2CAT) request. - The NFV Network Service for the ATSSS is up and running. - The NFV Network Service for the Obstacle Detection Function is up and running. Includes steps a-b described below. Step a -> OSM (@i2CAT), OSM (@5TONIC): no network services are instantiated in neither in the private infrastructure (left-side figure) or public infrastructure (right-side figure).
---	---



Step b -> OSM (@i2CAT), OSM (@5TONIC): The network services for ATSSS and the obstacle detection function are automatically instantiated as a result of the request issued by the Infrastructure Slice MF (@i2CAT) and the NSMF/NSSMF (@5TONIC). After some time, both network services are up and running.



2.3.3 PoC final stage: the E2E slice is provisioned

2.3.3.1 Scenario #1: Connecting to the deployed E2E slice

Goal	Connect the AGV CPE to the PNI-NPN that has been provisioned as a slice, on demand.
Pre-conditions	- Wi-Fi AP configured to radiate the dedicated SSID for this slice 5GNR gNB and 5GC are configured with dedicated PLMNID - CPE is preconfigured with SSID and PLMN ID credentials. IMSI is already configured in 5G as part of allowed devices when 5GC is deployed.
Post-conditions	- CPE can scan the Wi-Fi and 5GNR networks finding the expected network identifiers - CPE can connect to the Wi-Fi and 5G networks obtaining an IP address in each interface - Connectivity between CPE and 5GC in private segment is verified
Sequence flow	Includes steps a-c described below.

Step a -> CPE (@i2CAT): Scanning Wi-Fi networks named “etsi PoC”. 5G-CLARITY CPE shows wpa_supplicant configuration to connect to the AP. Then start the wpa_supplicant process. The CPE shows that the Wi-Fi interface is connected to the AP.

```

root@5gclarity-cpe:~# iw wlp4s0 scan | grep -i etsiPoC
SSID: etsiPoC
root@5gclarity-cpe:~# cat etsi_poc.conf
network={
    ssid="etsiPoC"
    #psk="etsiPoC22"
    psk=06357e0a4422fcd55c7b6b2034f38356a4376077270ba7d8bd5159e836e323
}
root@5gclarity-cpe:~# wpa_supplicant -B -Dnl80211 -iwlp4s0 -c./etsi_poc.conf
Successfully initialized wpa_supplicant
root@5gclarity-cpe:~#
(reverse-i-search)`: "C
root@5gclarity-cpe:~# iw wlp4s0 link
Connected to 02:00:f2:59:d2:e9 (on wlp4s0)
SSID: etsiPoC
freq: 5200
RX: 1063 bytes (14 packets)
TX: 808 bytes (7 packets)
signal: -74 dBm
tx bitrate: 24.0 MBit/s

bss flags:      short-slot-time
dtim period:    2
beacon int:     100
root@5gclarity-cpe:~#

```

Step b -> CPE (@i2CAT): A scan on 5G networks is triggered. Three networks are found. The first one is from a different testbed on our lab. The second one is the one recently deployed (plmnId = 00103) and the last one corresponds to a public network.

```

Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on Dec 23 2019, 02:06:26.
Port /dev/ttyUSB2, 16:22:32

Press CTRL-A Z for help on special keys

at+qscan=2
+QSCAN: "NR5G", 1,02,620352,42,-85,-11,45,1
+QSCAN: "NR5G", 1,03,648960,22,-110,-12,20,1
+QSCAN: "NR5G",214,03,640704,428,-,-,1
OK

```

Step c -> CPE (@i2CAT): the command displayed triggers the connection to the network with APN “etsipoc”. A DHCP request is sent and the CPE receives an IPv4 address. The ping to the 5GC is working.

```

root@5gclarity-cpe:~# qmicli -p -d /dev/cdc-wdm0 --wds-start-network="apn=etsipoc" --client-no-release-cid
[/dev/cdc-wdm0] Network started
Packet data handle: '2924264016'
[/dev/cdc-wdm0] Client ID not released:
Service: 'wds'
CID: '19'
root@5gclarity-cpe:~# udhcpc -i wwan0
udhcpc: started, v1.30.1
udhcpc: sending discover
udhcpc: sending select for 172.16.0.132
udhcpc: lease of 172.16.0.132 obtained, lease time 7200
root@5gclarity-cpe:~# ping 172.16.0.129
PING 172.16.0.129 (172.16.0.129) 56(84) bytes of data.
64 bytes from 172.16.0.129: icmp_seq=1 ttl=64 time=14.9 ms
64 bytes from 172.16.0.129: icmp_seq=2 ttl=64 time=16.2 ms
64 bytes from 172.16.0.129: icmp_seq=3 ttl=64 time=14.7 ms
64 bytes from 172.16.0.129: icmp_seq=4 ttl=64 time=15.1 ms
64 bytes from 172.16.0.129: icmp_seq=5 ttl=64 time=16.7 ms

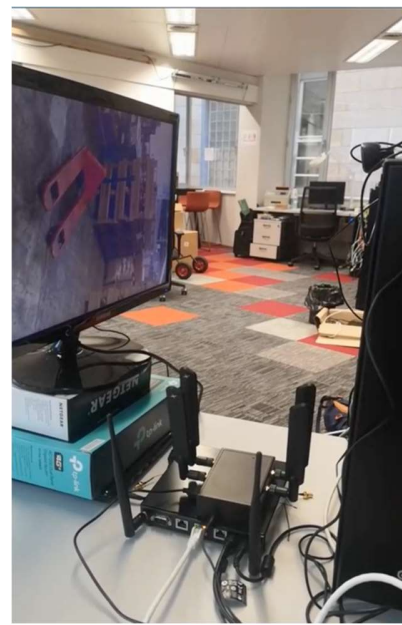
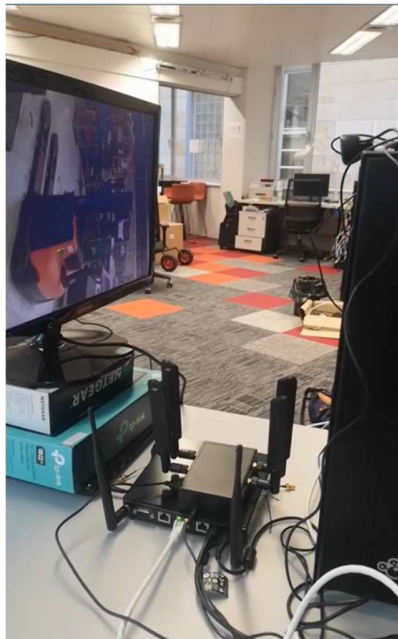
```

2.3.3.2 Scenario #2: Obstacle detection function in action

Goal	Verify end-to-end connection between CPE and obstacle detection function deployed on public segment.
Pre-conditions	• CPE connected to the slice provisioned. • Obstacle detection VNF instantiated on public network. • L2VPN connectivity between private and public domains established

	• Monitor in the lab periodically displays pictures of obstacles recorded in real factory
Post-conditions	• Camera connected to CPE takes pictures from monitors and transmits to obstacle detection function provisioned in public domain • Obstacle detection function successfully identifies the type of obstacle blocking the path of the AGV and reports result in a graphical user interface
Sequence flow	Includes steps a-b described below.

Step a -> Obstacle detection function (@5TONIC): We can see the 5G-CLARITY CPE taking pictures of a monitor displaying real factory obstacles. Recorded images are transmitted to the obstacle detection function deployed at 5TONIC.



Step a -> Obstacle detection function (@5TONIC): We now see the output of the obstacle detection function at 5TONIC successfully detecting the type of obstacle.

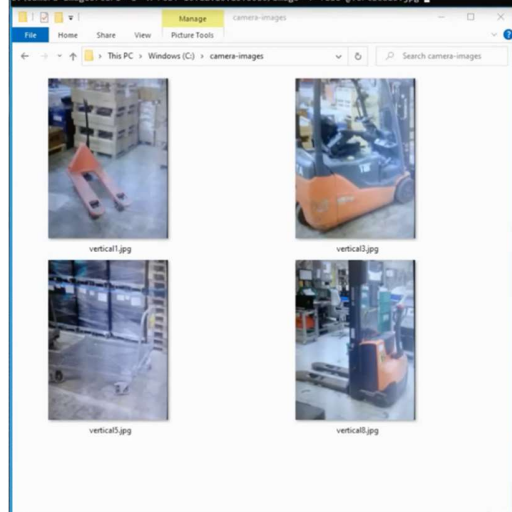
```

Command Prompt
Content-Type: text/html; charset=utf-8
Content-Length: 13
vertical3.jpg
C:\camera-images>curl -i -X POST 10.12.16.13:8080/image -F"file=@vertical3.jpg"
HTTP/1.0 200 OK
Server: Werkzeug/2.1.1 Python/3.8.10
Date: Mon, 30 May 2022 20:44:02 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 13
vertical3.jpg
C:\camera-images>

```

```
vertical3.jpg
C:\camera-images>curl -i -X POST 10.12.16.13:8080/image -F"file=@vertical5.jpg"
HTTP/1.0 200 OK
Server: Werkzeug/2.1.1 Python/3.8.10
Date: Mon, 30 May 2022 20:44:10 GMT
Content-type: text/html; charset=utf-8
Content-length: 11

vertical5.jpg
C:\camera-images>curl -i -X POST 10.12.16.13:8080/image -F"file=@vertical5.jpg"
```



10.12.16.13:8080/status

Not secure | http://10.12.16.13:8080/status



Detected Class: trolley
Confidence: 80.8%
Detection Time: 0.9s

PoC Sponsors

5G CLARITY 5GZORRO 5TONIC

PoC Team

Telefónica NEXWORKS i2cat interdigital uc3m Universidad Carlos III de Madrid

2.4 PoC Contribution to ZSM ISG

Use table B.1 to list any contributions to the ZSM ISG resulting from this PoC Project.

Table B.1

Contribution	WI/Document Ref	Comments	Meeting
ZSM NOC "Emerging Use Cases"	N/A (presentation tied to NOC industry vision)	One of the slides that conform the presentation is entitled "private 5G networks: drivers for massive adoption). This slide is a direct outcome of PoC #5, and claims two things that are the golden nuggets of this PoC report: i) the PNI-NPN is the option which will allow private 5G to gain scale in the medium-term; ii) slicing is an effective provisioning solution for PNI-NPN.	Layer123 Reunion (26-28 April 2022, Madrid)[15]
ZSM(22)000208 "CAMARA project presentation"	N/A (discussion paper not tied to any specific WI/doc)	5G-CLARITY project builds on the 'mediation function' [16] which is a management function which policies interaction between private network operator (CSP's B2B unit) and public network operator (CSP's MNO unit). This mediation function allows for a frictionless network-application integration based on the usage of CAMARA project [17] assets, including architectural blocks (e.g., transformation function, CAPIF-based API GW solution [18]) and service APIs. For further details on the relationship between 5G-CLARITY and CAMARA projects, see 5G-CLARITY deliverable D4.3, section 6.	ZSM#19

2.5 Gaps identified in ZSM standardization

Table B.2

Gap Identified	Forum (ZSM ISG, Other)	Affected WG/EG	WI/Document Ref	Gap details and Status
Integration fabric: no stage 2 & 3 specification	ZSM ISG		ETSI GS ZSM 008 [6]	One of the key enablers for a frictionless cross-domain service orchestration involving different ZSM operator domains (i.e., management domains administrated and operated by different parties) is the integration fabric. This management function was first introduced in ZSM 002 [5]; however, no stage 2 and 3 specification is available so far for this management, neither on ZSM 008 [6] nor any other ZSM specification. Without stage 2 & 3, it is quite difficult to showcase implementations of (domain and cross-domain) integration fabric instances, and therefore to assess their compliance with ZSM recommendations.

2.6 PoC Suggested Action Items

The PoC#5 has focused on the provisioning of a PNI-NPN using an end-to-end slice, spanning from the CPE to the data network, with all the network domains in between: access (combining 5G NR with Wi-Fi), transport network (ethernet switching) and core (lightweight 5GC and UPF with ATSSS agent). The demo has put the focus on three main features: **on demand** (i.e., provisioning PNI-NPN upon customer request), **full automation** (i.e., provisioning PNI-NPN with no human intervention) and **agility** (i.e., provisioning PNI-NPN in less than 10 minutes).

The PoC #5 exemplifies a complete technology evolution path, based on the triplet {research + experimentation + standardization} and with open-source communities (OSM) along the entire path. The PoC has also showed that it is possible to deliver end-to-end solutions combining open-source and commercial products from different technology providers; this sheds light on the old promise of a true multi-vendor 5G ecosystem.

The PoC#5 sets the ground for future experimentation in the future, with:

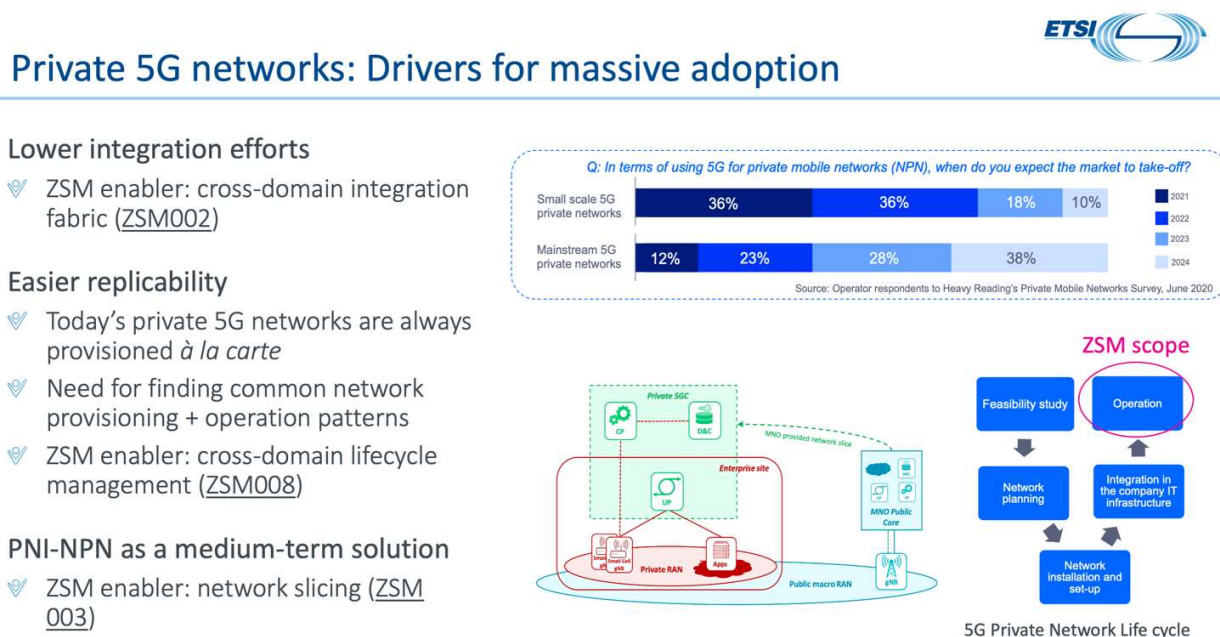
- Other advanced scenarios, where 5G control plane is migrated to the public cloud while keeping UPF on premises, taking advantage of Control User Plane Separation (CUPS).
- Focus on counterpart operational aspects, i.e., everything related to assurance such as monitoring and policy-assisted capacity scaling. Lessons learnt from ISG ZSM PoC#2 [19] and PoC#4 [20] can be used as guidance for this endeavour.

2.7 Additional messages to ZSM

Based on the gap identified in Table B.2, the PoC team recommends ZSM ISG to start working on the stage 2 & 3 details of the integration fabric, capturing these details into a new GS document.

2.8 Additional messages to Network Operators and Service Providers

The slide below is fetched from the ZSM NOC “Emerging Use Cases” deck, presented by ZSM Network Operator Council (NOC) at the Layer123 Reunion [15]. This slide was elaborated based on the objectives and expectations described in the ETSI ZSM PoC#5 proposal [11], when submitted in February this year.



The rollout strategy is a recurrent topic that acclaimed technology analysts have surveyed in the last months. One of the most recent surveys is the one shown in the figure above, from Heaving Reading, where operators are asked to specify by when they expect the private 5G market to take-off. The main conclusions for this survey are as follows:

- Small scale 5G networks are expected no later than 2022.
- Most of respondents are realist that private 5G is a medium-term opportunity for the operator enterprise market.

- Over half of respondents expect private 5G to be mainstream from 2023 onwards.

According to these conclusions, it is clear that Standalone NPNs will be the first ones to be commercialized. 5G innovation here is relatively easy, since there is almost no legacy. However, having greenfield environments does not mean low cost, but just the opposite. The fact that customized 5G networks need to be setup for very specific customer makes CAPEX and OPEX quite high, making this option only affordable by large-sized companies.

However, as the 5G technology matures, the transition from isolated private networks to PNI-NPNs will be reality. This will allow deploying private 5G networks at large scale, dramatically reducing costs and making them affordable for most of customers. And to make this happen, ZSM will play a key role in three main directions:

- Lower integration efforts, thanks to the capabilities provided by the cross-domain integration fabric.
- Easier replicability, with the definition of network provisioning and operation patterns which can be openly reusable in different private network scenarios. This is what drives economies of scale.
- Usage of network slicing as a provisioning solution to make hybrid (public-private) networks a reality.

References

- [1] H2020 project 5G-CLARITY [Online]. Available: <https://www.5gclarity.com/>
- [2] H2020 project 5GZORRO [Online]. Available: <https://www.5gzorro.eu/>
- [3] ETSI GS ZSM 001, "Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios", v1.1.1, October 2019 [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/001/01.01.01_60/gs_ZSM001v010101p.pdf
- [4] ETSI GS ZSM 003, "Zero-touch network and Service Management (ZSM); End-to-end management and orchestration of network slicing", v1.1.1, June 2021 [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/003/01.01.01_60/gs_ZSM003v010101p.pdf
- [5] ETSI GS ZSM 002, "Zero-touch network and Service Management (ZSM); Reference Architecture", v1.1.1, August 2019 [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf
- [6] ETSI GS ZSM 008, "Zero-touch network and Service Management (ZSM); Cross-domain E2E service lifecycle management", v1.1.1, July 2022 [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/008/01.01.01_60/gs_ZSM008v010101p.pdf
- [7] https://www.youtube.com/watch?v=heU_ceO315s&t=183s
- [8] <https://www.youtube.com/watch?v=9F4AVyadTB4&t=120s>
- [9] ETSI TS 123 501, "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 16.6.0 Release 16)", v16.6.0, October 2020 [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.06.00_60/ts_123501v160600p.pdf
- [10] Open5GS [Online]. Available: <https://open5gs.org>
- [11] ISG ZSM PoC proposal #5 [Online]. Available: https://zsmwiki.etsi.org/images/2/2b/ZSM_POC_5.pdf
- [12] <https://i2cat.net/project-cat/industry-4-0/>
- [13] <https://www.5tonic.org>
- [14] Vidal I.; Nogales, B.; Lopez, D.; Rodríguez, J.; Valera, F.; Azcorra, A. "A Secure Link-Layer Connectivity Platform for Multi-Site NFV Services". Electronics 2021, 10, 1868. DOI: <https://doi.org/10.3390/electronics10151868>
- [15] <https://congress.layer123.com/event/f6bbdefe-7441-4e9c-bcb8-9ae25cf1877b/summary>
- [16] 5G-CLARITY Deliverable D4.2, "Validation of 5G-CLARITY SDN/NFV Platform, Interface Design with 5G Service Platform, and Initial Evaluation of ML Algorithms", July 2021. [Online]. Available: https://www.5gclarity.com/wp-content/uploads/2021/11/5G-CLARITY_D42.pdf

- [17] CAMARA project, "The Telco Global API Alliance" [Online]. Available: <https://camaraproject.github.io/index.html>
- [18] CAMARA-CAPIF relationship [Online]. Available: <https://github.com/camaraproject/WorkingGroups/blob/main/Commonalities/documentation/Working/API-exposure-reference-solution.docx>
- [19] ISG ZSM PoC#2, "Automated Network Slice Scaling in Multi-Site Environments", Final Report [Online]. Available: https://zsmwiki.etsi.org/images/8/84/ZSM_POC_2_Final_Report.pdf
- [20] ISG ZSM PoC#4, "Autonomous network slice management", Final Report [Online]. Available: <https://portal.etsi.org/ngppapp/ContributionCreation.aspx?primarykeys=245933>