Deliverable from T72 – D7.2
Prototyping of Vertical Business Use Cases

Editors:	Haithem Afli, CIT
Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	30/11/2019
Actual delivery date:	13/12/2019
Suggested readers:	Verticals, Test-bed managers, WP8
Version:	1.0
Total number of pages:	83
Keywords:	Prototypes, test-beds, verticals

Abstract

The objectives of the WP7 are two folded. One task is to prototype an innovative cross-plane orchestrator to be able to automate the different functionalities (FCAPS) associated to the automation of the slice management. The orchestrator will coordinate the operations of the data plane, control plane, management plane and service plane for optimised network slicing, and deploy NFV actions for operational requirements on demand related to QoE sensors/actuators to monitor/optimise the QoE of a use case service. The second task, T7.2 described in this deliverable, is focussing on prototyping the demanding vertical business use cases.

Three selected representative use cases will be prototyped in this WP including Smart Grid use case, eHealth (Connected Ambulance) use case, and Smart City use case. The idea of this WP is to provide a set of enabling automated mechanisms required to perform the cross-plane configuration of all the architectural components involved for efficient slice management.

[End of abstract]

Disclaimer

The research leading to these results has received funding from the European Union Horizon 2020 Programme under grant agreement number H2020-ICT-2016-2/761913.

Impressum

[Full project title] End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks

[Short project title] SLICENET

[Number and title of work-package] WP7 - Cross-Plane Orchestration and Use Cases Prototyping

[Number and title of task] T7.2 – Prototyping of Vertical Business Use Cases

[Document title] D7.2 - Prototyping of Vertical Business Use Cases

[Editor: Name, company] Haithem Afli, CIT

[Work-package leader: Name, company] Pedro Miguel Neves, Altice Labs

Copyright notice

Executive summary

This deliverable first describes the task of prototyping all three vertical business use cases defined in SLICENET [1]. Then an overview of use cases utilisation of SN enabling technologies is provided with more details of the generic workflows involved in the network slice life cycle, according to the principles and concepts described in 3GPP TR28.801.

Details about utilization of specific SliceNet infrastructure, features and components are described in next section dealing with work-flows of the eHealth, Smart City and Smart Grid Use Cases. Also, more details about the adaptation of the existing UC business applications/services is provides with a description of the legal and regulatory environment for likely deployment and routable version of time-critical protocols.

The last section of this document is providing a description of the preparation work of the evaluation prototype for the three uses cases, that will be detailed in next deliverable D8.3.

List of authors

Company	Author	Contribution
CIT	Haithem Afli Mark Roddy	Editors
DellEMC	Thuy Truong Mustafa Al-Bado	eHealth Prototypes description
RedZinc	Ricardo Figueiredo Donal Morris Jeanne Caffrey Huyen Tran	eHealth Prototypes description
CIT	Mark Roddy Haithem Afli	eHealth Prototypes description
Altice Labs	Pedro Miguel Neves José Cabaça	Generic workflows descriptions; Smart Grid Prototypes description
Efacec Energia	Ana Aleixo Carlos Fernandes Carlos Arantes	Smart Grid Prototypes description Section head for evaluation preparations
Orange Romania	Marius Iordache Catalin Brezeanu Horia Stefanescu Cristian Patachia	Smart City Prototypes description
UWS	Jose Alcarez-Calero	UC utilisation of SN enablers
TEI	Ciriaco Angelo	UC utilisation of SN enablers

List of reviewers

Company	Reviewer	Comments
CIT	Haithem Afli	N/A
DellEMC	Mustafa Al-Bado	N/A
Altice Labs	José Cabaça	N/A

Table of Contents

List of figures

List of tables

Abbreviations

A list of abbreviations is strongly recommended

5G	Fifth Generation (mobile/cellular networks)
5G PPP	5G Infrastructure Public Private Partnership
API	Application Programming Interface
APM	Anomaly Prediction Module
DSL	Digital Subscriber Line
DSP	Digital Services Provider
E2E	End-To-End
FCAPS	Fault Configuration Accounting Performance and Security
FED	Federal Reserve System
HoN	Health of Network
IoT	Internet of Things
KPI	Key Performance Indicator
M2M	Machine to Machine
MEC	Multi-access Edge Computing
MRO	Maintenance, repair and operations
NAFTA	North American Free Trade Agreement
NS	Network Slice
NSP	Network Service Provider
OPEX	Operational Expenditure
OSA	One Stop API
QoE	Quality of Experience
OPEX	Operational Expenditure
P&P	Plug and Play
PNF	Physical Network Function
QoS	Quality of Service

RAN	Radio Access Network
R&D	Research and Development
RRH	Remote Radio Head
SDN	Software Defined Networks
SLICENET	End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks
SON	Self-Organizing Networks
SSO	Service & Slice Orchestrator
SWOT	Strengths, Weaknesses, Opportunities, and Threats analysis
VAT	Value-added tax
vEPC	virtual Evolved Packet Core
VIM	Virtual Infrastructure Manager
VNF	Virtual Network Function
VSF	Virtual Software Function
WAN	Wide Area Network

1 Introduction

T7.2 encloses all the activities related to the prototypically implementation of the three vertical use cases: Smart Grid, eHealth and Smart City, over the integrated SliceNet infrastructure (note the difference between infrastructure and framework/architecture presented in Figure 1).

The goal of this task is to develop the use cases' prototypes, leveraging the technology developed in WPs 3-6 and T7.1. For instance, the eHealth Connected Ambulance use case is an exemplar of a critical vertical/application with challenging performance requirements that must be delivered with an accompanying high level of reliability, resilience and security.

The use cases' requirements determined in T2.1 will also drive the development of the prototypes. These requirements will also be influenced by the legal and regulatory environment surrounding likely deployments.

For this task, T7.2 will identify the actors, the actions they can perform and their goals. The goals will guide the identification of the detailed functional and non-functional requirements of the 5G infrastructure and services that were developed in WPs 3-6 and T7.1.

T7.2 will cover early integration of slicing control, slice management and orchestration. The prototyping will include adaptation of the existing vertical business applications/services (application level) to run in the SliceNet infrastructure, operation of the applications over the Integrated infrastructure prototyped in WP3, utilisation of key enablers for slicing control (including verticals' P&P control) prototyped in WP4, early utilisation of key enablers for slice management (QoE & FCAPS) prototyped in WP5 & WP6, and early adoption of the orchestrator being prototyped in WP7. The aim is to provide the vertical use cases running in the execution environment where the SliceNet architecture is providing the slicing capabilities.

T7.2 will design and configure the environment required to stage the prototypes; the prototyping results will be fed into the testing and validation activities in T8.3.

To this end T7.2 has found it important to define this working document (WD) that will be used to clarify and direct the ongoing work from SliceNet work-packages 7 and 8 (WP7 and WP8).

This WD will include a description of the prototypes/demonstrators presented in the Figure 1 below to be committed to the final vertical test-beds, including the vertical specific workflows for those prototypes, the timelines for integration and the expected outputs to WP8.

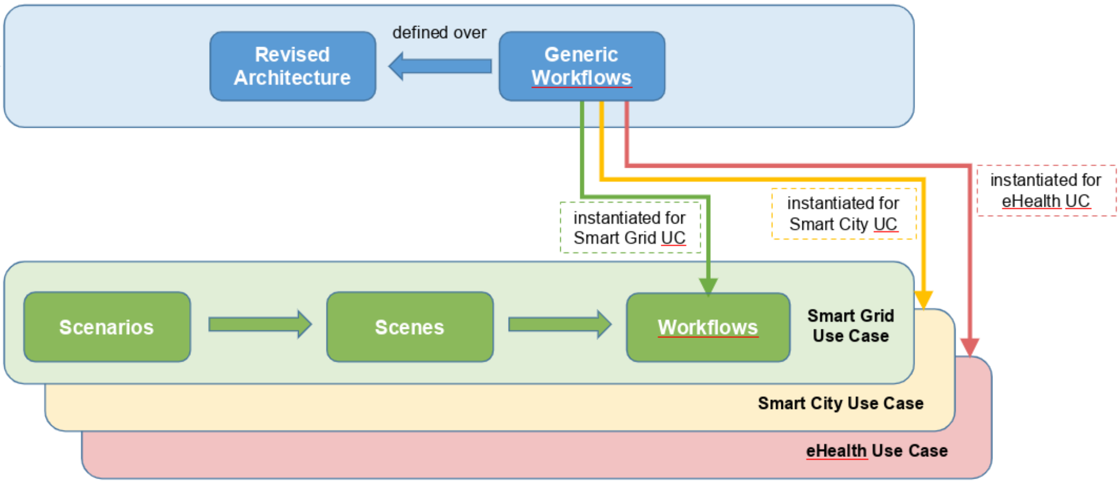


Figure 1: SliceNet Prototyping of Vertical Business Use Cases plan

The prototype implementation of the three Verticals Use Cases is developed over the SliceNet system integrated infrastructure leveraging the following slicing key enablers introduced by work packages WP3, WP4, WP5. WP6, WP7:

- Virtualised 5G RAN and MEC-Core Network offering end-to-end slicing-friendly infrastructure.
- End-to-end (E2E) programmability and dynamic control of the 5G/4G Data and Control Plane across multiple operators' domain
- QoE-aware slice management by combination of an autonomic control loop (Monitoring, Analysis, Planning, and Execution) with state-of-the-art data-driven management and AIOPS (Artificial Intelligence for IT Operations)
- Management framework allowing automated deployment and configuration of all the required artefacts for slice FCAPS handling
- Service and Slice orchestration for the deployment of the E2E services and Slices as requested by the verticals
- One Stop API offering different management views of the SliceNet system to various players in the context of their business role (Vertical, DSP, NSP)
- Plug & Play framework providing Verticals with a customized control exposure and view of their slices.

More details about utilization of specific SliceNet infrastructure, features and components are described in next sections dealing with detailed work-flows of the eHealth, Smart City and Smart Grid Use Cases.

2 Generic Workflow Descriptions

This chapter describes the generic workflows involved in the network slice life cycle, according to the principles and concepts described in 3GPP TR28.801, as can be seen in Figure 2.

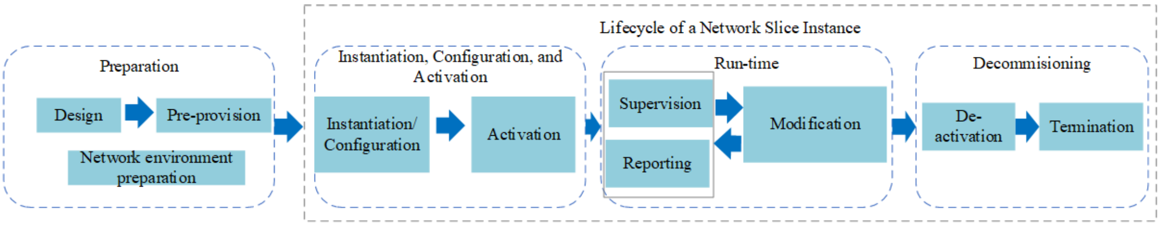


Figure 2: Life cycle phases of a Network Slice Instance (NSI) (3GPP TR 28.801)

The following phases and activities are defined:

- **Preparation Phase** – during this phase all the required procedures to create and validate the network slices will take effect. Its composed by the following core activities:
    - **Design Activity**: DSP E2E NS design and NSP NS design describing the business requirements to be offered to the Verticals and DSPs;
    - **Onboard Activity**: after designing the service (E2E NS) and the NSs, the produced blueprints and templates are onboarded to the DSP Catalogue and NSP Catalogue;
    - **Offer Activity**: the DSP Catalogue and NSP Catalogue are available to be offered, through the OSA, to the service consumers (the Vertical consults and potentially subscribes from the DSP Catalogue and the DSP consults and potentially subscribes from the NSP Catalogue);
- **Subscription Phase** – during this phase the DSP service (E2E NS) and the NSP NSs are subscribed by the Vertical and the DSP. Its composed by the following core activities:
    - **Provision (Instantiation/Configuration) Activity**: guarantee that all required services and resources to deliver the E2E NS and the NS are deployed and configured according to the Vertical and the DSP requests;
    - **Activation Activity**: the provisioned services and resources are activated and, as a result, the NSI starts running and is available;
- **Run-time Phase** – during this phase are included all the required procedures to keep the NSIs running healthy. Its composed by the following activities:
    - **Monitoring (Supervision) Activity**: monitor all the required information to evaluate the status of the NSIs, this includes reporting information towards the Vertical, the DSP and the NSP;
    - **Self-* Closed-Loops (Modification) Activity**: encompasses the policy-driven self-* closed loops in order to automatically and proactively manage and/or control the NSIs, this can include for example and among others, self-protection, self-healing and/or self-optimization closed-loops;
- **Decommission Phase** – during this phase the running NSIs are terminated. Its composed by the following activities:
    - **De-Activation Activity**: all the NSIs related services and resources configurations are removed;
    - **Termination Activity**: the registered NSIs are removed from the DSP and NSP inventories and no longer available.

Table 1 represents the NS life cycle generic workflows, which are valid across all three-vertical test-beds.

Table 1: NS life cycle generic workflows

Phase	Activities	Sub-Activities	Business Entities	Workflow	WF #
Preparation	Design, Onboard & Offer	NS Design, Onboard & Offer	NSP	NS Design, Onboard and Offer towards the DSP	**1**
		Service Design, Onboard & Offer	DSP	Service Design, Onboard and Offer towards the Vertical	**2**
Subscription	Actuation	Service Instantiation	Vertical, DSP, NSP	Service Subscription (Vertical Initiated)	**3**
			DSP, NSP	P&P Control Instantiation	**4**
Runtime	Monitoring	NS Monitoring	NSP	NS Monitoring	**5**
		E2E NS Monitoring	DSP	E2E NS Monitoring	**6**
			Vertical	Service Monitoring through P&P (vertical Initiated)	**7**
			Vertical, DSP	Vertical Service QoE/QoI DSP feedback through P&P	**8**
	Optimization	NS Optimization	NSP	NS Optimization	**9**
		E2E NS Optimization	DSP	E2E NS Optimization	**10**
	Actuation	Service Actuation	Vertical, DSP, NSP	Service/Slice Reconfiguration (through P&P)	**11**
			Vertical, DSP, NSP	Service/Slice NF Deployment (through P&P)	**12**
Decommission	Actuation	Service Decommission	Vertical, DSP, NSP	Service Decommission (Vertical Initiated)	13

2.1.1 WF 1 - Preparation Phase - NS Design, Onboard and Offer towards the DSP

The NSP is responsible for the design and onboarding phases of their network slices. In the design phase the NSP should also make all the necessary tests and validations in the new network slice in order to validate its requirements before onboarding it to the catalogue as a new NSP “product”/”service”. Figure 3 shows this workflow.

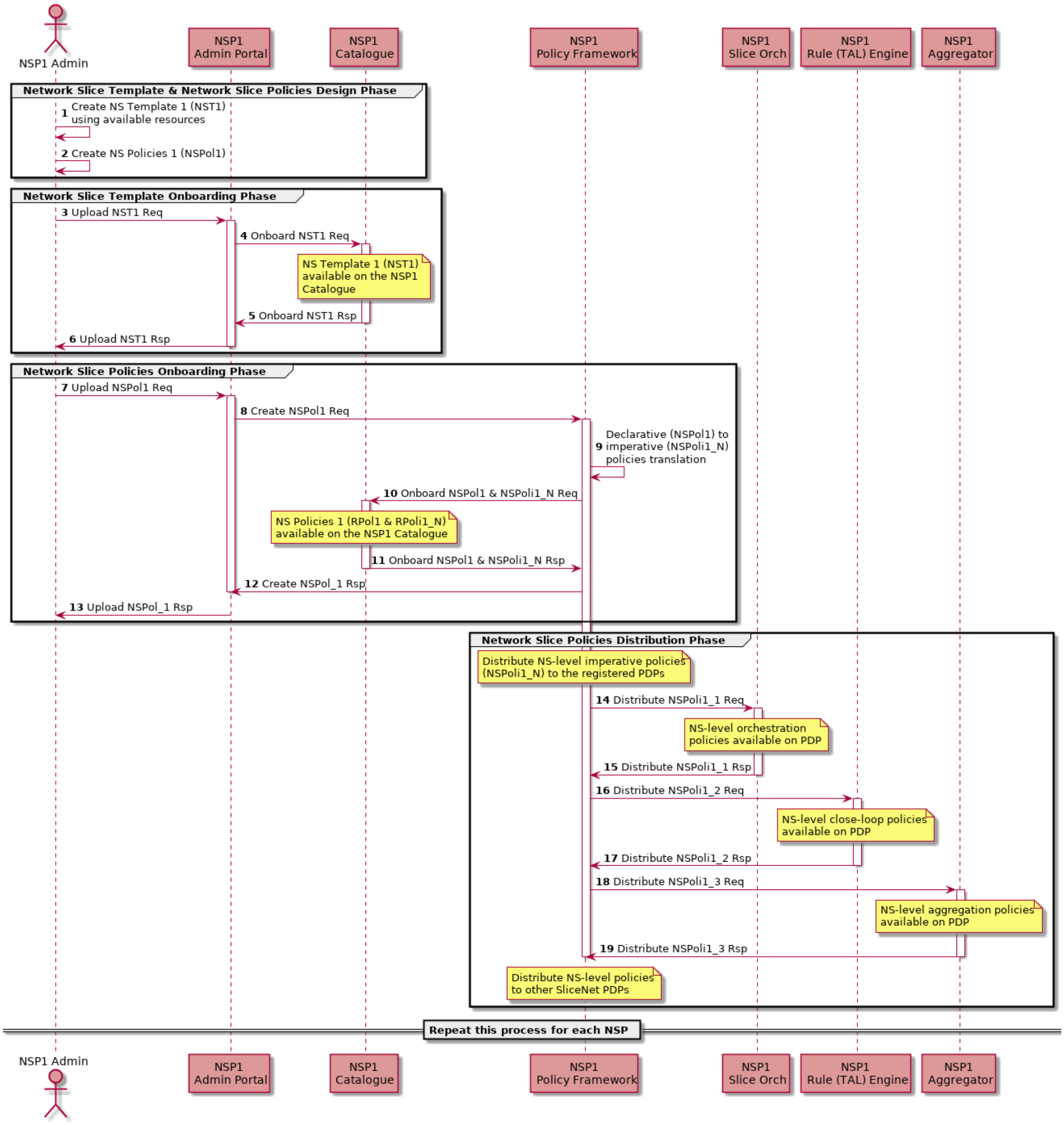


Figure 3: Network Slices Design and Onboard towards the DSP

The NSP next step will be to offer the NSs available in the catalogue to the DSPs according to Figure 4.

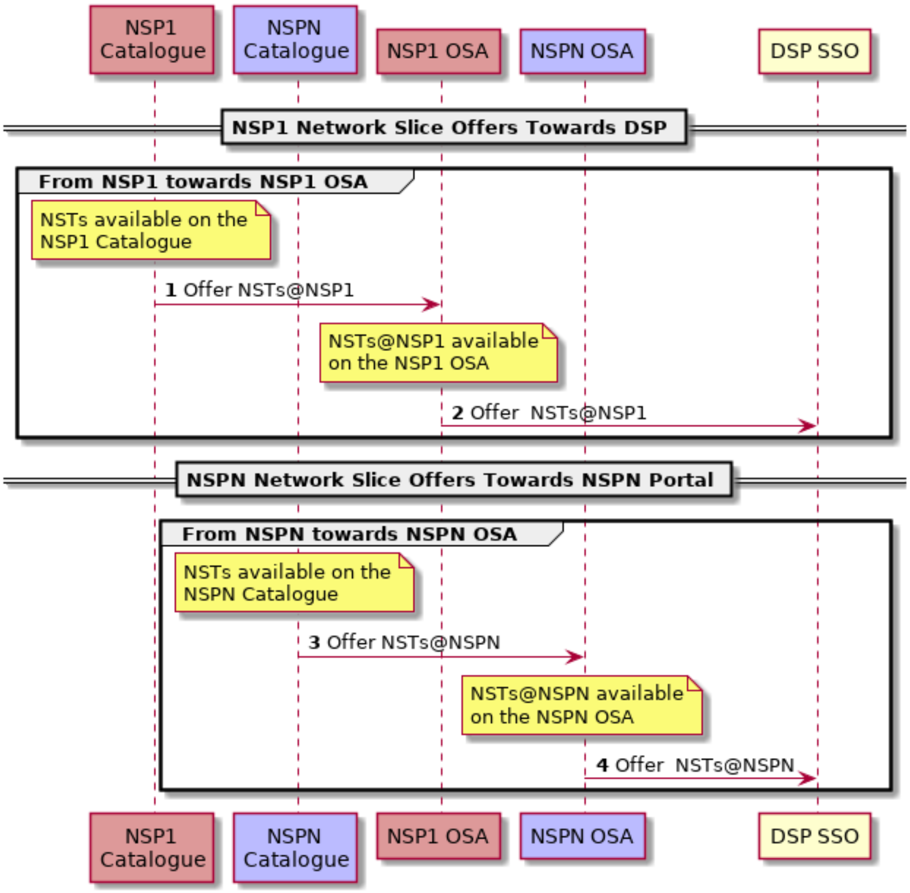


Figure 4: Network Slices Offer towards the DSP

2.1.2 WF 2 - Preparation Phase - Service Design, Onboard and Offer towards the Vertical

The DSP is responsible for the design and onboarding phases of their services. Each DSP service will be deployed by the DSP with an E2E NS. In the design phase the DSP should make all the necessary tests and validations in the new E2E NS in order to validate its requirements before onboarding it to the catalogue as a new DSP service. Figure 5 shows the DSP Service Design and Onboard.

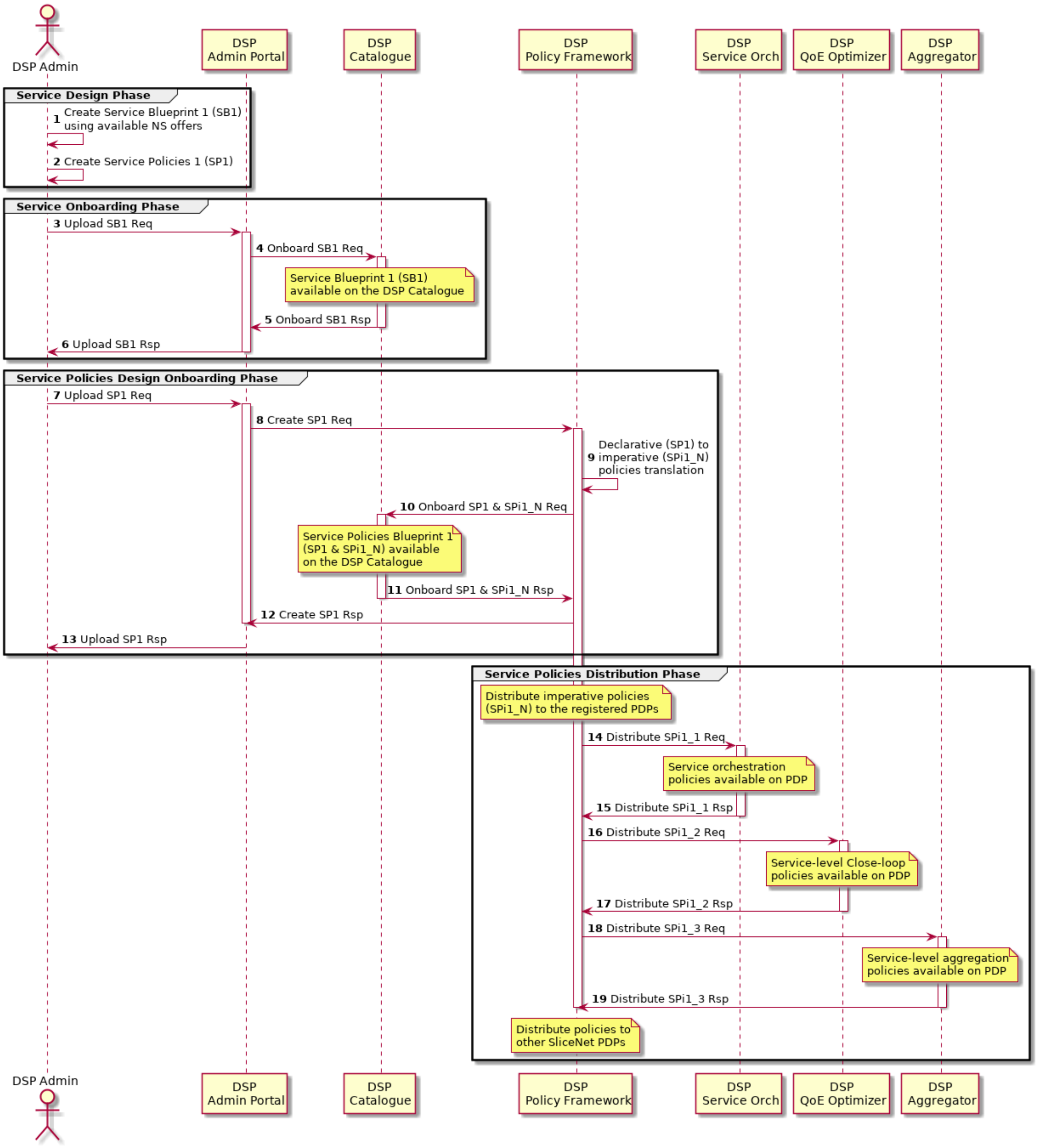


Figure 5: Service Design and Onboard

The DSP shall also make all the necessary tests and validations to the service (E2E network slice) to see if it complies with the service requirements that will be advertised to the Verticals.

The DSP next step will be to offer their services to the vertical according to Figure 6.

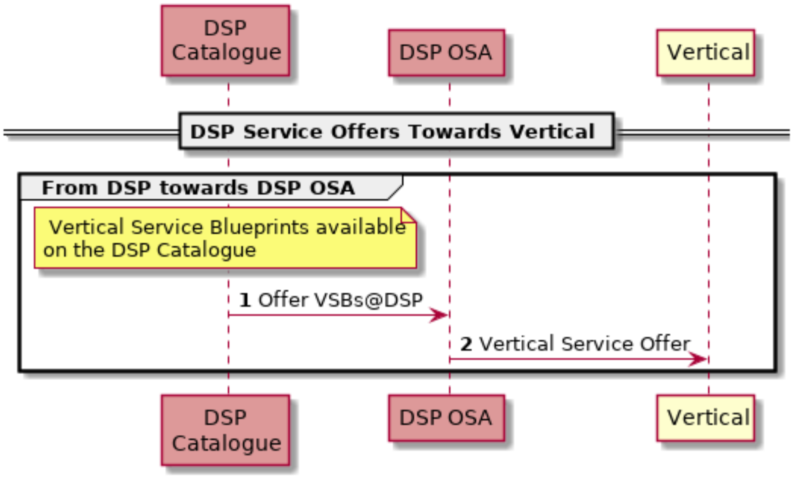


Figure 6: Service Offer towards the Vertical

2.1.3 WF 3 - Subscription Phase - Service Subscription (Vertical Initiated)

The Vertical subscribes a service from the DSP catalogue. Figure 7 and Figure 8 depict the subscription from the vertical and the subsequent DSP and NSP actions to instantiate the service.

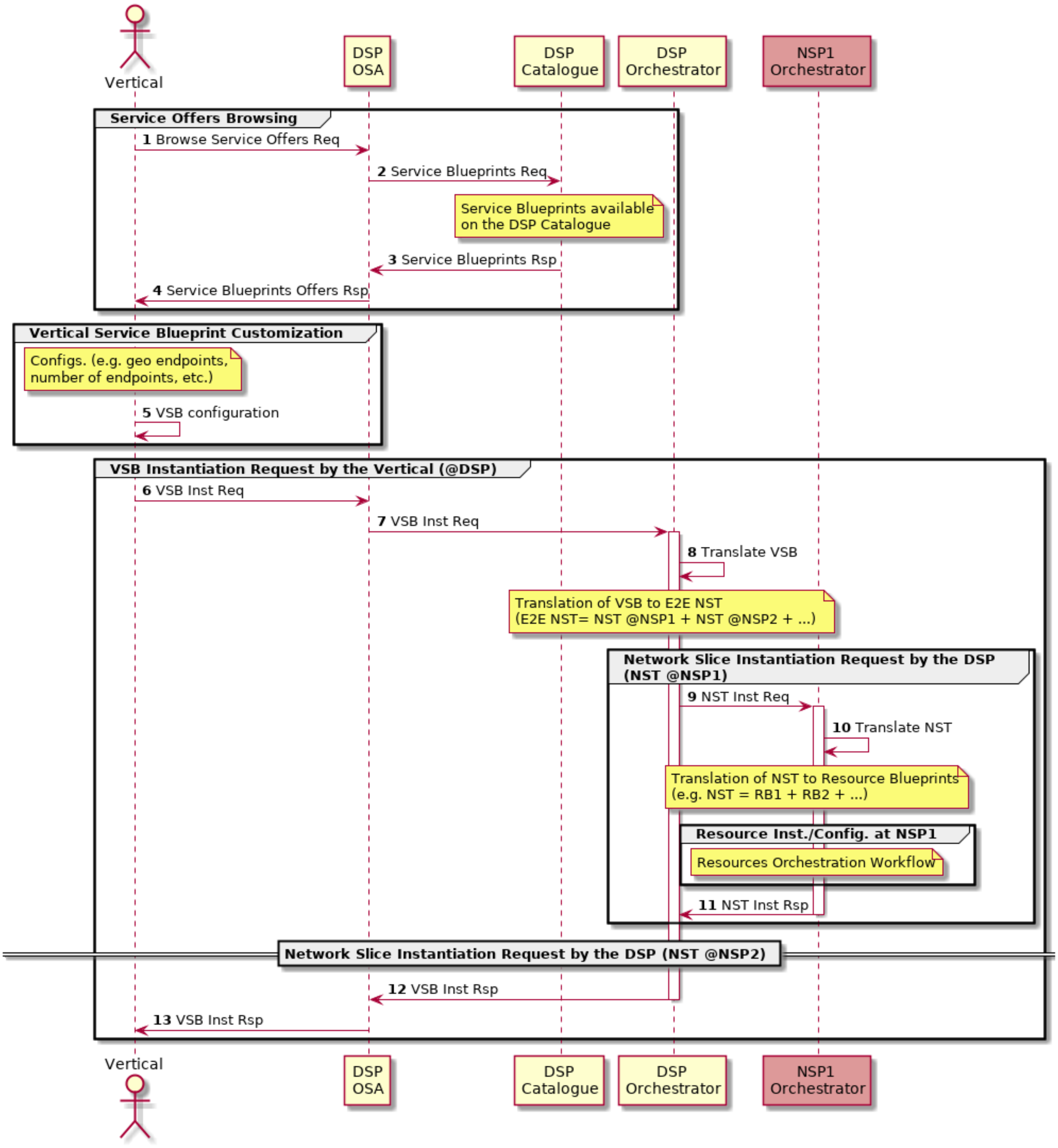


Figure 7: Vertical Service Subscription - DSP instantiations

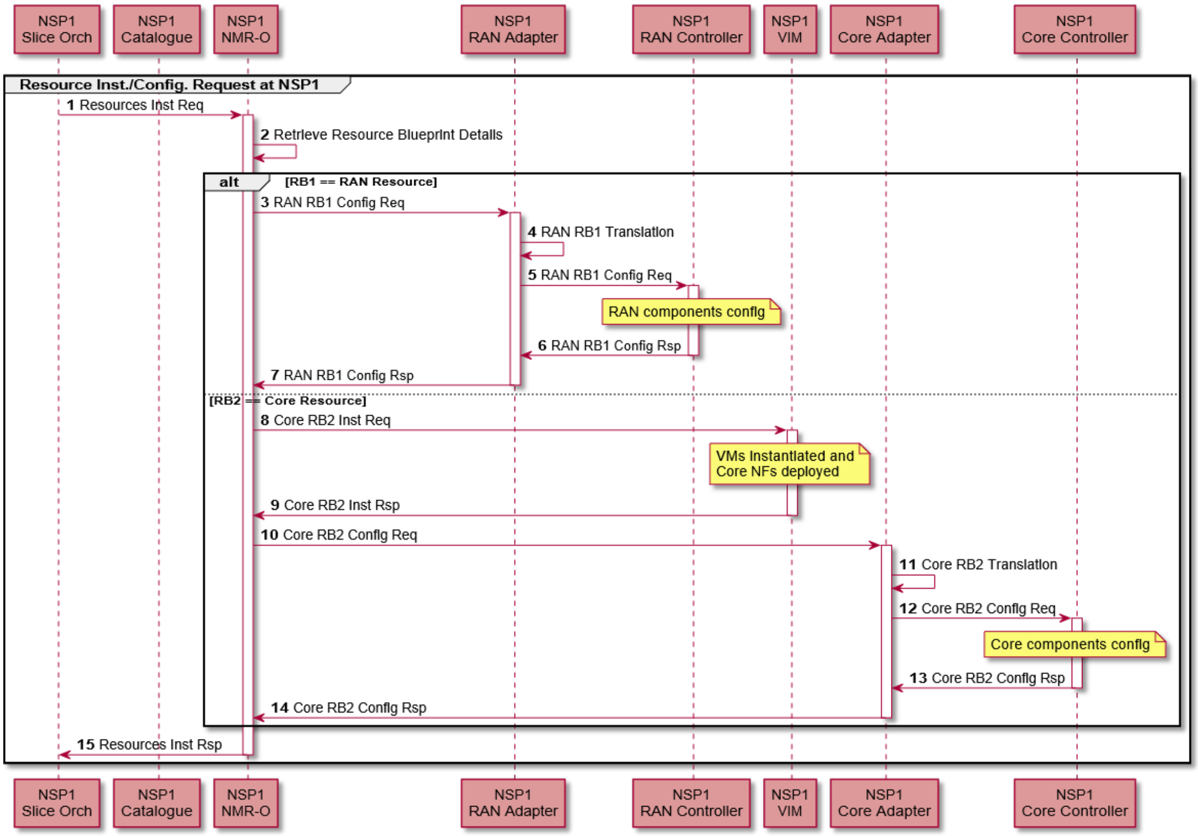


Figure 8: Vertical Service Subscription - NSP instantiations

2.1.4 WF 4 – Subscription Phase - P&P Control Instantiation

Figure 9 shows the P&P Control Instantiation workflow.

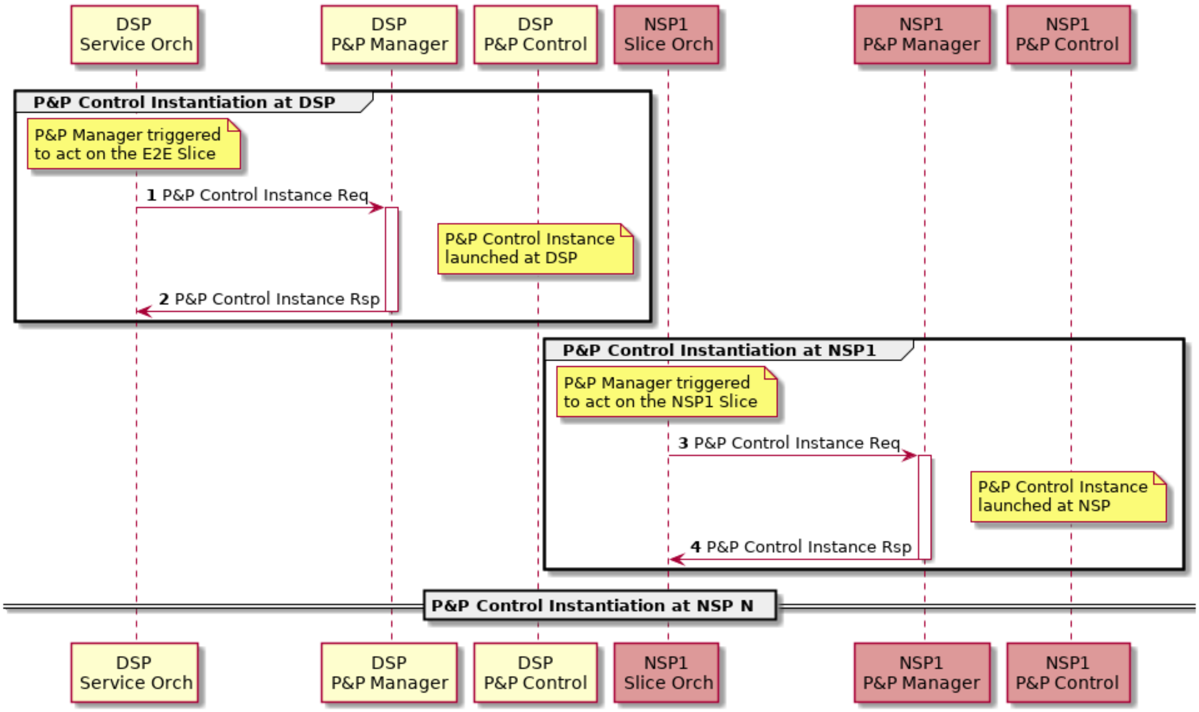


Figure 9: P&P Control Instantiation

2.1.5 WF 5 - Runtime Phase - NS Monitoring

At runtime the network slice is being monitored in all their network elements (PNFs/VNFs). Figure 10 shows the respective workflow.

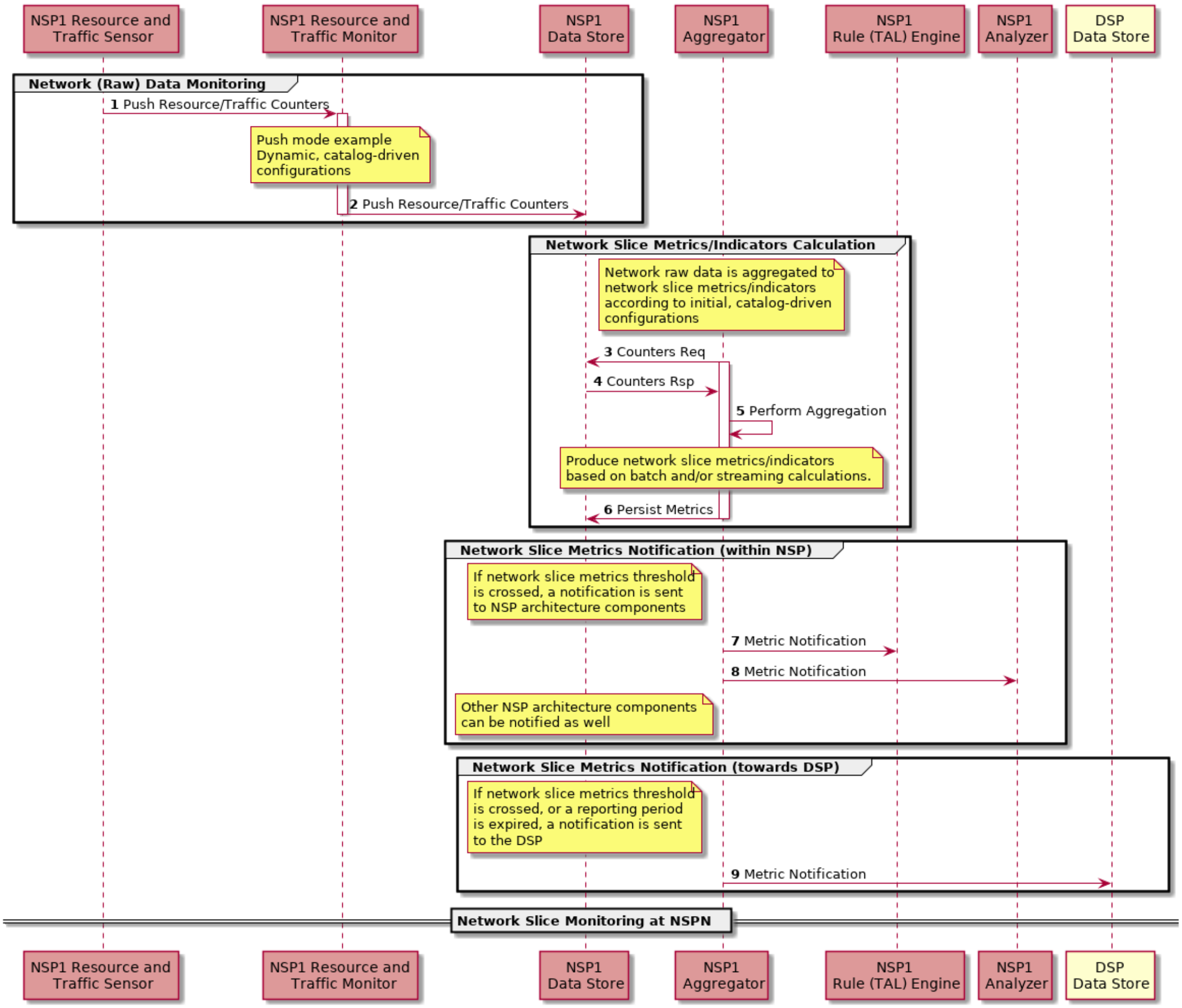


Figure 10: Network Slice Monitoring

2.1.6 WF 6 - Runtime Phase - E2E NS Monitoring

Also at runtime the DSP E2E network slice will be monitored. The monitoring will be done in each NS in order to validate if the agreed SLA/requirements are being accomplished (Figure 11).

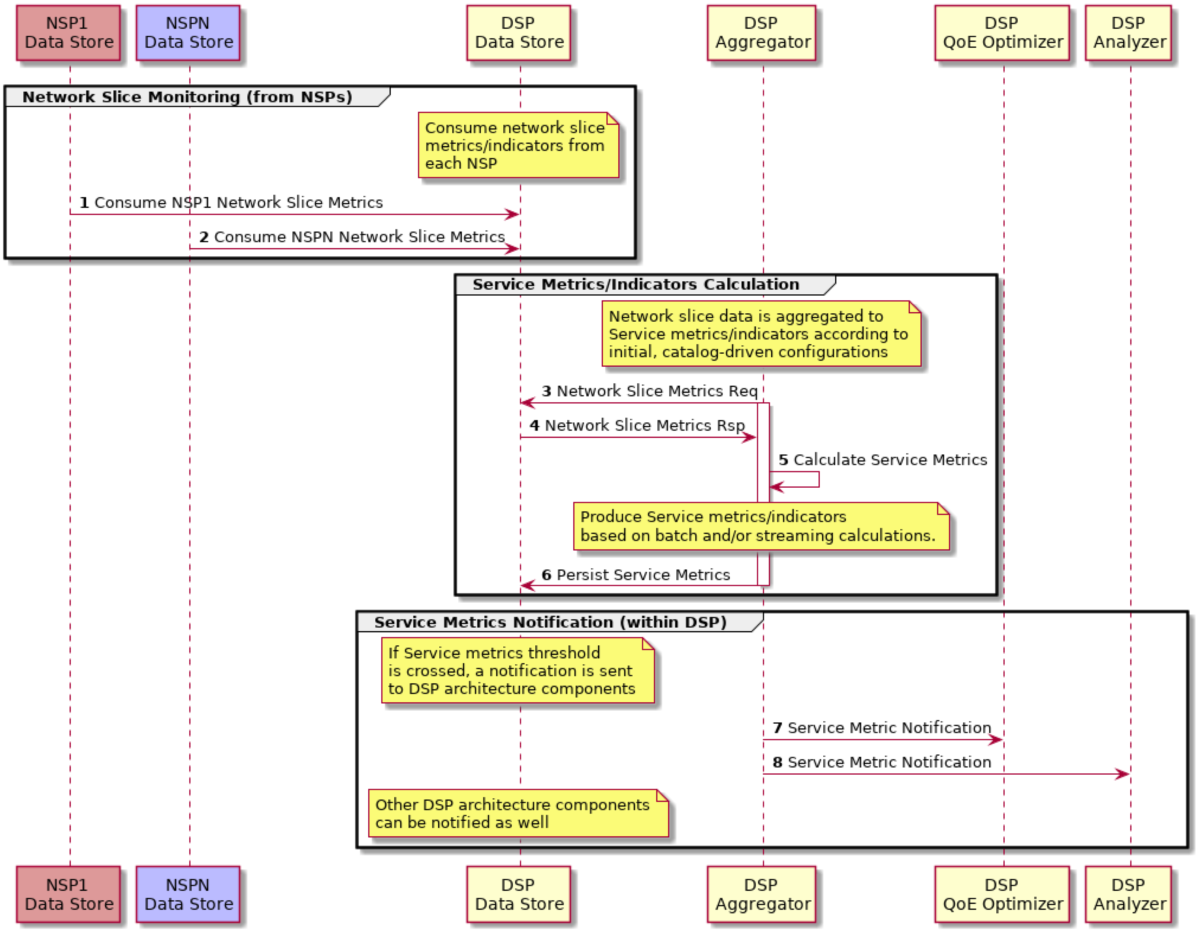


Figure 11: E2E Network Slice Monitoring

2.1.7 WF 7 - Runtime Phase - Service Monitoring through P&P (vertical Initiated)

The Vertical has the ability, through P&P Control, to check if the SLA is being within the agreed contract (Figure 12).

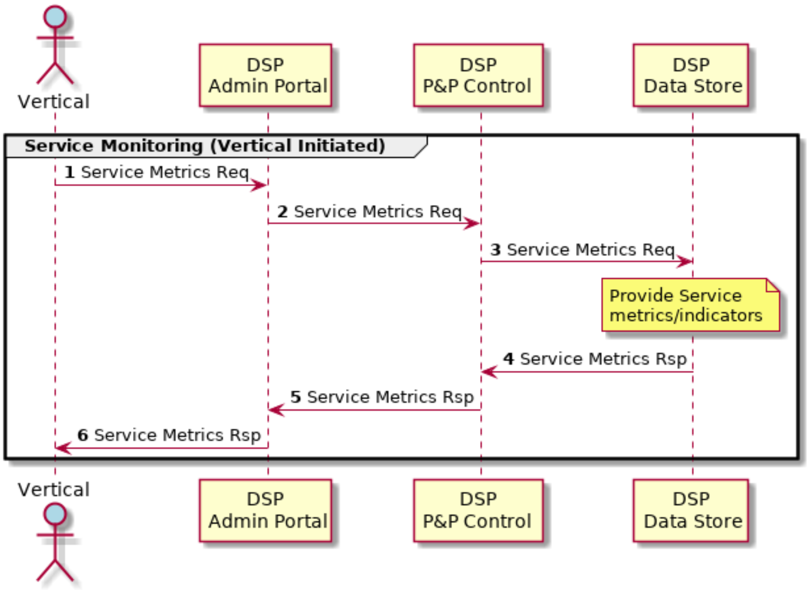


Figure 12: Service Monitoring through P&P

2.1.8 WF 8 - Runtime Phase - Vertical Service QoE/QoI DSP feedback through P&P

The Vertical has also the ability to inform the DSP about his QoE/QoI of the service being offered by the DSP (Figure 13).

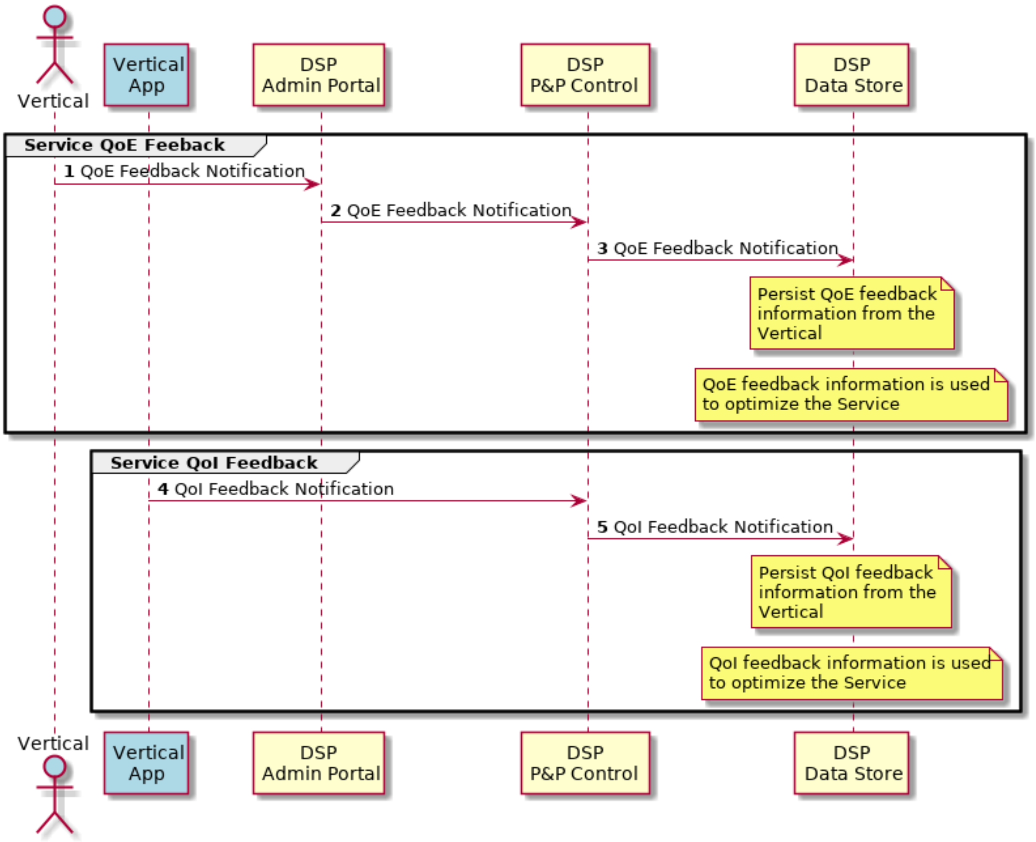


Figure 13: Vertical Service QoE/QoI DSP feedback through P&P

2.1.9 WF 9 - Runtime Phase - NS Optimization

The following workflow (Figure 14) describes the NS Optimization at the NSP level.

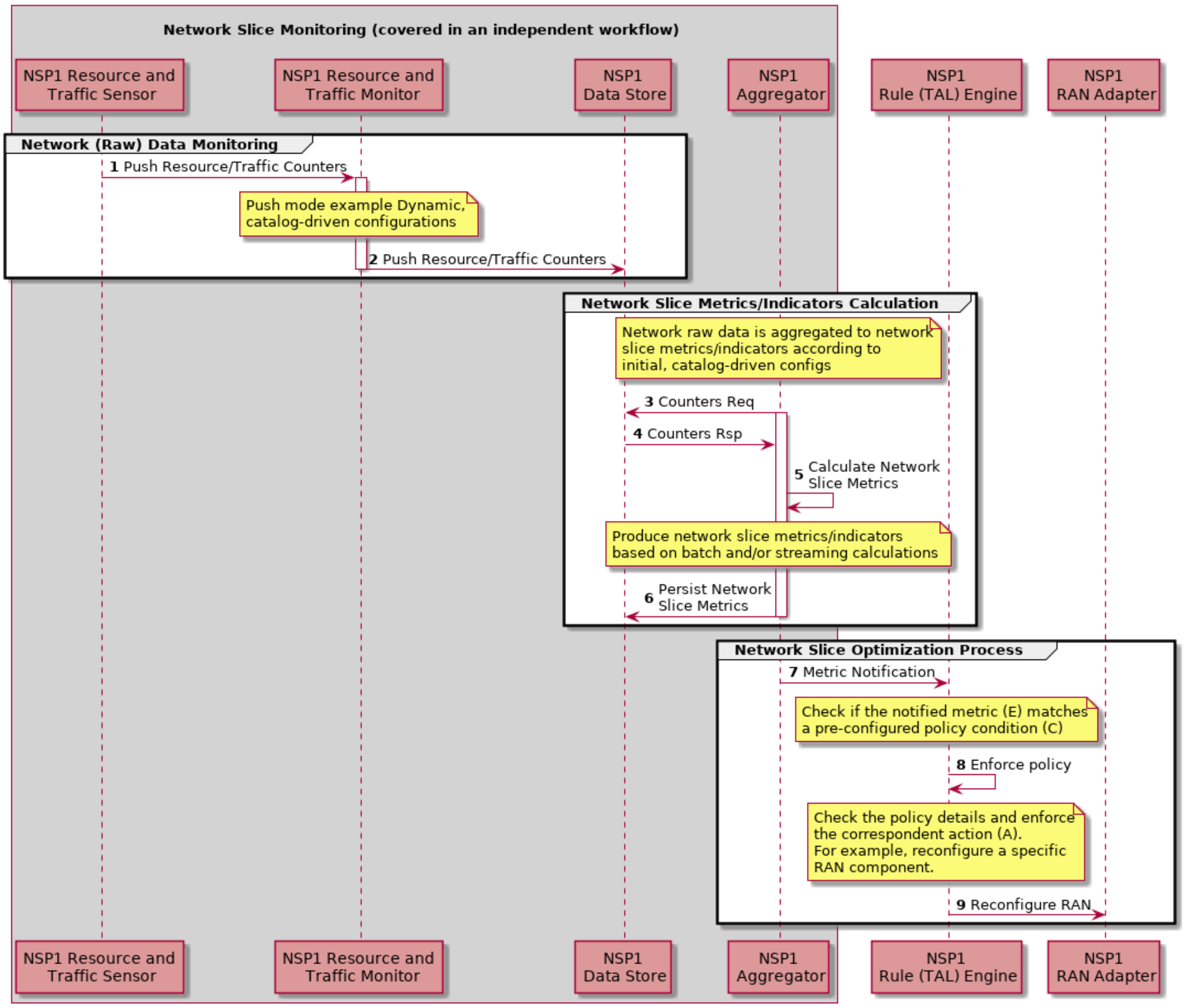


Figure 14: Network Slice Optimization

2.1.10 WF 10 - Runtime Phase - E2E NS Optimization

The following workflow (Figure 15) describes the E2E NS Optimization at the DSP level.

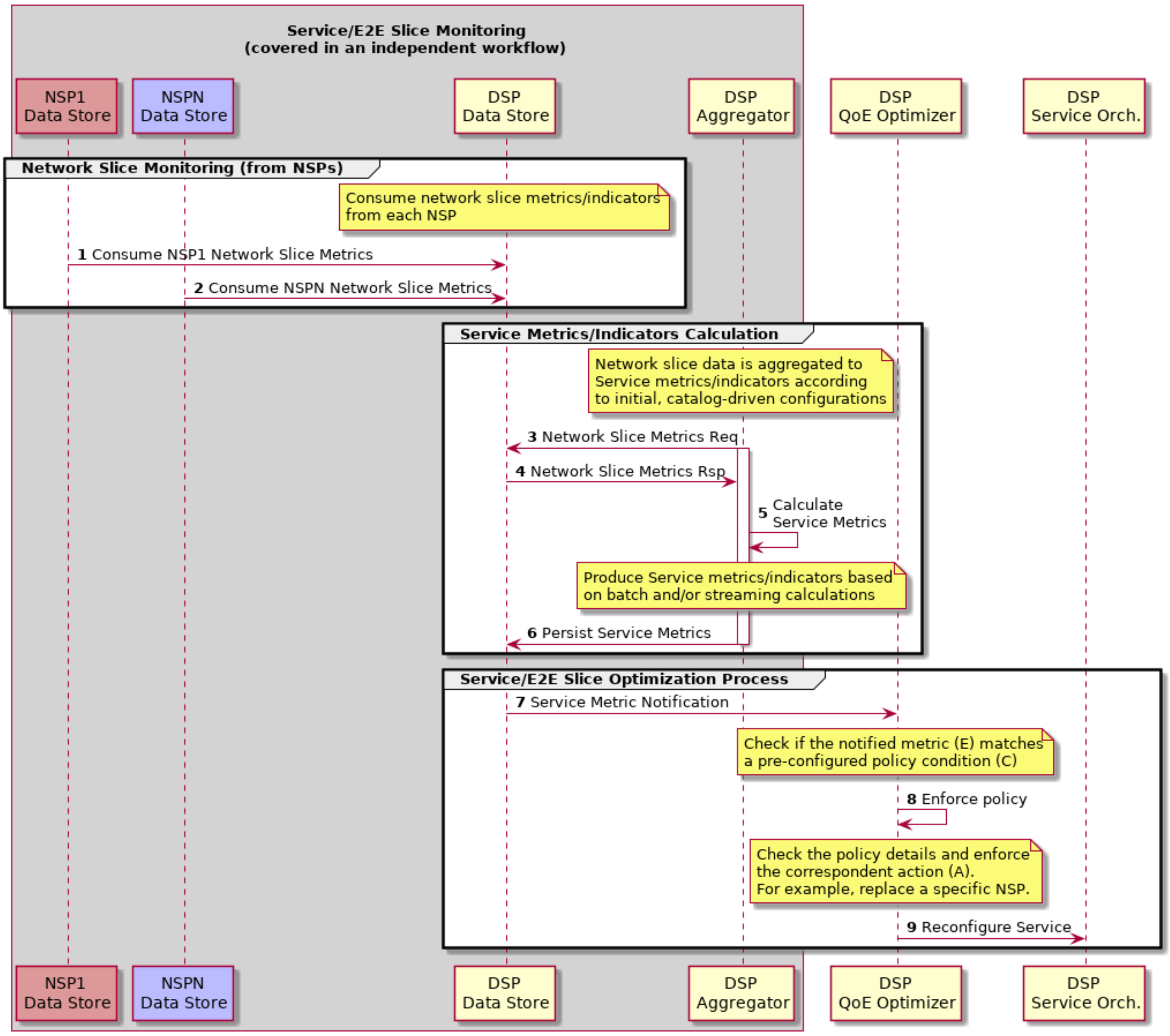


Figure 15: E2E Network Slice Optimization

2.1.11 WF 11 - Runtime Phase - Service/Slice Reconfiguration (through P&P)

The following workflow (Figure 16) describes the Service/E2E Network Slice reconfiguration (through P&P).

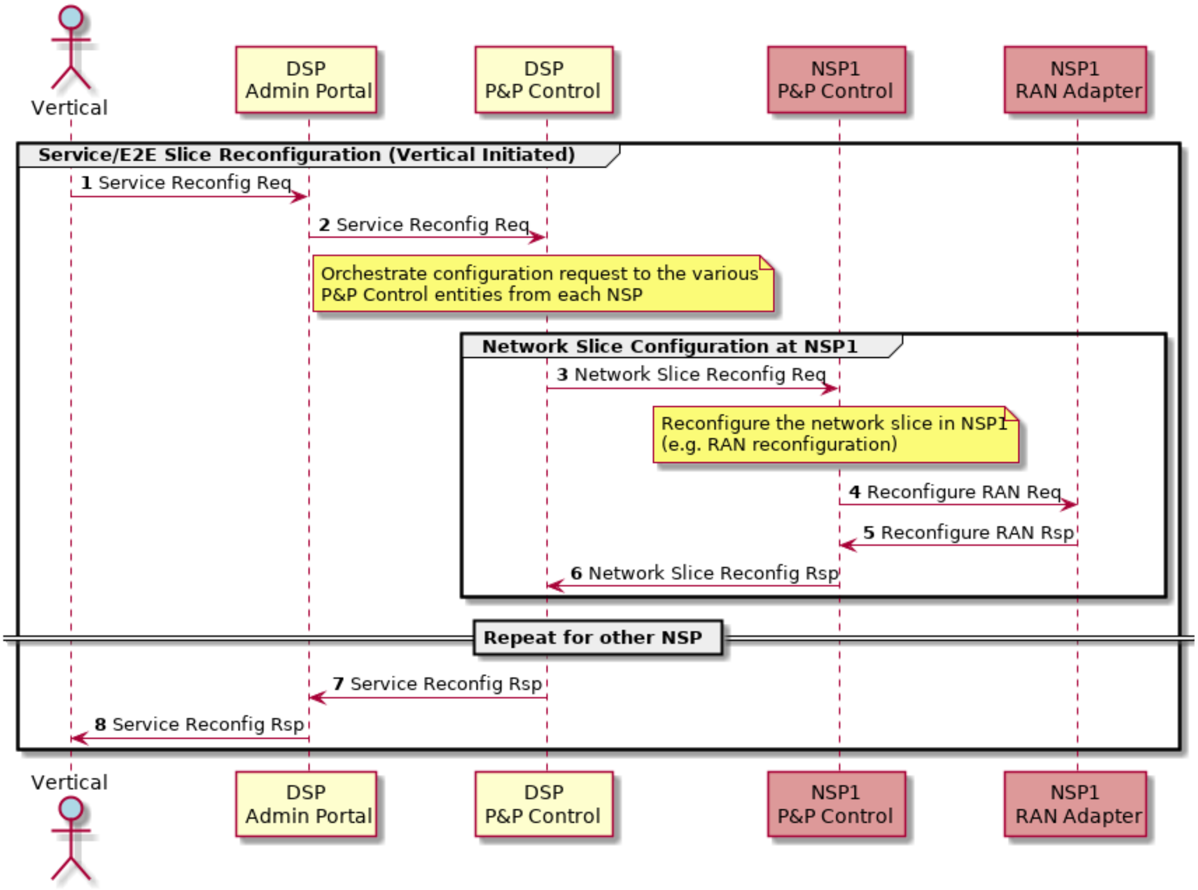


Figure 16: Service/E2E Network Slice Reconfiguration through P&P

2.1.12 WF 12 - Runtime Phase - Service/Slice NF Deployment (through P&P)

The following workflow (Figure 17) describes the Service/Slice network functions deployment (through P&P).

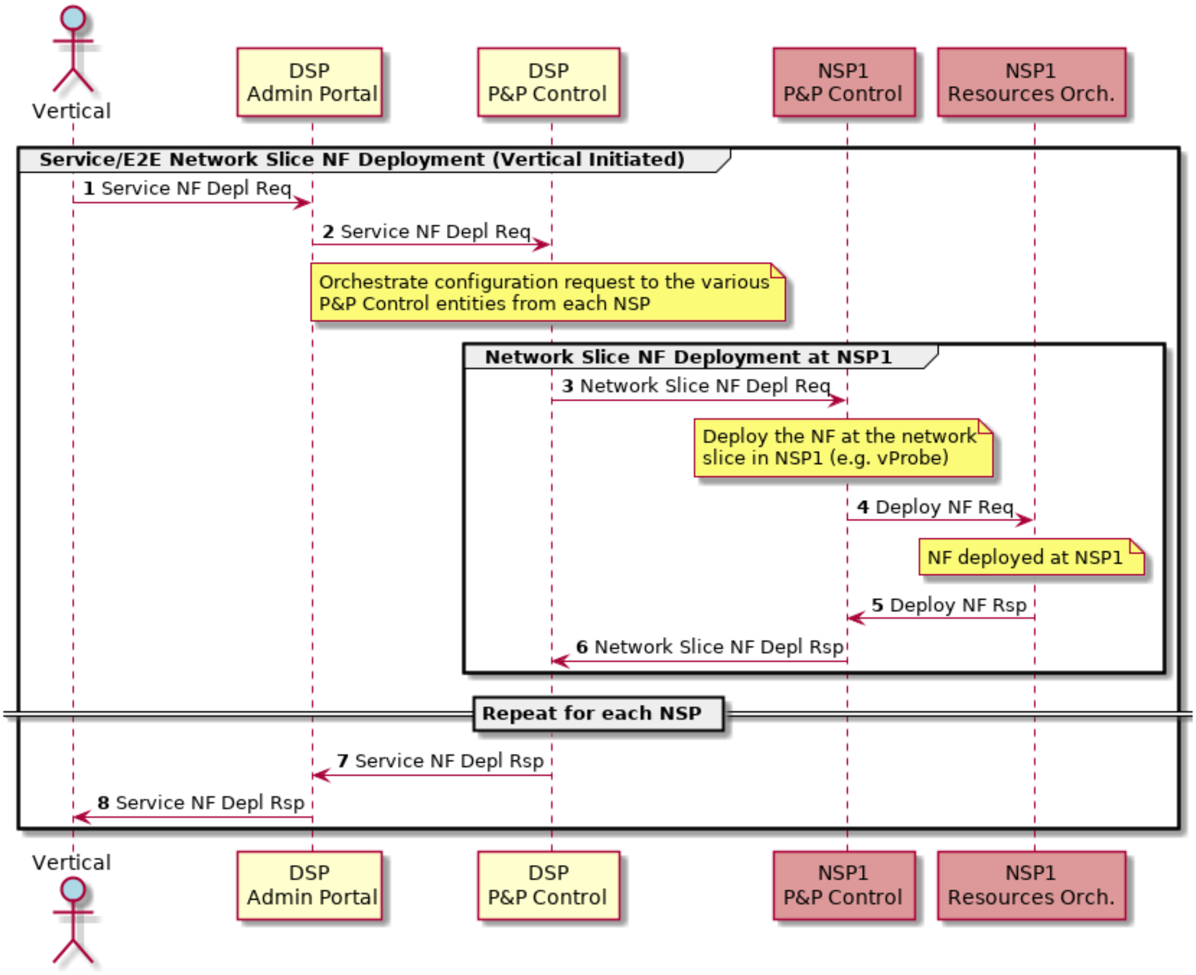


Figure 17: Service Slice NF Deployment through P&P

2.1.13 WF 13 - Decommission Phase - Service Decommission (Vertical Initiated)

The following workflow (Figure 18) describes the Service Decommission initiated by the Vertical.

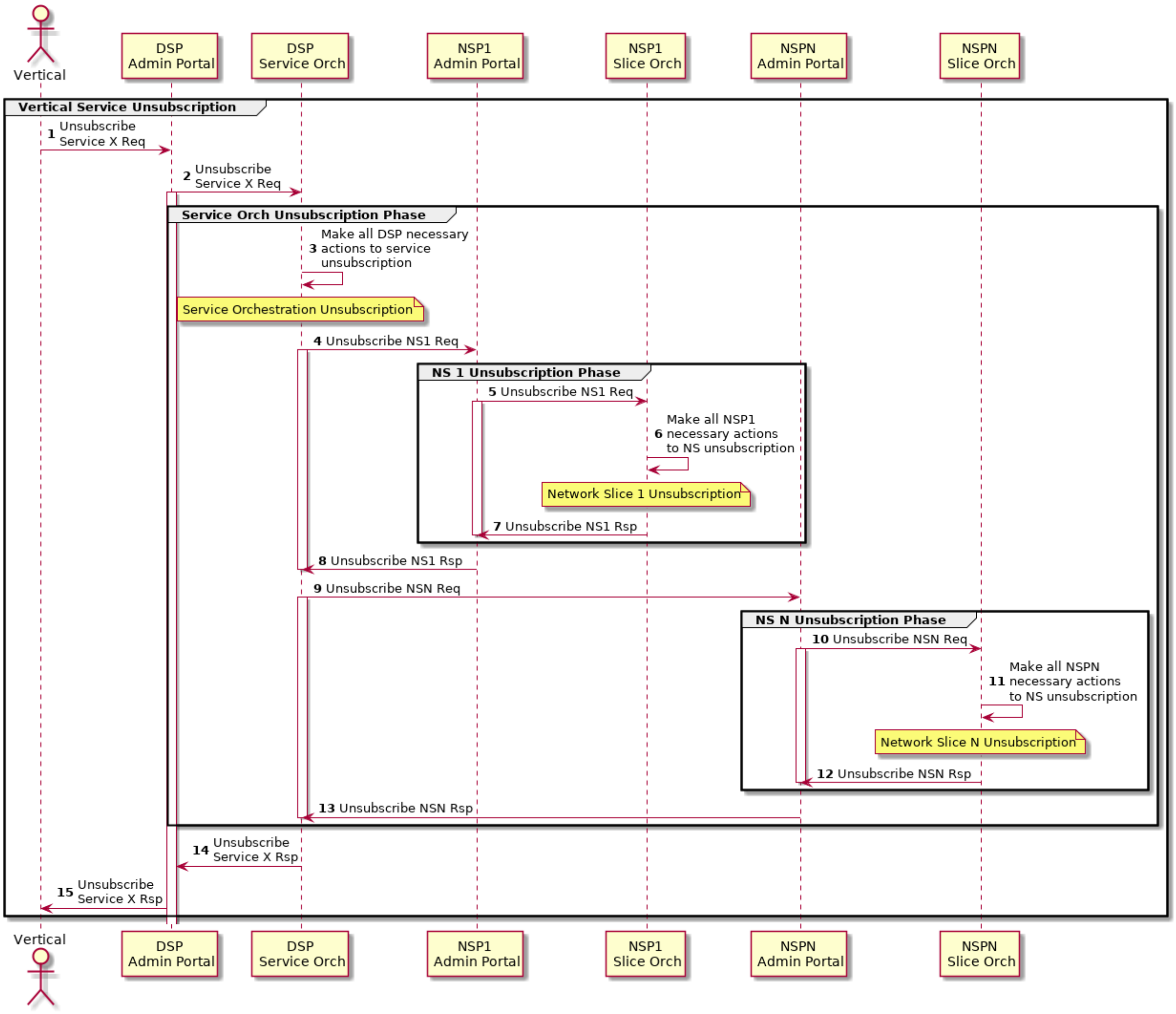


Figure 18: Service Decommission (Vertical Initiated)

3 Use Case Prototype Descriptions

3.1 Adaptation of existing UC business applications/services

3.1.1 Smart Grid

3.1.1.1 Routable version of time-critical protocols

The IEC 61850 standard constitutes the main reference for modelling modern power grid Protection, Automation and Control (PAC) systems and applications. The standard defines several services and communication protocols, including Generic Object Oriented Substation Events (GOOSE) [2], a protocol designed for time-critical event-driven device-to-device (D2D) communication. GOOSE is a layer 2 protocol, commonly used in substation environment for exchanging information between Intelligent Electronic Devices (IEDs). Recent and ongoing advances in Information and Communication Technology (ICT), such as 5G wireless radio technologies, are leveraging the development of new communication-based smart grid wide-area applications that require ultra-Reliable Low-Latency Communication (uRLLC) between devices. A routable version of the GOOSE protocol (R-GOOSE) [3][4] was developed in order to accommodate the protocol-level communication requirements for the wide-area applications that constitute the smart grid self-healing use case scenarios: Protection Coordination, Automatic Reconfiguration, and Differential Protection [5].

3.1.1.1.1 Layer 2 GOOSE protocol overview

IEC 61850 GOOSE is a layer 2 (non-routable) protocol, specifically designed for time-critical event exchange between IEDs installed in a substation. The protocol is based on a multicast publisher-subscriber mechanism that allows sending the same message to several IEDs without a significant overhead on the communication network and with a reduced impact on overall system performance.

GOOSE was originally created to replace wired connections, and relies on a heartbeat for allowing subscribers to detect communication failures regardless of the message contents. Since it is a connectionless protocol, when there is an event (i.e., when there are value changes) the publisher sends a burst of messages according to a configured retransmission curve, in an attempt to ensure that the subscribers have immediate access to the new data. This behaviour is represented in figure 19.

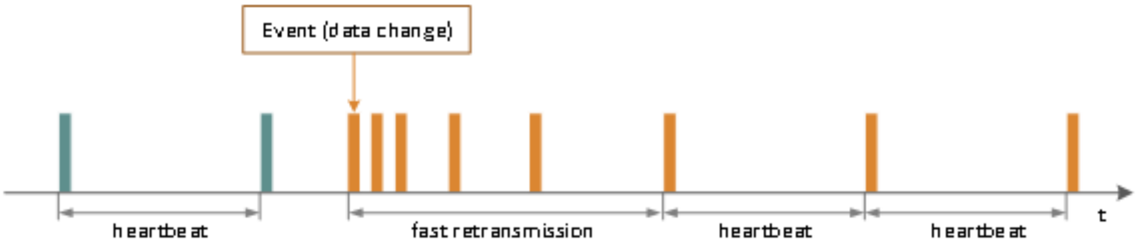


Figure 19: GOOSE retransmission mechanism

3.1.1.1.2 GOOSE protocol adaptation

Standardized ultra-reliable high-speed D2D communication is becoming a common requirement for a large number of emerging communication-based wide-area applications for the Smart Grid.

Consequentially, there have been ongoing developments in IEC 61850 with the goal of defining an extension to the GOOSE protocol that supports routing: R-GOOSE [3][4].

A version of R-GOOSE has been developed (by Efacec), aiming at responding to a set of industry requirements, provided there is access to an uRLLC-capable infrastructure that covers the demanding requirements imposed by the time-critical applications such as smart grid self-healing.

R-GOOSE encapsulates the GOOSE payload in an User Datagram Protocol (UDP) packet and adds security information. In order to allow the transmission of R-GOOSE messages over public networks, the streams can be configured with unicast addressing.

Figure 20 represents a R-GOOSE packet structure.

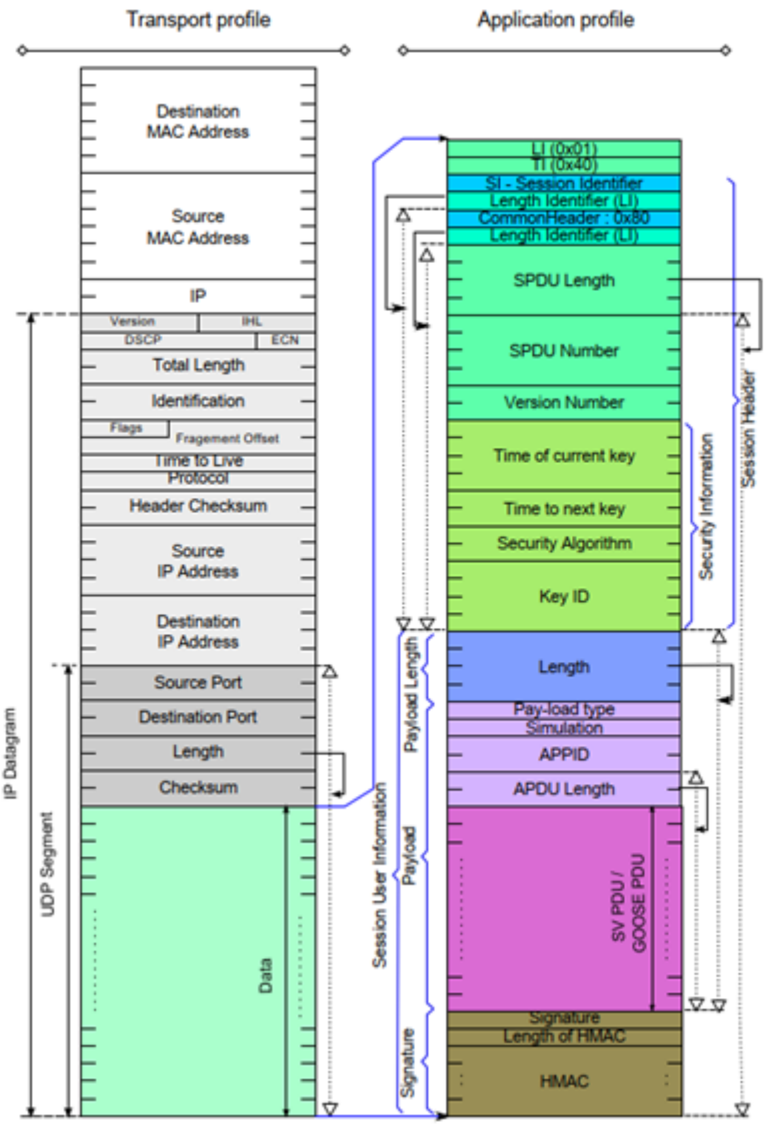


Figure 20: IEC 61850-90-5 R-GOOSE message specification [8].

The GOOSE security extension is addressed by the IEC 62351 standard [6][7] and has not been considered in the present R-GOOSE adaptation.

3.1.1.2 Communication-based distributed self-healing algorithm

Smart grid self-healing was created with the purpose of reducing outage time after electrical faults in power lines for customers connected to healthy line sections. Self-healing algorithms can reconfigure the grid topology automatically in a way that de-energized healthy sections are powered by alternative power sources.

There are several ways of implementing smart grid self-healing, each with their own advantages and disadvantages. Figure 21 illustrates three possible strategies: centralized or semi-decentralized self-healing, distributed self-healing without communications, and communication-based distributed self-healing. Although all self-healing solutions require the deployment of PAC IEDs along the power lines, distributed schemes can be implemented without the need of an additional element that controls all the IEDs integrated in the solution. Consequently, coordination is typically more complex in distributed schemes.

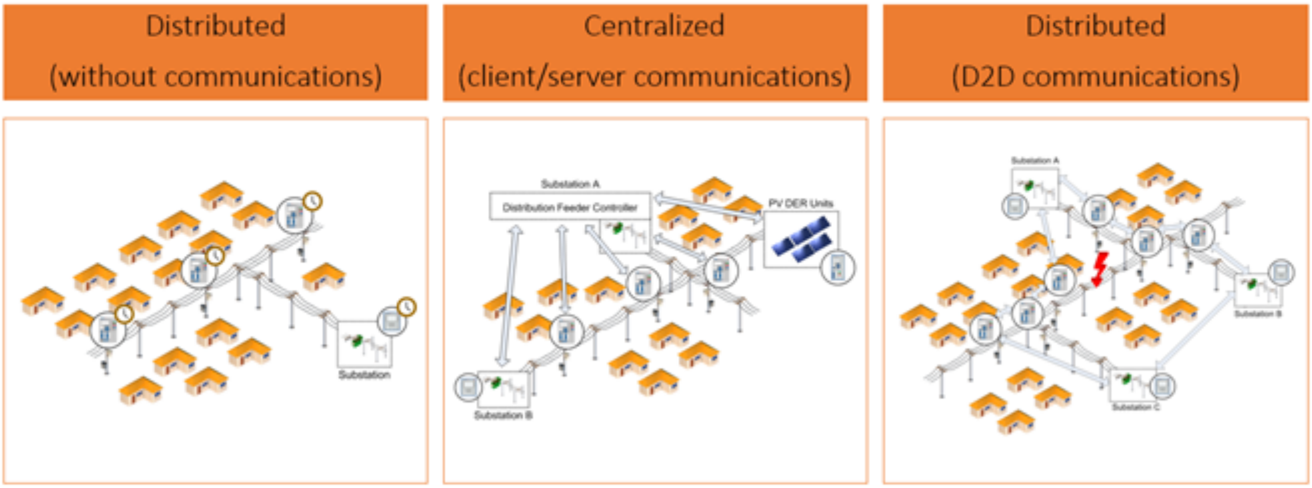


Figure 21: Example of different smart grid self-healing strategies.

Electrical distribution grid self-healing schemes integrate at least two Medium Voltage (MV) feeders with normally closed switching devices (reclosers) placed along the lines. The upstream end of a MV feeder is the substation circuit breaker and different feeders are interconnected by tie points (*i.e.*, normally open reclosers). Normally open and normally closed switching devices (reclosers and circuit breakers) are controlled by PAC IEDs. The decision-making process in distributed solutions is expressly taken on by these IEDs.

3.1.1.2.1 Conventional distributed self-healing overview

Conventional distributed self-healing solutions do not rely on communication. These self-healing algorithms can make autonomous decisions based solely on detecting the presence or absence of voltage for prolonged time periods, in key locations of the power lines. Despite not being dependent on having access to a communication infrastructure, these schemes require complex engineering and take a considerable amount of time to perform the self-healing topology changes (automatic reconfiguration may take a few minutes).

3.1.1.2.2 Distributed self-healing algorithm adaptation

There are considerable advantages to be attained by implementing communication-based self-healing solutions instead of the conventional solutions that rely on voltage-time coordination. Nevertheless, several of these applications require access to a reliable, low-latency communication infrastructure, which usually implies elevated costs.

With the aim of validating the gains and advantages provided by 5G technologies, Efacec adapted the conventional distributed self-healing solution so it supports communication-based coordination, using IEC 61850 R-GOOSE for horizontal communication (section 3.1.1.1). This allows for high-speed power grid reconfiguration, considerably reducing the power outage duration for customers that are being supplied by healthy line sections.

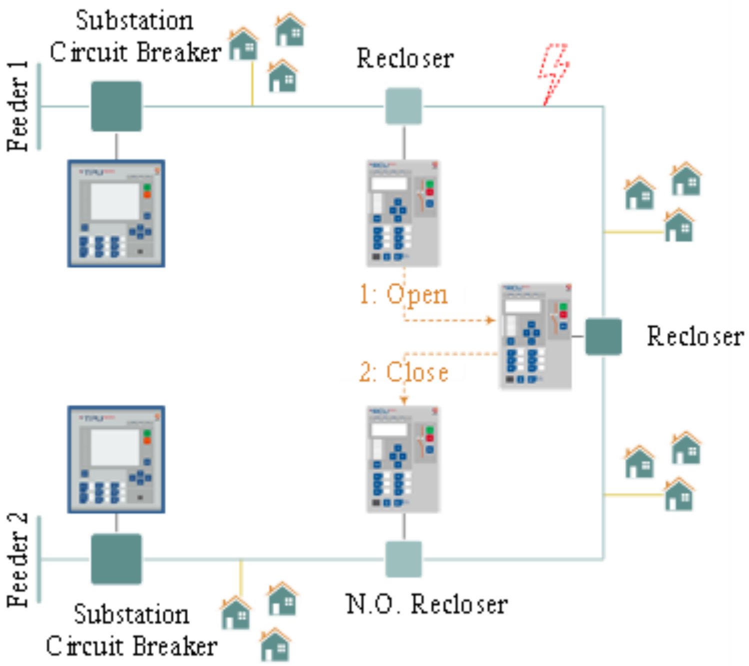


Figure 22: Example of self-healing sequence.

The improved version of the algorithm uses R-GOOSE messages for accelerating the decisions. Figure 22 illustrates an example of a self-healing workflow that is initiated after a fault has been cleared by one of the reclosers in feeder 1, leaving a large section of the grid de-energized. In this example, the IED in feeder 1 that has cleared the fault sends an open command via R-GOOSE to the neighbouring downstream IED and, in a further stage of the algorithm, after the recloser opens, the IED that received the open command sends a close command to the IED controlling the normally open recloser, energizing a section of the grid that was unaffected by the fault through feeder 2. Communication-based distributed self-healing makes it possible to execute the entire operation in under a second.

3.1.1.2.3 Communication-based protection coordination

The more significant gains of this approach rest on having the means to implement high-speed selective blocking for protection coordination. One of the basic principles of power system protection is selectivity, which implies that, if a fault is detected by multiple protection-capable devices, the grid must only be de-energized by the device immediately upstream from the fault. This way the fault is cleared without unnecessarily disconnecting costumers that are supplied by upstream power line sections unaffected by the fault.

Conventional wide-area selectivity schemes are based on time or current coordination, and do not require communication. These methods are not ideal because they require longer tripping times, causing the protection relays (*i.e.*, the IEDs) to take longer than necessary to clear a fault. Figure 23 illustrates an example of time-based coordination, in which upstream IEDs must be configured with increasingly longer tripping times.

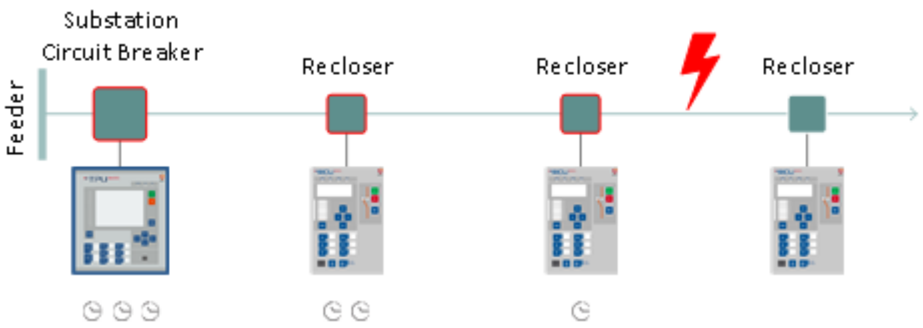


Figure 23: Example of time-based selectivity.

R-GOOSE communications over 5G enabled the implementation of high-speed protection coordination, in which selectivity is ensured by blocking messages sent to upstream devices, as represented in Figure 24.

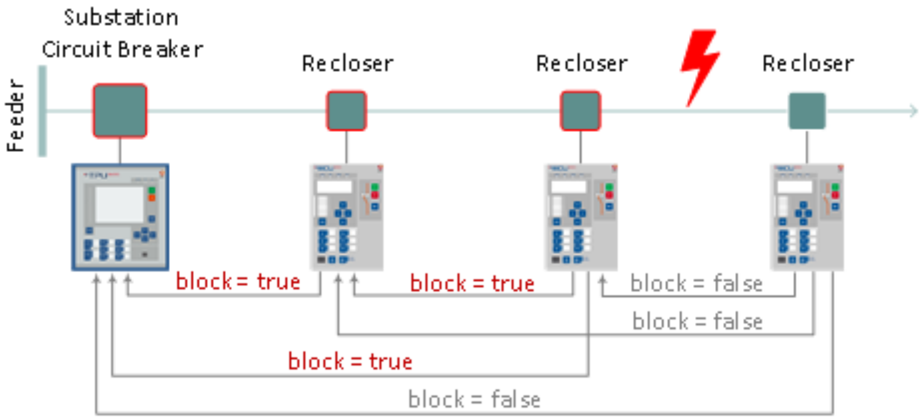


Figure 24: Example of communication-based selective blocking

3.1.1.3 Differential protection based on PMU data

Differential protection schemes are not commonly implemented in MV power grids due to the lack of a performant, reliable, and cost-effective communication infrastructure available along energy distribution networks. The arising of 5G technologies opens way to new possibilities in this area, one of which is being prototyped and validated in the SliceNet project.

The principle of differential protection rests on the assumption that, under normal operation conditions, the current that flows into the protected object (in this case, a power line section) is equal to the current that flows out of it. Comparing locally measured current values with the values measured in a remote line end in near-real-time requires a constant stream of data transmitted at a very high speed. An effective method for making power system quantities (e.g., line current values) available via communication is by using Phasor Measurement Unit (PMU). PMU transmit synchrophasor data, providing precise voltage and current phasor measurements (*i.e.*, magnitude and phase angle values), obtained using standard calculation methods [9]. It is critical that synchrophasors are time tagged by a precise clock, so it is possible to compare measurements from different locations.

The use of PMU data for this type of application ideally requires transmitting the data at ¼ power network cycle, which corresponds to 5 ms for 50 Hz networks and to approximately 4.17 ms for 60 Hz networks.

3.1.1.3.1 PMU publish/subscribe mechanism

There are several standard protocols that may be used for transmitting PMU data. With the emergence of IEC 61850 in the context of power system protection and automation, the legacy IEEE C37.118.2 [10] is being progressively replaced with IEC 61850 horizontal communications. The IEC 61850-90-5 technical report [3] recommends two suitable options for transmitting PMU data: GOOSE and Sampled Values (SV) [11].

Efacec IEDs are being upgraded with a software module that can calculate PMU measurements according to IEEE C37.118.1 [ref] and publish PMU data streams using R-GOOSE. Since the differential protection application requires IEDs to both publish and subscribe these streams, the software module also supports PMU subscription via R-GOOSE.

3.1.1.3.2 Line differential protection adaptation

As mentioned above, line differential protection works by comparing local and remote line current values. Disparate values indicate the occurrence of a fault somewhere along the monitored zone, which corresponds to the line section between the local and remote measuring points.

Line differential protection is currently available for Efacec relays fit for High Voltage (HV) power transmission networks, where it is typical to have access to dedicated physical communication network infrastructures. This, however, is not the case for MV power distribution networks, which usually need to resort to wide-area radio networks for exchanging information.

The existing application uses samples from the remote current measurements for calculating the differential current values. Since transmitting the sample data requires an extremely high transmission rate that would not be viable for public radio networks (even 5G), the line differential function was adapted in order to work with synchrophasor data.

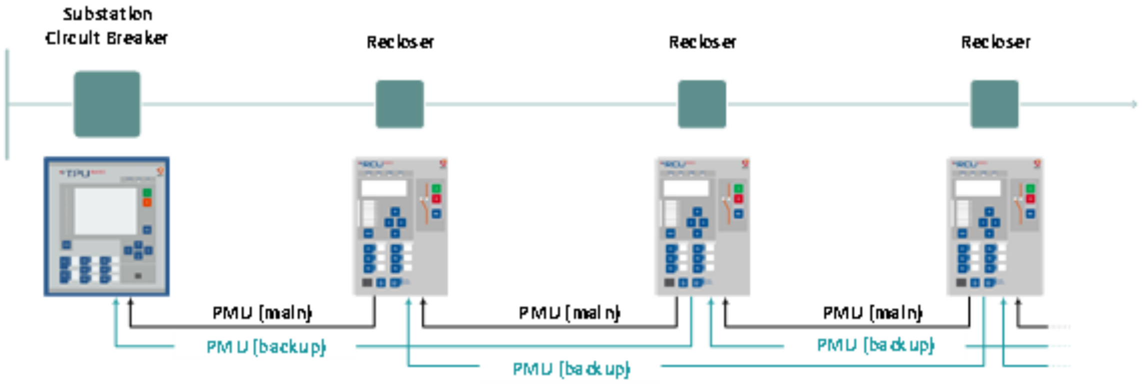


Figure 25: PMU streams used for line differential protection.

As represented in Figure 25, each IED will be subscribing PMU streams from two remote devices: synchrophasor values from the device immediately downstream will be used for the main protection element, synchrophasor values from the device further down the line will be used for backup protection. Each stream will contain three sets of magnitude, angle, quality and time stamp values, one for each current phase of the three-phase system.

New synchrophasor values will be sent every ¼ power network cycle (*i.e.*, 5 ms @ 50 Hz) and, although the algorithm is robust to occasional sub-cyclic delays, its correct operation depends on having a constant stream of information at the required rate.

3.1.2 eHealth

3.1.2.1 Telestroke

In-ambulance telemedicine is a recently developed and promising approach to improving health related emergency care. Research on prehospital telemedicine for stroke (Telestroke) assessment is proving to be acceptable, but reliable and available mobile broadband is acting as a take-up deterrent.

Our work in SliceNet project has built on these two studies and aims to facilitate widespread use of in-ambulance Telestroke diagnostics and improved patient treatment pathways, through the design of a 5G network slicing framework, as this could prove to be the solution required for reliable audio-video communication in high-speed moving ambulances.

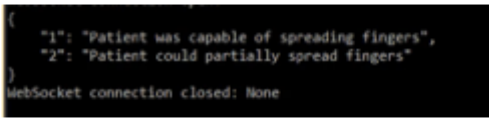
The Prehospital Stroke Study had implemented a system in which a teleconsultant could guide a patient through a protocol known as the Unassisted Telestroke Severity Scale (UTSS) [20]. The scale requires that patients perform a series of body movements and verbally answer questions or repeat phrases, which are then analysed by a clinical teleconsultant.

The potential to extend the state-of-the-art arises when using 5G network slicing and edge computing to develop a machine-learning application that can automate the UTSS.

The SliceNet Telestroke Assessment application took a selection of these UTSS protocols, and applied machine learning algorithms; for example, “Please spread the fingers of your right hand as far apart as you can”. The goal of the analysis here is to see if the patient is capable of separating the fingers on each hand. Using machine vision, the following prototype screenshots (*Fig.s 26, 27 and 28*) demonstrate how this step has been automated.

Figure 26: Example input: Fingers spread

Figure 27: Example input: fingers not spread



```
{
    "1": "Patient was capable of spreading fingers",
    "2": "Patient could partially spread fingers"
}
WebSocket connection closed: None
```

Figure 28: Telestroke output

Partial automation of the UTSS could be used as a pre-teleconsultant step when an initial indication of '*stroke*' or '*no stroke*' is provided, and then used to assist in a decision whether further diagnosis is needed from a teleconsultant. It might be beneficial in a situation where no teleconsultant is available, and a full automation of the UTSS could provide the time-gain referred to in Figure 26 and the pre-hospital diagnosis needed in emergency situations.

Fig. 5 shows a SliceNet business model, as applied in an eHealth use case. The end-to-end (E2E) slice customer is a national/regional health service organization (e.g., National Ambulance Service in Ireland), which operates multiple (static) hospitals, dispatch centres, and (moving) ambulances. The E2E eHealth slice offered to the customer by the Digital Service Provider (DSP) consists initially of a "base" Network Slice Instance (NSI) containing the minimal set of network functions & services. The base slice is fairly static and is centered around a geographical area in the vicinity of the hospital. The hospital/dispatch hosts experts who provide real-time support to the paramedics. As ambulances are dispatched, additional Network Sub-Slice Instances (NSSIs) may be instantiated in order to increase the geographical coverage of the slice (e.g., by adding RAN) or to guarantee the latency and availability requirements of the slice. For the latter, additional processing functions may be dynamically instantiated at suitable MEC locations. Dispatch may trigger a handover of a paramedic's communication stream to a different hospital. Handover between domains might be needed while the ambulance is moving.

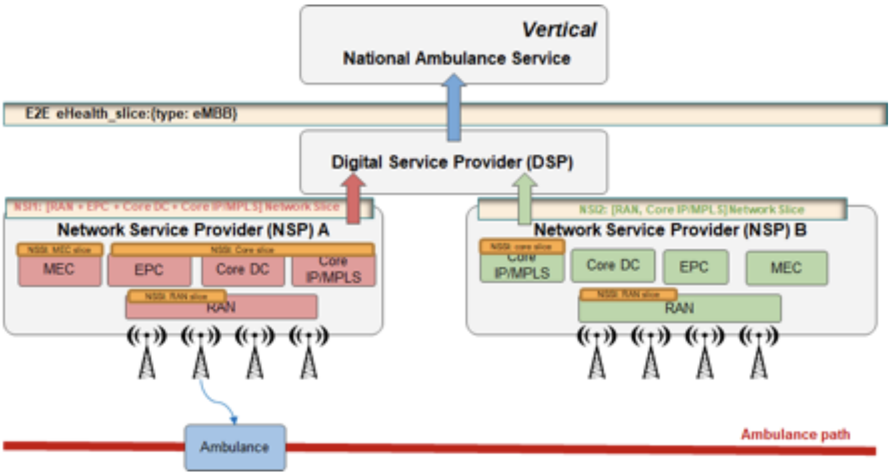


Figure 29: eHealth Business Model with vertical/service provider perspective

Vertical and DSP - The verticals only see services provided by their DSP. In the scope of SliceNet, the DSP will provide to the vertical E2E eHealth services:

i. E2E Telestroke Assessment service and

ii. E2E Video Relay service.

The Telestroke Assessment service consists of the Gateway application running in the ambulance, capturing the video of the patient, and the Telestroke Assessment application running at the edge, collecting the data from the Gateway and running a ML algorithm to analyse the images for the stroke condition. The assessment application sends the analysed result back to the in-ambulance paramedic and to the hospital for a clinical consultant to examine.

The Video Relay service is initiated with the Video Relay glasses worn by a paramedic in the ambulance capturing a live video of the scene. The glasses connect to the Video Relay Application running at the edge for authentication and to set up the communication with the hospital to provide a direct link from the Video Relay glasses to the hospital where the doctors can view video of the scene.

The DSP will add into its catalogue the Telestroke Assessment service descriptor and the Video Relay service descriptor, and then advertises to the vertical these two services. However, to specify what the DSP can deliver to the vertical, there are two scenarios from the DSP role:

- The DSP has established partnerships with a set of NSPs where it has agreed what each NSP can offer, and based on existing partnership agreements, the DSP will advertise the services which are also associated with a set of offering service assurances to the verticals.
- When the DSP has new customers, or new requirements from existing customers, and the requirements cannot be delivered with current DSP resources, the DSP will have to negotiate new terms with the NSPs or it will have to find new NSPs/new partnerships to meet these new requirements.

For the eHealth use case, the requirements from the vertical are specified in a Service Level Agreement (SLA), e.g., E2E eHealth slice with minimal bandwidth *bw*, maximum latency *l*, reliability *r%*, coverage *c%*, and secure communication.

DSP and NSP - Within an intra-domain network, the NSP will provide the network services that it guarantees to the DSP in the SLA between this NSP and DSP. For example, the DSP in *Fig.29* will create an NSI from NSP A that consists of RAN NSSI, MEC NSSI and Core NSSI and allocate the resources for these instances in a way that meets the QoS requirements, while the NSP B with an NSI of RAN NSSI and Core NSSI, and resources will be used for inter-domain if needed. Monitoring and optimisation will also be running in the domains to maintain service assurance.

SliceNet key innovations - As a public safety sliced service takes priority over all other network traffic (e.g., industries 4.0, smart city, ad hoc access), it is crucial to guarantee the SLA for the service, e.g., availability, delay, bandwidth, coverage, security, etc. SliceNet is meeting these requirements with the approaches below:

- One-stop API towards the vertical, with Plug and Play (P&P) functionalities for service monitoring, reconfiguring and autoscaling.
- Cross-domain, cross-plane orchestration to provide dynamic slicing, dynamic reconfiguration based on priority level.
- Cognitive, agile QoE management of slices for service assurance of vertical business.
- E2E slice FCAPS management to manage fault, configuration, accounting, performance and security of all slices across multiple planes and network operators domains.

3.1.3 Smart City

The Smart City use case description is based on the achievements of WP2 D2.1 and is supported by a fully virtualised network infrastructure, supported by the OAI-Core network and OAI-Radio network that connects the lighting poles through radio to the Smart City IoT application. The Smart City use-case and prototyping is composed by two scenarios:

(1) deployment and validation the smart-city use-case solution in the laboratory, with a limited number of devices;
(2) deployment and validation the smart-city use-case solution in the field, real use-case implementation in the campus.

The use-case scenario demonstration is single-domain, roles and respectabilities of NSP and DSP are played by ORO.

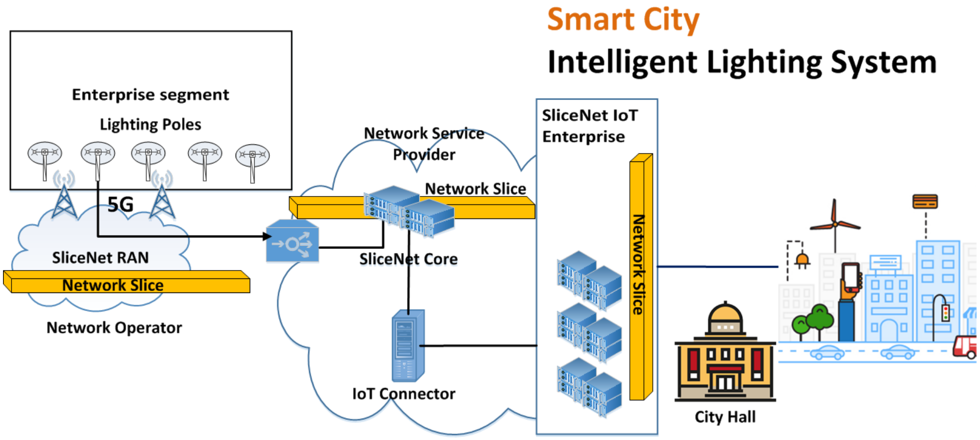


Figure 30: Smart City use case perspective

The vertical perspective for the specific Smart City use case implementation is described in the next figure:

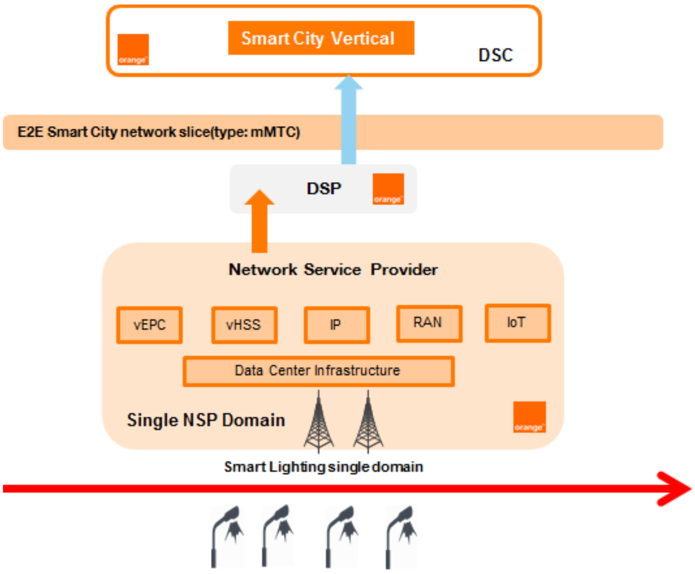


Figure 31: Smart City use case implementation

The use case scenario, as described in D2.1 contains several steps in achieving the implementation of the service, achieved during the use-case prototyping process:

1. Network technology used:

   a. Smart Lighting LoRaWAN connectivity based architecture (demonstrated during 1st review)
   b. Smart Lighting LTE-M connectivity based architecture (on-going integration, prototyping and demonstration)
   c. Smart Lighting 5G conectivity based architecture (further actions plans)
2. Network transformation
   a. from dedicated network functions to software network functions (virtualised CN, virtualised IoT application)
   b. virtualised-ready infrastructure (Openstack based)
   c. automated orchestration (resources; services; slices): NMRO; Slicer
   d. timing improvements for service creation
   e. resource allocation
3. Cognitive networks
   a. Noisy neighbour implementation, as described in D5.6
   b. QoE sensors and optimizers
4. Network and service metrics data collection
   a. infrastructure data collection
   b. QoS service collection
5. Actuation

3.2 Legal and Regulatory environment for likely deployments

3.2.1 Smart Grid

Markets across Europe are becoming more dynamic and liberalised, increasing the number of people implicated in the future of electricity supply. From government members to everyday users, every stakeholder will help to shape the Smart Grids system, broadening users' expectations and including value added services, energy services on demand and total connectivity. Network owners and operators are, therefore called upon to fulfil customers' expectations in an efficient and cost-effective way, undertaking necessary investments to guarantee high levels of power quality supply and system security.

The Smart Grid vision relates to a programme of research, development and demonstration that charts a course towards an electricity supply network that meets the needs of Europe's future. Europe's electricity networks must be reliable, assuring and improving security and quality of supply, consistent with the demands of the digital age with resilience to hazards and uncertainties [12].

The referred vision embraces the latest technologies to ensure success, whilst retaining the flexibility to adapt to further developments to increase power transfers and reduce energy losses heightening the efficiency of supply, whilst power electronic technologies will improve supply quality.

Advances in simulation tools will assist the transfer of innovative technologies to practical application for the benefit of both customers and utilities. Furthermore, developments in communications, metering and business systems will open up new opportunities to enable market signals to drive technical and commercial efficiency.

3.2.1.1 Continuity of service

Electricity continuity of supply concerns interruptions focuses on the events during which the voltage at the supply terminals of a network user drops to zero or nearly zero [13].

Power system protection is paramount for today's smart grid. The purpose of power system protection is to detect and clear electrical faults, which will consequently increase the system power quality and reliability. The fewer the interruptions and the prompter the return of electricity supply, the better the continuity from the network user's point of view. Therefore, one of the roles of network operators is to optimise the continuity performance of their distribution and/or transmission network in a cost-effective manner.

Continuity of supply indicators are traditionally important tools for making decisions on the management of distribution and transmission networks. Regulatory instruments now mostly focus on accurately defined continuity of supply indicators of frequency of interruptions, their duration, and energy not supplied due to interruptions. These instruments normally complement incentive regulation, which (either in the form of price or revenue-cap mechanisms) is commonly used across Europe at present. Incentive regulation provides a motivation to increase economic efficiency over time. However, it also carries a risk of network operators refraining from carrying out investments and proper operational arrangements for better continuity, in order to lower their costs and increase their efficiency.

In this sense, are defined the types of interruption in transient interruption, short interruption and long interruptions according to the EN 50160 standard regarding voltage characteristics in public distribution systems [14]. As a standard for most European countries, it is considered a transient interruption if it lasts less than one second, a short interruption if the electricity supply is unavailable between one second and three minutes and a long interruption if the duration is longer than three minutes. To ensure the reliability of distribution grids, the Council of European energy regulators issued several recommendations on a set of indices System Average Interruption Duration Index (SAIDI), System Average Interruption Frequency Index (SAIFI) and Momentary Average Interruption Frequency Index (MAIFI) suitable for pan-European benchmarking of distribution network performances [13].

The measurement of actual continuity levels through indicators and standards constitutes the basis for regulating continuity and quality of supply as a whole. In general, the actual measurement of continuity can be performed on two different levels, namely system level and user-specific level. The existence of incentives promoting improvements in continuity of supply is a pre-requisite or a main driver for the implementation of smart grid solutions based on network monitoring, protection and automation. European regulators have traditionally placed a strong importance on continuity of supply. Hence, bonus-malus schemes are widespread across EU.

However, the existence of these incentives is not enough by itself to promote such functionalities since an appropriate design and implementation, which can significantly differ on a per country basis, are also essential. For instance, countries like UK or Germany set incentives related both to the frequency and the duration of supply interruptions. On the contrary, in Portugal, despite the fact that both SAIDI and SAIFI are monitored, the economic incentives exclusively depend on an index measuring the duration of interruptions [15]. This can dilute the incentives seen by Distribution System Operators (DSOs) to implement network monitoring and automation for smart grid protection and reconfiguration, since these solutions may not only achieve a reduction in the duration of interruptions, but also the measured number of interruptions provided that all or part of the consumers that have suffered an interruption are re-supplied within the time threshold beyond which an event is considered as a long interruption, set at 3 minutes across EU countries [13], including partner countries.

3.2.1.2 Regulatory incentives

In addition to reporting obligations, DSOs are required to explicitly include strategies for loss reduction into their forward-looking business plans. Moreover, the regulator may provide DSOs with a discretionary reward on top of their allowed revenues when it may be considered that the DSO has, for example, managed to identify more cost-effective and innovative ways of reducing network losses.

However, QoS or energy losses are not the only types of incentive schemes for DSOs that may be found. Additional mechanisms may intend to encourage certain behaviour of expenditures from DSOs. Conventionally, these mechanisms were mostly related to what may be referred to as commercial quality indicators, such as timely connection of new network users or time taken to respond to a complaint. Nonetheless, a much more extensive use of output indicators is deemed necessary to promote a deeper change in the current distribution network planning and operation practices.

With increasing demand on the power supply system, as well as the need for improved reliability, prevention of power supply disruption is one of the key goals of the Smart Grid. Because of the inherently interconnected and interdependent nature of the grid, improving wide area monitoring and situational awareness is necessary to achieve this objective. A disturbance in the power supply in one area can quickly translate into a widespread problem, with cascading and deleterious consequences [16]. Additionally, information about the power supply in neighbouring areas can help utilities optimise the economic operation of the grid. Wide area situational awareness (WASA) refers to the implementation of a set of technologies designed to improve the monitoring of the power system across large geographic areas – effectively providing grid operators with a broad and dynamic picture of the functioning of the grid [17].

The communications requirements for synchrophasors vary depending on the nature of data being transmitted. For real-time monitoring and control, latency requirements are very low, ranging typically from 20 to 200 ms although the latest developments in wireless networks point to latencies up to 1 ms [18]. For post-event historical data, low latency is less imperative. In terms of data requirements, phasor measurement data will be continuous, rather than variable. It is estimated that synchrophasors will require between 600 kbps and 1500 kbps, thus requiring high speed, high throughput communications, pointing specifically to the IEC standard 61850, which is applicable for these types of communications [19]. Over time, with the proliferation of devices, the increased use of distributed generation, and the introduction of new applications for phasor data, the aggregate bandwidth demands shall increase.

3.2.2 eHealth

3.2.2.1 European Market

European health care systems and societies are challenged to use available resources optimally in the wake of medical, economic and ethical implications of budgetary constraints in emergency care. Thus, there is a strong need to find solutions to maintain or increase the quality of patient care, while considering socio-economic aspects as well. One possible solution is to use mobile telemedicine, which are information and communication technologies allowing medical diagnostics and treatment over geographical distances. Mobile telemedicine offers the opportunity to establish patient care earlier and increase the quality of patient care. This project approaches different aspects of medical care and analyses, how mobile emergency telemedicine can support medical care.

During the pre-hospital ‘golden hour’ Remote video can help with accelerated decision making for pre-hospital triage, diagnosis and treatment. This can impact stroke and heart attack patients where time is important to save brain tissue and heart muscle with thrombolysis clot busting drugs.

Using mission critical video to stabilise patients at home (e.g. COPD, frail/elderly, soft cases cohort) can reduce public administration costs in hospitals. Typical savings are €250 for ambulance transfer and €1000-€1500 per bed night if the process can avoid a patient bed night.

Demand for prehospital emergency care has increased significantly these last decades throughout the Western world, in terms of numbers of emergency calls and dispatched ambulances. This development represents a challenge for both the prehospital emergency communications systems and the emergency departments in the hospital, in terms of:

- Limited prehospital triage
- Riskier patient outcomes, due to a deficit in critical decision support at pre-hospital locations
- Hospital and ambulance operational inefficiencies due to resource constraints
- Increased costs due to high numbers of ambulance events and unnecessary hospital bed usage

3.2.2.2 Standards and Regulations for Emergency platforms

At the same time, legacy public safety and mission-critical communication systems (e.g. ETSI's Tetra) have been designed primarily as purpose-built mobile radio networks for the delivery of mission-critical voice, as well as a select number of narrow-band data services (e.g. text-based messaging). They operate at the level of 2G, which the mass market has used since the 1990s. Emergency services networks currently operate under three different protocols (i) ETSI based Tetra, (ii) Tetrapol which is defined by the Tetrapol Publicly Available Specification and (iii) P25 which is defined by Telecommunications Industry Association. These networks are based on the equivalent of 2G with a small amount of data capability.

These networks have been costly to design, deploy and service, and without a fundamental redesign, will not be able to deliver and exploit the media-rich type services currently accessible over public broadband networks. With early deployments well underway, next generation 5G networks are expected to start commercial launches across the world by 2020, working alongside existing 3G and 4G technology to provide faster speeds and more reliable connections than ever before.

Smartphones can stream video from public 4G network using, for example, WhatsApp or Facetime, but they must be held in place manually and pointed at the patient. So the paramedic loses the use of one hand. In addition, these platforms are not GDPR compliant as their business model is advertising driven and are not suitable for medical data governance. The data is not encrypted or prioritised for patient security.

3.2.2.3 Digital Service Provider for eHealth in 5G Market

Public safety and health are identified as key vertical industry sectors to be supported by public network operators. The potential for professional to professional wearable video supports lots of use cases in a clinical environment. But to deliver these benefits, market fragmentation needs to be overcome. There is fragmentation because:

a) wearable devices come from one set of vendors in manufacturing sector (usually China);
b) Wireless networks (WiFi, 4G & 5G) come from service providers all over Europe who deliver connectivity per national market in EU28, but have service creation/agility issues and need a middle provider;

c) Service and application software come from code developers such as RedZinc;
d) the users (e.g., doctors, nurses and paramedics) in a clinical community are totally disconnected from the technology providers.

The concept of a eHealth Digital Service Provider (as shown in Figure 35 below) which will overlay existing and future network infrastructure to provide a tailored, secure, virtual prehospital emergency communications network, focusing on the specialized clinical sector at European and global level.

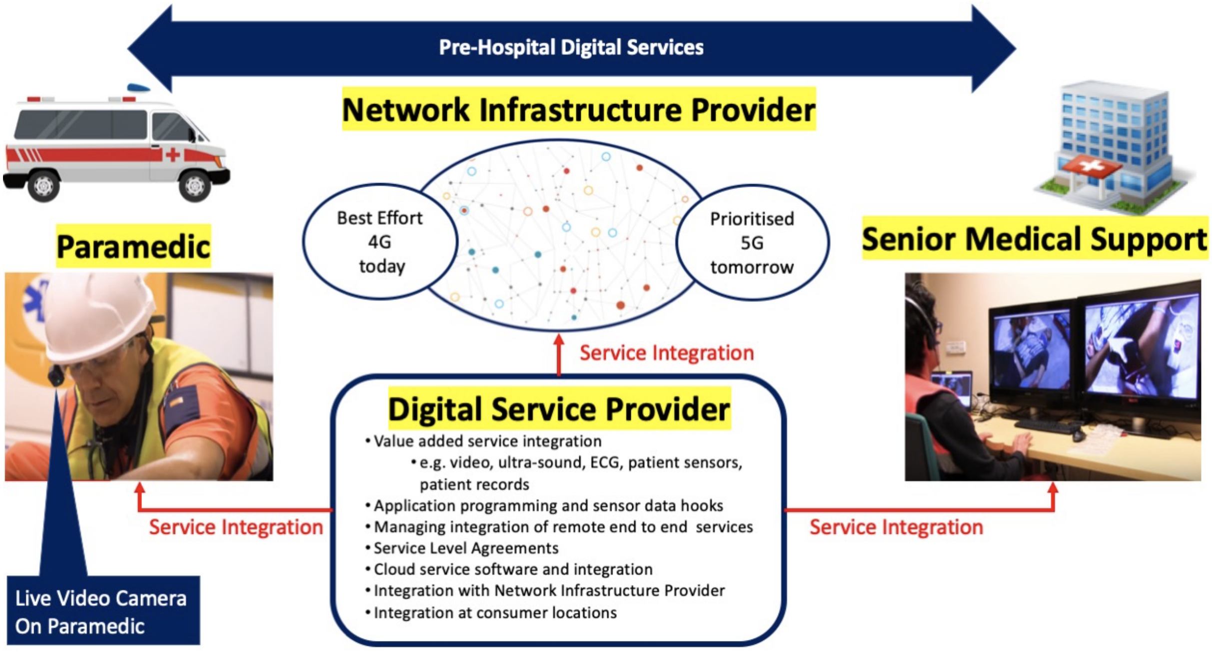


Figure 32: Digital Service Provider for eHealth

According to Oppenheimer Research[1]the cloud is the most important technology in our lifetimes. Every industry and segment of society is set to be radically altered by data feeding into the cloud from a wide spectrum of sources creating €10Trillion plus in global market value in the next decade. A remote healthcare platform as the inevitable future for modern ambulance communications services. A digital service provider provides video complimenting other clincal data.

3.2.2.4 Transforming pre-Hospital Processes

Wearable Paramedic Video transforms hospital processes. It has the necessary technical ingredients to provide an end to end solution for doctors, paramedics and community nurses to communicate by video. It uses a dedicated, network traffic prioritisation, a kind of ‘bus lane’ in the internet cloud for emergency healthcare data. This means that emergency video is given the same network priority as YouTube although it uses the same underlying wireless infrastructure.

Value Proposition is a remote health care platform transforming hospital and ambulance processes. The wearable, cellular, video streaming, telemedicine platform coupled with value added healthcare services, including patient records, heart monitor ECG and other bio-metric sensors (oxygen, blood pressure, ultrasound) can prioritize critical decisions thereby providing clinical, economic operational and social benefit to all concerned.

Rather than transport the patient to the emergency doctor we can first transport the doctor virtually to the patient as shown in Figure 36 below. The value summary for the stakeholders is:

Patient	• **More rapid decisions & treatment for acute pre-hospital patient events** • **Treat at scene for minor pre-hospital patient events avoiding hospital transfer**
Ambulance Service	• Operation efficiency increase through 15-30% reduced soft case transfers • Instantaneous collegiate and senior support meaning better decisions quicker
Hospital	• More accurate pre-hospital triage means reduction in soft cases arrival by 15-30% • More accurate pre-hospital triage means knowledge and earlier treatment for acutes
Funders	• Healthcare funders, whether insurance or governments obtain value by more efficiency and reduced costs emergency department and ambulance service costs

Table 2: The value summary for the stakeholders

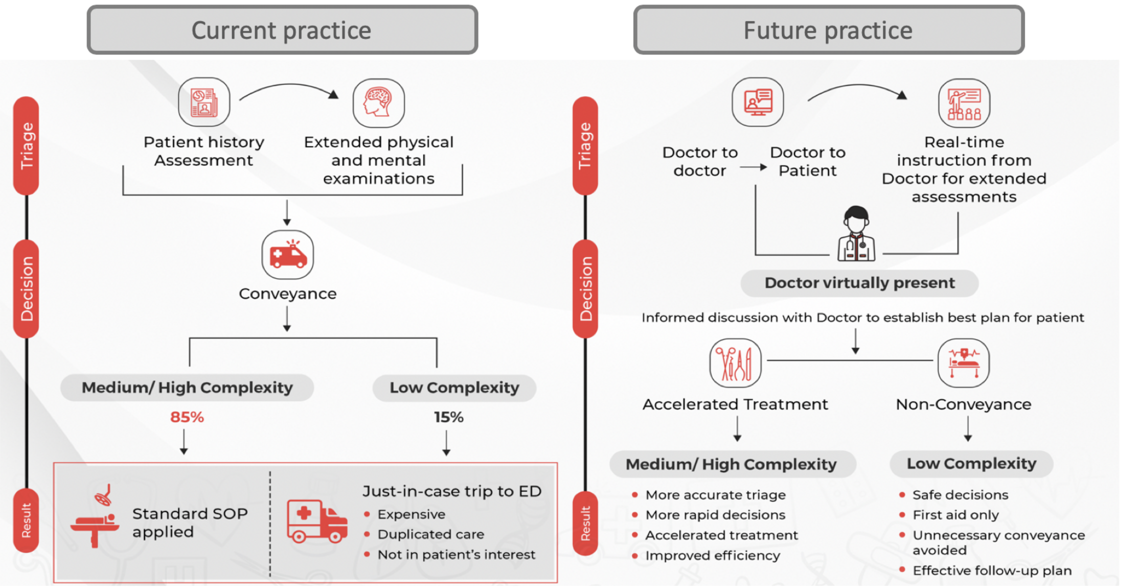


Figure 33: pre-Hospital Triage with Virtual Doctor

3.2.3 Smart City

According to this use case, the responsible entity will be able to remotely control in real time and in a secure way every single lighting pole from the target network, in order to adjust the lighting intensity and efficiently manage energy consumption.

---

[1] Cloud Set to Drive a New "Roaring 20s" Defined by Big Productivity Improvements A Once-in-a-Century General-Purpose Technology. Real Disruption Coming. Oppenheimer Equity Research October 11, 2019

The system will give public lighting distribution company reporting to the city manager, the ability to automatize the control of the lights, including the on/off and diming capability according to certain policies (e.g. day time moment, natural light intensity, location, traffic).

This system, combined with the adoption of more efficient LED based ballast lamps, is anticipated to generate a reduction of energy costs for up to 80%, and a return of investment in just four - five years. According to a report [Philips Lighting and World Council of City Data], only about 10% of the 300 million street lights poles in the world are using energy-efficient LEDs, and just 2% are connected thanks to legacy communication technologies such as PLC and 2G/3G.

Moreover, the system will allow real time and history based energy consumption measuring

The entity responsible with the streets lighting infrastructure operation and maintenance will be able to proactively spot the malfunctions, energy loss or energy theft tentative on the public lighting network, as the system will generate intervention ticket in real time per pole or branch of poles. This capability will highly improve the city lighting service availability and will decrease the operational costs with maintenance activities. There is an international standard [ISO 37120] that specifies a set of indicators meant to define and measure the performance of quality of life and city services. This is applicable to any city or municipality that targets to measure its performance in a comparable and verifiable manner, irrespective of size and location. Street lighting can consume between 15 – 50% of public electricity [ISO 37120]. Electricity consumption of public street lighting is calculated as the total electricity consumption of public street lighting (numerator) divided by the total distance of streets where street lights are present (denominator). The result shall be expressed as kWh per kilometer per year.

3.3 UC Infrastructure Descriptions

3.3.1 Smart Grid

The main purpose of the Smart Grid use case is to demonstrate that the new available technologies, 5G, NFV and SDN together with network slicing concepts, provide an adequate framework for power system protection and control device peer-to-peer communications.

The following topics are essential for the success of the Smart Grid use case:

- To provide an ultra-reliable communication infrastructure for smart grid devices;
- To exchange messages between remote devices at very high speed;
- To provide deterministic communications;
- To provide secure communications between smart grid devices, focusing on the operational technology cybersecurity principles availability, integrity and confidentiality;
- To guarantee QoS and QoE under all network conditions.

The use case testbed, represented in Figure 34, includes the hardware and software elements necessary for the Vertical, Digital Services Provider (DSP) and Network Services Provider (NSP) actors to perform their actions and play their roles in the final validation and demonstration trials. In the diagram, the Vertical is represented in purple, the DSP and NSP1 correspond to the same entity, represented in yellow, and the NSP2 is represented in blue.

The testbed is currently equipped with four Efacec protection relays (IEDs), all of which are connected to the LTE Radio Access Network (RAN). Three are field IEDs connected to Long Term Evolution (LTE) modems; the other is a substation IED, connected to the Egde/Core network through a physical Local Area Network (LAN). All four IEDs are also connected to a second LAN, separated from the RAN, which is used for management and Network Time Protocol (NTP) synchronization.

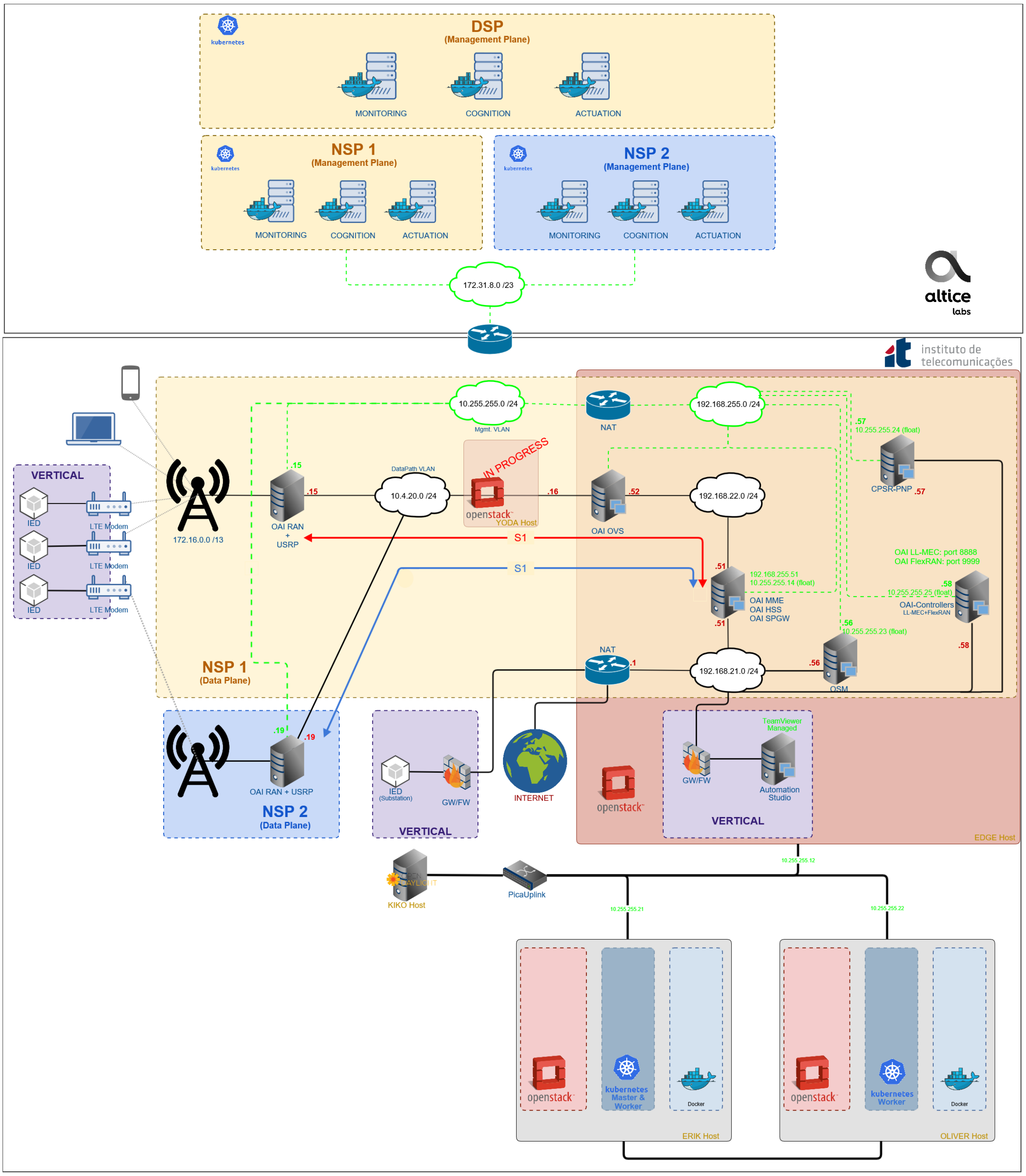
The mobile network used to provide LTE coverage to the IEDs and other terminals is based on the OpenAirInterface (OAI) open-source framework. This consist of three major components:

- OAI RAN - eNodeB (eNB) implementing the full LTE stack and a USRP B210 as the Radio-Frequency transceiver and antennas implementing the over-the-air interface.
- OAI CN – Implementing the Core Network services (MME, HSS, SGW, PGW).
- OAI FlexRAN and LL-MEC – RAN and Core Network controllers, respectively. They provided statistics and information about the mobile network and the ability to setup RAN slicing. This is done through the FlexRAN and LL-MEC APIs.

The OAI RAN is deployed in a physical machine due to real-time processing requirements of the eNodeB. Remaining components are deployed as virtual machines on OpenStack. Also virtualized on OpenStack is the Automation Studio VM used by Efacec to control and manage all four IEDs.

Efacec IEDs are connected to the RAN using a cellular-to-ethernet gateway (MOXA G3150A-LTE).

The entire infrastructure is divided in two VLANs separating the Management and Datapath connections.



Subtitle image:

At Instituto de Telecomunicações premises:
- Black line: Data Plane
- Green dashed line: Management and Control

Figure 34: Smart Grid UC Testbed

3.3.2 eHealth

eHealth use-case high level Overview

This section will discuss a high-level description of the eHealth use case and the infrastructure built for that use case.

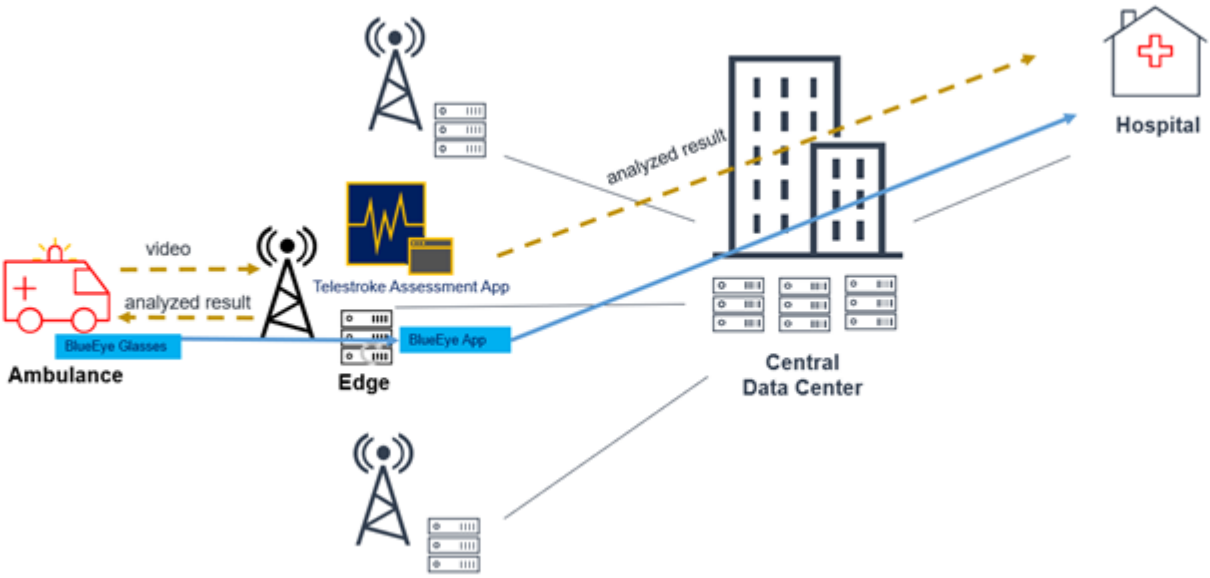


Figure 35: eHealth UC high level description

Figure 38 shows the scenarios of the eHealth UC where the ambulance is connected to the hospital with 5G network. There are two services running in this use case: i) the BlueEye service and ii) the Telestroke Assessment service.

Figure 39 shows the eHealth infrastructure at Dell premises Ovens, Ireland. On top of the infrastructure, the open source security software, pfSense, is running to provide different security services including the firewall, NAT rules, rule/policy-based traffic control and OpenVPN server with TLS protocol.

System access through web portal/one-stop API will require to run an OpenVPN client software and authorised with credentials and certificate to open connections with OpenVPN server configured and running at pfSense server. After this authentication phase, e.g., the user is successfully initiating the sequence, OpenVPN allocates an IP address to this user to enable the user in the tunnel, accessing the LAN network. The configuration in the OpenVPN server allows which LAN network the user is tunnelled into, and with firewall rules, pfSense controls which servers, VMs, services in that LAN network that the user can have access to. For eHealth, we have configured the VPN connections to have AES-256-CBC/SHA1 for cryptography and 2048 bits parameter length Diffie-Hellman for key exchange, remote access with SSL/TLS protocol.

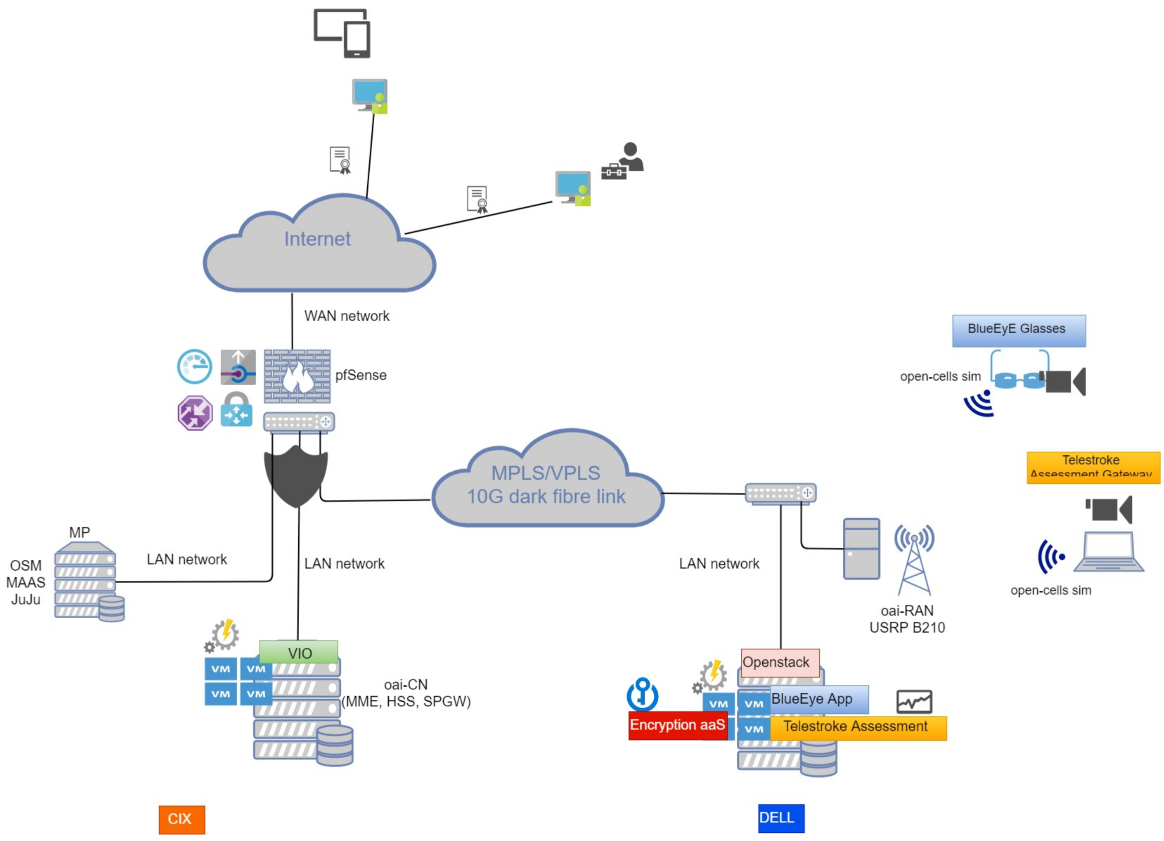


Figure 36: eHealth infrastructure at Dell premises Ovens, Ireland

Below the firewall and security services in pfSense, the infrastructure is spanning across 3 racks for different purposes: i) management rack with 3xR510 PowerEdge servers and 2xR610 (one for primary controller node and the other for secondary controller node to enable the HA feature), the servers in this rack are running management services such as OSM (release FIVE), MAAS and Juju, the rack will be dedicated for other management components/services that will be integrated in future; ii) core/enterprise cloud rack has an R430 server running oai-CN components (MME, HSS, SPGW) and 4xR640 servers are configured as cloud operating system, running VIO VMware (abstracting the VMware vSphere with NSX environment to have the outbound interfaces as Openstack API). The rack is dedicated to run core components/services, the VIO cloud is also for demonstration purpose where the services running here (as core/enterprise cloud services) should have longer delay compared to the services running at the edge; and iii) the edge rack with 4xR640 servers running Openstack. This edge VIM is hosting the two eHealth services (Telestroke Assessment and Video Relay above). LL-MEC and FlexRan controller are also deployed in this VIM for RAN virtualisation and traffic control. The two racks of MP and core/enterprise are located in CIX where the edge rack is located in Dell premises which is 15km away in geography and these are linked by MPLS connection with both PE devices enabling VLPS to have L2 encapsulation from the two sites.

Finally, a stand-alone eNB is composed by Dell Precision 5000 that is running oai-RAN software and is attached with USRP B210 radio. To have access to this eNB, open-cells SIMs are reprogrammed with uicc/sim programming software provided by open-cells. One of the SIMs is then inserted into the Dell Edge Gateway series 3003 with LTE modem built-in. This device with the SIM card is attached with an Intel Realsense camera for UE device that is running as the gateway in the ambulance, capturing the images of the patient for Telestroke assessment. Another SIM is then used for Video Relay device which starts to stream the video of surroundings to a normal device, e.g., doctor's laptop, connected at the hospital site to see what has happened at the ambulance site.

For prototyping, SliceNet focuses on the 4 unique scenes for eHealth UC:

- At the design phase, eHealth UC focuses on the Service Subscription where it shows the workflow of eHealth service subscription and onboarding which is different from the other 2 use cases regarding *the vertical owned services*, e.g. BlueEye and Telestroke Assessment services.
- At runtime, eHealth UC focuses on the Service Runtime Monitoring which is requested by the vertical owned services, to monitor the *performance (latency, throughput, jitter) of the services* they bring to the slice.
- At the optimisation phase, *delay-sensitive* eHealth UC focuses on i) Anomaly Detection and Response in Quality of Communication and ii) Handover Control to guarantee the QoS/QoE for the use case.
- Finally, the eHealth slice Decommission to decommission the slice instances including the vertical owned services.

3.3.3 Smart City

The Smart City infrastructure is composed by several components that provides the communication service needs for the use case:

- physical infrastructure layer
- virtualisation layer
- NVF/VNF layer
- Smart City IoT layer

The use case prototyping is focused on the Smart City implementation and consists in implementing 2 service networks, a mMTC service for the IoT Smart Lighting slice and eMBB slice that will consume the resources mainly from RAN and Core Network.

The use-case prototyping, following the preparation (design and offer), subscription (service instantiation), runtime (monitoring, optimization, actuation) and decommissioning is based on the generic worflows described in Chapter 1.

The services are instantiated following the SliceNet framework, using virtualised RAN and Core Network, programmability through single operator domain, management framework, resources, service and slice orchestration, P&P framework for vertical control exposure. The Smart City test-bed infrastructure was built to support all this capability and is detailed further.

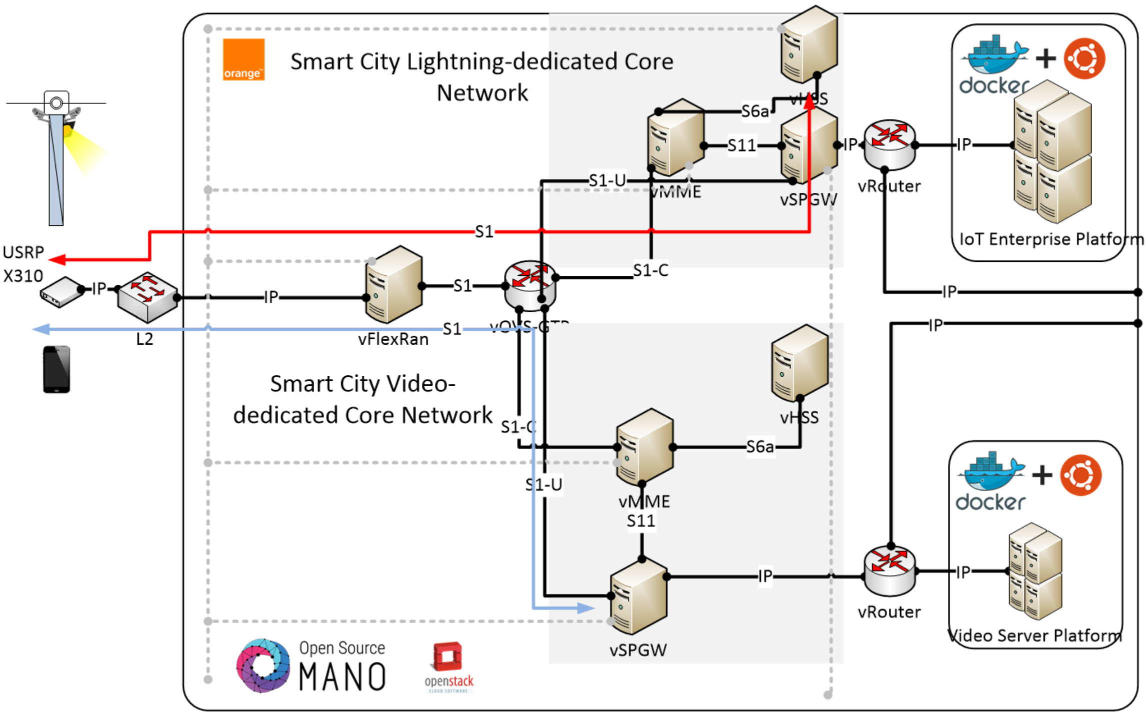


Figure 37: Smart City use case architecture

The IaaS deployed infrastructure is described by the next figure, and contains:

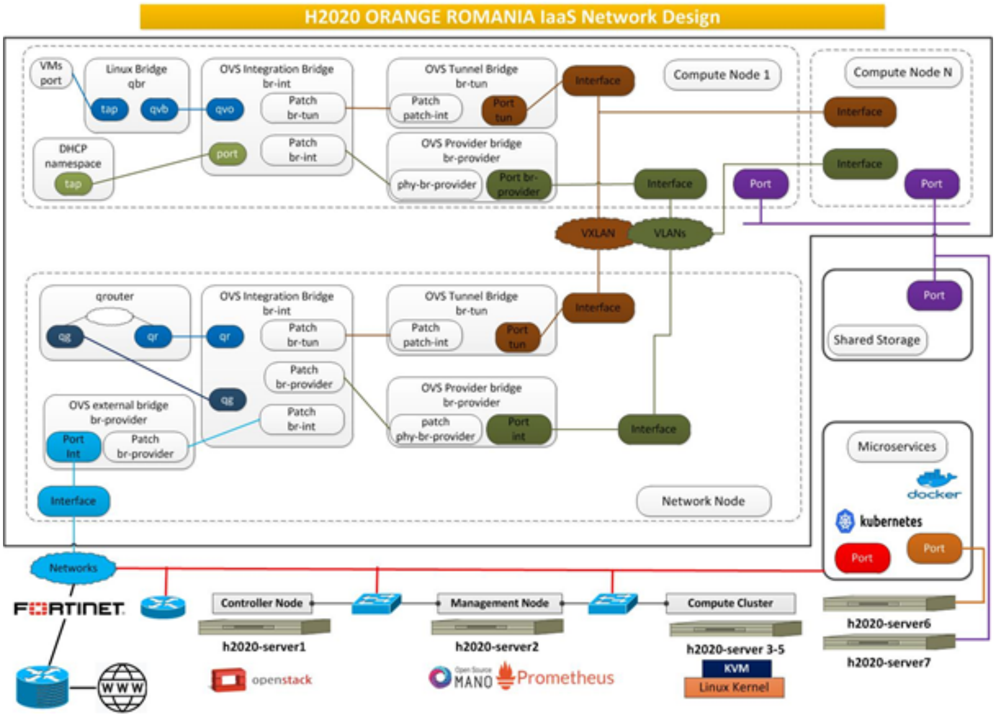


Figure 38: Orange IaaS for Smart City use case prototyping

Testbed Physical Infrastructure:

- hardware components: the entire suite of physical network elements (routers, switches, firewalls)
    - switches: Cisco NX-OS 9k
    - routers: ASR9k
    - firewalls: Fortinet 1500D
    - HP servers for IaaS: 1 controller node; 1 management node; 3 computes nodes; 1 bare-metal server for micro-services apps; 1 shared storage server
    - physical machine for eNodeB deployment
    - USRP Etthus x310
    - Lighting poles and LTE-M controllers
    - IP/MPLS transport infrastructure

Virtualization Layer:

The entire virtualization infrastructure is Openstack based, OCATA release, providing the capabilities of deploying 100s of VMs for different NFV/VNFs, ensuring proper communication between VMs inside the cluster and providing different physical interface outside the cluster. Inside the IaaS are configured three main bridges, as:

1. bridge br-tun with vxlan encapsulation, used for internal self-service VMs communication
2. bridge br-int, used for VMs tap level communication through ovs
3. bridge br-provider, used for external self-service communication

The provided IaaS ensures the proper service, slice and resources deployment and orchestration, use case Core Network instantiation, software developed inside the project, data collection for ML and training algorithms and live traffic migration for the described within WP5 activities of the noisy neighbour scenario.

NFV/VNF layer

The entire NFV/VNFs software components are based on VMs & container implementation, supported by the already described infrastructure.

Orchestration layer

The resource orchestration layer using the NMR-O, as deployed through OSMv5, integrated with Openstack, capable of vEPC monolithic deployment.

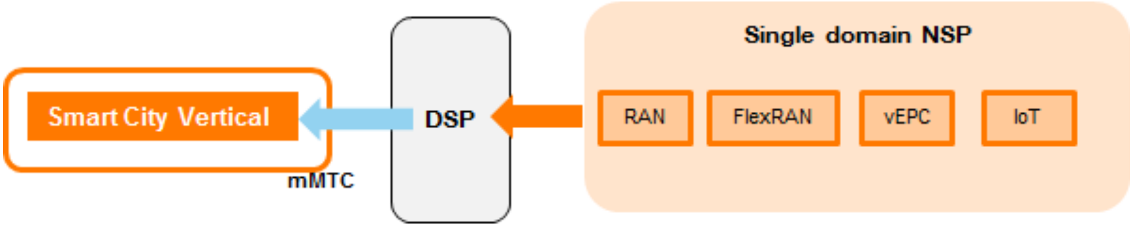


Figure 39: Smart City use case service instantiation - single domain

The system provides the network slice, E2E NS1, containing:

- RAN NSS resources -
  - centralized FlexRAN component for RAN slice provisioning
- EPC NSS resources (dedicated EPC distributed components per slice)
  - 1 VM MME; 1 VM SP-GW; 1 VM HSS
- IoT Enterprise multi-tenant application connectivity

For prototyping, the Smart City use case will demonstrate:

- the design phase, Service Subscription
- the runtime phase, Service Runtime Monitoring as latency, throughput, jitter of the services they bring to the slice.
- the optimisation phase, NN model implementation, provides the scenario of using two concurrent slices on the same testbed infrastructure, noisy-neighbour ML scenario
- the slice decommission

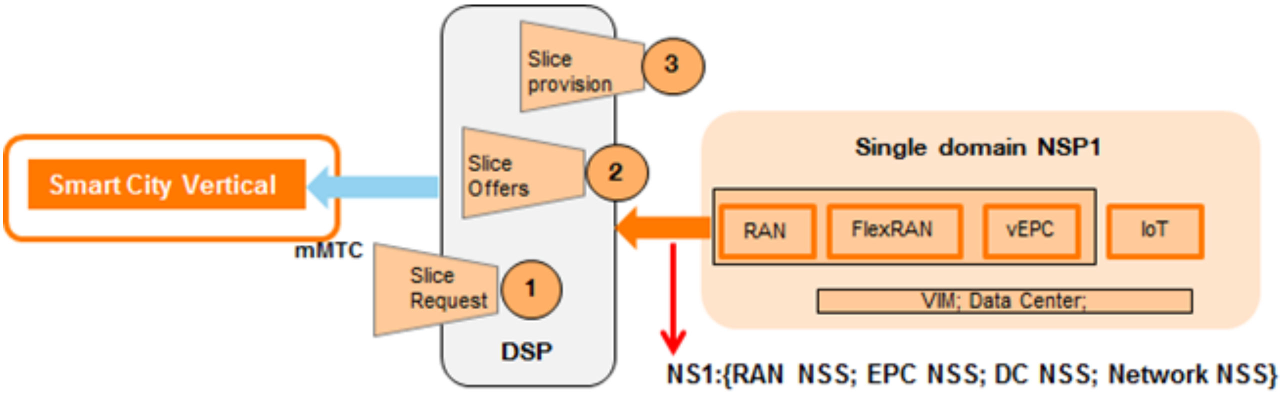


Figure 40: Smart City use case prototyping

3.4 UC Overview Descriptions

3.4.1 Smart Grid

3.4.1.1 Use Cases Storyline description

The Smart Grid use cases storyline can be seen as a set of scenes according with the next table:

Scene #	Scene title	Scene description
1.	DSP E2E NS and NSPs NSs preparation	The DSP E2E NS and the NSP1, NSP2 NSs preparation involves the design, onboard and offer workflows.
2.	Vertical service and DSP NSs subscriptions	The Vertical will subscribe the DSP service offer and the DSP will subscribe the NSP1 and NSP2 NSs offer.
3.	DSP E2E NS and NSP1, NSP2 NS runtime monitoring	In this scene the SG is working normally and collecting monitoring information from the network slices of all involved actors.
4.	SG protection coordination and reconfiguration	In this scene the SG fails and the protection and reconfiguration protocols are activated to self-heal the power grid. In this scene the DSP E2E NS as well as the NSPs NSs are working normally. More details about the SG protection coordination and reconfiguration schemes are available in section 3 of this document.
5.	NSP1 NS optimization	A fault prediction (e.g., RAN) is detected at NSP1 and the corresponding optimization is performed. This NSP1 protection scheme is only visible at the NSP1 level, the DSP and the Vertical are unaware of this occurrence.
6.	DSP E2E NS optimization	NSP1 predicts that a fault will occur in his NS and thus informs the DSP of this occurrence. The DSP then replaces this NS by an healthy NS from other NSP. Ideally, the NSP1 fault prediction, should be such that the DSP as time enough to provide a new NS from other NSP prior to a degradation/fault service to the Vertical.

Table 3: The Smart Grid use cases storyline

3.4.1.2 Scenes description

3.4.1.2.1 DSP E2E NS and NSPs NSs design, onboard and offer

In this scene the DSP is designing, onboarding and offering their services to the verticals (Figure 41, Table 4).

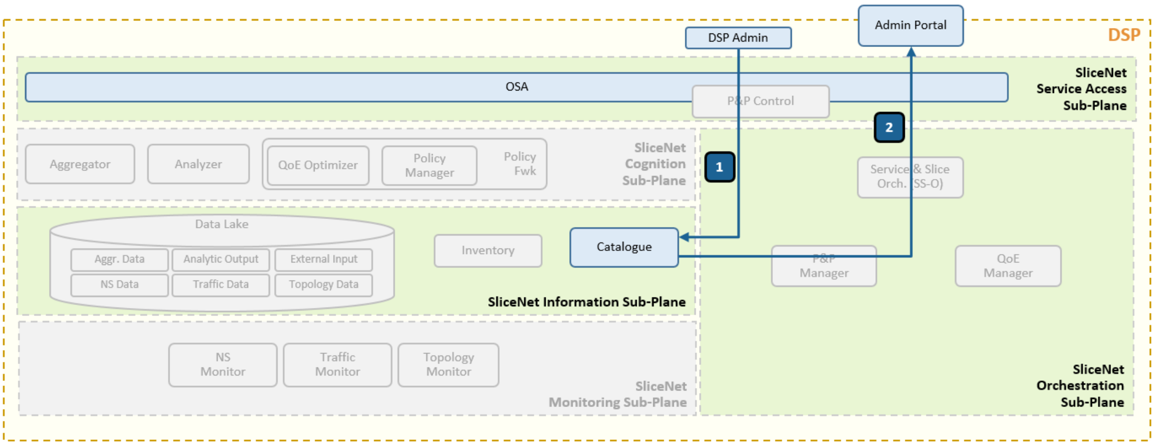


Figure 41: DSP E2E NS design, onboard and offer

Step	Description
1	The DSP will manually design and onboard their services. Each service can be translated into a Vertical Service Blueprint (VSB) that will be available to Verticals in a service **Catalogue**. The DSP shall be capable of translate the VSB in an E2E NS that is mapped in one or several NS from one or several NSPs.
2	The DSP offers the available services in the **Catalogue** to the Verticals.

Table 4: DSP E2E NS design, onboard and offer description

The NSP is designing, onboarding and offering their services, in the form of network slices, to the DSPs (Figure 42, Table 5).

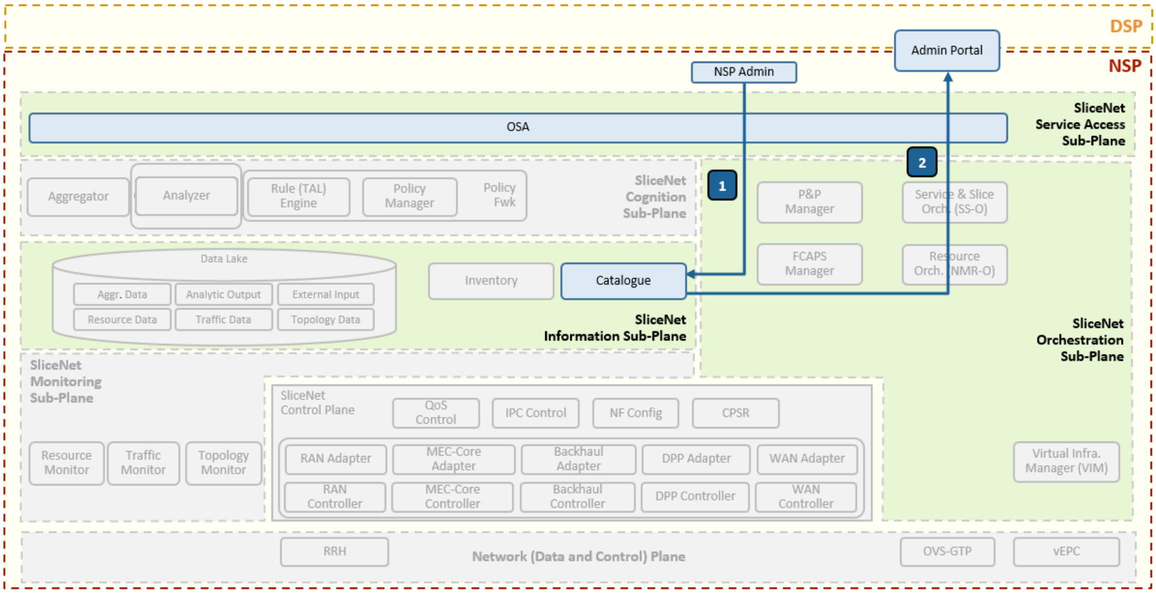


Figure 42: NSP NS design, onboard and offer

Step	Description
1	The NSP will manually design and onboard their services, in the form of network slices, to be offered to the DSPs. Each NS is translated into a Network Slice Template (NST) that will be available in a NST **Catalogue**. The NSP shall be capable of translate this NST into the several infrastructure network functions (PNFs/VNFs) that implements and comply with the NS requirements offered to the DSP.

2	The NSP offers the available services in the **Catalogue** to the DSPs.

Table 5: NSP NS design, onboard and offer description

3.4.1.2.2 Vertical service and DSP NSs subscriptions

In this scene the Vertical subscribes a service from the DSP (Figure 43, Table 6).

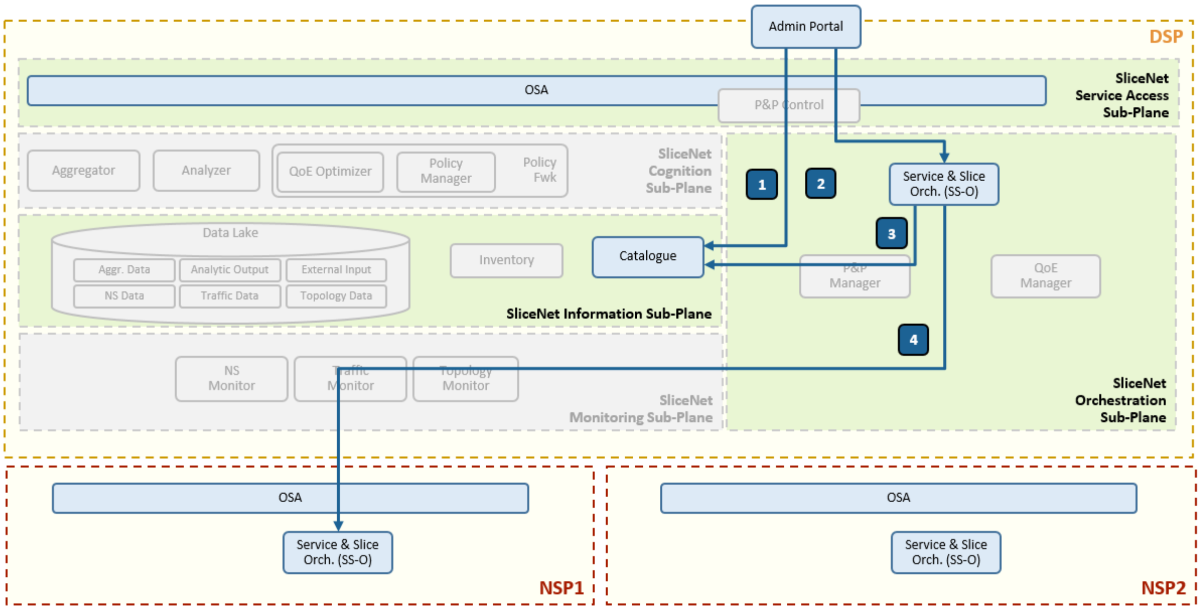


Figure 43: Vertical service subscription

Step	Description
1	The **Vertical** access the **DSP service catalogue** and selects the appropriate VSB (Vertical Service Blueprint). This VSB has open fields that allows the Vertical to fill in his needs in terms of requirements (latency, bandwidth, geography, etc.) providing thus all the necessary information for the DSP to instantiate the service.
2	After selecting and filling the VSB, the **Vertical**, through the Admin Portal, requests the instantiation of the VSB towards the **DSP SSO**.
3	The **DSP SSO** maps this VSD into an E2E Network Slice Template (NST) describing the NS details for this specific Vertical service.
4	The **DSP SSO** decomposes the end-to-end NST and selects the appropriate NSP NSs that comply with the service requirements and sends a NSI request to each one of the selected NSPs.

Table 6: Vertical service subscription description

The DSP will then compose an end-to-end network slice from one or several NSPs offering their NSs. Figure 44 and Table 7 depict the DSP subscribing to one NSP NS. This process is replicated for each NSP involved in the end-to-end NS.

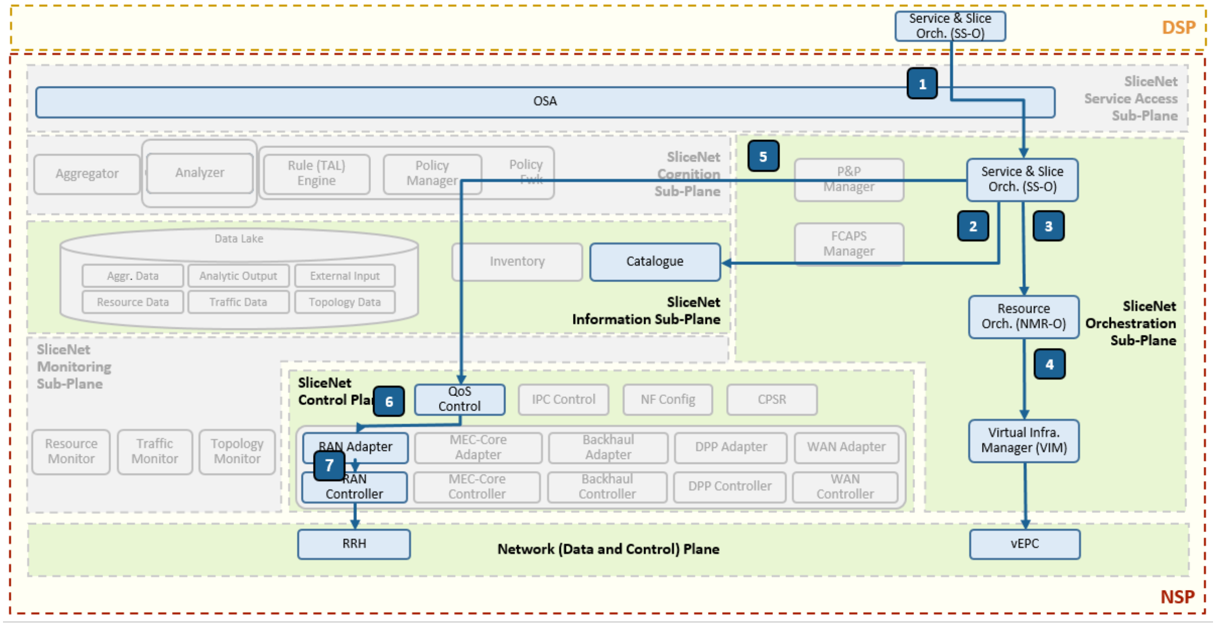


Figure 44: DSP NSs subscription

Step	Description
1	The DSP NSI request is delivered to the **NSP SSO**.
2	The **NSP SSO** then translates the NSI request into the Network Slice Descriptor (NSD). The network slice is then decomposed in the corresponding resources (PNFs/VNFs).
3	The **NSP SSO** then contacts the **NMR-O** to deploy and provision a vEPC on the data center
4	**NMR-O** deploys and configures, through the **VIM**, the vEPC on the data center.
5	After deploying and configuring the vEPC, the **NSP SSO** requests the **QoS Control** to configure the RAN segment with the appropriate NS parameters.
6	The **QoS Control** forwards the request towards the RAN segment responsible – **RAN Adapter**.
7	Finally, the **RAN Adapter** chooses the appropriate **RAN Controller** (depending on the RAN vendor) and requests the later to configure the required NS parameters.

Table 7: DSP NSs subscription description

3.4.1.2.3 DSP E2E NS and NSP1, NSP2 NS runtime monitoring

This scene describes the normal service operation in all its forms either at DSP and NSPs levels. Each actor involved is collecting all relevant data (events, performance, etc.) from their NS and infrastructure and storing it in the appropriate repositories. The Vertical should also have his “network” working in normal conditions. Figure 45 and Table 8 depict this workflow at the DSP level.

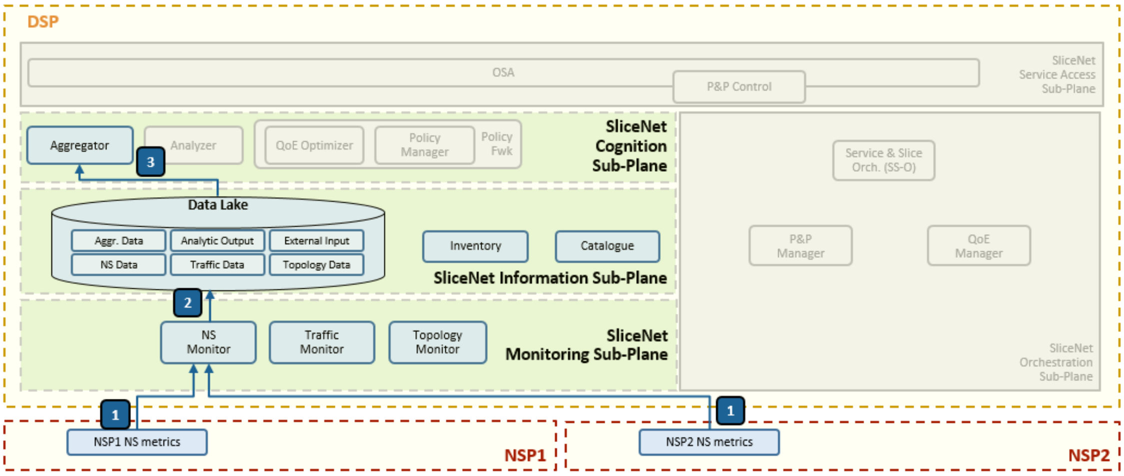


Figure 45: DSP E2E NS runtime monitoring

Step	Description
1	When the Smart-Grid low latency service is under normal operation, the DSP is collecting metrics from the NSPs. The metrics available are the ones subject to be measured to check if the SLA is according to the agreed contract (e.g., latency, bandwidth, etc.).
2	The raw metrics from each NSP are stored in the DSP **Data Lake**.
3	The **Aggregator** consumes the NSP-level metrics from the **Data Lake** and creates E2E level slice metrics to measure the performance of the low-latency service.

Table 8: DSP E2E NS runtime monitoring description

A similar procedure, illustrated in Figure 46 and Table 9, happens at the NSP to monitor the NS performance.

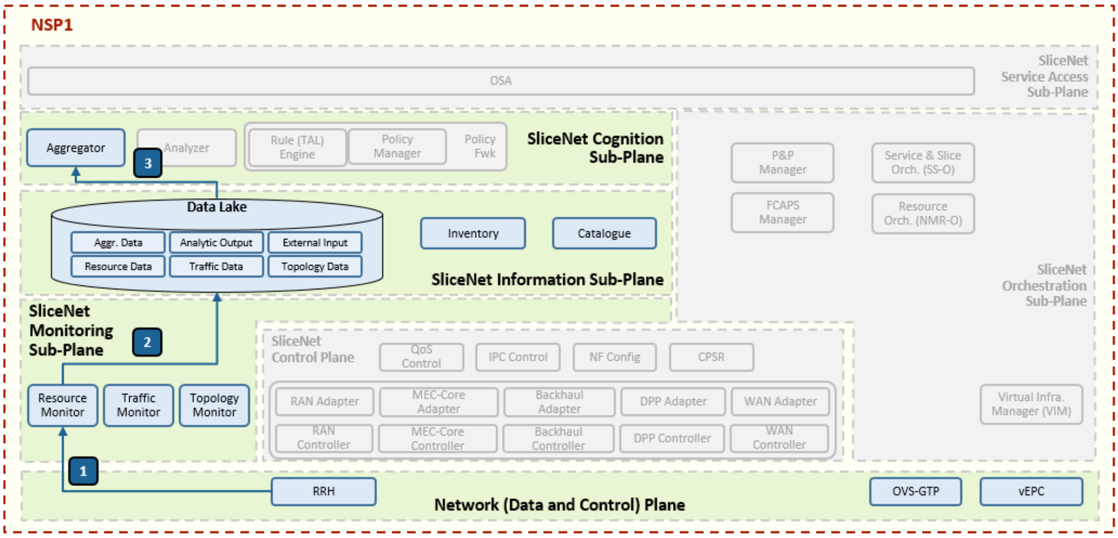


Figure 46: NSP1 NS runtime monitoring

Step	Description
1	When the network slice, for example the RAN NS from the E2E NS, is under normal operation, the NSP is collecting metrics from all the network functions (PNFs/VNFs) that can give measures to the Monitoring Sub-plane.
2	These metrics are then feed to the NSP **Data Lake**.
3	The **Aggregator** consumes the RAN NS raw counters persisted in the **Data Lake** and creates KPIs (Key Performance Indicators) about the RAN NS performance.

Table 9: NSP1 NS runtime monitoring description

3.4.1.2.4 SG protection coordination and reconfiguration

In this scene a failure is forced in the SG to trigger the SG protection and reconfiguration schemes (as described in section 3 - Use Case Prototype Descriptions). This is a failure in the Vertical power grid and thus will not affect the network actors, the DSP is still providing his E2E NS to the Vertical and the NSP is also providing his NS to the DSP which guarantees the communications between IEDs and between IEDs and the control centre. In practice our testbed has a URLLC network slice for the communications between IEDs and a second network slice for the communications between IEDs and the control centre. The second one does not need demanding requirements in terms of latency and/or bandwidth.

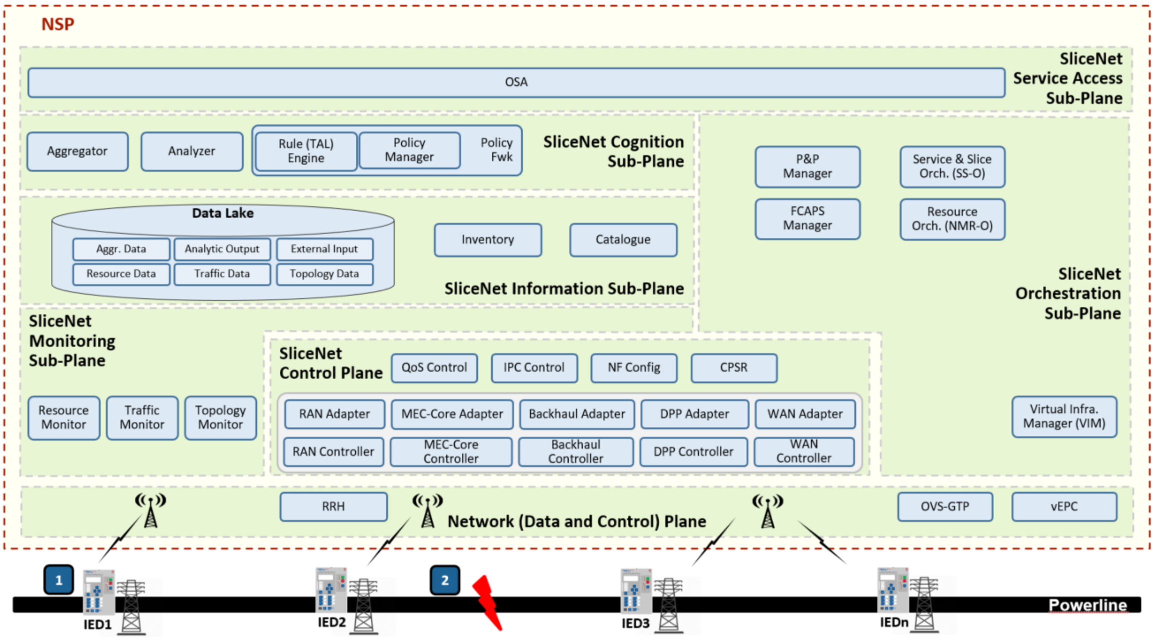


Figure 47: SG protection coordination and reconfiguration

Step	Description
1	The system is operating under normal conditions. All communications between IEDs and between IEDs and the control centre are up. Power system currents and voltages are stable and at normal levels.
2	A fault is simulated between IED2 and IED3. Line current levels rise abruptly to fault current levels. The IED2 and IED3 circuit breaker will open, thus clearing the fault de-energizing the section IED2 - IED3. All power system currents and voltages in the other sections are stable and at normal levels. All communications between IEDs and between IEDs and the control centre are up, even for IEDs in de-energized sections.

Table 10: SG protection coordination and reconfiguration description

3.4.1.2.5 NSP1 NS optimization

This scene shows a network optimization at NSP1 when the NSP1 predicts a failure and is capable of preventing it by actuating in his network resources to solve the predicted failure. It is a condition that may occur as a result, for instance, of a monitored “permanent bad performance” of a RAN and that usually results in an outage of this kind of RAN. The NSP1 can thus prevent that failure in advance and act accordingly, which can take several forms either an automatic switching handover of the service can be made or a field force should take care of the occurrence, etc. The major advantages of this procedure are the avoidance of a failure in the NSP1, which will have a great impact in all the services that are using that infrastructure, and also the fact that the SLA with the DSP will not be affected. This is an optimization at the NSP level and thus will not affect in any way the Vertical business.

Since this workflow is already described in detail in deliverable D5.7 [26], it will not be included in this document.

3.4.1.2.6 DSP E2E NS optimization

This scene shows an end-to-end network optimization at DSP. When the NSP1 is unable to solve a predicted failure and/or a severe alarm in his NS, the DSP is informed of this situation and can replace the NSP1 NS by an healthy NS, with the same requirements, of other available NSP. This is an optimization at the DSP level and thus will not affect in any way the Vertical business.

Likewise the NSP-level optimization workflow, also the DSP-level optimization is already described in D5.7 [26] and therefore will not be included herein.

3.4.2 eHealth

3.4.2.1. Vertical Perspective

Figure 49 shows an example of an E2E slice and how the E2E slice is mapped in the business model.

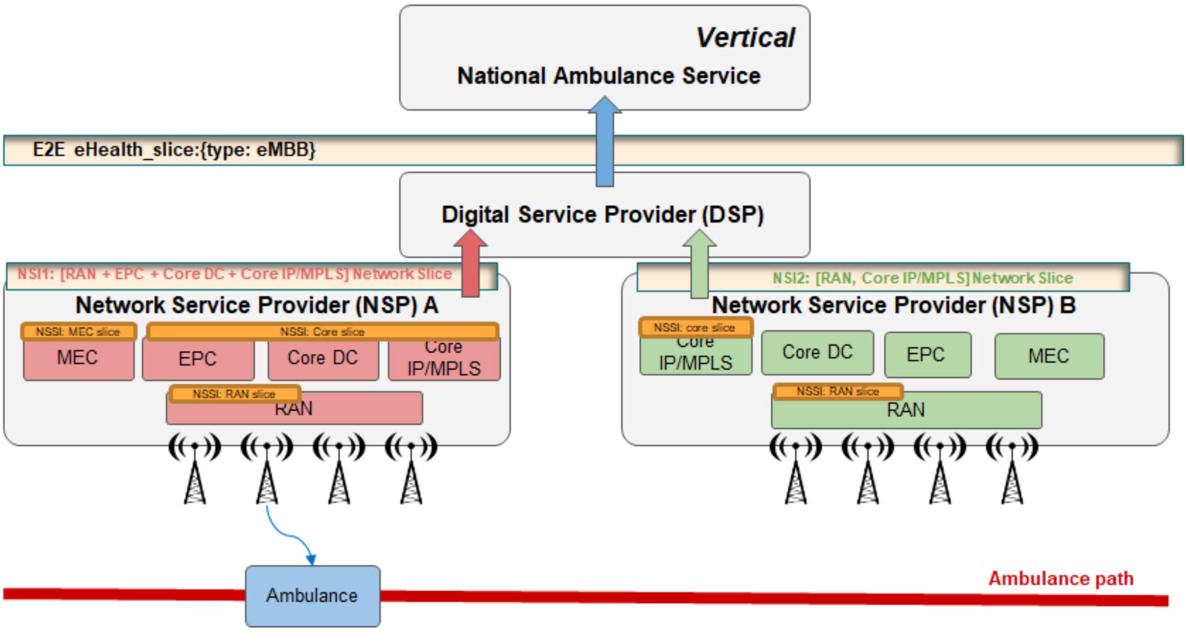


Figure 48: eHealth use-case Vertical Perspective

The red line at the bottom is showing the ambulance path where the ambulance can be moving from one network domain (NSP A) to another network domain (NSP B). At the current location of the ambulance, the E2E slice is composed of the RAN, the EPC/Core DC/Core IP/MPLS and the MEC network slices provided by the NSP A and the RAN and Core IP/MPLS slice from the NSP B. In this example, NSP B is providing the connectivity slice service so that remote consultants can be viewing the ambulance from anywhere as long as they are in the coverage of NSP A and NSP B. On the top, we have the vertical (e.g., National Ambulance Service) who is requesting the E2E slice service from the DSP and the E2E slice view from the vertical perspective is the connectivity from the ambulance to the hospital and remote consultants/doctors in hospital are having access to the vertical services (e.g., Telestroke Assessment and BlueEye) and seeing what has happened inside the ambulance and the patient's video/images.

3.4.2.2. Workflow Description

This section describes detail workflow descriptions of eHealth use-case prototyping. The use-case prototyping will focus on three main points:

- In the service subscription and onboarding, the prototype will focus on the vertical software (e.g., Telestroke Assessment and BlueEye software) design, onboarding and instantiation. It is to show an automated service orchestration with seamless composition and onboarding of the eHealth slice onto a VIM (either VMware VIO/Cloud DC or Openstack/edge stack).
- In the E2E slice runtime performance monitoring, the prototype will focus on the coordination work of the FCAPS monitoring system, P&P control and One-Stop API to shows how SliceNet can capture the performance of the eHealth slice during its runtime.
- In the optimisation phase, eHealth UC will demonstrate i) the Anomaly prediction and Response in Quality of Communication to show a PoC on how vertical feedback can be collected and SliceNet approach in exploiting the vertical feedback to improve network quality and to maintain QoS/QoE for the vertical; and ii) the Handover Control to maintain the QoS for the users.

3.4.2.2.1 Service Subscription and Decommission

The demo is to show a service orchestration with seamless composition and onboarding of the eHealth slice onto a VIM (either VMware VIO/Cloud DC or Openstack/edge stack). Figure 50 and Figure 51 show a high-level description for this prototype.

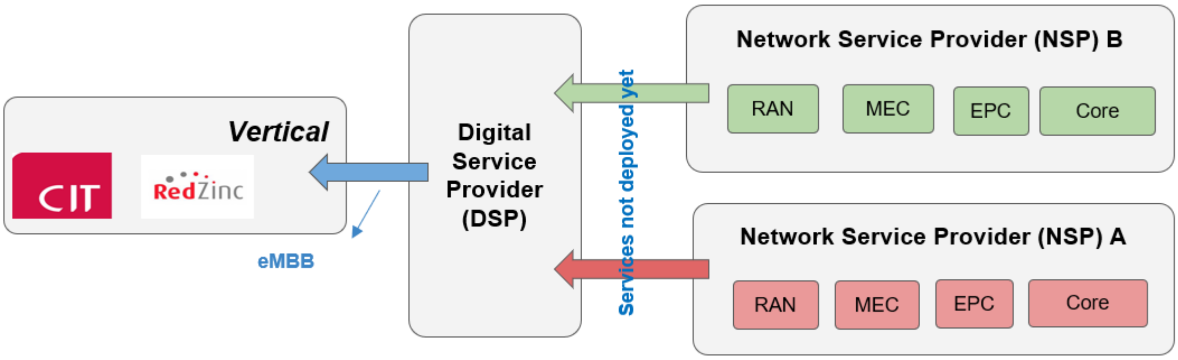


Figure 49: eHealth UC - Service Pre-subscription

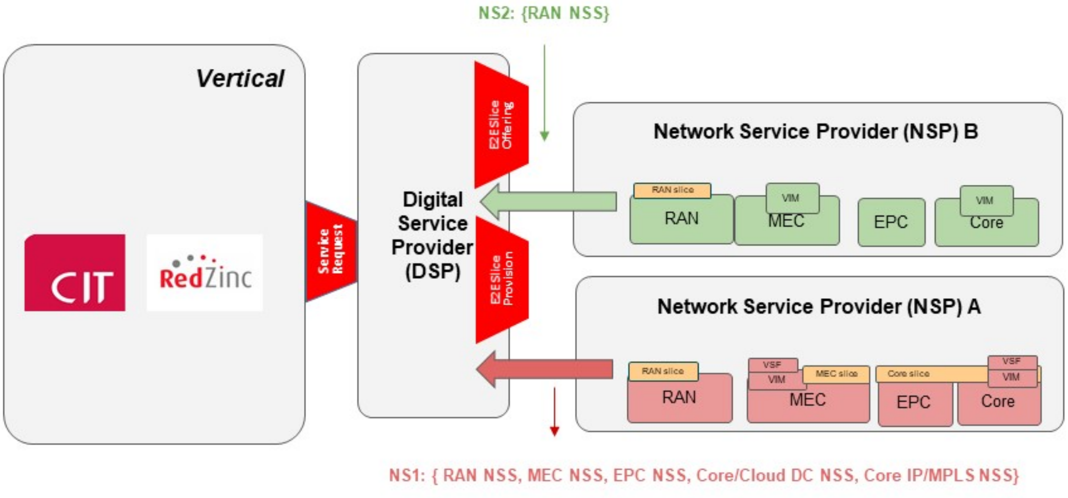


Figure 50: eHealth UC - Service Subscription

Mapping into this demo, Figure 52 and Figure 53 show a service orchestration with i) an eHealth slice is designed and onboarded onto the orchestrator and ii) the slice is instantiated, and resources are allocated into a specific VIM (VMware VIO or Openstack). After these steps, the eHealth service is up and running.

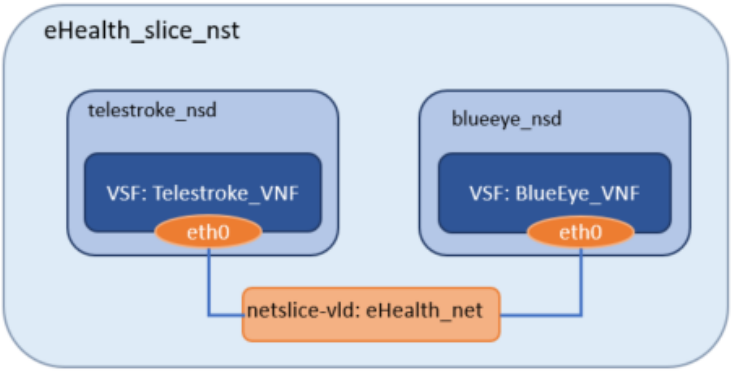


Figure 51: E2E eHealth slice template

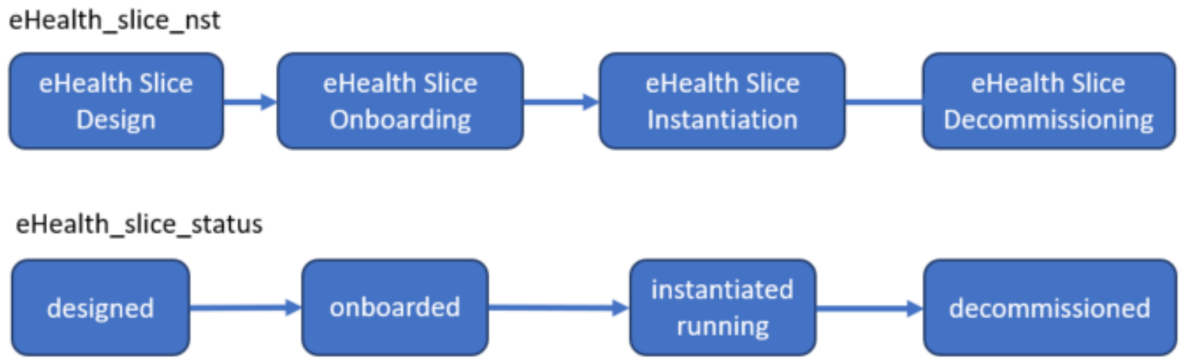


Figure 52: E2E eHealth slice design, onboarding and instantiation and its state transition

At this iteration of the system integration for eHealth UC, the starting point (one-stop API) will be the NMR-O, in which OpenSource MANO (OSM) is selected for service/resource orchestration. The automated process will be to create the eHealth slice with OSM, including the two services: Telestroke Assessment and BlueEye, packed in OSM in this eHealth slice as NSDs (telestroke_nsd, blueeye_nsd)) with corresponding VNFDs (telestroke_vnfd , blueeye_vnfd) with details of the deployment flavours (vCPU, vMemory, vDisk, networking, etc.). The instantiation of that eHealth slice will need to specify which VIMs (e.g., mec, cloud) will allocate the required resources and host the services.

The demo is to show a service orchestration with seamless composition and onboarding of the eHealth slice onto a VIM (either VMware VIO/Cloud DC or Openstack/edge stack). Figures 54 and 55 show the workflows for service subscription and, service instantiation consequently.

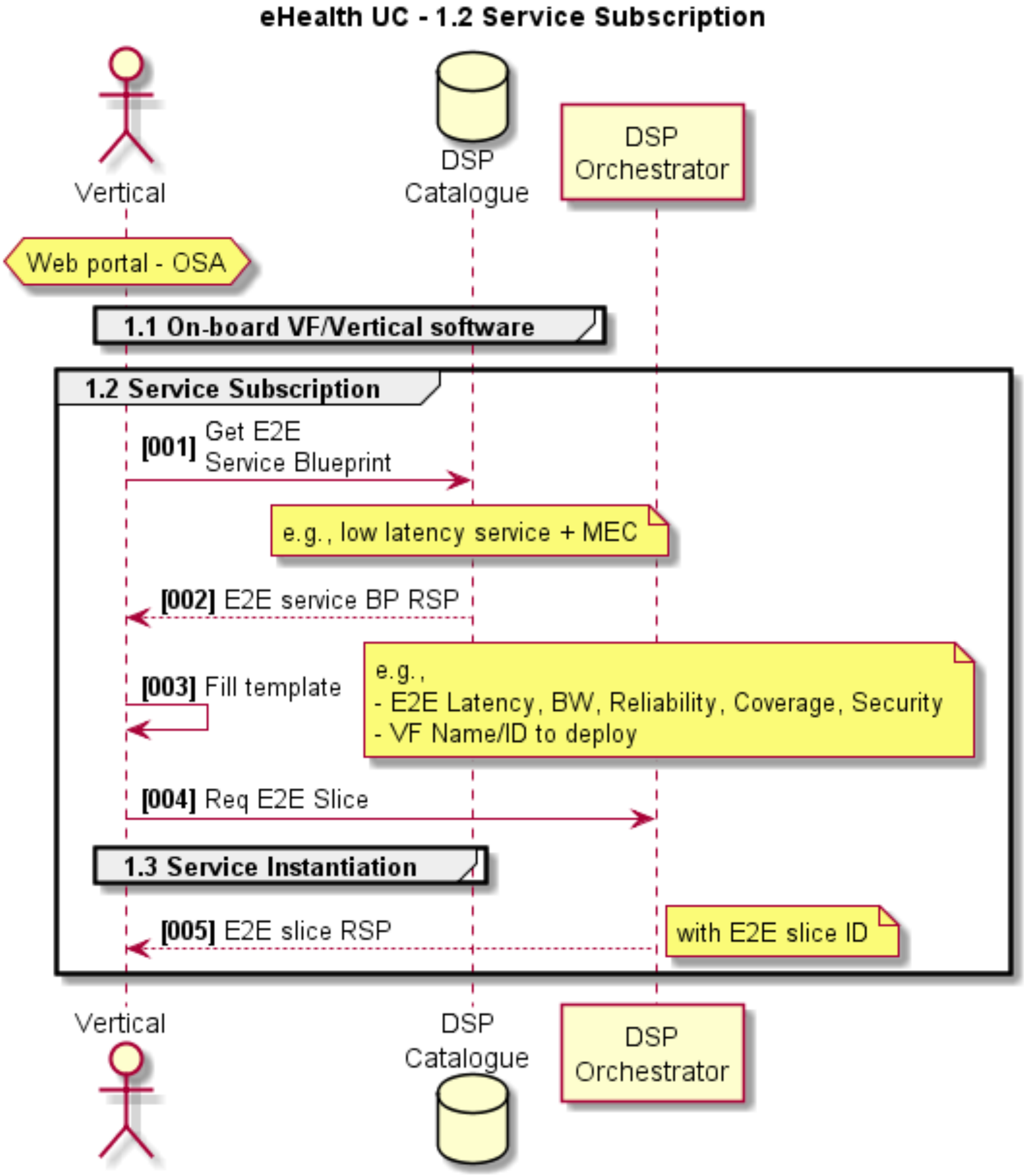


Figure 53: Service subscription

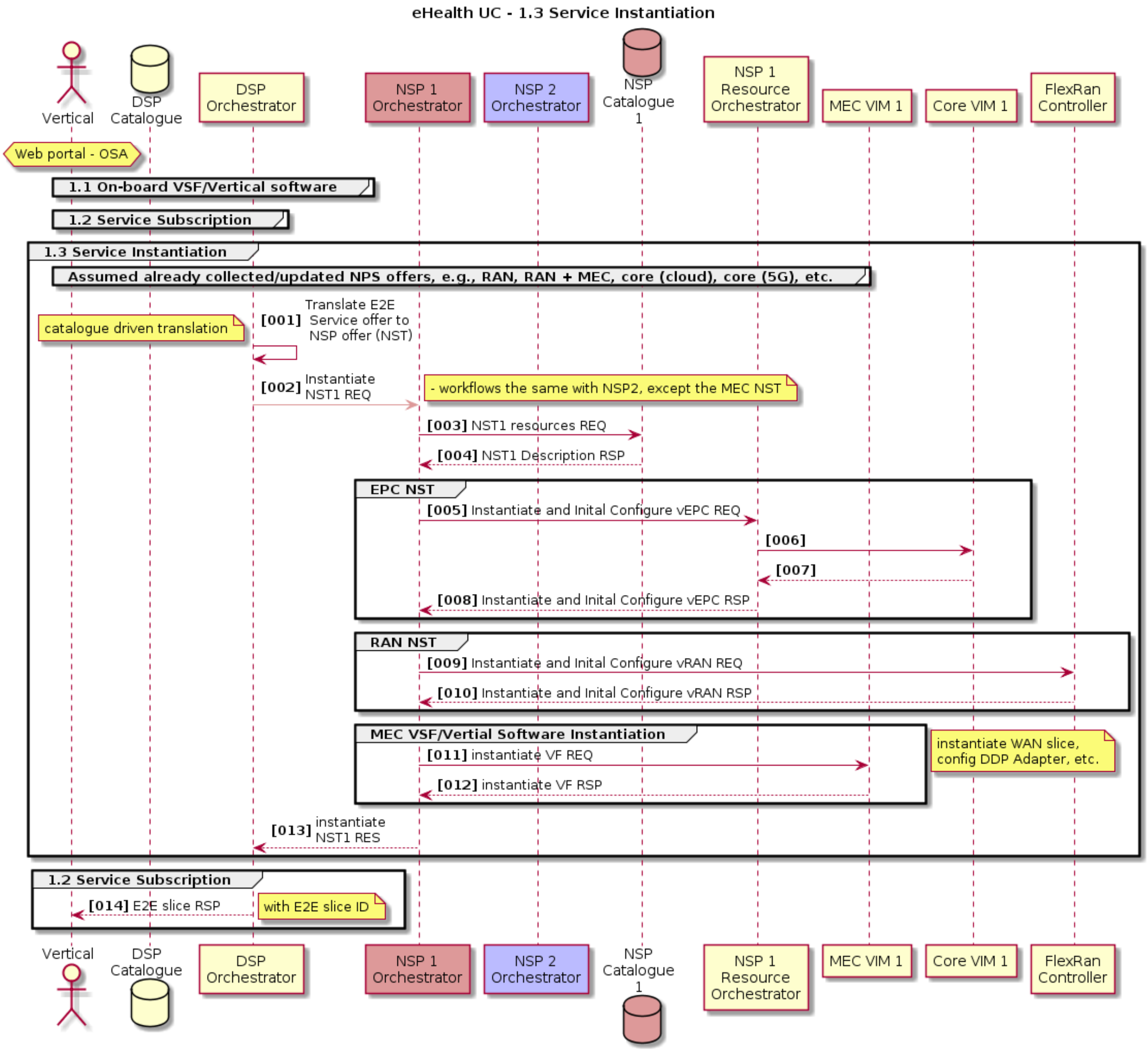


Figure 54: Service instantiation

3.4.2.2.2 Performance Monitoring

This demo shows how SliceNet can capture the performance of the eHealth slice during its runtime. The demo also shows how edge computing with hardware acceleration can assist with a continuous collection, processing and streaming of patient data that shortens the time to assess potential stroke patients. With the monitoring system, detail analysed results on the performance can also be performed and visualised.

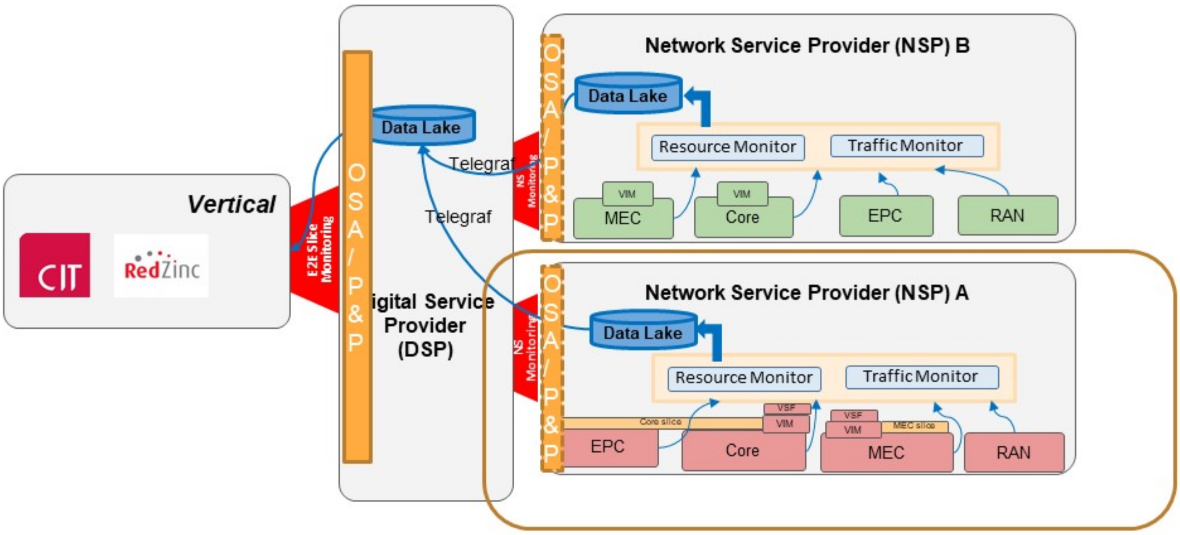


Figure 55: eHealth slice runtime monitoring

Figure 56 shows a high level depiction of the monitoring process and the interactions among the system components (i.e., Verticals, DSPS and NSPs) in SliceNet architecture. This monitoring information flow is the result of the runtime FCAPS configuration that is stemming from the resolution of the Vertical requirements as these are exposed as selectable offerings by the DSP through the capabilities of the related QoE, P&P and Congnitive modules. The high level options offered to the Vertical are related with the more fine grained NSP offerings supported by the NSP NF capabilities that are activated accordingly by the FCAPS subsystems following the Slice provisioning phase. Figure 57 depicts the workflow of the E2E monitoring services that initiated by the vertical.

The demo is integrated into SliceNet architecture with SliceNet sensors (E2E performance sensors with Skydive, VIM sensors with ANOVA, RAN sensors with FlexRAN, NAT and ll-mec sensors), FCAPS monitoring and database system as shown in the workflow in Figure 58, and the PnP control to visualise the application/network performance from the SliceNet One-stop API/web portal.

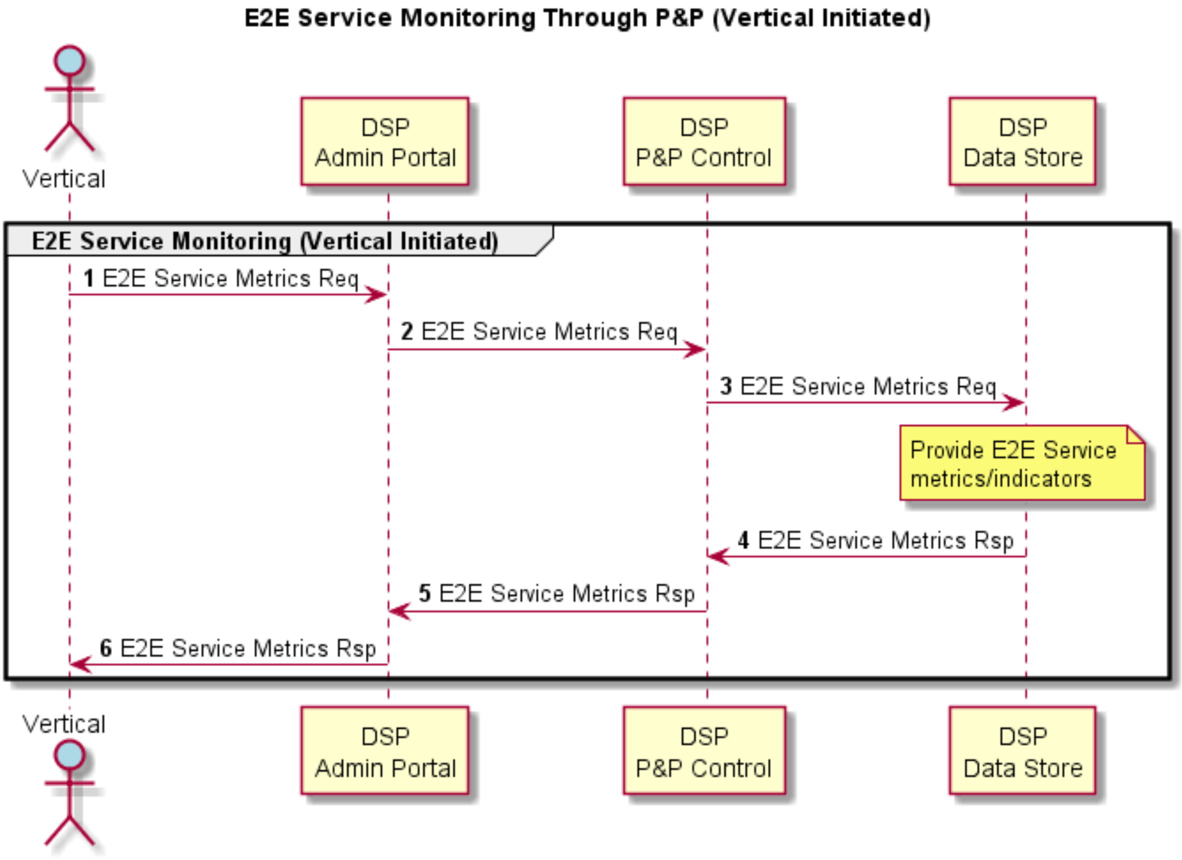


Figure 56: Vertical initiates E2E Monitoring through P&P

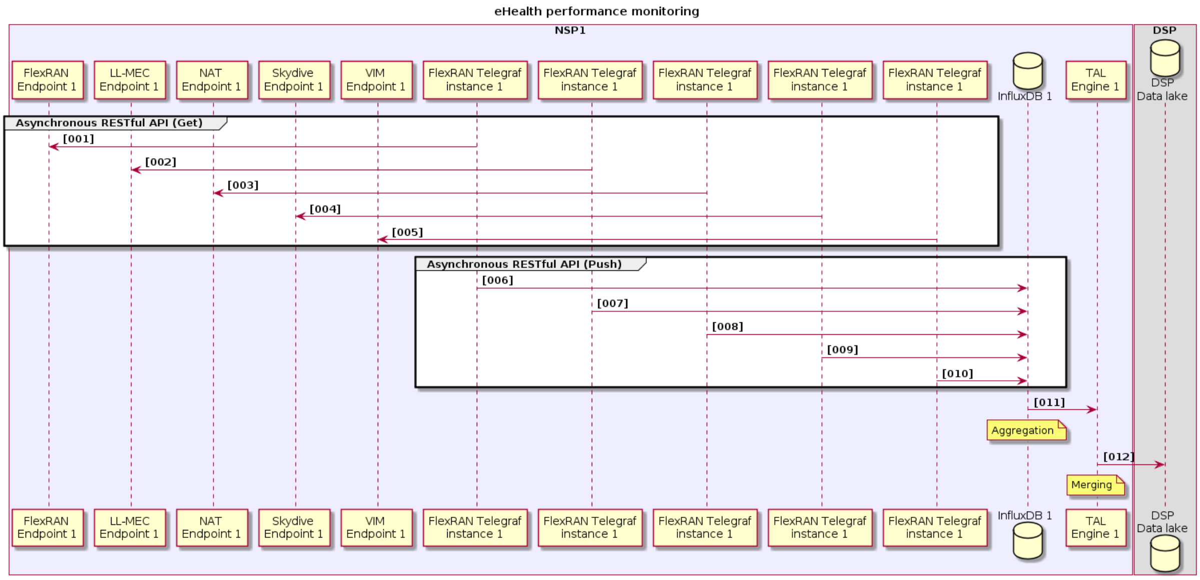


Figure 57: eHealth performance monitoring using five sensors

3.4.2.2.3 Optimisation

In the optimisation phase, eHealth UC will demonstrate two prototypes: i) Anomaly Prediction and Response in Quality of Communication; and ii) Fault prediction and Response.

3.4.2.2.3.1 Anomaly Prediction and Response in Quality of Communication

The demo is to show a PoC on how vertical feedback can be collected and SliceNet approach in exploiting the vertical feedback to improve network quality and to maintain QoS/QoE for the vertical. The scenario is setup where the ambulance with UE device captures patient’s images and transfers the images to a service running ML algorithms, image processing at the edge, for a preliminary stroke assessment. This UE device can measure a certain set of network parameters, e.g., SNR, RSRP, RSRQ, UL/DL throughputs, etc. that show a real-time network performance for the UE. With OAI software for RAN and Flexran controller, these parameters can also be measured at the eNB. The idea, however, is to demonstrate SliceNet vertical in the loop features via the P&P exposure for pushing the vertical generated QoE data to the data lake where SliceNet Analyzer has access to. Anomaly Detection model at the Analyzer component will be receiving the required data (thank to OSA and P&P control) and performs the prediction, estimating the Quality of Communication in advance (e.g., for simplicity, this demo focuses on predicting the Signal Attenuation in 5 minutes in advance). SliceNet DSP/NSP orchestrators will use this information to adjust the RAN resources (with QoS control process as in Control Plane Services section) for this UE accordingly, to maintain the QoS/QoE that the DSP/NSP promise to deliver. Figure 59 shows the workflow of enabling eHealth vertical feedback in SliceNet architecture. In the figure, the process staring with OSA Backend queries slice information from P&P Exposure. Then, OSA crates and endpoint to receive the feed from the vertical’s UE, which will be forwarded to P&P and finally to the Analyzer (Anomaly Prediction Module APM). APM triggers an even in the QoE optimizer if the model foresees the anomaly. The QoE optimizer applies the configuration policy and request an action from the DSP orchestrator.

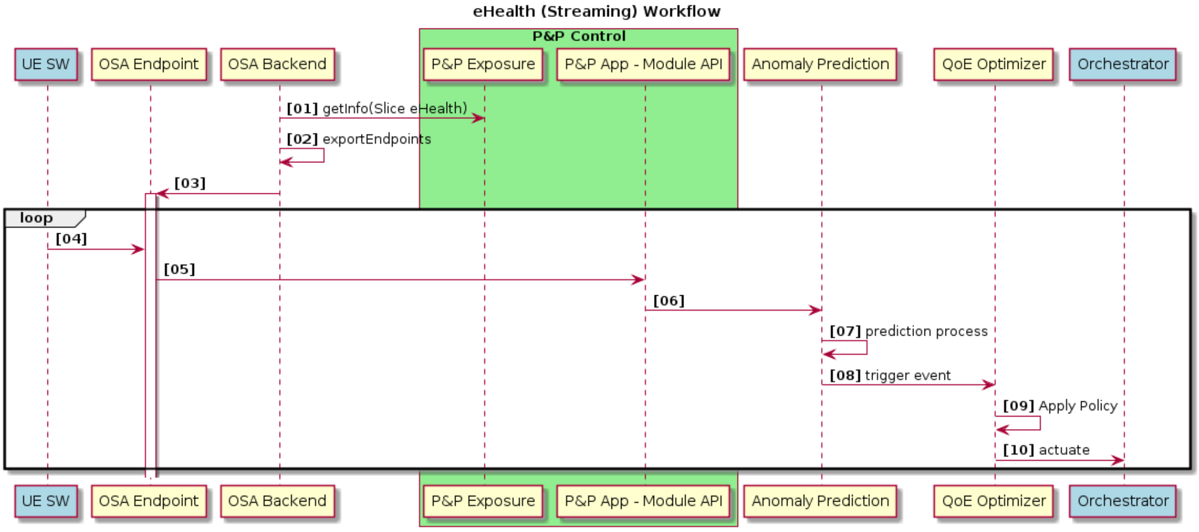


Figure 58: Vertical feedback workflow in DSP

The demo is standalone in eHealth testbed, data is pre-collected with an Android mobile app, collecting the network parameters on ambulance routes. There are 8 sets of data, 7 sets are used to train the prediction model and one set is used for demo purposes. The data is replayed, reporting in every second. The replayed data is fed to the model for signal attenuation prediction, to see if there will be an anomaly in the signal attenuation in 5 minutes ahead. The standalone demo shows red alert messages to notify the system/admin the anomalies if detected. Moreover, the demo shows the vertical feedback integration into DSP FCAPS system, P&P and Analyser components. Figure 60 shows the workflow of the actuation based on the cognition decision in APM and QoE optimizer. The actuation in this demo creates RAN and core slices in another NSP. Then, X2 handover is performed from the current RAN to the recommended one.

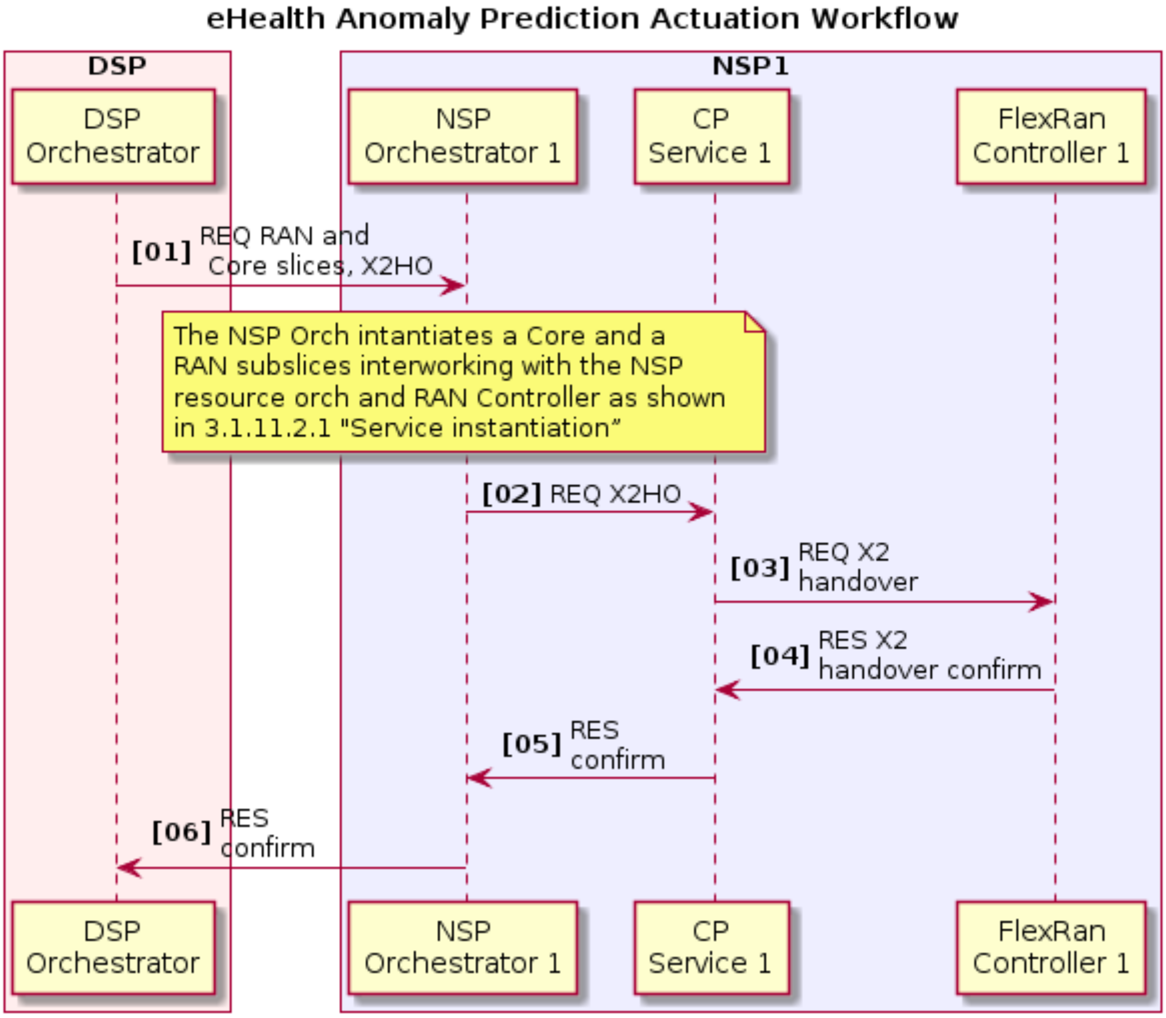


Figure 59: The Actuation workflow in Anomaly Prediction Demo

3.4.2.2.3.2 Fault Detection and Response

Figure 61 and Figure 62 show the sequence of events. Assuming the service is orchestrated to run at the core, at run-time, the service is failing, e.g., machine down/link disconnected, with sensors and monitors deployed at the resource/service level, SliceNet system is able to detect the failure and migrate the service to different VIM (e.g., Edge). This demo is to show the sustainability of the system.

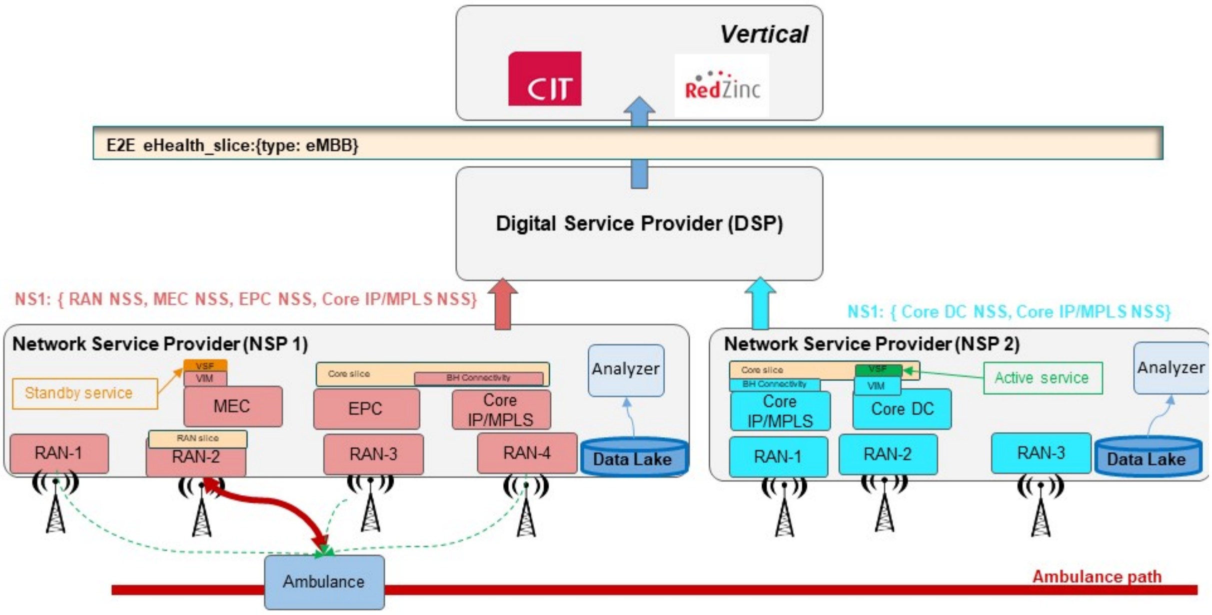


Figure 60: Active service is running at the core (green text/box)

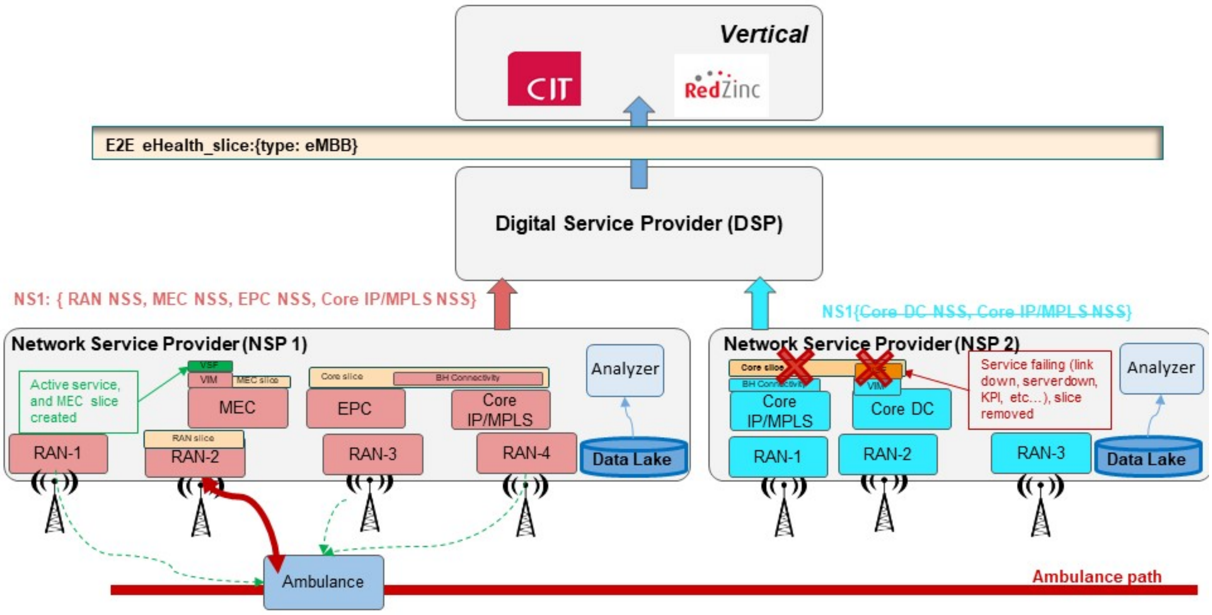


Figure 61: Active service is migrated to the edge (green text/box).

The demo is standalone in eHealth testbed and Telestroke Assessment service is applied for the demo. After the demo 3.1 for eHealth slice instantiation, the service is up and running at the core. By monitoring the VSF by FCAPS, SliceNet is able to view the status of the VSF during its runtime. With LL_MEC (MEC Controller) and OVS-GTP deployed in the testbed, when the system reports the failure of the VSF, SliceNet can divert the traffic to a standby VSF (for simplicity, this standby VSF is assumed to be already configured and only requires to be turn on at the edge). This traffic diversion should be transparent to the UE device and the application level. The demo is integrated into SliceNet architecture with MEC sensors, FCAPS monitoring system and Rule Engine, and the NSP orchestrator for CP services, e.g., reconfiguring the subslice to have new service function running in different VIM or NF_config with MEC_Adapter/Controller to divert current traffic to a standby/backup machine running the same service in different VIM. Figure 63 shows the workflow of detecting and responding to the VSF fault in the eHealth use-case (RTT or CPU/GPU utilization).

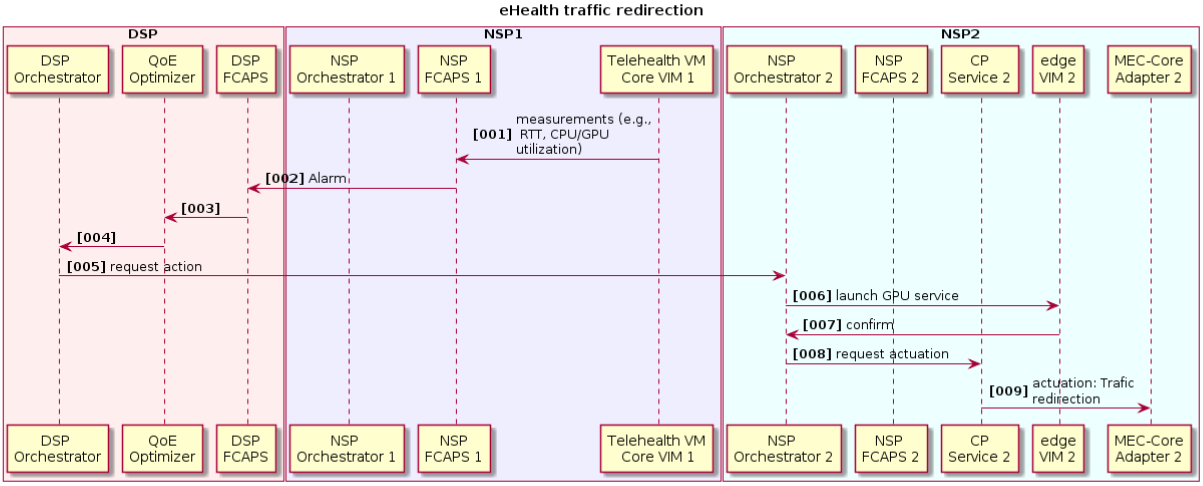


Figure 62: Fault detection and Response Workflow

3.4.3 Smart City

3.4.3.1 Detailed Workflow Descriptions

The Smart City Use case has several technical requirements, as described in the next table:

No.	Technical requirements	Description
1.	E2E Network Cognition	Normal System functioning and optimization through cognition
2. 2.	Network optimization One-Stop-API	service and slice optimization Smart lighting request for one-stop-shop solution
3.	Network Slicing	Network slice mMTC, dedicated NFV/VNFs for Specific Core elements
4.	RAN & Core	vRAN, vEPC VNFs, vHSS deployment, network connectivity
5.	Network KPIs	bandwidth, delay, automated system deployment, QoE sensing and actuation,
6. 7.	Network Monitoring E2E Monitoring	Network Slice monitoring Service monitoring

Table 11: Smart City technical requirements

The workflows are described in Section 2 and the storyline are mapped as in the next table:

Scene #	Scene title	Scene description
1.	Service preparation an subscription	The DSP E2E NS and the NSP1 NS preparation involves the design, onboard and offer workflows, DSP service offer and DSP subscribtion to the NSP
2.	service runtime monitoring	collecting monitoring information from the network
4.	optimization phase 1	anomaly detection in E2E Quality of service communication
5.	optimization phase 2	RAN resources adaptation optimization for the Smart City

Table 12: Mapped Workflows

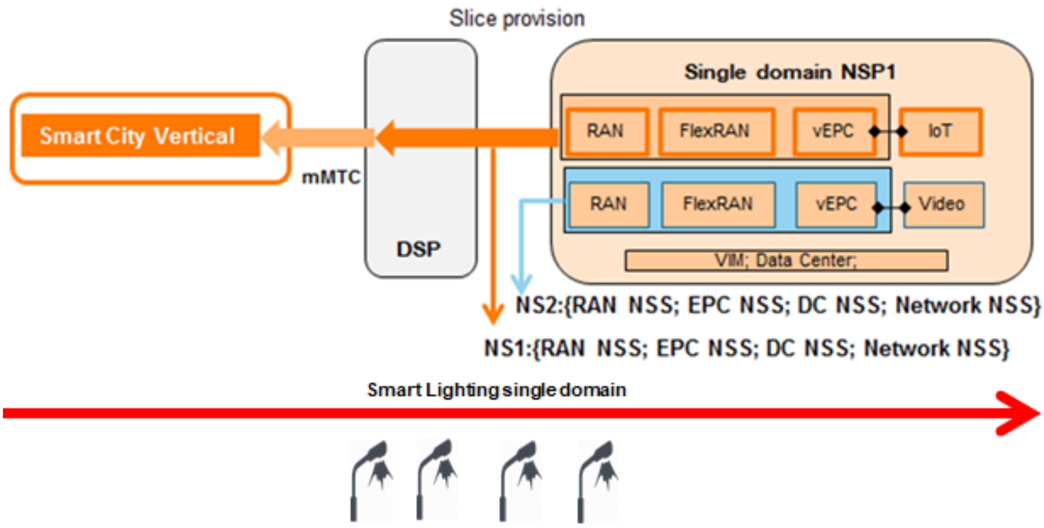


Figure 63: Smart City Smart Lighting provisioning

The lighting poles are installed in the field and the scenario is single network domain. The E2E slice is composed by the RAN, Core EPC and IoT platform. There is only one service provider, that connects the lighting poles to the control platform of the light.

There are described three main key points of the use case:

1. service design and subscription: network service slice is deployed using the NSP resources based on a process of service slice request, offer and provision

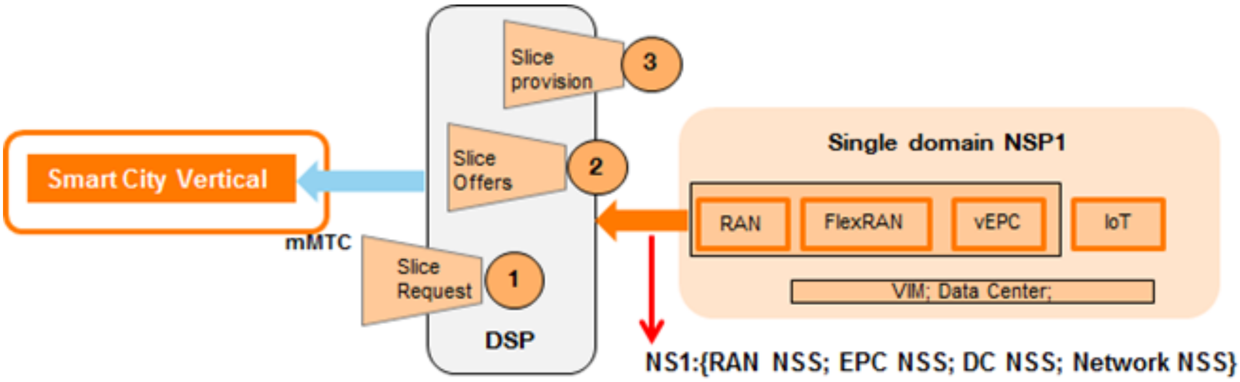


Figure 64: Smart City service design

2. performance monitoring - runtime monitoring - an IoT simulator is deployed and instantiated, to consume Smart City IoT slice resources (simulating as 10.000 proper traffic) and a QoE service tool monitors the set of basic KPIs (latency, packet loss, jitter).

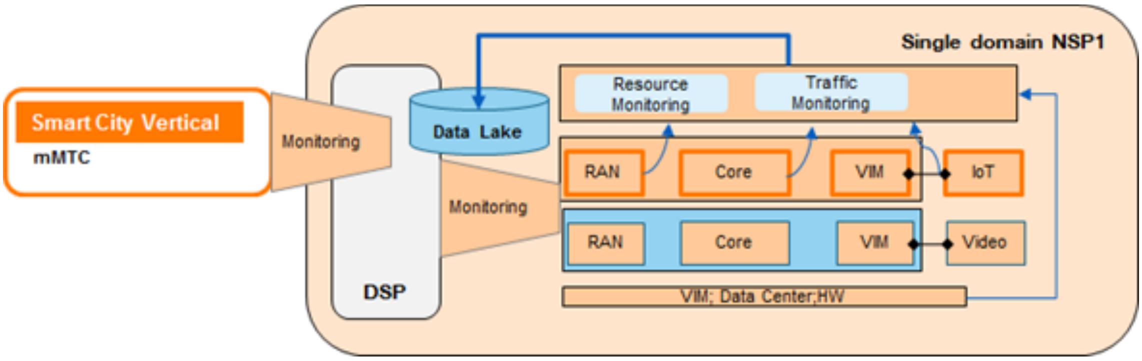


Figure 65: Smart City performance monitoring

3. optimization phase 1 - anomaly detection in E2E Quality of service communication, due to service VM overload or noised:

- event type due to overload, that triggers resize the VM
- event type due to noise, that triggers migration

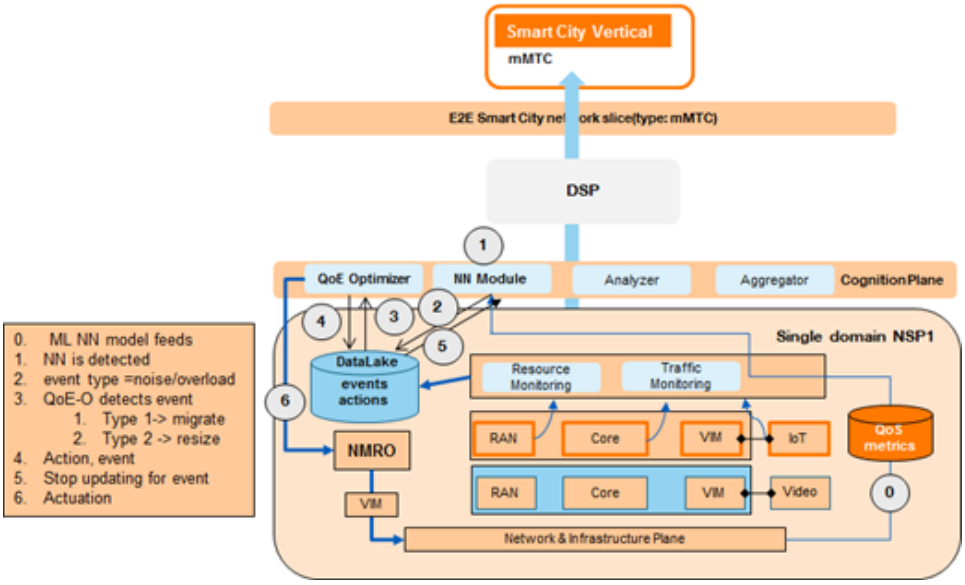
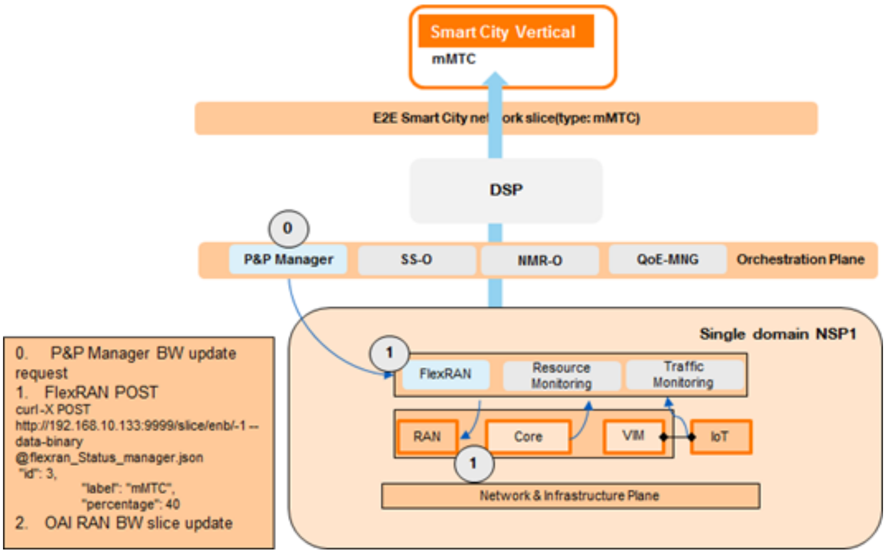


Figure 66: Smart City optimization phase 1

4. optimization phase 2 - RAN resources adaptation optimization for the Smart City use case slice. Increase slice bandwidth - through dynamically resource allocation , based on P&P and FlexRAN capabilities:



```
curl -X POST
http://192.168.10.133:9999/slice/enb/-1 --
data-binary
@flexran_Status_manager.json
 "id": 3,
            "label": "mMTC",
            "percentage": 40
```

Figure 67: Smart City optimization phase 2

For the demo, the flow from the P&P to FlexRAN to change the Bandwidth will go through the SSO-QoS-RAN Adaper-FlexRAN.

4 Preparation of Prototype for Evaluation

The main goal of T7.2 is to create prototypes for the three vertical use cases with the right characteristics for the test and validation activities that will take place in the scope of T8.3 (Integration, Validation and Demonstration of Use Cases in Integrated Framework). The vertical use case prototypes will be subsequently fed as inputs to T8.3, ready to be integrated in the SliceNet framework.

4.1 Smart Grid

The Smart Grid use case prototype testbed consists of the infrastructure described in section 3.3.1, with four Efacec PAC IEDs and an engineering station and Supervisory Control and Data Acquisition (SCADA) server. The devices have been installed in the testbed and they communicate with each other using Long Term Evolution (LTE) gateways connected to the SliceNet system. All the devices are also connected to a management network, allowing remote management and easy deployment of configuration and firmware.

The testbed is also prepared for integrating additional subsidiary equipment for the power grid simulation and an accurate time server. This additional equipment is not permanently installed in the use case testbed – it will be installed periodically during application tests.

Nevertheless, these devices are not necessary for continuity validation and integration tests focused on use case-specific communications. It will be possible, therefore, to stimulate the IEDs and maintain continuous and realistic communication flows regardless of the availability of the power grid simulation devices.

Although not permanently installed in the testbed, the power grid simulation device integration has been validated during T7.2. With these devices, the testbed is prepared for simulating the smart grid self-healing scenarios defined in D2.1, which will allow the validation of the adequacy of the SliceNet framework and services for the proposed Smart Grid applications. The IEDs keep timetagged logs with GOOSE statistics that provide useful metrics from the vertical applications that will be used for validating the smart grid applications and may be visualized during the final demonstration.

The smart grid use case prototype is assembled, installed and ready for the final integration tests and upcoming validation and demonstration phases, that are to be carried on throughout T8.3.

4.2 eHealth

The eHealth use case prototyping consists as showed in Figure 69 on the examination of the scenario of possible stroke patients at a remote location.

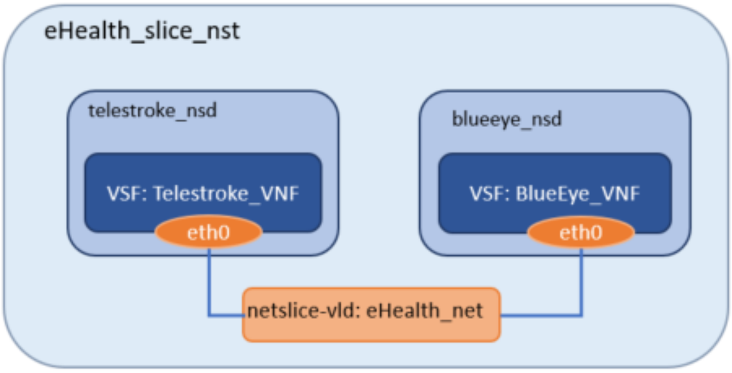


Figure 68: eHealth Slice template

With OpenMANO OSM, current experiment shows the seamless composition and onboarding of the eHealth slice onto Openstack VIM. More importantly, it shows how edge computing with hardware acceleration can assist with a continuous collection, processing and streaming of patient data that shortens the time to assess potential stroke patients. Experimental results will be detailed in 8.3 to show the deffirence between the performance of traditional Telestroke Assessment service running at the cloud and the performance of the service running at the edge with accelerated hardware.

4.3 Smart City

The Smart City use case prototyping consist in deploying the Orange testbed infrastructure, as described in Chapter 3.3, with described network elements, providing communication between the IoT Lighting poles, already installed in the Campus, and the IoT Platform, through LTE/LTE-M technologies.

The testbed is adapted to cope also simulated IoT traffic, for IoT network load, to simulate a real Smart City Smart Lighting use case scenario.

The use prototyping, as described in the next figure, consists of 56 Smart Lighting Poles, deployed in the live campus and connected to Slicenet RAN through LTE-M technology. The Slicenet eNB is connected through a secured link to Orange testbed Infratsructure, where the core network components, IoT platform and Slicenet developed component are installed.

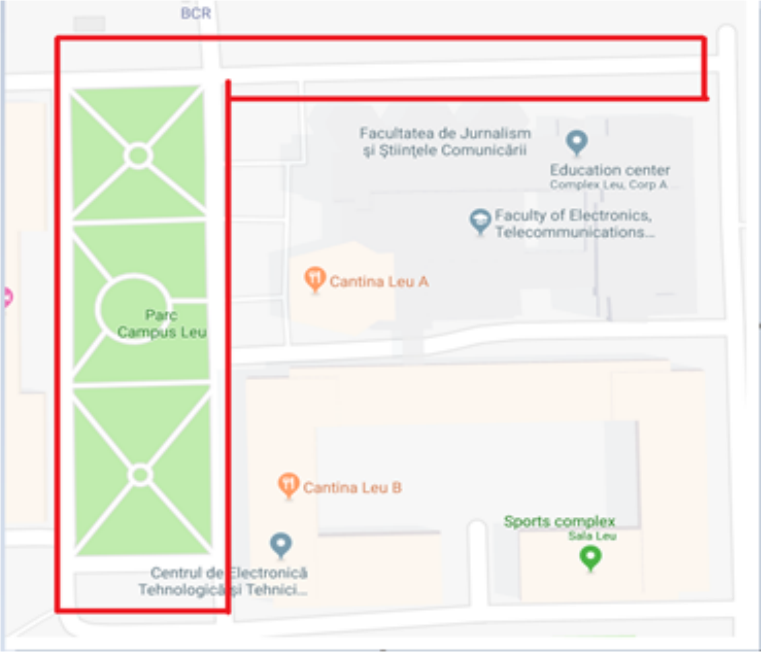


Figure 69: The Smart City scenario

The Smart City scenario, as described in D2.1 is prepared for live lighting services, instantiated over Slicenet testbed and ready for real demonstration and lighting capabilities used by the campus.

As all use case component are assembled and integrated, the next validation and demonstration phases will be carried during 8.3 effort work.

5 Conclusions

Global 5G R&D initiatives have been launched in major economic areas worldwide. Evidence of this are actions in Europe undertaken by the 5G Infrastructure Association (5G-IA) in a contractual Public-Private Partnership (5G PPP) with the European Commission, as well as several actions globally.

This document describes part of the research from the H2020 5G PPP SliceNet project [21], where three key use cases act as showcase test-bed demonstrators: the Smart Grid Use Case; the eHealth Use Case; and the Smart City Use Case. In this task, all the activities related to the prototypically implementation of the 3 use cases are enclosed. The use cases' requirements determined in T2.1 are driving the development of the prototypes. The document is detailing all these requirements for each use case in addition to the legal and regulatory environment surrounding likely deployments.

Following the requirements, the document is describing the adaptation of the existing vertical business applications/services (application level) to run in the SliceNet infrastructure, operation of the applications over the Integrated infrastructure prototyped in WP3, utilisation of key enablers for slicing control (including verticals' P&P control) prototyped in WP4, early utilisation of key enablers for slice management (QoE & FCAPS) prototyped in WP5 & WP6, and early adoption of the orchestrator being prototyped in WP7.

SliceNet will reach a maximum Technology Readiness Level 4/5 but full validation will require further field trial and real user evaluation.

The document finishes with a set of considerations in section 4 related with evaluation prototypes of the SliceNet three use cases.

References

[1] https://slicenet.eu/ © SLICENET consortium 2017

[2] IEC, “IEC 61850-8-1 Ed.2: Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3”, 2011.

[3] IEC, “IEC TR 61850-90-5 Ed.1: Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118”, 2012.

[4] A. Apostolov, “R-GOOSE: what it is and its application in distribution automation”, CIRED 2017, Glasgow, UK.

[5] A. Aleixo et. al., “Smart Grid Protection and Automation Enabled by IEC 61850 Communications over 5G Networks”, CIRED 2019, Madrid, Spain.

[6] IEC, “IEC TS 62351-6:2007: Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850”, 2007.

[7] IEC, “IEC 62351-9:2017: Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment”, 2017.

[8] S. R. Firouzi et. al., “Interpreting and implementing IEC 61850-90-5 Routed-Sampled Value and Routed-GOOSE protocols for IEEE C37.118.2 compliant wide-area synchrophasor data transfer”, Electric Power System Research, volume 144, pp. 255-267, March 2017.

[9] IEEE, “IEEE C37.118.1: IEEE Standard for Synchrophasor Measurements for Power Systems”, 2011.

[10] IEEE, , “IEEE C37.118.2: IEEE Standard for Synchrophasor Data Transfer for Power Systems”, 2011.

[11] IEC, “IEC TR 61850-90-2 Ed.1: Communication networks and systems for power utility automation – Part 90-2: Using IEC 61850 for communication between substations and control centres”, 2016.

[12] European Comission, European SmartGrids Technology Platform, Brussels: European Communities, 2006.

[13] Council of European Energy Regulators, "6th CEER Benchmarking Report On The Quality Of Electricity And Gas Supply," Brussels, 2016.

[14] CENELEC, "Voltage characteristics of electricity supplied by public distribution systems," CENELEC, Brussels, 2005.

[15] European Comission, "Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection," European Commission, Brussels, 2011.

[16] D. E. Bakken et. al., "Smart Generation and Transmission With Coherent, Real-Time Data," *Proceedings of the IEEE,* vol. 99, no. 6, pp. 928-951, 2011.

[17] USA Department of Energy, "Communication Requirements of Smart Grid Technologies," 2010.

[18] Gemalto, "Introducing 5G networks – Characteristics and usages," Gemalto, 2019.

[19] H. Gharavi and B. Hu, "Synchrophasor Sensor Networks for Grid Communication and Protection," *Proceedings of the IEEE,* vol. 105, no. 7, pp. 1408-1428, 2017.

[20] Valenzuela Espinoza, A. et al. (2016) “Development and Pilot Testing of 24/7 In-Ambulance Telemedicine for Acute Stroke: Prehospital Stroke Study at the Universitair Ziekenhuis Brussel-Project,” Cerebrovascular Diseases, 42(1–2), pp. 15–22. doi: 10.1159/000444175.

[21] SliceNet Consortium “End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks”, H2020 5G PPP https://slicenet.eu/ [Accessed 29 May 2019].

[22] Kafka Cluster: https://kafka.apache.org/

[23] WebRTC: https://webrtc.org/

[24] Janus Video Server: https://janus.conf.meetecho.com/

[25] STUN: https://tools.ietf.org/html/rfc5389

[26] Deliverable D5.7, Framework for Cognitive SLA and QoE Slice Management, November 2019.