Selfnet

Deliverable 2.1

Use Cases Definition and Requirements of the System and its Components

Editors:	Luis Javier García Villalba, Ángel Leonardo Valdivieso Caraguay, Lorena Isabel Barona López Universidad Complutense de Madrid
Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	31 October 2015
Actual delivery date:	31 October 2015
Suggested readers:	Telecommunication Operators, Service Providers
Version:	1.0
Total number of pages:	166
Keywords:	5G Architecture, Network Management, Self-Organized Network, System Requirements, Use Cases.

Abstract

This Deliverable presents the initial design of the overall SELFNET framework. SELFNET creates an autonomic network management framework to meet the requirements of advanced self-organizing network (SON) capabilities for the 5G network infrastructure providing insights into the key technologies involved. In particular, a seamless integration of Software-Defined Networking (SDN), Network Function Virtualization (NFV) and network intelligence is proposed. The deliverable specifies three use cases that are used to derive the system requirements, and to validate and demonstrate the capabilities of the SELFNET framework. The use cases propose innovative proactive/reactive actions in self-healing, self-protection and self-optimization of software-defined and virtualized 5G networks. Furthermore, it presents a detailed list of requirements for realizing each system component as well as the use cases.

Disclaimer

The research leading to these results has received funding from the European Union Horizon 2020 Programme under grant agreement number H2020-ICT-2014-2/671672.

Impressum

Full Project Tittle: Framework for Self-Organized Network Management in Virtualized and Software Defined Networks

Short Project Tittle: SELFNET

Work Package 2: SELFNET Network Management Framework

Task 2.1: System Requirements and Use Case Definition

Document title: “Use Cases Definition and Requirements of the System and its Components”

Editors: Luis Javier García Villalba, Ángel Leonardo Valdivieso Caraguay, Lorena Isabel Barona López; Universidad Complutense de Madrid.

Work-package leader: Pedro Neves, Portugal Telecom Inovação.

Copyright notice

Partner Organization Name	Partner Short Name	Country
Eurescom GmbH	EURES	Germany
Universidad de Murcia	UMU	Spain
Portugal Telecom Inovacao	PTIN	Portugal
Deutsches Forschungszentrum für Künstliche Intelligenz GmbH	DFKI	Germany
University of the West of Scotland	UWS	United Kingdom
Universidad Complutense de Madrid	UCM	Spain
Nextworks	NXW	Italy
InnoRoute GmbH	INR	Germany
Alvarion Technologies Ltd.	ALV	Israel
Ubiwhere Lda	UBI	Portugal
Proef	PRO	Portugal
Creative Systems Engineering	CSE	Greece

Executive Summary

SELFNET proposes an autonomic management framework based mainly on the combination of Software-Defined Networking (SDN), Network Function Virtualization (NFV) and network intelligence to provide self-organizing enhanced capacities to 5G networks. This deliverable is the first public deliverable of the project presenting the up-to-date proposal of the SELFNET architecture, use cases definitions and system requirements. Following a use case driven design approach, this deliverable describes in detail three use cases aligned with the 5G requirements and Key Performance Indicator (KPI) targets of the 5G-PPP initiative and recognised globally. The presented architecture constitutes the foundation for a coherent and successful development of components in each phase of the project.

The main goals of this deliverable are:

- To position SELFNET within the main challenges and needs of 5G network infrastructures.
- To define the use cases to be used to derive system requirements for SELFNET and to validate the proposed framework. Concretely, uses cases addressing the problem areas of self-optimization, self-healing and self-protection of 5G network infrastructures.
- To identify the system requirements for the overall framework and the system requirements associated with each defined use case.
- To refine the initial architecture of the SELFNET framework revisiting all the layers involved in the software providing a more detailed vision of the framework including the key technologies involved.
- To define the preliminary structure and requirements of the system components (modules of the SELFNET architecture).

The Deliverable starts with the requirements and challenges of 5G systems and describing the relationship between the SELFNET framework and the the fields in which SELFNET will have a relevant impact.

The SELFNET reference architecture is then described. Based on a layered approach, it is composed by the following layers: Infrastructure Layer, Virtualized Network Layer, SON Control Layer and SON Autonomic Layer.

The three proposed use cases are presented: self-healing, self-protection, and self-optimization, and how they can demonstrate the capabilities of the SELFNET framework to address 5G requirements and challenges.

The system requirements are aligned with two main domains: the corresponding use case and the relationship with each layer of SELFNET referential architecture.

The deliverable concludes presenting how the information delivered in this report will be used in the next stage of SELFNET activities.

It is acknowledged and agreed within the consortium that this deliverable will be considered as a working document evolving along the execution of the SELFNET project.

List of Authors

Organization	Author
Universidad Complutense de Madrid	Luis Javier García Villalba
Universidad Complutense de Madrid	Lorena Isabel Barona López
Universidad Complutense de Madrid	Ángel Leonardo Valdivieso Caraguay
Universidad Complutense de Madrid	Marco Antonio Sotelo Monge
Universidad Complutense de Madrid	Jorge Maestre Vidal
Universidad Complutense de Madrid	Ana Lucila Sandoval Orozco
Portugal Telecom Inovação	Pedro Neves
Portugal Telecom Inovação	Rui Calé
Portugal Telecom Inovação	Bruno Parreira
Portugal Telecom Inovação	Gonçalo Gaspar
Portugal Telecom Inovação	Carlos Parada
University of the West of Scotland	Jose M. Alcaraz-Calero
University of the West of Scotland	Qi Wang
University of the West of Scotland	James Nightingale
University of the West of Scotland	Enrique A. Chirivella Pérez
Alvarion Technologies Ltd.	Jesus Alonso
Alvarion Technologies Ltd.	Udi Segev
Creative Systems Engineering	Konstantinos Koutsopoulos
Deutsches Forschungszentrum für Künstliche Intelligenz GmbH	Hans Dieter Schotten
Deutsches Forschungszentrum für Künstliche Intelligenz GmbH	Wei Jiang
InnoRoute GmbH	Andreas Foglar
InnoRoute GmbH	Marian Ulbricht
Nextworks	Gino Carrozzo

Nextworks	Giacomo Bernini
PROEF	Nuno Esteves
PROEF	Maria Sousa
PROEF	José Pedro Santos
Ubiwhere Lda	Rui A. Costa
Ubiwhere Lda	Ricardo Preto
Ubiwhere Lda	Tiago Batista
Ubiwhere Lda	Tiago Teixeira
Universidad de Murcia	Gregorio Martinez Perez
Universidad de Murcia	Manuel Gil Pérez
Universidad de Murcia	Félix J. García Clemente
Eurescom GmbH	Maria Joao Barros
Eurescom GmbH	Anastasius Gavras

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Explanation
5G	Fifth Generation (mobile/cellular networks)
5G PPP	5G Infrastructure Public Private Partnership
API	Application Programming Interface
BGP	Border Gateway Protocol
BSS	Business Support System
CAPEX	Capital Expenditure
CIDS	Collaborative Intrusion Detection System
CLI	Command Line Interface
COTS	Common Off-The-Shelf
DPI	Deep Packet Inspection
DDoS	Distributed Denial of Service
DMS	Data Management System
EL	Enhancement Layer
eTOM	Enhanced Telecom Operations Map
ETSI	European Telecommunications Standards Institute
FG	Forwarding Graph
FW	Firewall
GI	Graphical Interface
HoN	Health of Network (metrics)

HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
IPS	Intrusion Protection System
KPI	Key Performance Indicator
LTE	Long Term Evolution
M2M	Machine to Machine
MANE	Media-Aware Network Element
MANO	Management and Orchestration
MPD	Music Player Daemon
MOVNO	Mobile Virtual Network Operator
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NE	Network Elements
NF	Network Function
NFV	Network Function Virtualization
NFVI	NFV Infrastructure
NFVO	NFV Orchestrator
NS	Network Services
ONF	Open Networking Foundation
OPEX	Operational Expenditure
OR	Orchestrator
OSPF	Open Shortest Path First

OSS	Operation Support System
PAYG	pay-as-you-go
PC	Parental Control
PDP	Policy Decision Point
PNF	Physical Network Function
PNE	Physical Network Element
PoP	Point of Presence
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
REST	Representational State Transfer
RM	Resource Manager
SDO	Standard Developing Organization
SDN	Software Defined Networking
SELFNET	Self-organized Network Management in Virtualized and Software Defined Networks
SH	Self-Healing
SLA	Service Level Agreement
SME	Small Medium Enterprise
SO	Self-Optimization
SON	Self-Organizing Network
SP	Self-Protection

TAL	Tactical Autonomic Language
TAM	Telecommunications Applications Map
TS	Traffic Shaping
TMForum	TeleManagement Forum
TOC	Total Cost of Ownership
U-HD	Ultra High Definition
vHGM	virtualized Home Gateway
VIM	Virtualized Infrastructure Management
VLAN	Virtual Local Area Network
VNF	Virtualized Network Function
VNE	Virtual Network Element
VNFM	VNF Manager
WAN	Wide Area Network
WIM	WAN Infrastructure Manager
ZOOM	Zero-touch Orchestration, Operations and Management

1 Introduction

Advances in mobile technologies and the user-driven growth of an increasingly diverse range of services has triggered the requirements to create a new generation of efficient network management mechanisms and architectures able to support these new mobile technologies, services and applications. Currently, in financial terms, the cost to mobile operators of operational expenditure (OPEX) is three times that of capital expenditure (CAPEX) [1]. Primarily this disparity is a direct result of the complexity of the systems used to launch new, faster portfolios of voice and data products and to roll out technology upgrades or new customer service functions.

In this context, the SELFNET H2020 project will design and implement an autonomic network management framework to provide self-organizing network (SON) capabilities in new 5G mobile network infrastructures. By automatically detecting and mitigating a range of common network problems, currently manually addressed by network administrators, SELFNET will provide a framework that can significantly reduce operational costs, at the same time improving the user experience.

By exploring the integration of novel technologies (Software-Defined Networks (SDN), Network Function Virtualization (NFV), SON, Cloud computing, Artificial Intelligence, Quality of Experience (QoE)) and next generation networking. SELFNET will provide a scalable, extensible and smart network management system. The framework will assist network operators to perform key management tasks such as automatic deployment of SDN/NFV applications that provide automated network monitoring and autonomic network maintenance delivered by defining high-level tactical measures and enabling autonomic corrective and preventive actions to mitigate existing or potential network problems. SELFNET will address three major network management concerns by providing self-protection capabilities against distributed network attacks, self-healing capabilities against network failures, and self-optimization features to dynamically improve the performance of the network and the QoE of the users. The facilities provided by SELFNET will provide the foundations for delivering some of the 5G requirements defined by the 5G-PPP initiative.

This document is the first public deliverable of the SELFNET project and presents the system requirements and use case specifications that will guide the technical development work of the project. The ideas presented in this document provide the starting point for the subsequent phases and deliverables of this project. It is important to note that this version will require to be revisited to clarify or expand some specific aspects at a later stage of the project. These changes will occur as a result of the feedback on the project and any potential new needs that may be identified within the modules or activities of the SELFNET reference architecture.

1.1 Objectives

The main objective of the project is to design and implement an autonomic network management framework. This framework will deliver self-organizing capabilities to manage network infrastructures by automatically detecting and mitigating a range of common (mobile) network problems that are, for the moment, manually addressed by network operators. This approach will significantly reduce operational costs. In support of these aims SELFNET considers the following key management tasks:

- **Automated network monitoring**: SELFNET is capable of deploying NFV applications to monitor the network. These applications are considered sensors

that can be spread across the mobile network to enable context awareness in both traditional low-level metrics and a set of high-level Health of Netowrk (HoN) metrics. In particular, HoN metrics will facilitate greater control by delivering direct and precise knowledge of network status. These capabilities will enable network administrators to reduce significantly the time spent in identification and diagnosis of these concerns.

- **Autonomic network maintenance:** SELFNET defines high-level tactical corrective and preventive measures to enable autonomic reactive and proactive network maintenance. These tactical measures define the reactive actions in response to detected network problems, and define how to proactively configure, protect, improve and repair the network capabilities. The combination of reactive and proactive strategies with advanced intelligent algorithms drives the autonomic response of the system.

- **Automated deployment of network management tools:** The management of a set of automatic reactive and proactive actions against existing or potential network problems respectively, implies automatic deployment of various distributed services in the network. For example, intrusion protection tools and honeynets could be automatically deployed in order to mitigate different kinds of security threats.

- **Automated network service provisioning:** This capability is related to the efficient management and optimization of the usage and deployment of NFV applications. Efficiency will be achieved by dynamic smart selection of the best location where the services should be deployed (or migrated to) for optimization of network performance, health and security, and by timely release of the resources occupied by the services once they have completed their jobs.

In order to accomplish these aspects, SELFNET is focused on the following specific goals:

1) To design, implement and validate a self-monitoring and detection subsystem that will enable status awareness of the network infrastructure in terms not only of low-level metrics but also of a customizable and extensible set of HoN metrics addressing information about potential network failures, bottlenecks, security threats, etc. The monitoring framework should be able to deal with not only the metrics gathered from the system but also the aggregated metrics and analytical capabilities to provide trends and predictions over the network status to be used for proactive responses.
2) To design, implement and validate an extensive and distributed SON autonomic management engine subsystem based on new artificial intelligence, data mining, pattern recognition and QoE algorithms designed to provide the autonomic diagnosis, decision planning and enforcement of corrective and preventive measure to manage the network. This also includes the design of a new and extensible description language for defining the tactical strategies that will determine the autonomic actions.
3) To design, implement and validate a SON orchestration and virtual infrastructure management subsystem. The orchestrator is able to coordinate and schedule the enforcement of different corrective and preventive action plans provided by the SON engine into the network infrastructure by means of interaction with the

infrastructure managers. The virtual infrastructure manager performs remote deployment, installation, configuration, and lifecycle and resource management of the different SDN-enabled NFV sensors and actuators distributed in the system.

4) To apply the SELFNET framework in a range of essential SON use cases designed to address the major problems in current network management capabilities. These use cases will serve as the key drivers that will determine the set of SDN/NFV Apps SELFNET will need to implement in the framework in order to demonstrate its efficiency and suitability. The use cases will be focused on three main fields: self-protection, self-healing and self-optimization capabilities.

The innovation provided by SELFNET is in line with the key requirements and objectives of the 5G-PPP initiative as it is further discussed in Section 2.

1.2 Approach and Methodology

In order to achieve these objectives, as well as to facilitate alignment with 5G requirements, SELFNET focuses on a smart combination of SDN, NFV and SON. Given the complexity of integrating these three technologies, different design principles and methodologies have been taken into account. This analysis was conducted in three stages: 5G requirements analysis, use case definition and system requirement specification, as presented in Figure 1.1.

- **5G Requirements Analysis**. This analysis presents an overview of the 5G requirements and challenges, providing the context and introducing the motivation for each of the three general use cases proposed in SELFNET.

- **Use Case Definition**. Each use case has been designed to facilitate validation of the different objectives of the project. They have also been used to determine the requirements of the system.

- **System Requirement Specification**. The system requirements were defined by taking into account the use case requirements and the general needs of SELFNET architecture and its components.

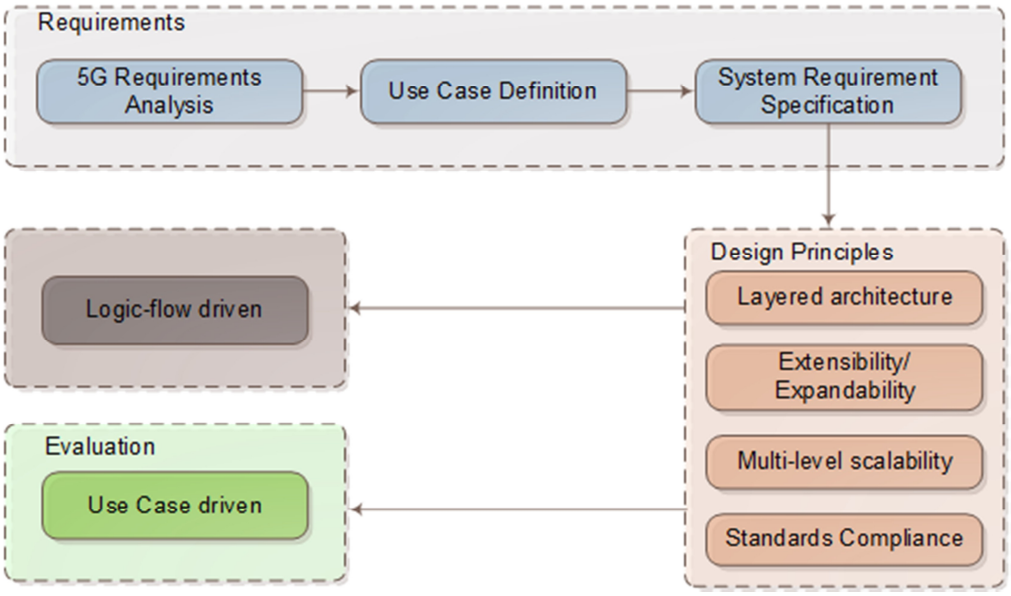


Figure 1.1 Development of the Methodology on SELFNET

Several system design principles have been highlighted (layered architecture, extensibility, expandability and multi-level scalability), leading to the adoption of a logic-flow driven design methodology, and a use case driven evaluation scheme. These design principles are described below:

- **Layered architecture**. SELFNET framework follows a layered architecture, including a number of ordered and logically separated layers. This design approach has been adopted by most complex systems; offering a number of well-known advantages such as reducing complexity in system design, implementation and evaluation, or increasing interoperability between different vendors and technologies. The use of this approach supports the standardization process. Additionally, the layered architecture allows correct distribution of workloads between the different partners according to their field(s) of expertise.

- **Extensibility/Expandability**. A modular design has been employed when determining the building block modules in each of the layers. SELFNET takes advantage of the modularity, especially in terms of its usefulness in extensibility/augmentation. This characteristic is achieved by combining modular design, open interfaces and APIs to enable third parties to create their own automatic network management applications and services. It is envisaged that SELFNET supports extensibility of operators' platforms. It means that networks can be expanded, by integrating additional resources, on the basis of seamless inclusion of new technologies. SELFNET NFV applications can be deployed to permanently or temporarily expand the network resources of an operator in order to, for example, extend the geographical coverage or empower an existing infrastructure. In this context, a new paradigm in the operation, maintenance and upgrade of a backbone network can be tested and formulated by exploiting new and flexible "as-a-service" patterns.

- **Multi-level scalability**. A multi-level scalable management framework is required to address network management concerns in large-scale networks.

Firstly, distributed network health monitoring and localized diagnosis functions are spread over virtualized network elements allowing service-level HoN metrics to be reported to the Monitors and Aggregators. The HoN metrics are the result of local diagnosis intelligence, meaning that upper-level Analyzer only need to concentrate on regional and global diagnosis thereby reducing their workload and increasing their scalability. Secondly, the Aggregator and Analyzer follow a hierarchical structure to facilitate handling/analysis of HoN reports at local, regional and global levels (depending on which area is affected). Scalable service composition will allow the creation of services ranging from micro services (service lets such as those fine-grained service slices proposed in the UNIFY project [2]) to macro monolithic services (e.g., Monitoring as a Service implemented in the MCN project [3]) in response to the use case demands and the resource constraints of the system. Further elastic scalability is built into the SELFNET framework by employing the Cloud Computing Layer.

- **Standards compliance.** To allow high interoperability and wider adoption of the technologies proposed in SELFNET, the design of SELFNET adheres to the standards that are considered relevant to the domain. Specifically, SELFNET explores ETSI standards for NFV [4], Open Networking Foundation (ONF) standards for SDN [5] and TMForum ZOOM [6] standards for business transformation aspects, respectively. The works of IETF/IRTF in this area are also closely monitored. Further detail can be found in Section 3.2.

Taking into account the previous design principles, a use-case driven research methodology is implemented. It implies that the system design methodology is primarily driven by the control logic of the proposed automatic network management functionalities, especially those of the three use cases (self-protection, self-healing and self-optimization). Evaluation of the SELFNET framework will also be performed against the essential use cases described below:

- **Design**. When designing the system, the three use cases provide the logic flows for autonomic operations. An initial monitoring/discovering stage includes context (especially network status) sensing and collection based on a range of SDN-enabled ‘sensors’ (in their broad sense) and localized network health diagnosis. Sensors are configured to provide information to the Monitor module, in an adapted version of traditional distributed monitoring software, which is able to provide an overview of the managed systems by gathering metrics from different network devices. The Analyzer module uses this information to perform correlation and deep analysis and infer “predicted values” not only at a local level but also at a regional/global level. The network administrator is then provided with an API through which the entire network status can be viewed (provided by the Monitor and Analyzer modules) and can define corresponding autonomic behaviours, by means of artificial intelligence algorithms, to govern the behaviour of the system. This latter facility will be provided by a purpose defined tactical autonomic language. The Decision Making Planner will then define which actions will be conducted in the system when it reaches a particular state (as reported in the output of the Analyzer). The set of actions are directly related to the control of the lifecycle of all NFV functions and also to the specific configuration of NFV. Subsequently, these actions will be enforced in an orchestrated way by the “Orchestrator” module, which will perform

operations such as installation, uninstallation, configuration, starting, stopping, backup, etc.

- **Evaluation**. SELFNET evaluation involves the three essential use cases (self-protection, self-healing and self-optimization) plus a composed use cases involving characteristic of the other ones. They will be implemented to validate the SELFNET framework against a set of major challenges currently faced by network operators, and will be piloted in a combination of network operator infrastructures and large-scale evaluation platforms using existing EU test beds to establish the applicability of the results to industrial/business environments.

1.3 Terminology

This subsection provides definitions of some terms that will appear frequently throughout the document. This description aids understanding of the context in which these terms are used in SELFNET project as shown in
Figure 1.2. These are described below:

- **Use Case**: A use case is a description of steps or activities that should be accomplished to carry out a particular process. In this deliverable, they represent a sequence of interactions that takes place between SELFNET and its actors in response to an event that initiates a major player on the system itself. They play a very important role in its development process, as a system evaluation against use cases is applied. It also implies that they represent the set of major challenges of capabilities to be covered by SELFNET. For better understanding, the use cases are divided in four categories: self-healing, self-protection, self-optimization and composed proposals, aligned with 5G requirements.
- **Requirement**: A requirement is a condition or capability that must be displayed or fulfilled in a system. In SELFNET, the satisfaction of requirements is necessary to successfully complete any of its use cases or to deploy the different modules and subsystems. These may cover different required conditions such as compliance with certain regulations and standards, or ensuring suitable functionality of particular actors.

- **Key Performance Indicator (KPI)**: A key performance indicator is a previously agreed performance measurement that reflects the critical success factors of a proposed solution. In SELFNET, the KPI's are linked to use cases, and capture the goals and challenges of each one.

- **Challenge**: Challenges are defined as fundamental technical difficulties within a new technology or systems. They are usually illustrated by scenarios, which represents the main aspects of the underlying technical problems. 5G technologies and systems will need to address a number of key performance indicators (KPIs). They involve different features, such as throughput, energy efficiency, and latency, among others. These features must be dealt by SELFNET in order to facilitate its integration.

- **Legacy solution**. A legacy solution is a previous or outdates approach. This term commonly refers to solutions that provide limited services (or not enough for specific needs) or cannot improve their function, technology or economic

use. In the context of SELFNET, it refers to previous approaches with similar goals and use cases. Thus, it must complement the legacy solutions or to be competitive to them.

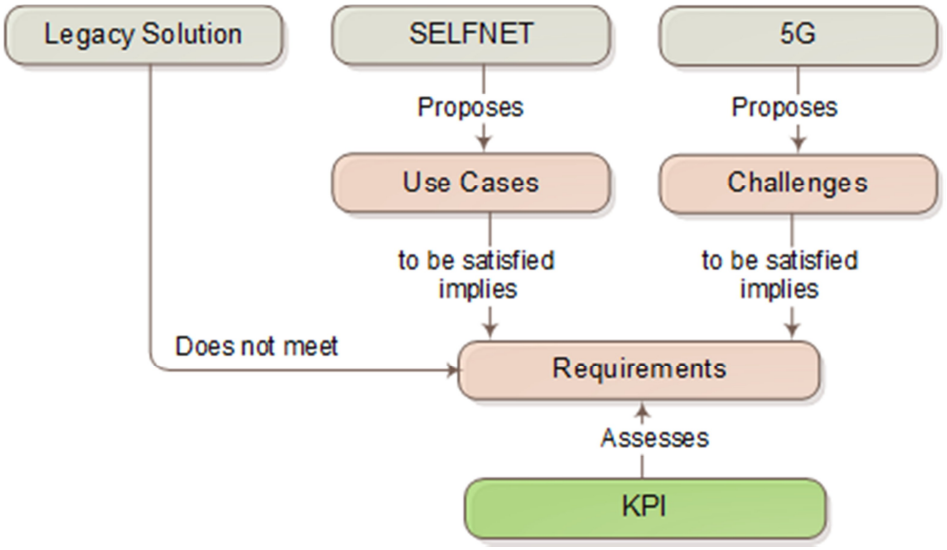


Figure 1.2 SELFNET Terminology

1.4 Document Structure

This document is organized as follows:

- Section 2 describes the requirements and challenges of 5G systems and describes the relationship between the SELFNET framework and the fields in which SELFNET will have a relevant impact.
- Section 3 describes the SELFNET reference architecture based on a layered approach. It defines the following layers: Infrastructure Layer, Virtualized Network Layer, SON Control Layer and SON Autonomic Layer.
- Section 4 presents the three proposed use cases: self-healing, self-protection, and self-optimization, and how they can demonstrate the capabilities of the SELFNET framework to address 5G requirements and challenges.
- Section 5 provides the system requirements aligned with two main domains (the corresponding use case and the relationship with each layer of SELFNET referential architecture).
- Finally, section 6 shows the conclusions and describes how the information delivered in this report will be used in the next stage of SELFNET activities.

2 5G Challenges and Requirements

This section describes the challenges and requirements, of the envisioned 5G system, which have motivated and inspired the SELFNET reference architecture and its use cases.

2.1 5G Vision

5G aims to provide a sustainable and scalable 5G network infrastructure to meet the exponentially-increasing demands on mobile broadband access [1] [7] [8]. Therefore, a principal design requirement for 5G is high system efficiency in both CAPEX and OPEX. Significant advances in network management automation are therefore needed to minimize the costs incurred by current manual or semi-automated management regimes which, although time-consuming and costly, are still commonly found in the current generation of mobile networks. Moreover, the average revenue per user (ARPU) is continuously decreasing, while the demand on mobile traffic keeps growing. This trend has had a negative impact on continued investment by network operators in the deployment of network hardware infrastructure. To address these challenges, 5G will combine networking, computing and storage resources into an open architecture driven by intelligent software networking [9] [10] [11]. In this context, an innovative integration of SDN, NFV, cloud computing and other related cutting-edge technologies will play a leading role in achieving higher flexibility, scalability and improved performance. This common vision, shared in this Consortium, has led to the initial definition of the SELFNET framework.

5G will provide a secure, reliable and high-performance communication environment addressing wider societal challenges in smarter cities, public safety and security, entertainment and other applications [12] [13]. Therefore, an essential requirement on 5G systems is to offer greatly varied network services to a wide range of applications, with substantially reduced service creation times [14]. This vision indicates that automated network operations should be realised in 5G as enabling technologies to support various applications in a timely manner. Furthermore, 5G users will expect a high-quality experience with minimal disruptions in their services/applications regardless of time, location or devices. To this end, 5G requires advanced mechanisms towards guaranteeing high service availability, service continuity, security, and optimal service performances. These 5G requirements have motivated the Consortium to further develop the three essential use cases for self-healing, self-protection and self-optimization.

Different key stakeholders [1] [15] [16] are devoted to the research, requirements' definition, standardization, regulation and development of 5G systems. The ones included in the main 5G groups of stakeholders are manufacturers, service providers, regulatory bodies, SME, standards developing organizations (SDOs).

These organizations have helped in the definition of a set of Key Performance Indicators (KPIs) in line with the needs of 5G systems. In particular, 5G-PPP aims to achieve the following KPIs [1]:

- Providing 1000 times higher wireless area capacity and more varied service capabilities compared to 2010.

- Saving up to 90% of energy per service provided. The main focus will be in mobile communication networks where the dominating energy consumption comes from the radio access network.
- Reducing the average service creation time cycle from 90 hours to 90 minutes.
- Creating a secure, reliable and dependable Internet with a "zero perceive "downtime for services provision.
- Facilitating very dense deployments of wireless communication links to connect over 7 trillion wireless devices serving over 7 billion people.
- Enabling advanced user controlled privacy.

In order to cover the aforementioned KPIs and capabilities, some specific system-level challenges [16] are outlined by NGMN as follows:

- **Quality of service and Quality-of-Experience** in the domain of 5G services delivery are key factors. They should provide specific Quality of Service (QoS) levels, taking into account diverse dimensions such as throughput, latency, resilience and costs per bit. In addition, QoE challenge targets at providing a service delivery model that transparently considers the impact of network management actions on the user's perceived quality and always seeks to maintain an acceptable QoE level irrespective of prevailing QoS state.

- **Design principles** should guarantee user privacy by some means of accountability within the communication substrate. In addition, simplicity must be achieved avoiding complex customer journeys in the process of delivering the best network services, mainly in mobile environments. On the other hand, several control mechanisms for relocation functions, protocol entities and corresponding states should be devised to provide enough flexibility, by the use of programmable network technologies such as SDN and NFV. These design principles will ensure better management of resources.

- **Deployment of 5G services** should address new density challenges, increasing the number of connected devices, in multi-tenancy environments.

- **Diversity** in 5G must prove the support of wide range of wireless solutions, multiple connected devices, and efficient management of traffic types, taking advantage of any communication capability, including device-to-device (D2D). In this field, 5G will provide robust communication systems against network attacks.

- **Energy efficiency** should require novel enhanced power capabilities, considering also power harvesting from surrounding environment in greater levels of mobility across different networks.

- **Service provisioning** should be improved. It will take into account location and context-aware capabilities by means of geo location and positioning schemes that can contribute in the provision of location-based services.

- **New business models** could be deployed, by the use of interfaces within the system in order to enable flexible operator models, in a multi-tenancy fashion. These new models will open novel and efficient management schemes in order

to achieve a lower OPEX. 5G should also provide new methods for flexible pricing between different stakeholders in the value chain.

- **Evolution** in 5G should prove adaptation mechanisms to several communications environments, in order to allow a transparent migration from current network infrastructures, as well as novel 5G deployments of current and future scenarios.

2.2 5G Requirement Domains

The response to these challenges and KPIs will facilitate an open ecosystem for encouraging technical and business innovation. In order to fulfil this objective, NGMN classifies 5G requirements in six main dimensions [15], derived from the 5G vision and aligned to the main 5G challenges. These dimensions are shown in Figure 2.1.

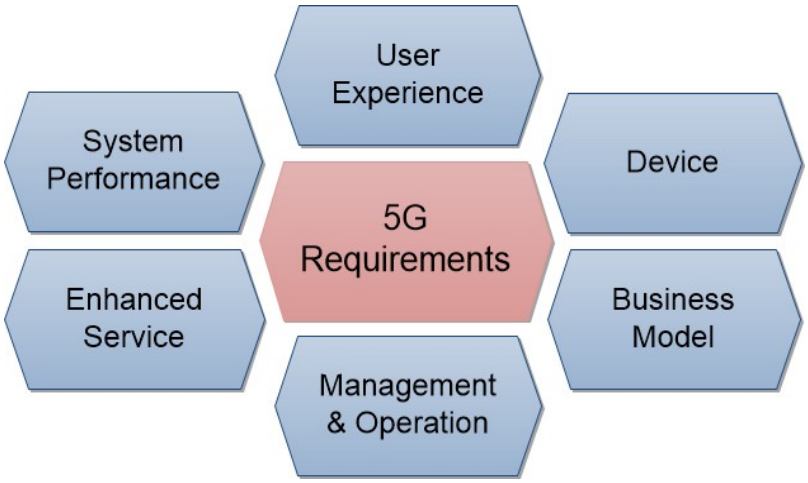


Figure 2.1 5G requirements proposed by NGMN

These areas take into account different characteristics and requirements defined in the following subsections.

2.2.1 User Experience

This NGMN requirement focuses on maintaining and improving the user experience by, at a minimum, providing users with consistently high QoS levels (in terms of bandwidth & delay) across a broad range of mobility scenarios. A 5G user should be able to obtain a consistent, high-quality service, regardless of the networks, operators or locations with enhanced user experience compared with 4G systems even in critical situations such as very crowded areas, emergency events, network failures, etc. Given the other 5G requirements [16] [17] for high quality video services at HD or U-HD resolution this extends to providing services that meet users' QoE expectations not just operator QoS KPIs. For video services this means availability anytime and anywhere with high picture quality, no visual artefacts and no buffering waits [18]. Achieving the zero service downtime KPI is a target that should be met if real time applications are to meet user expectations of service quality and continuity.

2.2.2 System Performance

The system performance of a cellular network is a traditional way to divide the generations of systems. As the most important KPI, the 3G system can provide a minimal data rate of 3.84 Mbps. LTE (LTE-A) achieved a data rate of at least 100 Mbps in mobile scenario, which can be regarded as a symbolic parameter of 4G. For the 5G system, the requirement on data rate will be substantially increased, measured by Gbps, due to the exponential growth on mobile traffic demand [19]. Recently, the spread of new services and devices, such as Internet of Things (IoT), autonomic automobiles, smart robots, virtual reality, wearable electronics, bring new requirements on system performances, such as the number of simultaneous active connections per square kilometre, ultra-reliability, low end-to-to latency, which go beyond the traditional performance metrics, like capacity, coverage, the maximal mobility speed, and the number of active terminals per cell.

2.2.3 Device

5G terminals should have a high degree of programmability and configurability by the network to allow operator control, Multi-Band-Multi-Mode support to enable true global roaming and to achieve high data rates and the resource and signalling efficiency of devices should be enhanced in order to increase the battery life. The concept of “mobile terminal” should be redefined, as it is now far beyond that of a traditional mobile phone. Smart phones, tablets computers, wearable electronics, sensors, automatic automobiles, robots, and some new wireless-enabled devices on the horizon should be now considered. These new devices will not only bring x1000 times mobile traffic increase by 2020, but also impose a wide range of differentiated QoS requirements that will need to be met by 5G systems.

2.2.4 Enhanced Service

The requirements of this domain are related to improving the following key characteristics of achieving transparent connectivity on a combination of radio access technologies (RATs) [20] and LTE technologies accessible to 5G terminals, improvements related to the use of location as an important contextual attribute and enhanced security services provided by robust authentication and user privacy. 5G targets to enable extremely high network availability and reliability and self-healing capabilities to improve network resilience.

2.2.5 Business Model

In contrast to physical infrastructures in the traditional mobile systems, the 5G design will enable operators to configure the data flow to use only necessary functions in the virtualized network. This will be done on demand and in a programmable manner, in order to reduce operational and management expenditure. 5G will facilitate the creation of new business models and the evolution of the Partner Service Provider and XaaS Asset Provider by supporting different levels of abstractions. The 5G system should provide methods and instruments for various infrastructure sharing schemes developed to maximize the overall synergies of network sharing agreements between service provider and operators, and between operators [21].

2.2.6 Management and Operation

The simplified operation, administration and management of 5G infrastructure will also benefit the whole 5G ecosystem through a decrease in the Total Cost of Ownership (TCO). Furthermore, 5G will reduce complexity of planning, configuration

and optimization tasks in the whole system, giving the capability to reuse and smoothly upgrade existing network infrastructures. Additionally, the 5G design [17] [22] should provide reliability, not only on equipment uptime, but also in the provision of required data. They must be received in the required time and not be dependent of a specific technology. Reliability is more critical on mobile communications for control and safety [23].

2.3 SELFNET Impact on 5G

SELFNET will introduce intelligent, self-organizing and autonomic capacities to 5G networks, taking into account the main advantages of 5G key enabling technologies, such SDN [24], NFV [25], SON [26] and the Cloud [27]. These concepts will provide an open environment to foster innovation and decrease the CAPEX and OPEX of new applications. As an example, SELFNET proposes three use cases (self-healing, self-protection, and self-optimization) that demonstrate its usefulness in meeting 5G KPI's and will propose an use case composed by these ones.

2.3.1 Expected Impact at Societal, Operational and Innovation Levels

SELFNET aims to generate a significant impact on the development of 5G, mainly in societal, operational and innovation levels.

At societal level, SELFNET will contribute by enabling ubiquitous, robust and continuous service access for subscribers underpinned by a reliable self-managing network. SELFNET will perform QoE oriented self-optimization of the network traffic, especially video traffic. SELFNET will also be able to provide early reactive (or in certain cases proactive) responses against cyber-attacks and therefore effectively reduce the number of attacks reaching the target destination, in concordance with the security requirements of 5G. In addition, autonomic management when combined with SDN and NFV in SELFNET will help to reduce the number of physical devices and the utilisation of existing devices thereby reducing in energy consumption.

At operational level, the scalability and extensibility in SELFNET will also help to decrease the capital and operational costs directly related to deployment and management of new network functions. Consequently, SELFNET contributes to reduce the TCO of the network infrastructure, according to the management and operation requirements of 5G. Additionally, through automation, SELFNET will reduce the lifecycle of creating and deploying new service, a KPI proposed by 5G PPP.

At innovation capacity and knowledge integration level, SELFNET will open up a wide range of opportunities in low density areas, facilitating the prompt and cost-effective creation and deployment of virtualized network functions without any significant investment. SELFNET will also provide a new innovative business ecosystem based on open APIs and software, which will allow operators to lease resources on demand.

2.3.2 Expected Impact of SELFNET Use Cases

The SELFNET use cases will demonstrate the ability of the SELFNET framework to meet 5G KPI' such as a reduction of average service creation, saving energy consumption, providing virtual services, improvements on user experience with a "zero perceived" downtime for provisioning, among others. This is line with the six 5G requirement domains [1], of user experience, management and operation, business model and system performance, with each use case covering specific requirements.

Firstly, the Self-Optimization use case will allow SELFNET to improve the 5G user experience through the use of video adaptation techniques and development of new QoE metrics at both video stream and network levels. It will also address the low latency 5G KPI by considering real time, bidirectional video services. 5G Business Model requirements will be addressed by demonstrating underpinning technologies for potential new high value video services including support for new Machine to Machine (M2M) video applications. Furthermore, active network element management and energy aware capabilities will simplify network deployment and reduce the TCO of the network infrastructure, which will in turn impact on the fulfilment of Management and Operation 5G requirements.

Secondly, the self-protection use case will contribute to System Performance, Business Model and Management and Operation requirement domains [28]. In the context of user experience requirements, self-protection capabilities will provide secure and reliable communications, by ensuring the availability of the network services [29]. Furthermore, the deployment of security virtual functions will help prevent network disruption, facilitating very dense deployments, a key requirement of 5G.

Finally, the self-healing use case will allow SELFNET to provide higher levels of network availability and lower latency by taking the required actions to preserve network state in critical conditions [30]. 5G's system performance requirements will be covered by seamless network operation under abnormal/unusual conditions such as in crowded areas by, supporting the agreed data rates for thousands of users. In addition, this use case will demonstrate high resilience and availability by dealing with network failures in proactive and reactive modes. The infrastructure will be managed under a common flexible scheme, facilitating network agreements between service users and operators. Last but not least, self-healing will reduce complexity of network operations and management (reduce TCO), applying automation recovery actions.

2.3.3 Expected SELFNET Impact on 5G PPP KPIs

- **Performance KPIs:**

  - **Reducing the average service creation time cycle from 90 hours to 90 minutes:** SELFNET will provide an engine to perform automatic deployments of NFV services in cloud infrastructures. This engine will contribute to this KPI. It is difficult at this stage to see how much improvement will be achieved but the mere fact of enabling this type of technology is expected end up in reducing the deployment time significantly. In addition, combined with the self-organizing capabilities provided by SELFNET, the detection of the "need" of such a deployment or configuration will also contribute to such metrics. SELFNET will cover three use cases where the validation of the framework can be evaluated but the framework itself can be seen as an enabling technology to be extended to other potential use cases in order to work toward the achievement of such KPIs.

  - **Creating a secure, reliable and dependable Internet with a "zero perceived" downtime for services provision:** SELFNET is a self-organized autonomic framework and its use cases will deal with self-healing, self-optimization and self-protection capabilities within the 5G network. As a result of these use cases, SELFNET will contribute to the achievement of "zero perceived" downtime for service provisioning for these particular use cases. In

addition, SELFNET can be foreseen as an enabling technology to be extended in order to cover more use cases, thus reducing more the “zero perceived” downtime of services.

- **Societal KPIs:**

  - **European availability of a competitive industrial offer for 5G systems and technologies:** SELFNET will provide a demonstrator of the different innovations carried out in the project. As a result, our consortium will significantly increase their industrial offer for 5G systems and technologies.

  - **Stimulation of new economically-viable services of high societal value like U-HDTV and M2M applications:** SELFNET will address a particular use case based on U-HD video, which will investigate optimized U-HD video delivery for improved users’ QoE. These innovations will contribute to optimizing the delivery of this new service. This KPI has “medium” importance for SELFNET; however, it is difficult to foresee how far SELFNET can go through the achievement of this KPI because it is mainly explicitly covered in one of the use cases.

- **Business-related KPIs:**

  - **Target SME participation under this initiative commensurate with an allocation of 20% of the total public funding:** SELFNET has allocated 20% of the total public to SME partners.

  - **Reach a global market share for 5G equipment & services delivered by European headquartered ICT companies at, or above, the reported 2011 level of 43% global market share in communication infrastructure:** SELFNET will not address any hardware vendor or will not be focused on 5G equipment. However, SELFNET will deliver a self-organizing framework for 5G Networks to be exploited commercially through our consortium. All our industries are headquartered in Europe.

3 SELFNET Reference Architecture

In this section, the SELFNET reference architecture is defined with all architectural design considerations to meet 5G requirements and visions taken into account. The reference architecture provides a uniform operation framework for the use cases described in Section 4.

3.1 SELFNET Actors and Roles

As a system, the SELFNET framework includes the (virtual) network. Hence all actors that interact with the network should be represented: all Business and Operations Support and other enterprise systems. For simplicity, in this approach only actors that are considered relevant for the Self-Organizing behaviour of the framework are explained in this section (Figure 3.1).

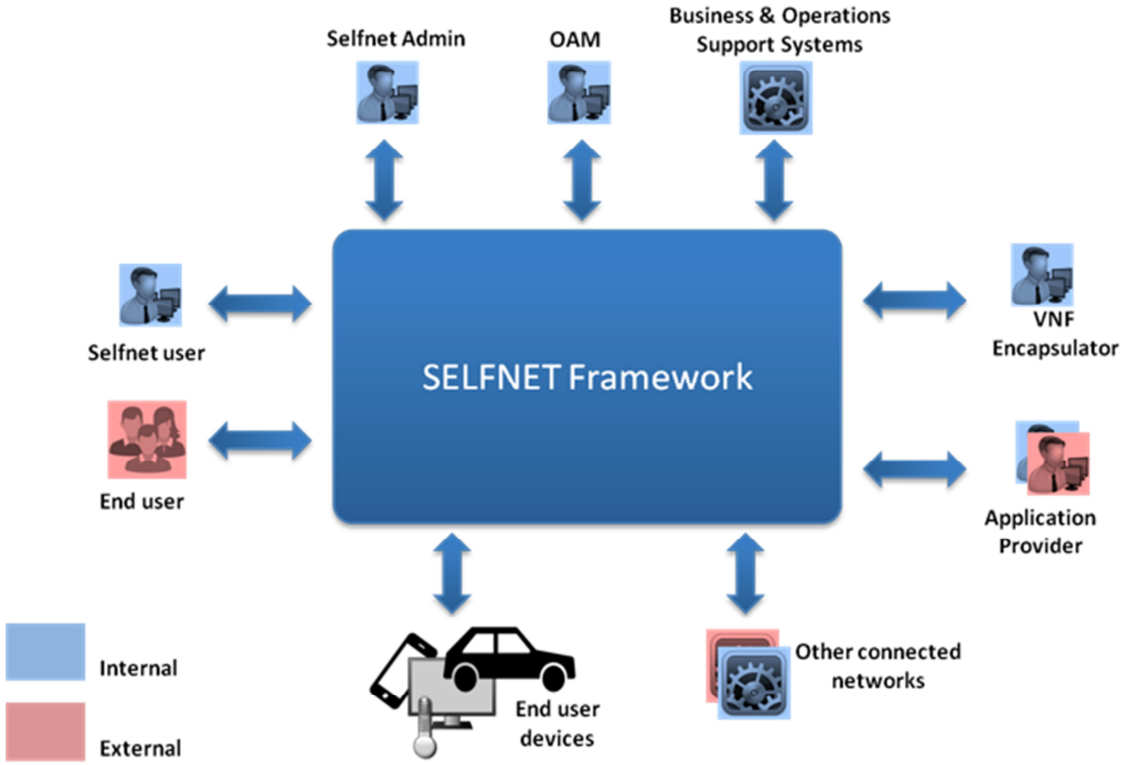


Figure 3.1 SELFNET System Context

Entities are represented as External or Internal, respectively if they are within or outside the operational scope of the SELFNET Framework, as shown in Table 3.1.

Table 3.1 Average number of ICT devices per user

Role	Scope	Description
Application Provider	Internal External	Provides VNFs to be used in the scope of autonomic processes. This may be an external actor if the VNFs are acquired in the market or an internal actor if they are developed internally.
VNF Encapsulator	Internal	Deals with the Acceptance/registration of new tools for autonomic behaviour, provided by the Application Provider. Manages the Lifecycle of such tools and sets up the policies for their usage.
OAM	Internal	General Operation, Administration & Maintenance of each of the system components.
SELFNET Admin	Internal	Is responsible for the configuration of the whole SELFNET Framework.
Business & Operations Support Systems	Internal	Information Systems that relate to the SELFNET Framework in the scope of the various enterprise processes, either Operational or Business related.
Other Connected Networks	Internal External	Networks that are connected to the Network under the scope of the SELFNET Framework, either in the scope of the same operation or external networks.
SELFNET User	Internal	User that is allowed to access internal information on the status of the framework, and obtain performance data.
End user device	External Internal	Devices that are used and/or managed by end users. Usually these devices have a purely functional relation to the network, but may also produce data worth analysing. In such case they may be considered as Internal.
End user	External	End Service Users, which may relate with the SELFNET Framework directly, e.g. via a self-management portal, and/or indirectly, via the End User Devices.

3.2 SELFNET Architectural Context

Figure 3.2 illustrates the focus of SELFNET on the end user services lifecycle, as described by ITIL [31]. As the figure highlights, SELFNET is positioned on the service Operation/Optimization states. Nevertheless, the implementation of a SELFNET Use Case may be mapped to the whole service lifecycle. In such case, the SELFNET framework will have to support the various phases, from the arising of a “Business need” - e.g. the need to automate the optimization of certain network behaviour up to the “retirement” of the deployed mechanism.

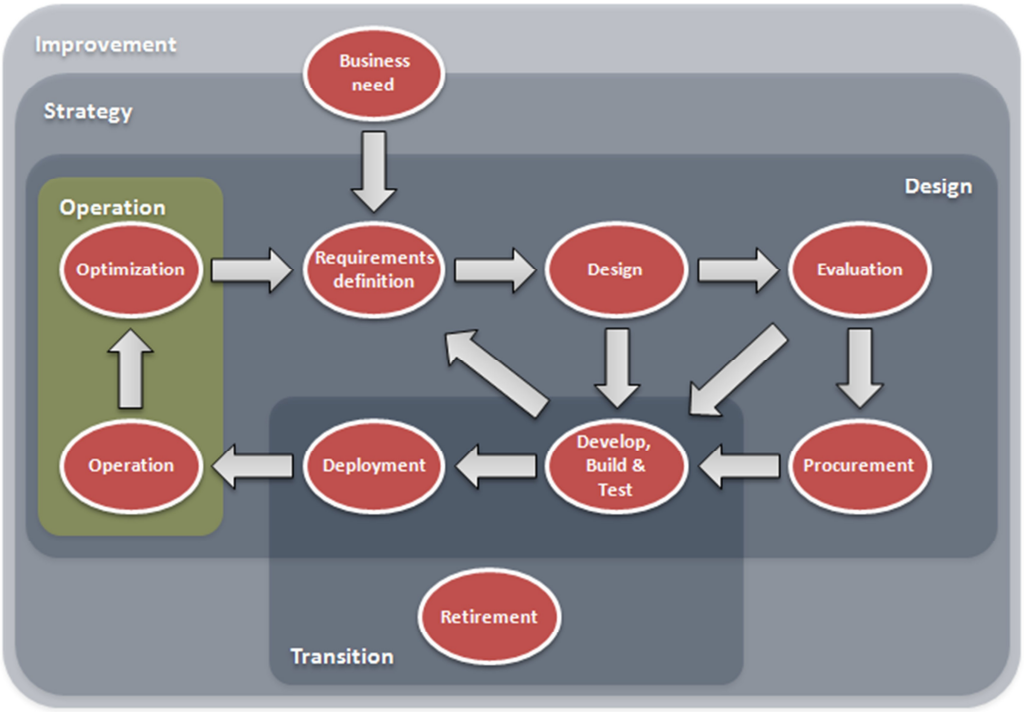


Figure 3.2 SELFNET Service context [31]

3.3 SELFNET Architectural Standard Foundations

The specification of the architecture takes into account all the requirements expressed by the SELFNET use cases, and is aligned with the most relevant standards which are the foundations of the project: ETSI NFV [4], Open Networking Foundation (ONF) [REF 26] and TMForum [6].

NFV [4] is the ETSI group devoted to standardize the virtualization of Networks Functions (NFs). It intends to define the complete architecture required to accommodate the challenges of the new virtualization paradigm. The architecture covers runtime and management aspects, capable to manage the entire lifecycle of a Virtual Network Function (VNF). Furthermore, it also comprises the management of Network Services (NSs), which are built by orchestrating multiple VNFs, according to a forwarding graph (FG), using a catalog-driven approach.

ONF [5] is an organization devoted to promote the utilization of software-defined technologies to program the network. Following a Software-Defined Networking approach, the network is separated into three different parts: the user-data plane, the controller plane and the control plane. The user-data plane is responsible to forward the user traffic, while the controller plane is composed by SDN controllers which provide high-level APIs to the control plane above. The control plane is responsible to program the network, easing the creation of new applications and speeding up the rollout of new services.

The TeleManagement Forum (TMForum) is a telecom industry association devoted to provide guidelines to help operators to create and deliver profitable services. One of the biggest TMForum achievements is the definition of a complete business process (eTOM) and application (TAM) maps, including all activities related to an operator, from the services design to the runtime operation, assurance, charging and billing of the customer, among others. In order to accommodate the SDN/NFV impacts, the TMForum has created the Zero-touch Orchestration, Operations and

Management (ZOOM) program [6], which intends to build more dynamic support systems, fostering the service and business agility.

3.3.1 ETSI NFV

The creation of ETSI NFV [4] intended to bring to the Telco sector some IT (Information Technology) tools, in order to take advantage of cloud principles, like on-demand, agility, scalability or pay-as-you-go (PAYG), among others. The decoupling of hardware and software and consequent utilization of Common Off-The-Shelf (COTS) hardware can also be applied on network functions, leading to a cost reduction and vendor independency.

The first basic step to take towards NFV is the "cloudification" of network functions (NFs). For this, the network function has to be implemented apart from a dedicated/specialized hardware, and be able to run on top of COTS hardware. Typical examples of VNFs are common routers or firewalls, but it can also be mobile or fixed components, like P-GWs, eNBs or OLTs. Figure 3.3 depicts this simple concept.

For the sake of simplicity, it is assumed that the resulting VNF has the very same set of features as the equivalent Physical Network Functions (PNFs). However, the "cloudification" may also lead vendors to reshape their offers, in order to accommodate them to the cloud environment. This way, multiple PNFs can be collapsed into a single VNF, one PNF can be separated into multiple VNFs, or any other N:M combinations. These changes can be decided to optimize resources or to improve the management of the function.

The "cloudification" of network functions can be further enhanced by using the management and orchestration environment. In such case, the platform manages the entire lifecycle of VNFs, performing not just the deployment and disposal, but also managing the runtime operations, by migrating or scaling in/out VNFs, according to the function load, making a more efficient use of resources. Such platform is also able to orchestrate combinations of VNFs according to a given Forwarding Graph (FG), in order to create complex Network Services (NS).

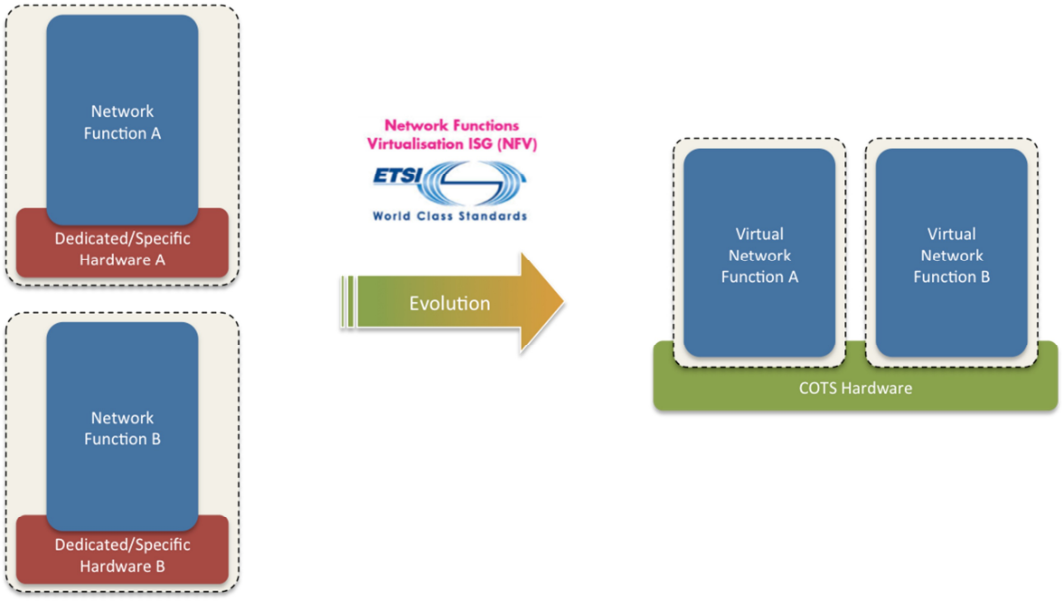


Figure 3.3 NFV concept

Figure 3.4 depicts a simplified version of the full ETSI NFV architecture. In the left side it can be seen the execution and control (runtime) operations, while the right side shows management and orchestration. The bottom left shows the virtual infrastructure, which comprises hardware resources (COTS), the virtualization layer, (e.g. KVM, VMware hypervisors) and the virtual resources (e.g. VMs, VLANs). VNFs run on top of one or multiple VMs and use network resources. On the top left, the Management Support Services (OSSs/BSSs) interact with the Management and Orchestration (right side) and with the VNFs. In the right, on the bottom, the Virtual Infrastructure Management (VIM) (e.g. Open Stack) interacts with the NFVI (hypervisor) to manage resources. On the top right, the Orchestrator and Management module manages the complete lifecycle of VNFs and orchestrate NSs.

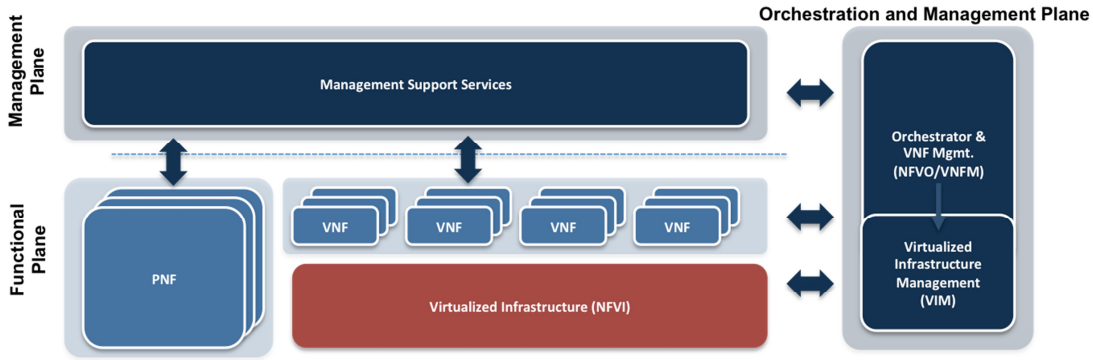


Figure 3.4 NFV architecture

3.3.2 ONF SDN

SDN intends to make the network simpler, more flexible and more programmable. For that purpose, the SDN architecture splits the network functions into three parts: the user-data plane, the controller plane and the control plane. The user-data plane (or Data Plane) is composed by simple switching Network Elements (NEs), responsible to forward the user traffic according to the basic commands received from the north (controller) interface. The Controller Plane is composed by SDN controllers, which provide basic commands to the south (user-data) and high-level APIs to the north (control or application plane). Controller APIs are abstractions used to program the network, speeding up the creation of new services.

Figure 3.5 depicts the SDN concept. In the Figure, it is assumed that the starting point is not a traditional NF relying on a dedicated/specific hardware, but an already virtualized NF (VNF), as described in the section above.

Overall, the NEs forwarding process is fully commanded by the applications, which use high-level APIs provided by the SDN controllers. The SDN controllers interact with the NEs through low-level southbound APIs to enforce basic forwarding rules, using Command Line Interface (CLI) scripting or protocols like Netconf [32] or the most recent OpenFlow [33]. SDN controllers provide a northbound interface, abstracting the programmer from the network details and making simpler the network service creation. This is one of the key advantages of the SDN model.

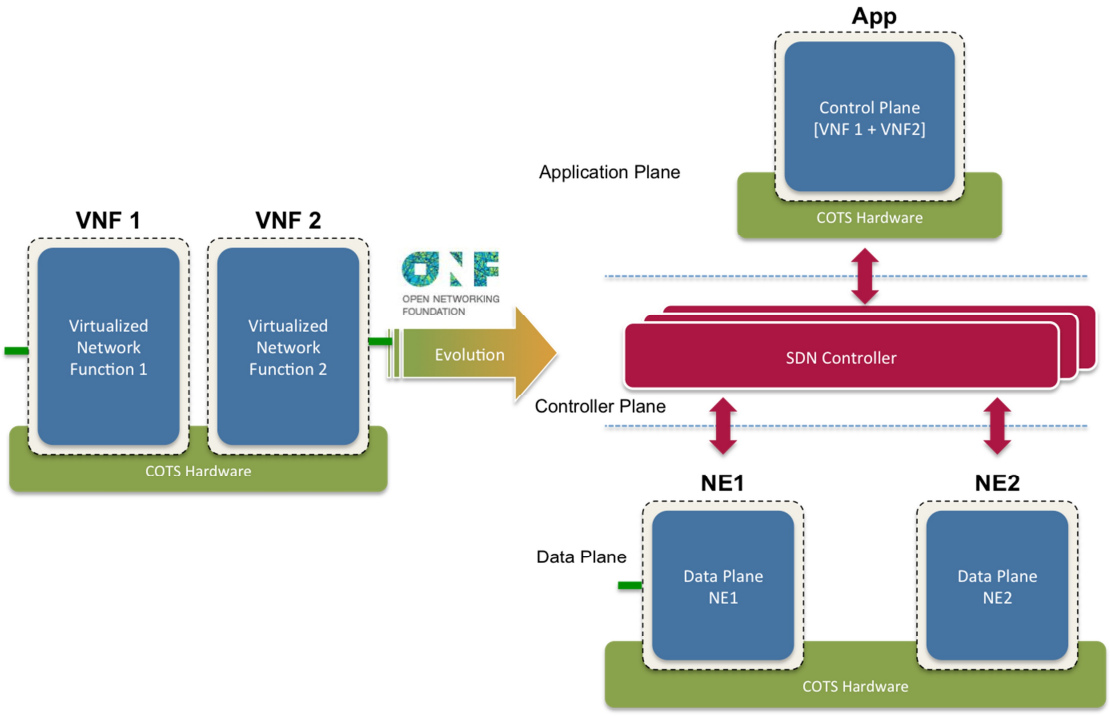


Figure 3.5 Software-Defined Networking (SDN) concept

Figure 3.5 shows the evolution from a traditional world to an SDN approach. Sometimes the transformation has not to be done 1:1. This means that a VNF may not move directly to the SDN paradigm by splitting itself into three parts. In fact, a single VNF can result into multiple applications and/or multiple NEs (N:N). To make this clear, two examples of "SDNificiation" are provided below.

In the first example (see Figure 3.6), the original scenario is a set of already virtualized routers. Each router has an IPv4 and IPv6 forwarding feature as well as the traditional routing protocols, like OSPF, BGP, etc. (for simplicity, other features can be ignored here). On top of that, operators can configure the routers and build services like IPv4 connectivity, IPv6 connectivity or enterprise VPN, among others. Moving to the SDN paradigm, control and forwarding planes are decoupled. On the bottom, NEs are deployed with forwarding-only capabilities, applied according to the policies provided by the control plane. Control logic is implemented on the top, e.g. OSPF, BGP, as well as all the service logic that permits e.g. the provisioning of a new Access, VPN or VPN site. In this particular case, there is an N:N mapping between the control plane (SDN Apps) and the user-data plane (NEs); i.e. multiple applications implement different services on top of a common set of NEs. NEs can be virtual software switches (e.g. OpenvSwitch [34]) or more performing hardware specific switches.

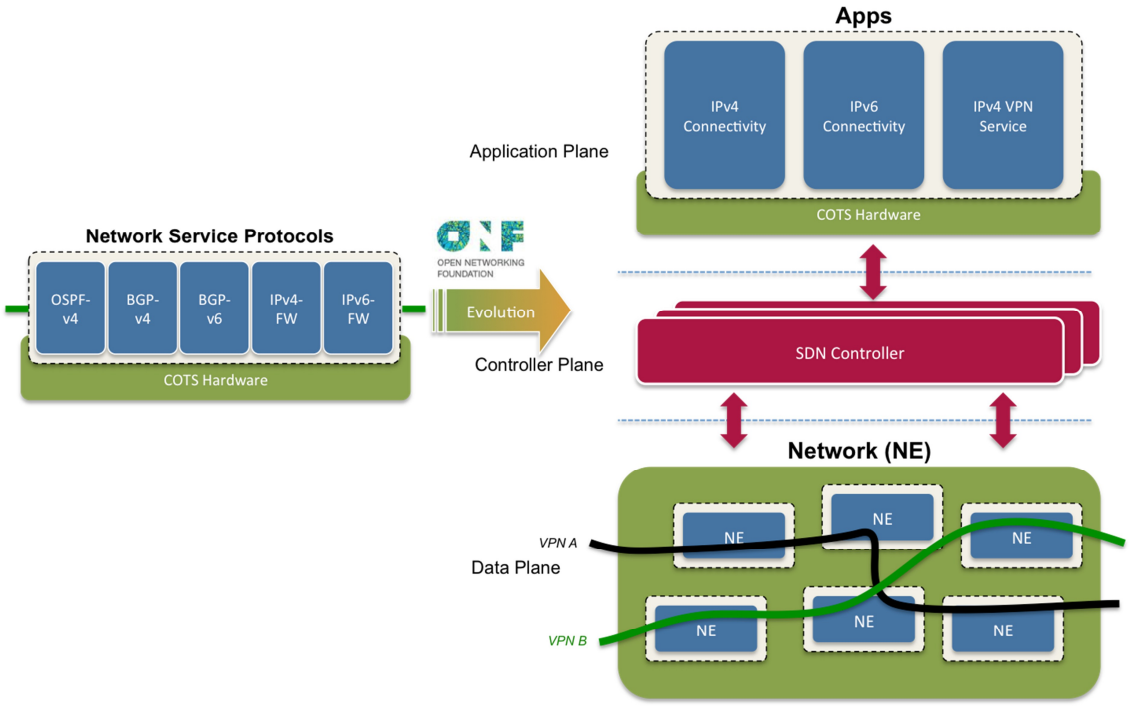


Figure 3.6 Software Defined Network (SDN): example Transport Network

In the second example (see Figure 3.7), the original scenario is again an already virtualized Home Gateway (vHGW). This vHGW is the equivalent to a residential router, but implemented on top of COTS. This network function is able to forward IPv4 and IPv6 traffic, and perform other functions like Firewall (FW), Parental Control (PC), Traffic Shaping (TS), or IPv4 Network Address Translation (NAT), among many others. Moving to the SDN paradigm, the monolithic HGW is split into multiple functions, which are split into a user-plane, controller and application part. Furthermore, the functions are sequenced (chained) according to a specific graph (FG) for a particular customer profile. As a result, there is an App per HGW function and a global HGW App, which implements the desired sequencing (chaining).

It is noted that this is not the only option to implement the HGW using SDN. Another option is to have a single HGW Application, where each function is just an HGW App plug-in.

In this particular case, although it seems an N:N mapping between the control plane (SDN App) and the user-data plane (Network Element), it is in fact more a 1:1 mapping. The SDN Apps that implement each function have a counterpart on the user-data plane layer, while the HGW App has a counterpart on the switch, which basically implements the chaining logic according to the customer profile.

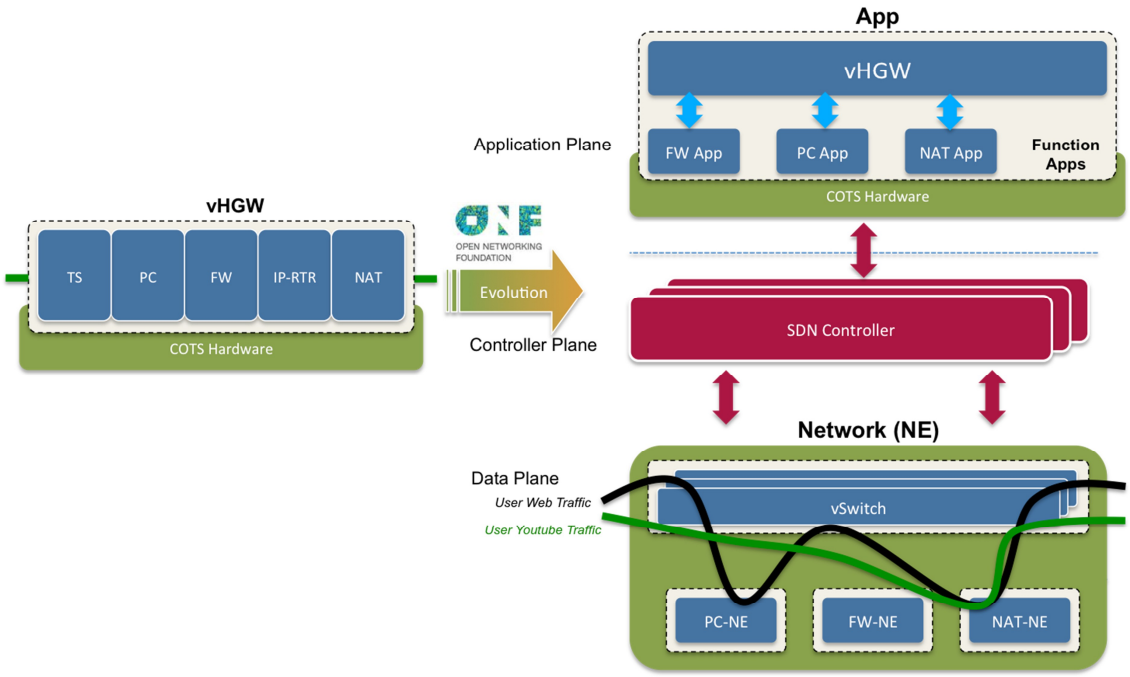


Figure 3.7 Software Defined Network (SDN): example Home Gateway

3.3.3 Combining SDN and NFV

NFV and SDN have been created by different standardization threads; however, they are complementary technologies; that is why many times they are referred to as NFV/SDN. Although they have value separated, combined they create an extra-value. The NFV technology brings the possibility of creating new network functions on-demand, placing them on the more suitable location and using the most appropriate amount of resources. However, this requires the SDN to be able to adjust the network accordingly, enabling network (re)configuration (programmability) and (re)sequencing of functions (chaining).

As NFV and SDN come from different SDOs (Standard Developing Organizations), at the time of writing this Deliverable, none of them has combined both architectures into a single one. For this reason, this section aims to seamlessly integrate NFV and SDN for SELFNET, taking the ETSI NFV architecture as a starting point and introducing the SDN paradigm. Firstly, the ETSI NFV architecture depicted in Figure 3.4 shows the VNFs (in the left part) which represent the virtualized network functions. Next, according to the SDN model, depicted in

Figure 3.5, the monolithic VNF is separated into three parts. Finally, integrating both concepts, results in the architecture depicted in Figure 3.8.

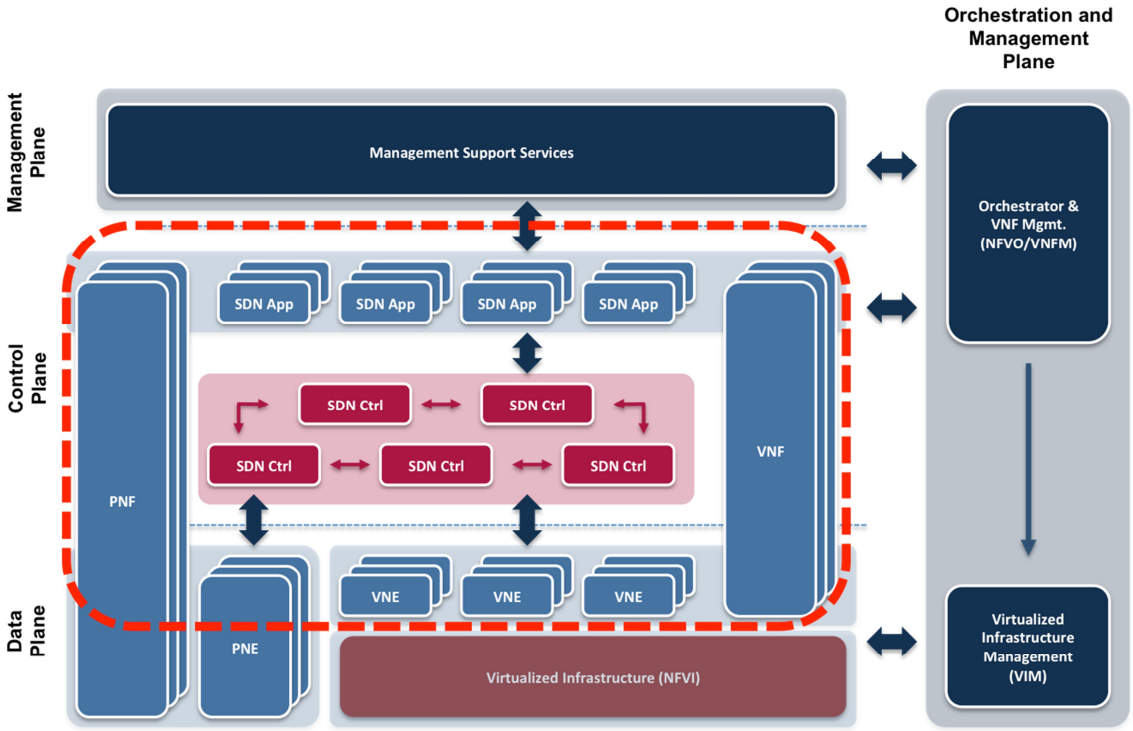


Figure 3.8 NFV and SDN combined architecture

The integrated architecture is compliant with the one defined by the ETSI NFV [4] changes are introduced regarding the additional layers. The naming of the components is another issue that need to be decided, since similar boxes have different names, depending on whether one looks at them from the NFV or the SDN perspective. In order to consider "legacy" components (non-NFV, non-SDN), we kept the physical NFs in the leftmost side of the dashed red square of the architecture, meaning that we may have **Physical Network Functions (PNF)**, which do not apply the NFV and SDN models. The same way, one may have virtualized NFs (VNFs), but with no SDN capabilities. For those, the **Virtual Network Functions (VNF)** naming is kept, as shown in rightmost side of the dashed red square. In the middle, all components are SDN-aware, meaning that they are split into three layers. In the bottom layer (user-data plane), one may have physical or virtualized Network Elements (NE), which can be **Physical Network Elements (PNEs)** or **Virtual Network Elements (VNEs)**, respectively. In this case, the names are chosen from the SDN world, since they describe the roles they are performing more clearly. On the controller layer, it is assumed that SELFNET may have multiple controllers at different levels, naming all of them **SDN Controllers (SDN Ctrl)**. Finally, for the control layer, we used the naming **SDN Application (SDN App)** is used. This case does not specify if it is virtual or not as it can be both, although it is believed that this layer will be mostly populated by virtual applications, considering that hardware specific utilization is declining.

3.4 Architecture Overview

Figure 3.9 illustrates the architecture of the SELFNET framework.

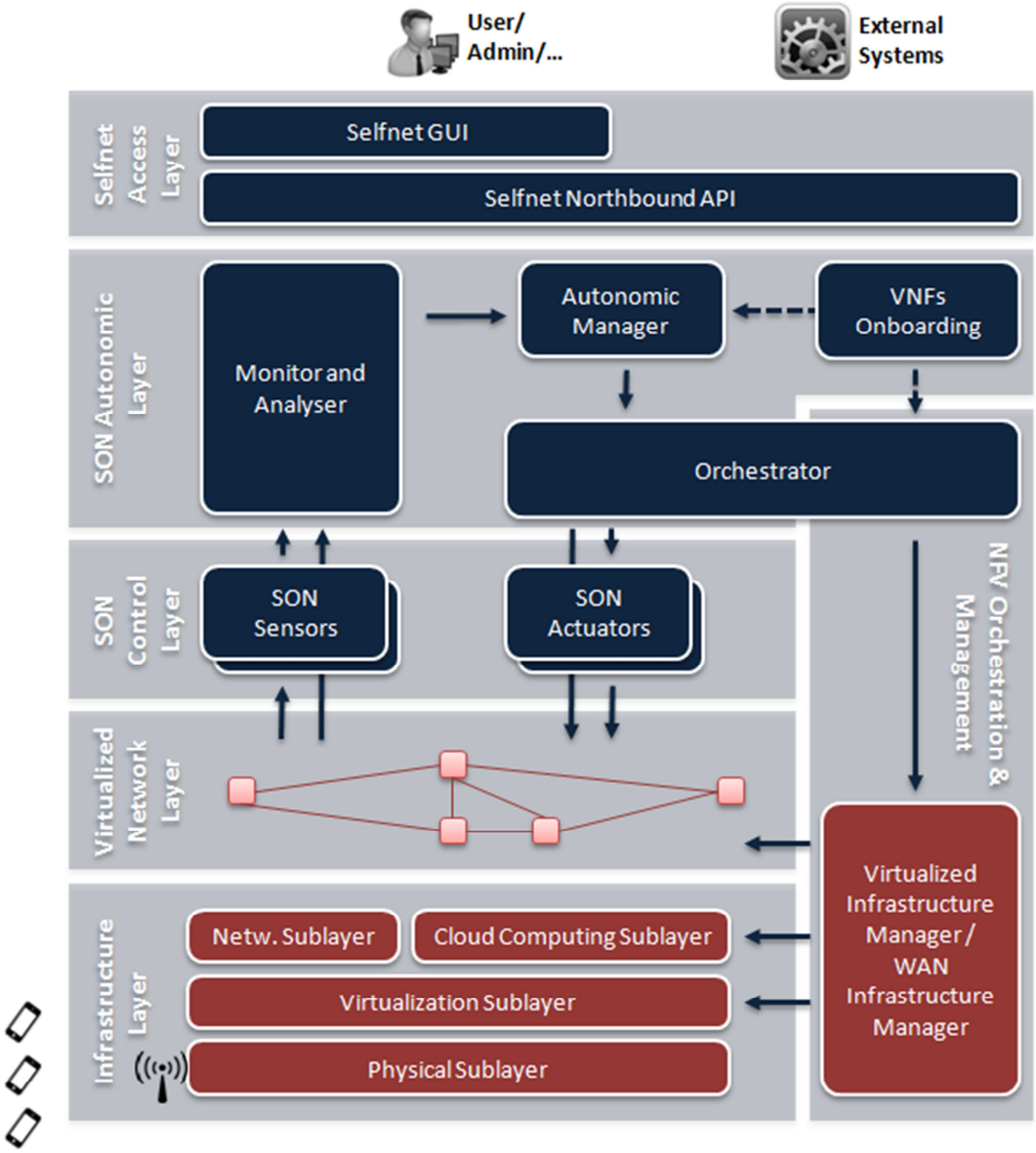


Figure 3.9 SELFNET Architecture Overview

Self-Organizing capabilities over 5G networks are provided by means of an architecture based on five differentiated layers with the following logical scopes:

Infrastructure Layer: This layer provides the resources required for the instantiation of virtual functions (Compute, Network and Storage) and supports the mechanisms for that instantiation. It represents the NFVI (Network Functions Virtualization Infrastructure) as defined by the ETSI NFV terminology [35]. All network functions managed autonomously by the SELFNET framework will be based on this infrastructure. To achieve its functionality, this layer encompasses different sublayers. The Physical sublayer provides physical connectivity, networking, and computation and storage capabilities over bare metal. The Virtualization sublayer provides virtualization capabilities to instantiate virtual infrastructures. Finally, the

Cloud Computing sublayer provides multi-tenancy support to the infrastructure layer together with a centralized point for facilitating the management of the infrastructure.

Virtualized Network Layer: This layer represents the instantiation of the Virtual Networking Infrastructures created by the users of the infrastructure as part of their normal operational plan and those created by the SELFNET framework as part of the SON capabilities. The layer is composed by a number of NFs interconnected in a designed topology in order to provide the functionalities required by the user. In the context of SELFNET, all Network Functions will be virtual functions and they will be chained across the virtual network topology.

SON Control Layer: This layer contains the applications that will enable the collection of data from sensors deployed through the entire system (SON Sensors) and the applications that will be responsible for enforcing actions into the Network (SON Actuators) as part of the enabling mechanisms to provide network intelligence in 5G networks. **SON Control Layer** and **Virtualized Network Layer** have associated Control and Data Planes of the network. These planes are not represented in Figure 3.9, but are shown in Figure 3.8.

SON Autonomic Layer: This layer provides the mechanisms to provide network intelligence. The layer collects from the network pertinent information about the network behaviour, uses that information to diagnose the network condition, and decides what must be done to accomplish the system goals. It then guarantees the organized enforcement of the actions that are determined.

The components of the SON Control and SON Autonomic Layers will be detailed in subsequent sections. An analogy is drawn here between network health and human health to facilitate the understanding of the main functions of the components in the chain of SELFNET SON:

- **Sensors and Monitor**: They act as nurses who measure and collect a patient's physical and mental (virtual) conditions such as body temperature, heart beat rate, weight etc., which are analogous to conventional QoS-level metrics.

- **Aggregator and Analyzer**: They act as a doctor's assistants who correlate the measurements and derive critical symptoms and trend (prediction) such as consistent high temperature, loss of weight, abnormal signs from scan, mental stress, etc., analogous to the SELFNET HoNs to allow diagnosis.

- **Decision Making Planner**: This is the doctor who diagnoses, i.e., identifies the disease (pending or existing network issues) and makes decisions on treatment, and possibly prognoses, i.e., predicts how the disease will develop with/without the treatment, and writes the prescriptions and treatment plan.

- **Action Enforcer**: This staff reviews the treatment plan, schedules the different stages of the treatment, and prepares the treatment e.g., an operation in a theatre by providing a list of required tools (Apps, mainly Actuators) and resources.

- **Orchestrator**: This staff organizes the required resources to support the staged treatment, obtains medicines and other treatment necessities/tools from the pharmacy and medical apparatus room (Apps Repository/**VNFs Onboarding**), and deploy the medical team to execute the treatment.

NFV Orchestration & Management Layer: This layer roughly corresponds to ETSI MANO [36] layer, and to its Basic Functions: Orchestration, VIM, VNF Management, i.e. Compute, Network, Storage. It is worth emphasizing that the control of the chaining of the NF applications is envisioned as a management functionality to be able to control the topology of the Virtual Network layer depicted in the figure as Network Controller (SDN App) and included logically in the VIM functionalities.

SON Access Layer: This layer encompasses the interface functions that are exposed by the framework. Despite the fact that internal components may have specific interfaces for the particular scope of their functions, these components contribute to a general SON API that exposes all aspects of the autonomic framework, which are "used" by external actors, like Business Support Systems or Operational Support Systems.

A GUI is also provided on top of the SON API where a network administrator can interact and configure SELFNET and also obtain the complete status of the network, acting as a command and control centre. This GUI will also enable the network administrator to stop, verify or manually enforce any of the actions that SELFNET is governing, allowing always network administrators to have control over their infrastructure.

3.4.1 Infrastructure Layer

The infrastructure layer envisioned in SELFNET has been intentionally aligned with the information available so far in terms of the architectural designs, principles and components of 5G Networks. SELFNET architecture has been designed to be as flexible as possible in order to deal with later modifications over such architectural decisions as part of the natural evolution of 5G networks.

The SELFNET infrastructure has been divided in different layers to split the functionality of the infrastructure in different architectural components. Figure 3.10 provides an overview of the infrastructure layer whose sublayers have been summarized in Figure 3.9.

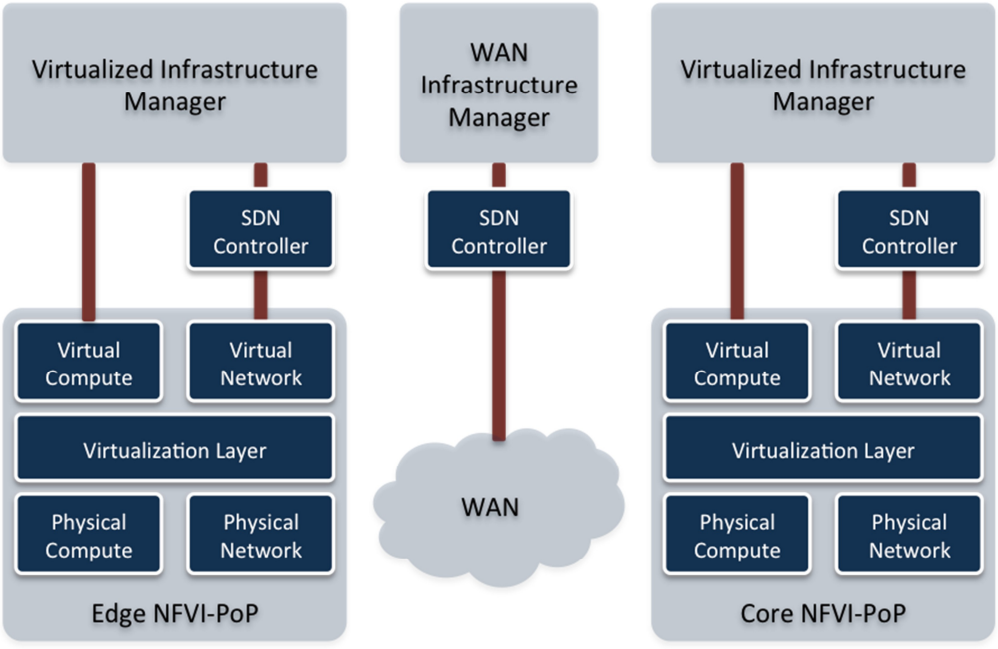


Figure 3.10 SELFNET Infrastructure Layer

3.4.1.1 Physical Sublayer

In the Physical sublayer, SELFNET infrastructure is based on the principles of mobile edge computing where a star topology is deployed in such a topology, a central logical location allocates a data centre to provide high computational and communicational capabilities and a number of other logical locations on the edges of the access network are connected to the central location to provide restricted and specific computational and communicational capabilities. It has been represented in Figure 3.10 with the central part and the edge parts of the figure, respectively. It has been defined a logical location as a way to logically control where different services are allocated within the architecture. However, from the deployment point of view, such logical location can be allocated either in different physical locations geographically separated or within in the same physical location. This concept would provide SELFNET with the flexibility to cope with the requirements posed by a large number of infrastructure deployments covering traditional 4G deployments and emerging cloud-RAN 5G deployments.

Communications between different elements of the infrastructure has to be considered from two different angles: physical and virtual connectivity. The physical connectivity to establish communications between different edge locations and data centre will be assumed by SELFNET using either existing/traditional communication channels or assuming a natural evolution of that communication channels to face the KPIs imposed by 5G networks. SELFNET is not going to explore any innovation in the data plane of these communications channels. An architectural decision that could take significant impact in terms of performance is to consider the usage of a high-end hardware switches with SDN support in the connectivity between edges and data centre to enable efficient data processing rates. This has been considered as an optional aspect to be analysed in SELFNET.

3.4.1.2 Virtualization Sublayer

On top of the Physical sublayer, SELFNET framework will use a Virtualization sublayer to provide the capability of providing virtual infrastructures on top of physical ones in order to enhance the management, isolation and consolidation of computational resources. This sublayer is envisioned as an interoperable and interchangeable layer where different virtualization technologies (hypervisors) can be plugged and accessed by means of an abstraction access technology. This sublayer will provide a significant number of added values within the SELFNET since that it will enhance the reliability, security and continuity of services. The virtual connectivity between different VMs will be performed using software-based switching solutions that enable the connectivity of different virtual machines together and can provides SDN support.

3.4.1.3 Cloud Computing Sublayer

On the control plane, the Control Computing sublayer will be able to provide multi-tenancy capabilities over the current virtualized infrastructure enabled by the lower layers. This multi-tenancy will enable different tenants to use resources in an isolated and controlled way within the same physical infrastructure. In essence, this sublayer will be in charge of managing the physical infrastructure and providing functionalities to create, delete and administer virtual infrastructures in a multi-tenant domain. The

optimization and control in the usage of physical resources within a truly multi-tenancy virtual infrastructure will significantly reduce capital costs and will be an enabling technology to open new exploitation scenarios where multiple network operators are sharing computational and communicational resources and where the same network operator is providing services to multiple customers simultaneously.

3.4.1.4 SDN Controller Sublayer

The usage of SDN-enabled switches is an architectural decision of the SELFNET infrastructure due to the fact that it will enable SELFNET to deal with the management of network services at two different ends: control and data plane. The combination of software-based and hardware-based SDN-enabled switches is being considered within the SELFNET architecture to provide more alternatives in terms of architectural locations and flexibility to deploy SDN App to better fit the purpose.

3.4.2 Virtualized Network Layer

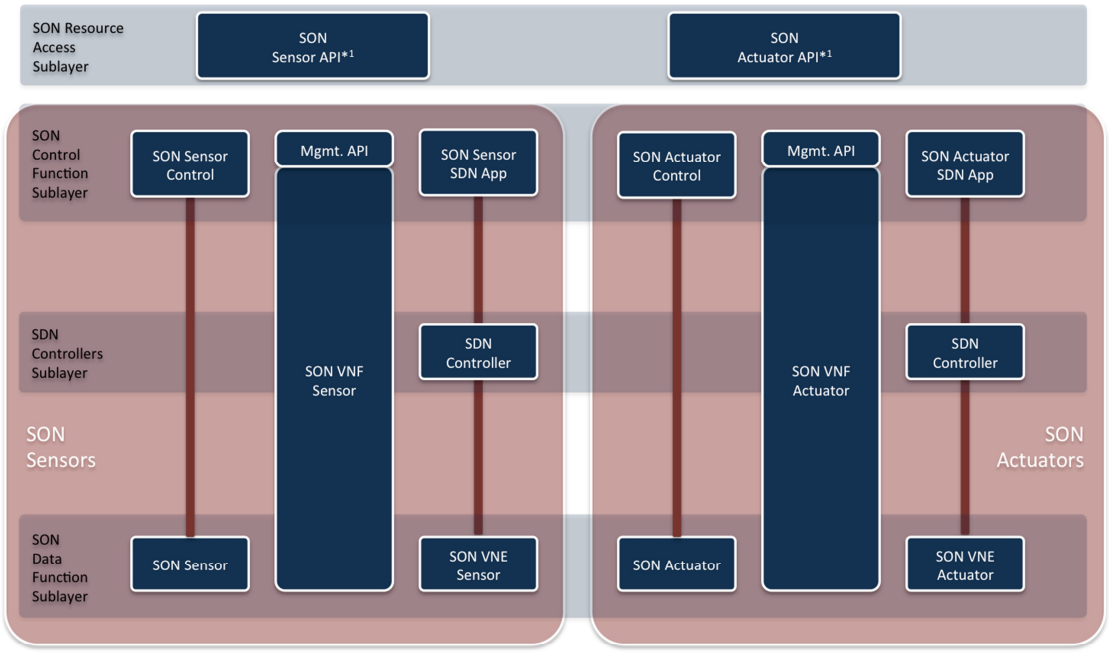
This layer represents the instantiation of a number of NFs and VMs interconnected in a designed topology in order to provide the functionalities required by the user. The Virtualized Network layer is logically divided between control and data planes and will be in charge of providing virtualized network functions. This point is where Figure 3.11 can be used to refer to VNE and SDN App to denote data and control plane respectively. Also, each application can be allocated in both data centre and edge locations. In the data plane, VNE will provide services over the network traffic circulated through the virtual machines where such VNE are running. In the control plane, it has been envisioned the usage of SDN Controllers in order to plug different SDN applications with such a controller. The number of SDN controllers will depend on the performance required by each controller, the number of flows being processed, scalability requirements etc. Therefore, conceptually SELFNET architecture has envisioned the differentiation of at least two logical places where SDN Applications can be logically allocated: an edge SDN controller and a data centre SDN controller in order to provide a mechanism to control the allocation of the SDN applications within the 5G networks.

It is worth mentioning that multi-tenancy support over the SDN applications running within the controller is an innovation that SELFNET will analyse in order to explore different ways to deal with the management aspect of SDN applications.

3.4.3 SON Control Layer

This layer contains the applications that will enable the collection of data from sensors deployed through the entire system (SON Sensors) and the applications that will be responsible for enforcing actions into the Network (SON Actuators) as part of the enabling mechanisms to provide network intelligence in 5G networks. Figure 3.11 depicts an overview of all the sublayers of the SON Control Layer.

The SON Control Layer must deal with complex network architectures in the Data Function sublayer and at the same time ease the management and deployment of novel services. To support these requirements two mechanisms play a pivotal role: the use of a homogeneous Actuation APIs and the abstraction of network infrastructures to simplify management and orchestration. A policy-based interface can combine these two mechanisms integrating monitoring and control functionalities in a common language. The role of the SON Control Layer is to translate autonomic network-wide policies into specific network elements' configurations.



*1 Represents a logical perspective; from a physical perspective, we can have one or more SON Sensor and Actuator APIs either available on top of each component of the SON Control Function Layer or a single instance in charge of interacting with such components.

Figure 3.11 SELFNET SON Control Layer

3.4.3.1 SON Data Function Sublayer

The SON Data Function Sublayer provides the VNEs executed in the data plane of all the components used by SELFNET framework. Although SDN concepts are of significant importance in the SELFNET approach, the fact that specific implementations of VNF may integrate as well control logic (i.e. legacy routing equipment or standalone network functions), leads eventually to an additional classification of the VNF according to this aspect: VNF with no control plane named simply as VNF in SELFNET terminology according to Figure 3.8, and VNF with control plane. Depending on the API accessed, it can be considered an SDN compliant VNE and proprietary VNE. The coexistence of all these options is expected to be the norm for the following years. This is why the reader can see different alternatives in Figure 3.11. VNFs can be conceptually divided into two categories dedicated to sensors and actuators, referred to as SON Sensors and SON Actuators, respectively. SON Sensors collect data related to network activity to be processed by the higher layers of the SELFNET network. SON Actuators apply network configuration that affect the way in which network traffic is processed and forwarded among networking nodes.

3.4.3.2 SDN Controllers Sublayer

This sublayer has already been explained in the infrastructure sublayer. In summary, it will enable the communication between the control and data planes of the SON Sensors and Actuators in the same way that it enables the communications between any VNE and SDN-Apps.

3.4.3.3 SON Control Function Sublayer

The Control Functions sublayer consists of all the functionalities that are required to cope with the control of the instances available in the data plane. These

functionalities will control VNEs using SDN Apps, proprietary control protocols or management APIs to interact with the monolithic VNFs. Control functions can be conceptually divided into two categories dedicated to SON Sensors and SON Actuators, respectively. They will be exposed through the SON Resource Access sublayer in order to be able to orchestrate and control the VNF components.

SON Control Functions are required to support the following functionalities. Firstly, they provide the representation of the data plane resources in the context of the orchestration and management procedures, typically they provide the endpoints to be invoked for the integration and delivery of higher level sensing/actuation concepts. Secondly, they provide the mapping of the sensing and actuation commands onto the proper control commands according to the actual implementation of VNE.

Control Functions can be designed in different ways: virtual machines hosting a single application, physical computing resources hosting a number of applications, virtual computing resources hosting a number of applications, etc. SELFNET will provide flexibility for most of them and will try to provide support for the most appropriate design to fit its purpose efficiently. Accordingly, instantiation of a control function may involve deployment of a virtual machine, or provisioning of apps in application containers.

3.4.3.4 SON Resource Access Sublayer

The SON Resource Access sublayer provides a homogeneous Sensing and Actuation API. It will make easier the integration of new SON Sensors and SON Actuators. In addition, it will enable the integration between the SON Autonomic layer and this layer in order to enforce the autonomic decisions.

3.4.4 Self-Organized Network (SON) Autonomic Layer

The SON Autonomic Layer is the top-most layer of the SELFNET architecture. This layer provides the mechanisms to provide network intelligence. The layer collects from the network pertinent information about the network behaviour, uses that information to evaluate the network condition, diagnose any pending/existing network issues, and decides what must be done to accomplish the system goals. It then guarantees the organized enforcement of the actions. This layer and its internal sublayers are depicted in Figure 3.12.

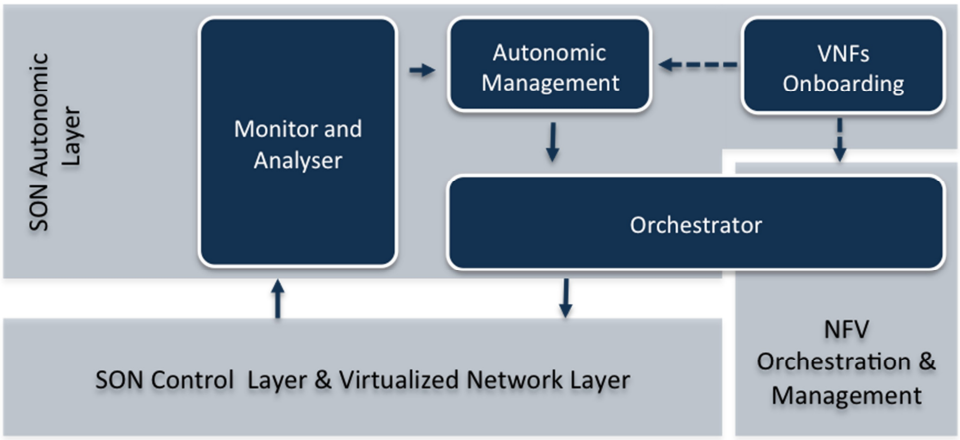


Figure 3.12 SON Autonomic Layer and Sublayers

In essence, the SON Autonomic Layer is split in four main sublayers: Monitor & Analyzer, Autonomic Management, Orchestrator, and VNFs Onboarding. These sublayers and their modules will be described in the upcoming subsections.

3.4.4.1 Monitor and Analyzer Sublayer

The main purpose of this sublayer is to provide a general overview of the framework that will be designed for monitoring and analysing the network behaviour or incidents. This sublayer is divided into three data processing levels, as shown in Figure 3.13. Each of them is briefly described below.

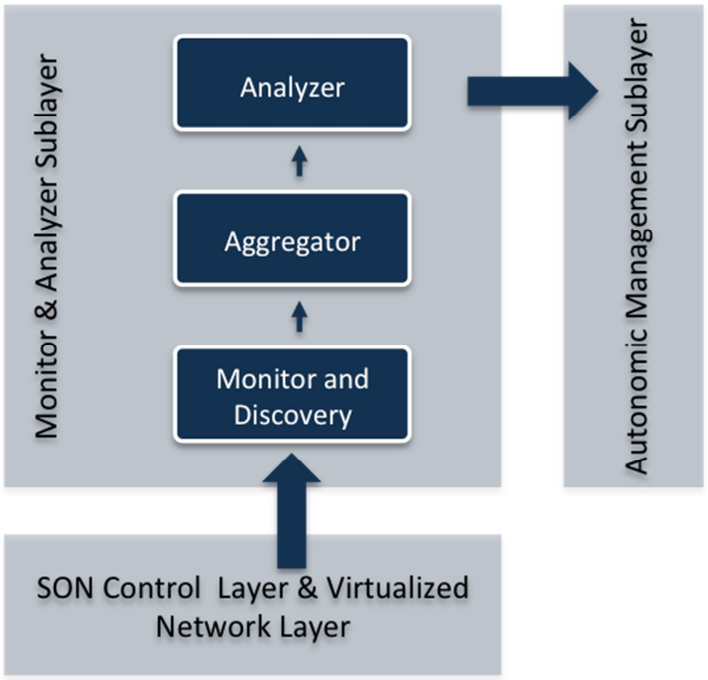


Figure 3.13 Monitor & Analyzer Sublayer

Monitor and Discovery Module

The Monitor and Discovery stage collects and stores all data from SDN-sensors and NFV-sensors. In addition, it must detect and notice changes in devices and NFV-Sensors involved in SELFNET. The required information is provided by SON Control Layer and Virtualized Network Layer. At this point, information provided by SDN/NFV sensors is differentiated from SDN/NFV devices. This differentiation is to speed up the processing tasks, and facilitate the later correlation/classification.

Gathered information is treated by a Data Management System (DMS). The DMS manages a database containing all the collected information. Among DMS responsibilities are storing/querying, access/privacy control or refresh DB content. It also involves removing obsolete entries, which do not correspond to the current state of the network. DMS also deals with orchestration of information distributed in different DBs or SELFNET regions, or with applying the required control access functions and privacy policies.

Aggregation Module

This module performs aggregation and correlation of the low-level metrics provided by the Monitor and Discovery Module. This may involve performing different actions

such as data normalization, verification or correlation. In order to facilitate the later processing stages, redundant information will also be removed. At the end of this stage, aggregated, higher level metrics must be available at later stages of processing.

Analyzer Module

The goal of the analyzer module is the analysis of information provided by the Aggregation Module, thereby deriving information required for facilitating decision making. For this purpose, a comprehensive analysis of the information received is performed. Activities in this stage are divided into five main sub-modules: identification, assessment, review, prediction, and situation awareness. They are described below:

- **Identification**. The main objective of the Identification sub-module is the recognition of anomalous or suspicious SELFNET behaviours. Identified situations could match with different natures, such as deployment of new NFVs or devices, congestion because of legitimate reasons, or suspicious threats labelled by Self-Protection sensors. Consequently, recognition of these events is required for allowing triggering Self-Optimization, Self-Healing or Self-Protection actions.

- **Assessment**. Once a new/suspicious situation is identified, the Assessment sub-module evaluates its relevance; a value which summarizes its impact is calculated based on predefined HoNs. It is important to highlight that the assessment will differ depending on the use cases features. For example, if an attempt of intrusion is detected, the impact of the situation will be calculated by taking into account Self-Protection measures, such as kinds of intruders, methods, pre/post conditions, or preview of the threat evolution. The assessment is in direct relationship with the latter decision making stages, and facilitates adopting SELFNET response in proportion with relevance.

- **Prediction**. A forecast of the coming situations is provided by the Prediction sub-module. It considers the global state of the system, and particular situations triggered by the Identification sub-module. This allows making proactive decisions and a better understanding of the Situation Awareness on SELFNET.

- **Review**. Whilst the Assessment sub-module deals with previously identified situations, this Review sub-module analyses the impact of decisions made. This allows an evaluation of whether to adopt decisions that will involve different course of action or to continue with the current strategies based on historical decisions for a similar scenario. Through such a review, it is also possible to improve the assessment of identified situations.

- **Situation Awareness.** Situation Awareness refers to the global situation of SELFNET, but also displays particular events discovered on the previous processing stages. In order to enhance the behaviour of the coming processing stages, this Situation Awareness sub-module summarizes the information gathered and calculated by them.

3.4.4.2 Autonomic Management Sublayer

The Autonomic Management Sublayer can be regarded as the “brain” of the SELFNET framework, which takes advantage of mechanisms in the field of self-organizing networks, artificial intelligence, data mining, and pattern recognition to enable autonomic and automated network management. As illustrated in Figure 3.14, this sublayer will provide the capabilities of self-healing, self-protection and self-optimization by means of proactively and reactively dealing with existing and/or potential network problems. This sublayer also defines the Tactical Autonomic Language (TAL) that specifies the resolution strategies to guide the automatic actions provided. The Autonomic Management Sublayer consists of the following modules:

- **Tactical Autonomic Language (TAL)** includes the autonomic language and its associated library, which define the autonomic strategies inside the SELFNET framework.

- **Diagnostic module** takes advantage of artificial intelligence, data mining and stochastic algorithms to provide intelligence in diagnosis of the network problems and provide the information of the best strategy to be taken. This will be achieved by using tactical strategies to determine the resolution actions to be taken in the network for the cases where no completely defined, well-known strategies about how to react exist.

- **Decision Making Planner module** in charge of deciding a set of corrective and preventive actions to deal with the identified and potential network problems, in both reactive and proactive manners, based on the incoming diagnostic information. For such purposes, this framework will interrogate the HoN Query Services in order to know the state of the network. This module will make use of two different approaches for providing a response. The first approach will be the direct application of the resolution strategies defined in the TAL. The second approach will be the integration of artificial intelligence algorithms guided by such tactical strategies in order to determine resolution actions to be taken in the network, even for the cases where there are not completely defined tactical strategies about how to react.

- **Action Enforcer module** is responsible for providing a consistent and coherent scheduled set of actions to be enforced in the network infrastructure. For this purpose, this module will receive and recognize the messages provided by the Decision Making Planner and will validate, organize and refine such messages by means of applying conflict detection and resolutions techniques, language refining techniques, etc. in order to provide an implementable plan ready to be enforced.

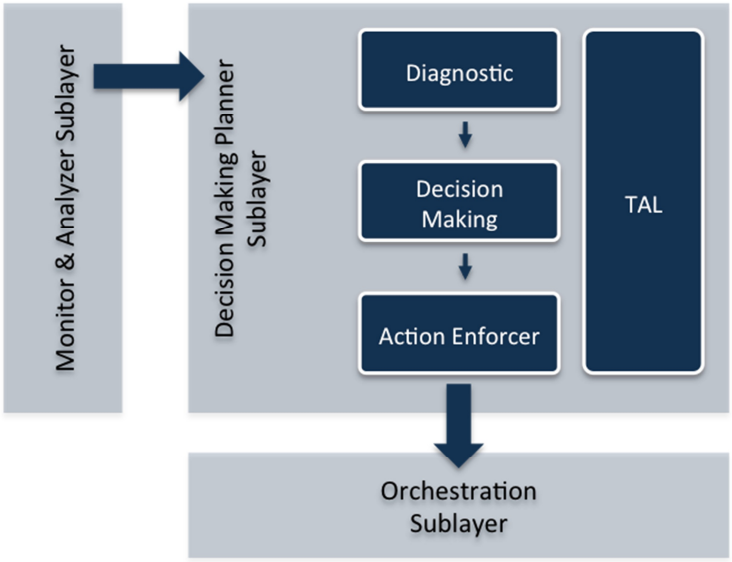


Figure 3.14 Autonomic Management Sublayer

3.4.4.3 VNFs Onboarding Sublayer

The VNFs Onboarding sublayer is composed by those VNF management functions, mechanisms and tools responsible for the encapsulation of the SELFNET actuators and sensors into common and homogeneous VNFs. The main target of the VNFs Onboarding is therefore to provide a unified abstraction of the SELFNET VNFs while exposing common lifecycle management primitives to be used for automated deployment, configuration, re-configuration and termination of any VNF.

This means that the VNFs Onboarding sublayer should provide mechanisms and tools to containerize the developed SELFNET actuators and sensors into encapsulated VNFs that can be managed, configured and controlled through common APIs. On top of this unified VNF abstraction that aims to standardize the way SELFNET actuators and sensors are stored, advertised and used by the SELFNET platform, the VNF Onboarding also provides automated mechanisms and procedures for the deployment of the encapsulated VNFs into the virtualized infrastructure.

With respect to the standardized ETSI approach [4] for VNF management and coordination, the VNF Onboarding sublayer advances the traditional ETSI NFV architecture and in particular the Management and Orchestration (MANO) part (as depicted in

Figure 3.15) with the aim of enriching its well-defined APIs for a common management, configuration and control of heterogeneous VNFs. The left side of Figure 3.15 shows the building blocks of the ETSI NFV architecture, highlighting in the dotted box the MANO components. The NFV Infrastructure (NFVI) comprises all those hardware and software components to be virtualized that build the environment over which the VNFs are deployed, managed and operated. The same NFVI can span across multiple physical location, e.g. geographically distributed data centres. In this case, the network interconnecting these remote locations is part of the NFVI itself. The Element Management System (EMS) is a key component in the NFV architecture since it enables the management of one or more VNFs, mostly for

configuration and lifecycle evolution actions. It represents (for most of the management actions) the access point to the VNF for the MANO components.

Moreover, the NFV MANO provides orchestration and lifecycle management at two levels: for physical and/or software resources building the NFVI, and for VNFs. Therefore it focuses on all virtualization specific management tasks within the ETSI NFV architecture, and it is built by three main components: the Virtual Infrastructure Manager (VIM), the VNF Manager (VNFM) and the NFV Orchestrator (NFVO). The VIM is basically responsible for controlling and managing all those hardware and software components deployed in the NFVI (compute, storage and network resources), providing virtualization primitives to other MANO components and maintaining the association of the virtualized resources to the physical ones. On top of the VIM, the VNFM is responsible for the actual lifecycle management of VNF instances; most of the VNFM functions are assumed to be generic common functions applicable to any type of VNF, like instantiation and configuration, software upgrade, modification and termination. Ad-hoc VNF functions may be also implemented according to the specific type of VNF. As a supervising and coordination component, the NFVO is responsible for the composition of multiple VNFs in network service chains. In practice, the NFVO takes care of instantiating new network services by coordinating one or more VNFMs and VIMs; it is responsible for the lifecycle management of network service chains, dynamically re-configuring inter-VNF connectivity or VNF instances when needed.

In SELFNET, the goal is to containerize both VNF and EMS components of the ETSI NFV architecture to provide a common and uniform approach to lifecycle management across all the heterogeneous SELFNET sensors and actuators VNFs that will be developed. In addition, the enhancement of pure management and orchestration functions performed by MANO components (NFVO, VNFM and VIM) will provide automated deployment and configuration functions for the encapsulated VNFs.

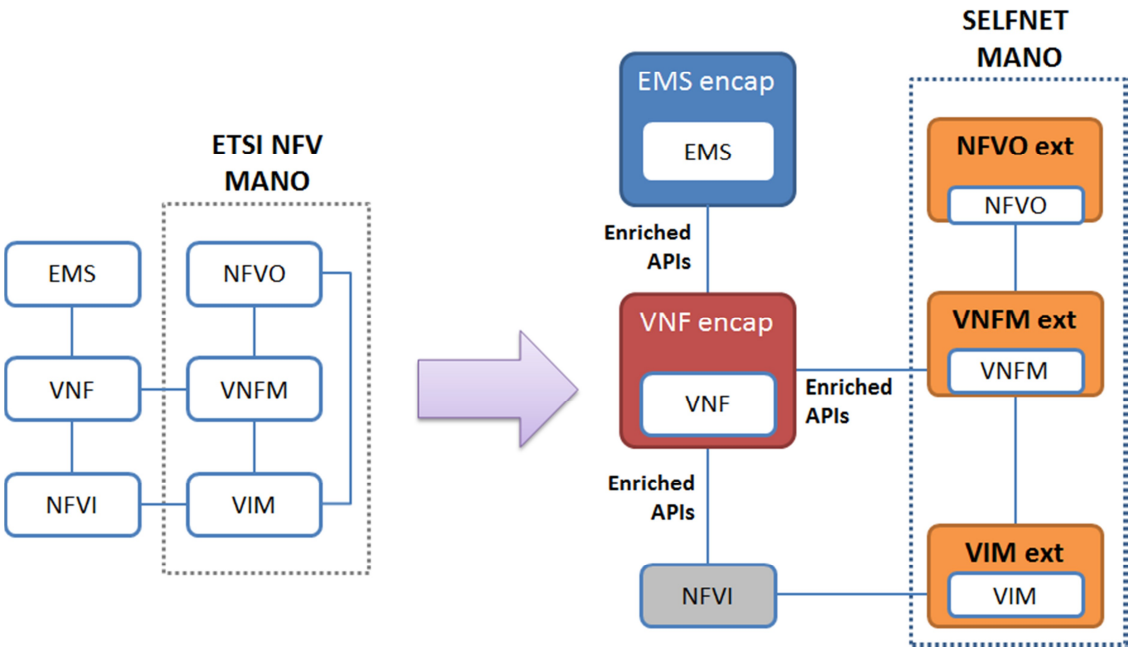


Figure 3.15 SELFNET VNF Onboarding Sublayer: Evolution of ETSI NFV and MANO Functions

3.4.4.4 Orchestration Sublayer

The Orchestration Sublayer is in charge of the real deployment of the NFV and SDN Apps (mainly actuators, and/or sensors depending on different use cases), following the specified instructions (action plans) from the Decision Making Planner Sublayer. As shown in Figure 3.16, this sublayer is composed internally by three modules: the Orchestrator whose role is to receive and process action requests, and implement the actions; the Application Manager who enables the Orchestrator with management capabilities of the VNE, SDN and VNF Apps; and the Resources Manager who allows the management and configuration of infrastructural resources to support the actions of the Orchestrator. Further description of these elements is available below.

Orchestrator module

- **Apps Deployment**. This sub-module processes the received action plans from the Decision Enforcer module, resolves the dependency/order/priority among different actions, and executes the actions by calling and deploying the selected Apps to the right place at the right time.

- **Resource Brokering**. The role of this sub-module is to provide a resource brokering service to optimize system-wide resource usage especially virtual/cloud resource brokering. This also ensures that the Apps are allocated with sufficient resources to execute their actions and fulfil their tasks.

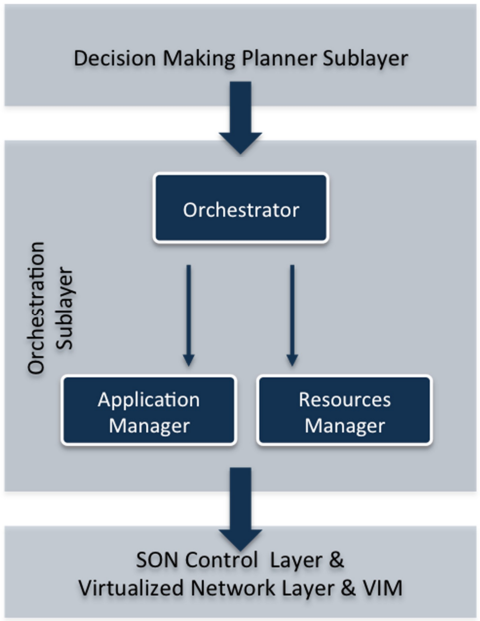


Figure 3.16 Orchestration Sublayer

The translation of the requirements in resources can be obtained through resource mapping algorithms. The result of the mapping algorithms is a workflow that after completion will fulfil the intent. Moreover, to execute the workflow, the Orchestrator will process the dependencies between the steps in the workflow so that an ordered list of steps is obtained. A single step can be an action on an application or infrastructure resource, which are available through the Application Manager and the Resources Manager respectively.

Application Manager Module

The main role of the Application Manager is to manage the lifecycle of the Apps, thereby enabling the Orchestrator to install, remove, update, configure, start/restart, stop or resume a selected App based on the action plan being executed. A uniform application layer is provided to the Orchestrator for executing the actions via deploying Apps. Moreover, the Application Manager maintains the current status of the Apps, which can be queried by the Orchestrator.

This module deals with provisioning both of data layer artefacts that are not subject to virtual resource management but rely on deployment of application components in application container that may be in a VM provisioned in earlier steps, and control layer artefacts that are linked with associated data layer resources via the appropriate control APIs and that are responsible for abstracting the NFV Apps under the Sensor/Actuator Abstraction API. To fulfil this set of events, the Application Manager will use processes common in IT environments to configure applications, such as configuration agents, specific protocols, automation tools or scripts.

Resources Manager Module

This component provides a reference point for the Orchestrator to interact with the cloud controller and network controller. Moreover, the Orchestrator can use this component to request the provisioning of virtual resources and subsequent management. The Resource Manager provides an abstract, uniform representation of available resources and their dependencies to facilitate the successful call, deployment and operation of the Apps by the Orchestrator.

Also as a part of its role, the Resources Manager is to provide an overview of the resources, which will equip the Orchestrator with service/application and resource mapping capabilities. The Resources Manager will have means to access the availability, discovery and current load of resources. In addition, although this component has limited autonomy, it should still be able to perform automated management and optimization procedures, e.g. releasing virtual resources that are idle for some time.

3.4.5 NFV Orchestration and Management Layer

This layer contains the management capabilities to control both compute infrastructures and network infrastructures available in the architecture. Figure 3.17 shows the different components available in this layer.

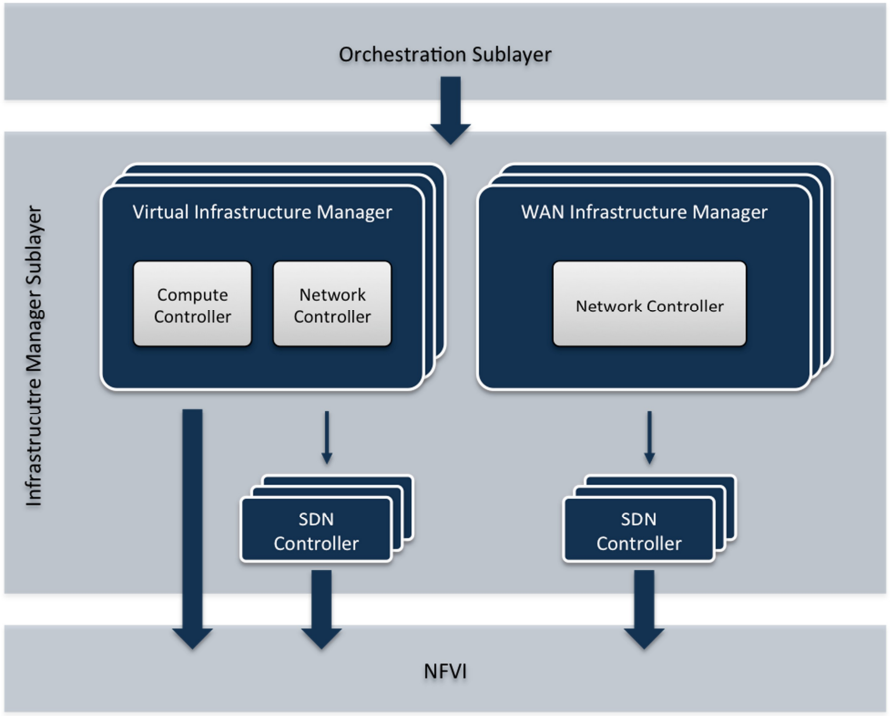


Figure 3.17 NFV Orchestration and Management Layer

3.4.5.1 VIM Cloud Management Sublayer

The VIM is a multi-tenant service platform used in data centres to provide cloud computing services (e.g. Open Stack). Through this platform tenants previously registered in the platform, can request infrastructure resources such as computing, network, storage or other supporting resources (e.g. load balancers, DNS, etc.). In NFV infrastructures, VIMs are used to manage data centres that can be in a central location or at the edge of the network, also known as PoPs. In SELFNET the VIM will provide the necessary resources for the provisioning of SDN Apps, VNFs or other components deployed on top of COTS. At the north of VIM, the Orchestration Sublayer, more specifically the Resources Manager, will request resources (e.g. VMs, internal virtual networks) that will be provisioned using hypervisors and SDN controllers.

3.4.5.2 WIM NFV Management Sublayer

The Wide Area Network Infrastructure Manager (WIM) is the wide area network counterpart of the VIM. Likewise, it is a multi-tenant service platform used by network operators to control the networking services. In legacy environments, WIMs typically use technologies such as Multiprotocol Label Switching (MPLS) which were not designed to support NFV services. The movement to SDN in the WAN plays an important role to fulfil these novel services with heavier dynamic requirements. In SELFNET the WIM uses SDN controllers to provide dedicated and isolated virtual networks. These virtual networks, which enable the Virtualized Network Layer are requested at the north by the Resources Manager, part of the Orchestration sublayer. This layer provides the enabling technologies to perform the deployment of new SDN Apps within the SELFNET framework by interfacing with the SDN Controller sublayer. The SDN Apps running in this layer will be provided by a number of other layers of the SELFNET architecture. For example, the NFV Orchestration and Management Layer will provide the SDN Apps for the management functionality to be able to

control the topology of the Virtual Network layer. Moreover, the SON Control Layer will contribute to this layer by providing the SDN Apps for the monitoring of network metrics and for the enforcing of actions within the network. Finally, this layer will also provide support to perform the deployment of non SDN-compliant control applications if it is appropriate to optimize the control plane of the architecture.

3.4.6 SELFNET Access Layer

The Access Layer is located at the top of SELFNET architecture and is the interaction point between the service administrator and service platform, providing an abstraction to manage the service's lifecycle. As shown in Figure 3.18, this layer is composed by firstly a northbound Application Programming Interface (API), divided as a set of APIs with very specific goals which are based on a Representational State Transfer (REST) and secondly a Web Graphical Interface (GI).

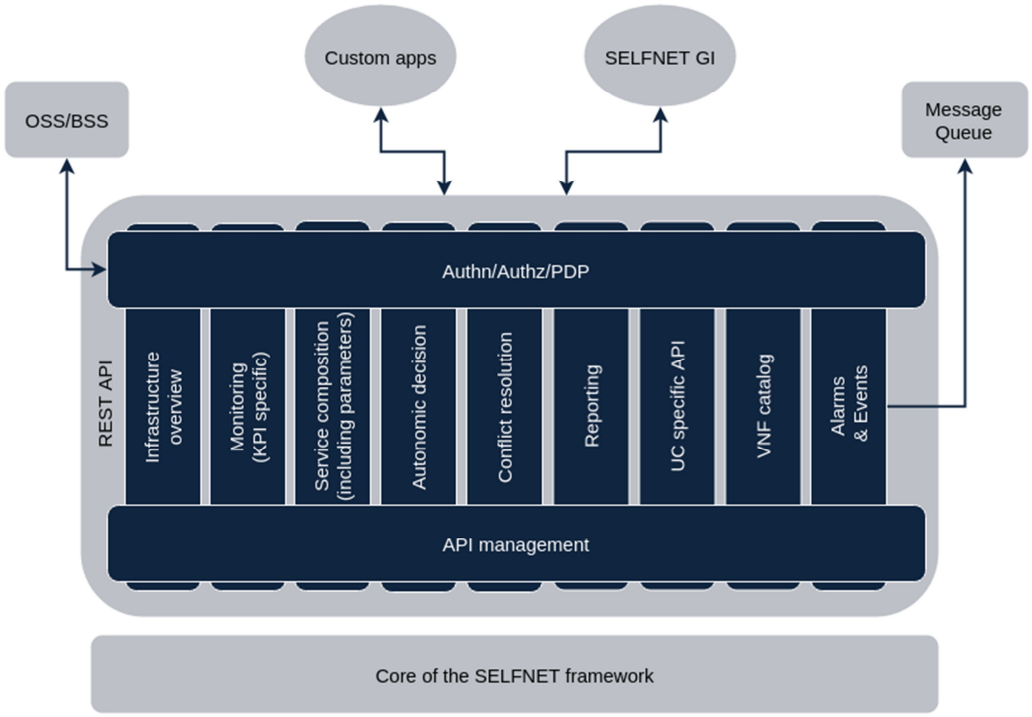


Figure 3.18 SELFNET Access Layer

3.4.6.1 SELFNET Northbound API Sublayer

The northbound APIs' main goal is to provide a network abstraction, i.e., a uniform way of communication between the control layer and the user interface while producing an abstraction for GI interactions. The GI is heavily dependent on the REST API, and these components will interact with each other in order to favour a simple way of work hiding the complexity from the administrator.

These APIs provide interfaces to control and manage the SELFNET's services lifecycle, divided in authentication, authorization and a Policy Decision Point (PDP), infrastructure overview, monitoring, service composition, autonomic decision, conflict resolution, reporting, UC specific API, VNF catalog and alarms and events. Although at this stage this API has not been designed yet and it will be done as next step along the road map of SELFNET project, the following list represents some functionalities envisioned so far.

AuthN/AuthZ/PDP

The AuthN and AuthZ API control not only the access to the platform, but also the actions that each user can perform, i.e., manage user groups and permissions. Within this API, exists a PDP that, via a service adapter, interacts with other layers, like OSS/BSS, and controls higher permissions out of SELFNET's scope. This is the entry point not only for SELFNET's GI but also allows for the appearance of other custom applications to be developed in the future or the integration of already existing applications.

Infrastructure Overview

The Infrastructure Overview offers functions to control and manage SELFNET service provider physical resources consumed by a specific service. Using this, the service administrator can evaluate the service performance.

Monitoring

The primary goal of the API Monitoring is to facilitate the network administrator to understand if all SLAs or KPIs are being fulfilled as requested. Through this, the administrator will be capable of recover HoN, QoE and QoS metrics.

Service Composition

The Service Composition API offers an overview of the service, i.e., all the VNFs that composed the service, but also an interface to control and manage this VNFs. Changing service's SLAs or KPIs and manual operations like scaling, removing, re-configuring or migrating the service will be available on this module.

Autonomic Decision

Based on the defined SLAs and KPIs, SELFNET will perform autonomic decisions, like scale service's physical resources. The Autonomic API will not only list these decisions but also allow a feedback system that will improve the data mining system responsible to improve these decisions. In addition, it will provide capabilities to assist in the configuration of the autonomic policies that govern SELFNET self/organized capabilities.

Conflict Resolution

Whenever an autonomic decision creates a serious conflict between rules and it cannot be resolved by SELFNET SON automatically, some level of human intervention will be required, and thus the Conflict Resolution API will be called to action providing methods to solve the conflicts and overrule actions. In fact, the network administrator has the privilege to stop, verify or manually enforce any of the actions.

Reporting

All service logs will be available through the report interface, differentiated by its own category and level, so the logs can easily be traced by service, date and level.

UC Specific API

Any specific API, related to a Use Case, can be included in the SELFNET northbound. This adaptation falls under the UC specific API.

VNF Catalog

In order to have an overview of the available VNFs there is an interface, VNF Catalogue, responsible to list and describe each VNF available on the SELFNET's catalogue. The services can query this interface in order to select which VNF to use in different situations.

Alarms & Events

In order to report every alarm and system event, e.g., whenever a VNF fails or a VNF instance is scaled, there is an alarm and report interface. These operations will be sent to an external message queue that will be used to report this cases to systems that need this information. This module allows a control over who receives a specific alarm and where an alarm must be sent.

3.4.6.2. SELFNET Graphical User Interface Sublayer

The GI will be the main interaction point between SELFNET's operators and the SELFNET framework. In order to retrieve and send information to/from the SELFNET's framework, the REST API client allows seamlessly accessing SELFNET Northbound APIs' features. All information displayed by the GI as well as all the features provided by it will use SELFNET Northbound APIs' provided features. GI will authenticate its usage by requesting users to insert a valid set of credentials and not only check if a given user can access the SELFNET's GI but also identify the respective role of the authenticated user. This role will be used by GI to filter which features will be unlocked and displayed to the user.

SELFNET's GI will allow viewing and managing SELFNET both on a high level and on a low level. On a higher level, allowed users will be able to see the current status of SELFNET monitoring system's KPIs as well as listing system errors, messages and warnings. Users will be able to audit SELFNET's autonomous decisions allowing users to understand if autonomously taken actions are valid. Users will also be able to take actions on these autonomous behaviours, correcting problems that may arise. As mentioned before, SELFNET will provide a low-level view on SELFNET's deployed sensors and devices listing them and allowing selecting each one of them in order to view its information or take an action. For each device, its performance, logging information and errors will be available allowing operators to check the status of each one of them. Furthermore, the connections with other devices and sensors will also be listed allowing operators to understand its interactions and communications flow. By using this GI, operators will be able to take actions on these sensors' and devices' behaviours by reconfiguring their properties or reconfiguring to which or how these devices and sensors interact with each other.

3.4.7 Summary of SELFNET Architectural Layering Structure

Figure 3.19 shows a complete graphical summary of the different sublayers described in the previous subsections in order to enhance the readability of this document.

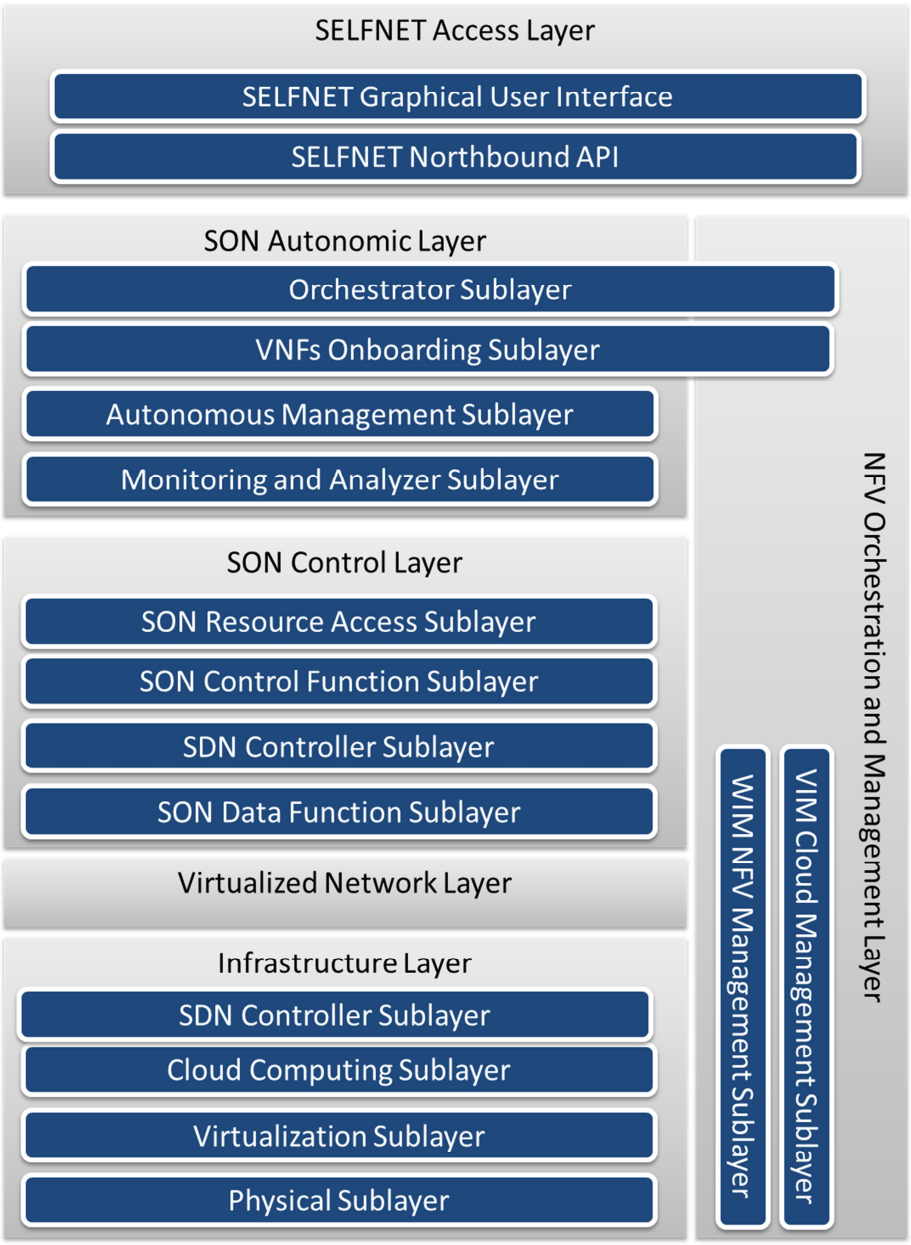


Figure 3.19 Structure of the Architectural layering of SELFNET Framework

4 SELFNET Use Cases

To demonstrate the self-organizing networking capabilities of the SELFNET framework, three uses cases are designed in this section, to be deployed and operated on the same paradigm as specified in the SELFNET reference architecture. The development of the proposed SELFNET system has also been primarily driven by the specification of three independent, ambitious use cases that will play crucial roles in realizing the highly autonomic network management capabilities required by 5G networks. These use cases, including self-healing, self-protection and self-optimization, are defined to meet the challenging 5G requirements and to show the key functionalities and huge potential and capacity of SELFNET. Innovation has been emphasized in the design of these use cases to greatly upgrade the current 4G network management practices to the next-generation level. For instance, all the use cases aim to achieve not only reactive, corrective actions but also proactive, preventive measures against potential or forthcoming network problems or challenges in terms of fault/failure risks, cyber-attacks, QoS/QoE maintenance and enhancement and so on, far beyond the state of the art. The successful design and implementation of these use cases will significantly improve the overall performance of 5G networks in reliability, availability, security, user experience, etc., all of which will jointly contribute to achieving the ambitious 5G KPIs in reducing service creation time and OPEX/CAPEX, minimizing service downtime, whilst optimizing users' QoE.

4.1 Use Cases Overview

4.1.1 Self-Healing Use Case Overview

This use case will focus on providing self-healing functionalities for detecting and avoiding network failures that may occur on the network infrastructure. As of today, networks are complex sets of heterogeneous and vendor-dependent equipment that use proprietary management applications, which implies a huge cost, a large effort, and a time-consuming process to manage all the network elements. Therefore, it is expected that 5G infrastructure, integrated with new technologies such as SDN, NFV, SON and the Cloud, will lead to a major paradigm shift from configurable to programmable networks, which will facilitate advanced self-healing capabilities.

Proactive self-healing for resource/power supply

This scenario addresses the need of constant monitoring of the resources and power supply on the network infrastructures. One of the main innovations of this scenario is the detection of network failures that trigger alarms allowing proactive actions to be taken before to correct these failures before they become critical or even lead to a serious outage. One of the technical challenges is to provide an intelligent control of precision cooling and critical power in order to achieve better proactive self-healing capabilities. Moreover, SELFNET will monitor not only physical but also virtual resources to ensure that the virtualized functions and operation environments will not fail due to the shortage of the required resources.

Reactive self-healing in critical/disaster/unpredictable scenarios

This scenario addresses the need for a reactive self-healing functionality as a necessary backup. Moreover, prediction-based proactive actions may be unsuccessful, and as a result a failure is not avoided. Therefore, a fast reactive action

is activated. One of the technical challenges of this scenario is to provide a quick deployment and execution of self-healing VNFs in order to mitigate the network failures and restore the network infrastructure to a normal operation state.

Proactive self-healing based on Network Slicing and Cyber-Footing Human Dynamics

This scenario addresses the need of verticals, e.g., new user groups with independent business models that depend on the availability of networking services. SELFNET self-healing concepts will address this challenge by enabling a cost-efficient control of strict levels of coverage, redundancy and availability based on proactive measures as well as timely healing avoiding negative implications on the services of the verticals.

One of the technical challenges of this scenario is to provide self-healing mechanisms that guarantee network slice SLAs in a cost-efficient way by providing actions re-establishing pre-defined levels of SLAs (resilience, security and availability) when they got lost. Moreover, SELFNET based on collected historical references from the network elements will use data mining and learning algorithms (identification of cyber-footing human dynamics and classification of infrastructure metrics) in order to predict high resource demands before they happen and take actions before these demands lead to even more critical mobile traffic situations.

4.1.2 Self-Protection Use Case Overview

This use case will focus on providing self-protection capabilities for detecting and mitigating potential cyber-attacks. Although cyber security is a well-known challenge required for covering all layers of any ICT system, it is expected that 5G will still be a major challenge due to the massive number of connected devices. They can be compromised by attackers to serve as stepping stone for flooding the 5G network with useless traffic so as to cause disruption in user experience.

In this use case, the SELFNET framework will be capable of addressing two kinds of cyber-attacks. Firstly, the detection and mitigation of Distributed Denial of Service (DDoS) attacks, which are actually being conducted by attackers after compromising users' devices for building a botnet. Botnets are one of the most powerful cyber threats nowadays for subverting communication links. Secondly, the detection and mitigation of virus spreading pattern for cognitive radio networks' attacks, which have a high relevance in 5G networks. The attackers' objectives are to manipulate the cognitive radio components in order to gain operation advantages in 5G networks, through self-propagating viruses.

4.1.3 Self-Optimisation Use Case Overview

This use case will focus on video networking optimization since it is widely envisioned that Ultra High Definition (U-HD) video applications are a main driver of deploying 5G networks. In recent years, video traffic has dominated the bandwidth of Internet and mobile networks, and this domination is ever-increasing, e.g., Cisco forecasts video traffic to account for nearly 75% of global traffic by 2019 [37].

One of the principles which will be applied for self-optimization is to empower the RECEIVER to influence the quality he wants to receive from a video stream. However, in order to maintain network stability and to ensure fairness to all users, SELFNET will perform autonomic actions, that are transparent to the user. This concept is very unusual as normally the sender decides how to insert a data stream

into the network. Today the originators of data streams are mainly the big service providers (Google, Facebook, etc.) and therefore regulation bodies have a difficult task in deciding between market pressure and consumer interest. Large service providers are lobbying for traffic shaping while regulators would like to preserve network neutrality.

High-quality video with improved QoE on any device anywhere at anytime

This scenario addresses the requirement to deliver high-quality video streaming services to users, including new services at U-HD spatial resolutions, in a manner that satisfies the expectations of 5G devices and services. The focus of service delivery is placed on achieving a consistently high QoE for the user, irrespective of underlying quality of service conditions through advanced optimization and adaptation mechanisms.

One of the biggest technical challenges (and thus innovations) in this scenario is to provide real-time methods of estimating QoE from both the compressed and uncompressed domain of U-HD videos, including encrypted streams, and then to intelligently deploy SELFNET actuators such as Media-Aware Network Elements (MANEs) to ensure that expected QoE levels are maintained or further improved.

Interactive video applications using U-HD and HD resolutions anywhere at anytime

As consumers migrate to new 5G services promising high bandwidth and low delay, they are likely to explore the 5G capabilities to their maximum. It is therefore likely that they will expect to be able to become increasingly engaged in demanding bi-directional, interactive video applications that are currently only available in broadband wired networking environments. This may also be accompanied by the emergence of new services where end users can stream video content acquired by mobile devices in real time (e.g., for collaborative video applications such as entertainment or surveillance) rather than uploading pre-recorded sequences to a content delivery network or social media platform.

The technical challenges in this scenario are to ensure that uplink bandwidth can be provisioned at both ends of the video session, even when massive numbers of such sessions are concurrently happening. This use case scenario looks to ensure that network bandwidth is optimized through the use of the most efficient video codecs rather than what may be available on the mobile device.

Ensuring the video content of M2M video applications is fit for purpose

New M2M video applications such as automated video surveillance are likely to be commonplace in future networks. These applications can be both bandwidth hungry and demanding in terms of real-time operation. This scenario addresses the requirements of quality and service continuity for such services at scale, when competing with consumer U-HD video traffic. An example for M2M video is work piece control in manufacturing which needs high resolution and fast transmission.

In this scenario, the technical challenges arise from the different quality evaluation methods required by M2M applications. Rather than QoE metrics for human consumers that estimate perceptual quality, new metrics and estimation tools must

be found that consider the utility of a video in performing a particular mission-critical task or aiding an automated decision making process.

Reduce the end-to-end energy consumption of the video delivery network

This scenario runs across the previous three scenarios and considers how to optimize the energy usage of the video content networks described in the previous three scenarios.

The technical challenge is to monitor the energy consumption of all network devices and functions and to proactively enable and disable devices and functions in a way that both ensures that the objectives of the previous three scenarios are met and concurrently minimises energy consumption on the end-to-end path. Normally energy saving and quality are antipoles, but there is room for a trade-off when excess bandwidth is to be distributed. The starting point is: whenever the bandwidth is not fully used there is room for energy saving.

4.2 Self-Healing Use Case

The aim of this use case is to demonstrate how the self-healing capabilities of the SELFNET network management framework can be applied to deal with a wide range of detected or predicted network malfunctions and failures, leading to a remarkable reduction upon OPEX and an improvement of QoE/QoS provision in 5G systems. The self-healing SDN/NFV sensors will enable the detection of common failure/malfunction in the current network infrastructure, such as hardware/software failures/faults, infrastructure/operation vulnerabilities and power supply interruption issues. Then, SELFNET will analyse the information provided by the sensors and apply recovery actions if needed, in order to mitigate the anomalies, thereby returning the network infrastructure to a normal operating state. These recovery actions will be enforced by the use of self-healing actuators. Moreover, SELFNET self-healing capabilities are not just about making remedies to faulty network components, they are also about providing safety, resilience and availability actively by providing not only reactive but also proactive measures. Therefore, SELFNET self-healing capabilities go beyond the traditional self-healing definition that follows a “Break and Fix” approach. If the network performance is downgrading or part of the infrastructure is failed in certain circumstances that may cause network failures and disruption of services, SELFNET self-healing capacities will also be triggered to take the most appropriate proactive healing actions based on SELFNET intelligence, which will allow the system to mitigate or avoid these failures and disruptions before they become critical. Thus, by extending the self-healing capabilities of the SELFNET framework, SELFNET will be able to provide network intelligence-based self-detection, self-repairing, self-configuring and self-management features in the network infrastructure towards maximising the reliability and availability of the 5G mobile network.

4.2.1 General Background

It is expected that 5G infrastructure, integrated with new technologies such as SDN, NFV, SON and the Cloud, will lead to a major paradigm shift from configurable to programmable networks, which will facilitate advanced self-healing capabilities. Firstly, the introduction of autonomic principles on SDN would enable an immediate detection and reparation of any malfunction or network failure [38]. Secondly, using NFV could significantly reduce the OPEX and service recreation/redeployment/

recovery time. Therefore, SELFNET is expected to yield sustained quality of services under critical situations in terms of service continuity, availability and resilience by predicting/identifying network faults/failures and then making proactive/reactive remedies.

4.2.2 Storyline

This section describes several scenarios where existing or potential failures are detected or predicted, and shows how the self-healing functionality is triggered to automatically respond to such problems.

4.2.2.1 Scenario 1 - Proactive self-healing for inadequate/misallocated resource supply and App aging

Network infrastructures are constantly under pressure and test for their complex operations that demand sufficient resources supply. For instance, electricity supply is essential to keep the whole network system up and running for uninterrupted operations. Sensors can be deployed to monitor the energy distribution system, including generators and their power output, rack conditions, fluid leaks, batteries and temperature fluctuations in hot and cold aisles, in order to trigger alarms allowing proactive actions to be taken to correct problems/malfunctions before they become critical or lead to a serious outage. Moreover, an intelligent control of precision cooling and critical power may be performed in order to achieve better proactive self-healing capabilities. By extending and applying the concept in this power supply example to generic network resources, SELFNET self-healing will target to monitor not only physical but also virtual resources supply to ensure that the virtualized functions and operation environments will not fail due to the shortage or misallocation of the required resources, through the deployment of Virtual Resource Broker actuators. This scenario is demonstrated in Figure 4.1.

To achieve the above scenario, firstly constant monitoring and control of the network resource usage and infrastructure performance will be in place to strengthen the robustness of the infrastructure. Furthermore, the self-healing analyzer will infer HoN metric reports based on infrastructure QoS metrics and Service level Agreements (SLA) indicators. Consequently, the self-healing diagnosis intelligence will derive the potential problems and the decision making intelligence will release proactive healing responses. It should also be noted that all the information collected from the network infrastructure will be saved on a healing database, including the network response to the proactive healing actions. If the healing actions are unsuccessful, SELFNET must trigger a rollback mechanism returning the network infrastructure to a previous operational state.

In another proactive self-healing scenario, an App running in the system may be aging, which would lead to a crash if not dealt with in time. Once this is detected, an App Rejuvenator actuator can be deployed to resolve this pending problem and thus avoid the potential crash.

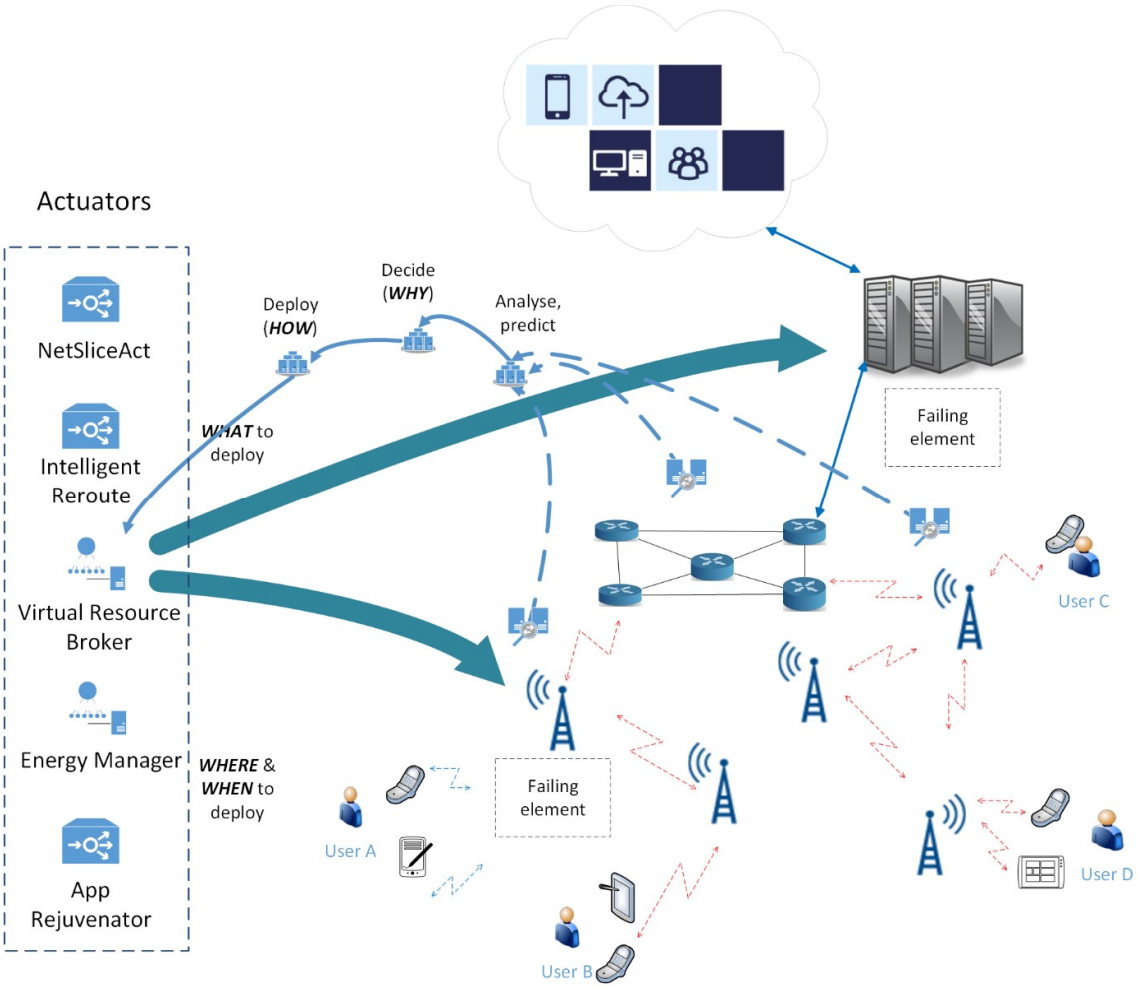


Figure 4.1 Proactive Healing Scenario

4.2.2.2 Scenario 2 – Reactive self-healing in critical/disaster/unpredictable Situations

It is noted that not all the potential failures in the network can be predicted or identified in advance to allow proactive corrections. Therefore, SELFNET also offers reactive self-healing functionality as a necessary backup, e.g., a recovery action will be triggered when a failure is detected through the use of anomaly detection mechanisms in self-healing sensors, as illustrated in Figure 4.2. Moreover, if a critical failure occurs on the network infrastructure, e.g., a network server or link fails, SELFNET can deploy an Intelligent Reroute actuator in order to reroute the network traffic through alternative links, thereby reassuring reliability and availability to the current services operating on the network. The Energy Manager actuator in this case can also be utilized to switch off the failed network if it still consumes energy.

In addition, prediction-based proactive actions may be unsuccessful, and as a result a failure is not avoided. In this case, a fast reactive action is activated. Consequently, among other possible actions, an expedited deployment of a self-healing actuator may be determined and then executed in order to mitigate the failure/disruption and restore the system to normal operations. In case of an unpredictable software failure on a network element (e.g., a routing problem on a router) or a physical failure caused by a natural disaster, SELFNET self-healing will aim to recover quickly, e.g., by deploying speedy and cost-efficient recovery and redistribution mechanisms, in

order to work around the failures, to recover at least partially first to minimize service disruption, e.g., by providing an alternative network path to reroute the traffic. The main innovation in this reactive mode is the prompt and efficient service redeployment/recreation enabled by the SELFNET framework compared with existing recovery mechanisms in current network management systems.

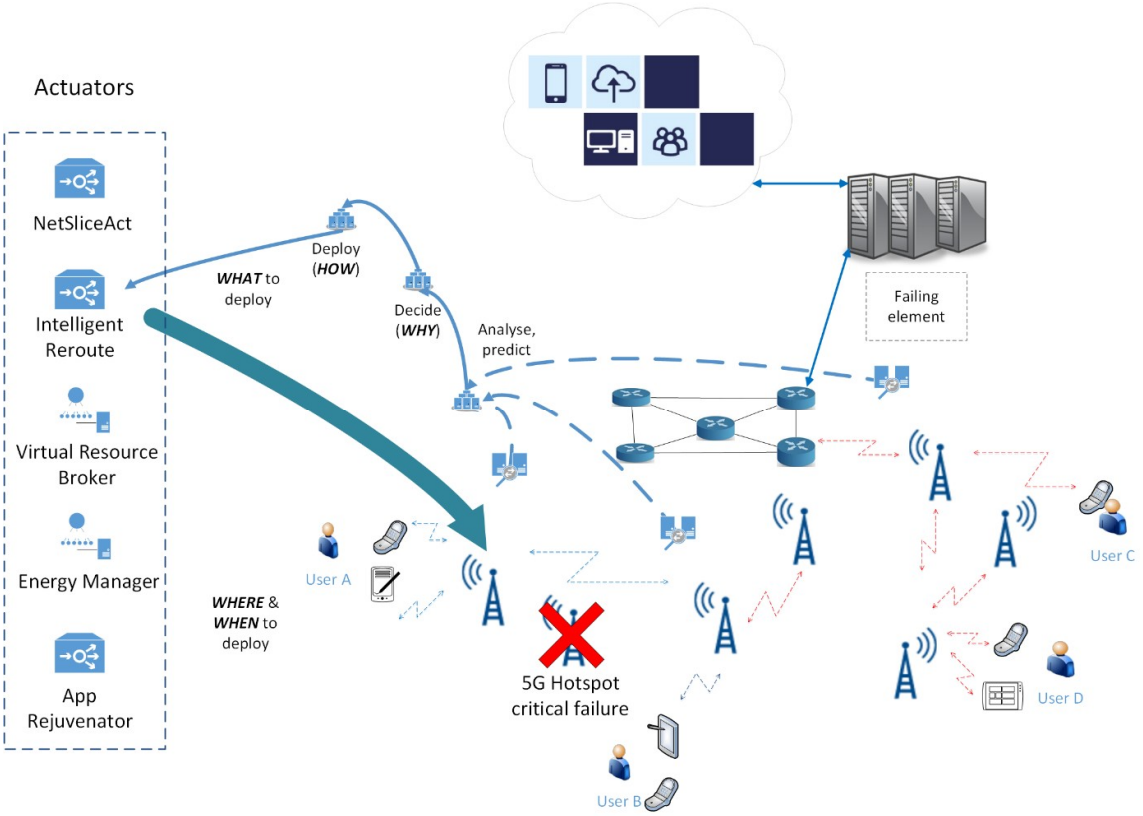


Figure 4.2 Reactive Healing Scenario

4.2.2.3 Scenario 3 – Proactive self-healing based on Network Slicing SLAs & Cyber-Footing Human Dynamics

It is commonly accepted that 5G will in particular address the needs of verticals, e.g., new user groups with independent business models that depend on the availability of networking services. Examples are the automotive, automation, transport and logistics, intelligent traffic service, some e-health as well as public transportation industries. In order to describe the network services that the public networks have to provide in order to meet the specific needs of the verticals, the concept of network slices covering the connectivity but also management functions is requested. In contrast to today's users of public network infrastructure, very strict requirements on safety, availability, coverage and security will have to be realized that can make the implementation of the network slices unacceptably expensive. SELFNET self-healing concepts will enable a cost-efficient control of strict levels of coverage, redundancy and availability based on proactive measures as well as timely healing avoiding negative implications on the services of the verticals. Therefore, this use case scenario (Figure 4.3) demonstrates how SELFNET mechanisms can help to guarantee network slice SLAs in a cost-efficient way by providing actions re-establishing pre-defined levels of SLAs (resilience, security and availability) when they got lost through the deployment of NetSliceAct actuators.

To this end, SELFNET will collect historical references of the network elements and store them in a healing database. Based on this enhanced knowledge about the network performance and by using data mining and learning algorithms (identification of cyber-footing human dynamics and classification of infrastructure metrics), SELFNET can then predict high resource demands before they happen and take actions before these demands lead to even more critical situations such as extreme mobile traffic bursts. The healing database also saves the unsuccessful responses, which means that these set of actions could not be taken in a similar situation. Thus, this enhanced knowledge will allow a better identification and classification of correlations between network behaviour and the users' social dynamics improving the proactive healing actions.

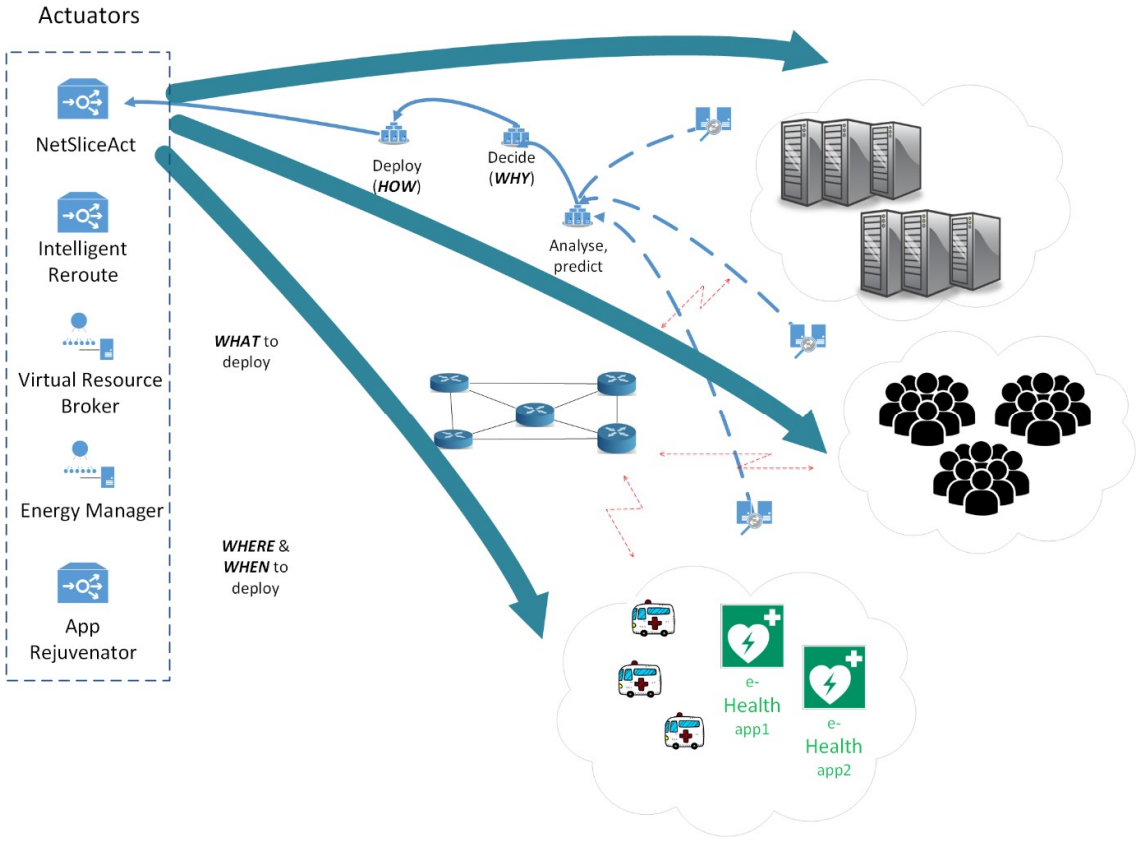


Figure 4.3 Network Slicing Scenario

4.2.3 Relation to 5G requirements/ visions

Enhanced physical and virtual infrastructure management and proactive detection and mitigation of network failures are crucial for realizing highly robust and usable 5G systems, especially for mission-critical applications in addition to everyday operations. The proposed use case is expected to meet such requirements by means intelligence-based self-monitoring, self-detection and self-organizing capabilities enabled by the SELFNET framework. In fact, through the deployment of SDN/NFV applications in the network infrastructure, SELFNET aids to achieve the automated network monitoring and maintenance of the network systems.

The proposed use case is in line with the following 5G requirements, visions and 5G-PPP KPIs [22] [39]:

- 5G systems shifting from Reactive to Proactive SON: Predict the problem in its infancy by inferring network-level intelligence from big context data and then take pre-emptive actions to resolve the problem before it occurs.
- “Preserve the robustness, integrity and security of the network, services provided via this network, and the end-users' devices.”
- “The future 5G infrastructure shall flexibly and rapidly adapt to a broad range of requirements”. “Preventing congestion and optimizing traffic management are essential on a mobile network and its importance will only grow with the industry moving towards 5G. High reliability and low latency will be key drivers for 5G services and can only be achieved with proper network management tools.“
- "Increasing resilience, continuity, and much higher resource efficiency". (Performance KPI)
- “Creating a secure, reliable and dependable Internet with a ‘zero perceived’ downtime for services provision”. (Performance KPI)
- “Provide a reliable and trustworthy communications infrastructure, which secures critical infrastructures”. (Performance KPI)
- “Reducing service creation reaching a complete deployment time from 90 h to 90 minutes” (Performance KPI)
- Substantial reduction (5 times lower) in network management OPEX. 5G is expected to aid in “mission critical services requiring ultra-high reliability, global coverage and/or very low latency, which are up to now handled by specific networks, typically public safety, will become natively supported by the 5G infrastructure”. (Societal KPI)
- 5G-PPP envisions that “5G needs to support in an efficient way three different type of traffic profiles, namely high throughput for e.g. video services, low energy for e.g. long – lived sensors and low latency for mission critical services”.

4.2.4 Stakeholders

The Self-Healing Use Case is aligned with the following 5G groups of stakeholders:

- Manufacturers
- Industry associations
- Research community
- Regulatory bodies and universities
- Network operators
- Vertical sectors like energy, health, manufacturing, robotics, environment, broadcast, content and creative industries, transport, smart cities.
- Communication service providers
- Public administrations

4.2.5 Contributions and Innovations of the SELFNET self-healing use Case

The self-healing use case will contribute with intelligent management capabilities to deal with a wide range of network malfunctions and failures in both reactive and proactive manners, which can not only remarkably reduce the OPEX of network operators but also improve the QoE/QoS of 5G systems. Therefore, this use case proposes self-healing mechanisms that will guarantee network slice SLAs based on strict levels of SLAs (resilience, redundancy, and availability), taking advantage of proactive actions as well as fast-enough healing measures avoiding negative implications on the services of the verticals. For example, new user groups with

independent business models and different QoS requirements will be serviced depending on the availability of networking services. In this way, SELFNET will use NetSliceAct actuators to establish, configure, monitor and re-establish a specific network slice profile within the physical infrastructure. Moreover, the self-healing capabilities provide the identification of Cyber-Footing Human dynamics by using data mining and learning algorithms that will help to predict high traffic demands before they happen, which will allow an intelligent proactive response to alleviate the effect of these critical traffic mobile situations.

The self-healing use case will also introduce the use of infrastructure metrics and SLAs indicators for inferring HoN metric reports that will be used to detect existing or potential failures and malfunctions in the network infrastructure. Moreover, the use of context-aware information in the Control Plane and the detection of vulnerabilities on the virtual execution environment will enhance the self-healing capabilities of SELFNET. The deployment of reactive and proactive self-healing functionalities will automate the healing actions by means of self-organizing and self-configuring procedures to dynamically and flexibly deploy actuator NFVs in the network infrastructure when and where needed.

4.3 Self-Protection Use Case

This use case strives to increase security, resilience, continuity, and delivery of much higher resource efficiency which will highlight the 5G disruptive capabilities at a societal level. 5G networks are expected to support many more users than today's 4G. This is due to an anticipated large diffusion of M2M and IoT interconnected devices, often with significantly higher committed data rates than the general bandwidth currently available to LTE and broadband network users. The expected large number of 5G subscribers therefore provides a new opportunity to compromise new devices, which in turn allows the attackers to trigger a much larger attack. In this context, cyber security, that is already a key aspect to provide resilience against cyber threats, becomes increasingly important in 5G due to the large number of 5G subscribers' devices which could potentially be compromised.

The self-protection capabilities of the SELFNET framework will provide a novel way of developing the necessary concepts and measures to ensure that required levels of security can be attained. This entails providing advanced mechanisms and techniques to collect large volumes of information gathered from multiple, heterogeneous sensors; and later analyse it to detect an alleged cyber-attack, or even the possibility of cyber-attack detection in an early stage thereby mitigating it proactively. This could be achieved by launching corresponding countermeasures in an orchestrated way so as to proactively mitigate any potential damage, whilst at the same time starting-up learning processes in parallel that will be able to handle new attackers' methods in subsequent detections.

4.3.1 General Background

As part of the 5G vision, future networks are expected to support new business domains (so-called verticals). Many of these new application areas will result in new and rather strict requirements on safety and security. Cyber security has become a top priority for governments, organizations and private industries across the world, with the aim of providing high levels of resilience against cyber threats. In this matter, in addition to SELFNET novel solutions providing detection of cyber-attacks and mitigation of potential cyber-attacks in a scenario like 5G, with a massive connectivity and massive number of connected devices, it will also learn from such cyber-attacks

and be able to improve reasoning in future detections. DDoS and virus spreading pattern attacks on cognitive radio networks are amongst the potential threats for 5G networks and therefore the target objectives for this use case. Both of these potential attacks are likely to take on a new critical relevance in 5G networks [40]. As such, 5G subscribers' devices may come under the control of the attackers using bots, or zombies, who establish a botnet to perform DDoS attacks, or even trigger self-propagating viruses to manipulating cognitive radio elements as a means of gaining operational advantages in 5G networks.

By providing a means of sensing and mitigating cyber-attacks, the self-protection use case addresses the deployment and enforcement of security services in multi-tenant environments through tenant-aware security VNFs chaining. Through this use case, the SELFNET framework will show how increasing security, availability, session continuity, resilience and delivery assurance for a wide range of 5G services and applications can be addressed.

4.3.2 Storyline

The proposed use case is oriented to detect and mitigate the effects of cyber-attacks and restore 5G network traffic to a steady state of security [41]. It is worth pointing out that detection and mitigation processes can not only act the reactive mode, but may also be employed proactively. Early detection of potential cyber-attacks will allow the system to reconfigure its components in preparation for an imminent attack. However, the main idea in SELFNET is to conduct detection at two levels of abstraction.

In a first stage, the 5G core network and radio access network (RAN) are analysed from a high-level point of view, monitoring only basic information of network flows very quickly. Then, once information on a potential cyber-attack is observed as the result of the high-level process, a low-level Deep Packet Inspection (DPI) is conducted. This is achieved by deploying and enforcing a virtualized and personalized honey net to isolate the cyber-attack, while applying corresponding countermeasures to protect assets. Due to the massive amount of traffic in the network, deep inspection of network packages is not feasible in a first step therefore a two-step process is needed.

This use case also addresses the challenge of deploying security services in multi-tenant environments, mainly by adopting a distributed self-protection approach where multiple, differentiated and specialized security VNFs are chained for each tenant. This approach offers end-users and customers a high performance, dynamic and reliable security infrastructure. Specific elements (potentially candidate VNFs) for this use case are split across two major phases of the cyber-attack service lifecycle. Firstly, sensing, where the system has to deploy traffic monitoring probes to collect and correlate traffic data used to identify cyber-attacks. Secondly, actuation, where the system deploys a chain of mitigation virtual network functions and configures appropriate traffic steering policies to force malicious traffic to pass through threat management systems where it can be mitigated/filtered.

The multi-tenant security services concept in this self-protection use case is depicted in

Figure 4.4. The main idea is that a VNF security service provider (which could be a network operator) offers multi-tenant security services to its customers (e.g. enterprises with multiple headquarters/branches). Virtualized network security functions for security service may include virtual TAP, virtual Traffic monitor/DPI, virtual firewall, virtual Threat Management System, virtual honeynets, virtual Intrusion

Protection System (IPS), adaptive firewalls, vector attack identification tools etc. They can be deployed and chained on demand or permanently in data centres at different locations in the network e.g., at the mobile access, PoP or in the core, in response to distributed attacks or intrusions that could potentially affect all the 5G network portions (RAN, micro/PoP DCs, core network, core DCs). They are selectively and dynamically deployed according to the specific type of protection required at each location, thus building a network for distributed security functions.

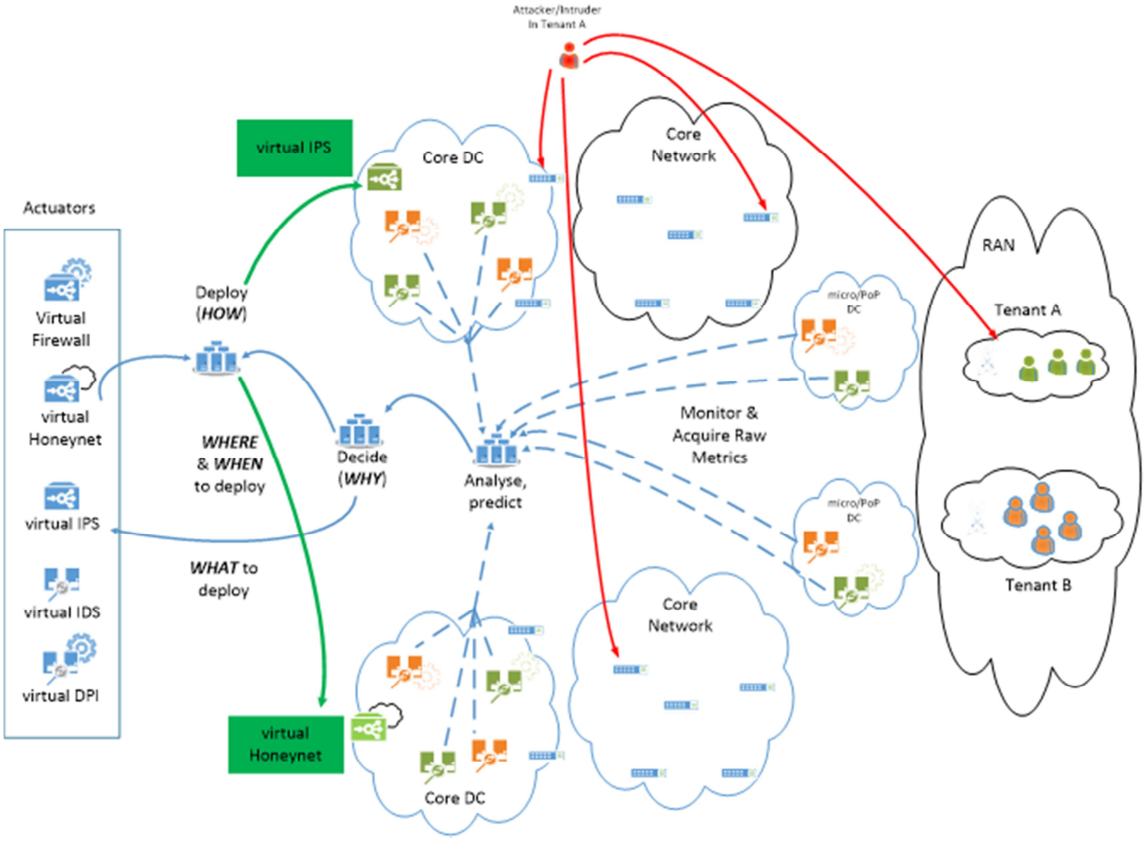


Figure 4.4 SELFNET multi-tenant security services distributed across edge and core

Although there are a potentially large number of cyber threats involving 5G networks, this use case is focused on DDoS attacks and other types of intrusions such as virus spreading attacks. As shown in Figure 4.5, a DDoS attack is conducted after compromising a number of users (5G subscribers' devices) for being part of a botnet. All these devices will be under control of the attacker as bots or zombies, blindly executing the actions requested by the attack through a given number of controllers.

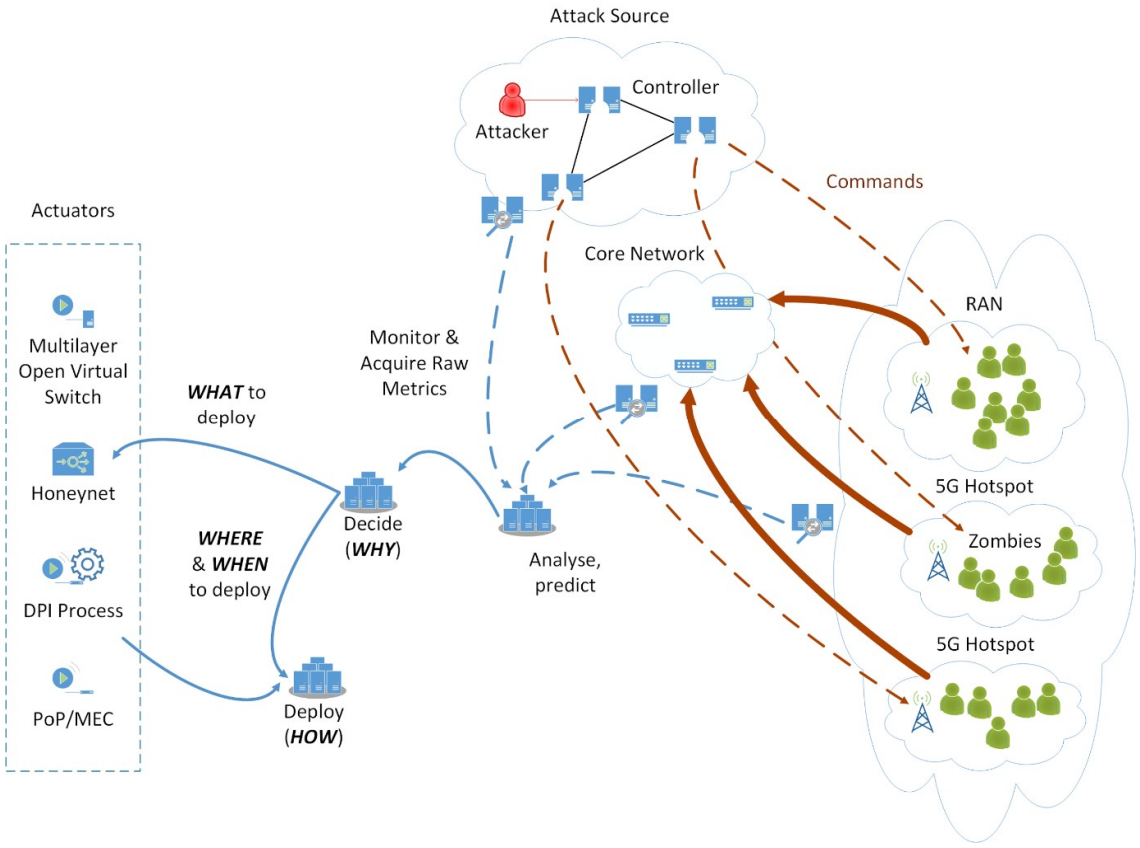


Figure 4.5 Execution of a DDoS attack by injecting large volumes of malicious traffic

In all cases, when information on a potential cyber-attack is obtained from the monitoring and analysis, the SELFNET framework responds using one of the two response modes:

- Proactive mode, that leverage the SELFNET's ability to monitor, detect and analyse patterns and aim at exploring different patterns/staged features of DDoS or virus spreading attacks as part of a proactive approach. In proactive mode self-protection actions are, where feasible, triggered before the cyber-attack (the botnet links or the virus) can become widely spread or reach its ultimate target.

- Reactive mode, that make use of a Collaborative Intrusion Detection System (CIDS) to detect the cyber-attack through a fine-granularity detection procedure underpinned by data mining techniques. This is a DPI process. The different IDSs belonging to the CIDS should be placed as virtual services as close as possible to the monitoring area [42]. As soon as the source of the attack is detected it must be isolated following a properly coordinated approach. A virtualized and personalized honey net (for the type of service/network which it is intended to protect) is deployed to defend the users against the attack and learn from it; and its connections are redirected to that honey net by reconfiguring the flow tables of the virtual switches (e.g., OpenvSwitches [34]). An example of a honey net is depicted in Figure 4.6, where the attacker continues its execution over a virtualized network which it is not real. In the meanwhile, the legitimate users follow using the real network on as usual. It will effectively reduce the number of attacks reaching the target destination.

Note that the differentiation between (high-level) network flow analysis and (low-level) packet inspection allows the proposed multi-level protection scheme to offer the required levels of scalability and granularity in 5G environments.

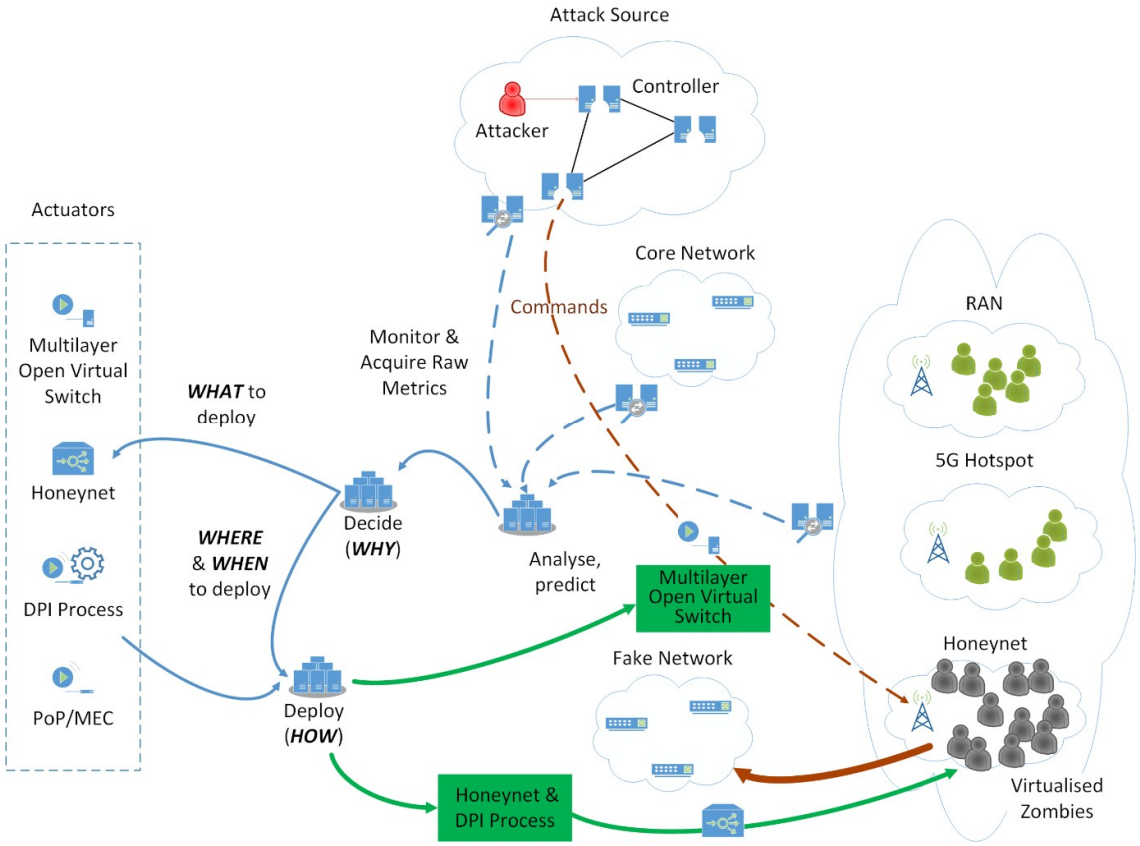


Figure 4.6 Countermeasures by building a honey net to counter the cyber-attack

The following differentiated security VNFs are considered in this use case:

- Backend VNFs: security VNFs deployed in the PoP data centres that aim to provide security functions for PoP-to-PoP and PoP-to-core data centre traffic. These are security functions mostly dedicated to network traffic that stays within the network (e.g. related to traffic across the headquarters).

- Frontend VNFs: security VNFs deployed in the core data centres to provide perimeter security functions. Therefore, these VNFs provide gateway protection functionalities for the tenants' network traffic towards the Internet (and vice versa).

Additionally, another level of distribution can be implemented on top of this distributed deployment of virtual functions across different data centres and network locations. The aim of this additional layer is to optimize the performance of security services and to reduce latency. This can be achieved by splitting each virtual function across several child virtual security sensors (still implemented as VNFs). Each child sensor is responsible for a given set of rules, signatures or traffic types that can then be matched in parallel. A coordination function, possibly deployed as an SDN App, and then becomes necessary for each virtual security function in the multi-tenant

distributed service. This function will coordinate and balance its associated child virtual sensors. In the interests of simplicity and readability,

Figure 4.4 only depicts child VNFs deployed in the network. The coordination SDN App is embedded in the SELFNET framework box.

Virtual sensors for security are generally deployed, configured and chained at the instantiation of the service for any given tenant network. However, virtual security actuators are automatically instantiated and configured at the appropriate network location as part of the self-protection approach. This means that, when a sensor VNF detects an intrusion or attack, the SELFNET framework managing and orchestrating the multi-tenant security service can properly react to block and mitigate the attack. This reaction should aim to have no impact on end-user traffic and services. Deployment of a new actuator VNF at the proper location in the security service chain (with re-configuration of the chain itself) and deployment of a new sensor VNF specialized for the given traffic pattern or intrusion type are examples of the range of possible reactions that could be employed.

In this use case, the SELFNET framework also provides automated control and orchestration functions to steer the traffic through distributed VNFs of each tenant. The framework also includes self-organization functions that can perform automated reconfiguration of service chains as part of the SELNET response to a cyber-attack.

4.3.3 Relation to 5G Requirements/Visions

The latest working assumptions on potential 5G architectures and network design have been used as the basis for the design of the SELFNET framework and its associated use cases. Although still under discussion, it is commonly agreed that adaptability and flexibility will become key attributes of 5G networks where a primary requirement will be to support a wide range of 5G services and applications. Cloudification with at least an edge cloud and a centralized cloud environment is also part of most visions. Finally, virtualized network functions are expected to have a prominent role in 5G. These are expected to be virtualized at a level that is only limited by practical implementation considerations and to be capable of being adapted and reallocated in accordance service, traffic and context needs. Each of these 5G trends has been taken into account in this use case.

Security is as a fundamental concept in 5G and an essential requirement for 5G systems at all layers and levels and also in all resource domains. 5G-PPP has identified, in [22], the need for mainly "increasing resilience, continuity, and much higher resource efficiency" to the 5G disruptive capabilities at the societal level. In this context, cyber security is a key aspect as its role is to provide resilience against cyber threats including, but not limited to, powerful cyber threats such as botnets. These concepts, rather than being new 5G-specific issues, are traditional issues continually at the forefront of research and development across all ICT systems. [15].

In 5G, network security is required to provide explicit, measurable and enforceable capabilities that will enable the network to behave consistently in a prescribed way [43]. These capabilities must include increased security, availability, session continuity, resilience and delivery assurance for a broad spectrum of 5G services and applications.

The expected, very large numbers of attached devices and their anticipated levels of mobility will encourage the evolution of current security infrastructures towards the adoption of more distributed solutions based on chains of virtual functions. These

virtual function chains will be dynamically and flexibly deployed, configured and operated [44]. Any large scale deployment of virtualized network functions may, in the near future, bring new security threats requiring a new flexible, dynamic security and protection approach.

The multi-tenant security (by use of virtual network functions distributed across edge and core), outlined in this use case, is therefore perfectly aligned with the aforementioned requirements and visions for 5G systems. This approach offers self-protection capabilities against cyber-attacks, particularly debilitating attacks such as DDoS botnets and virus spreading patterns. In respect of the former, the Defence Advanced Research Projects Agency (DARPA) has recently reported in Aug 25, 2015 [45] that "The number of DDoS attacks in first quarter of 2015 more than doubled the number of attacks in Q1 of 2014 and attack sites are growing more dangerous, and more capable of launching attacks in excess of 100 Gbps, according to a recent Akamai Technologies State of the Internet Security report." The growth and scale of these types of attack has prompted Joseph Demarest, assistant director in the cyber division at FBI, to publically comment in July 2014 on this new major challenge before the U.S. Senate Judiciary Committee, Subcommittee on Crime and Terrorism [45]. In his evidence to the committee he said "cyber-criminal threats pose very real risks to the economic security and privacy," and he estimated annual global cost of cyber-attacks at $110 million. Cyber security is expected to also be a challenging task in 5G as both quotations indicate the growing impact of cyber threats and the need for more revolutionary security and' protection approaches.

4.3.4 Stakeholders

The self-protection use case is aligned with the following 5G groups of stakeholders:

- Industry associations
- Research community
- Regulatory bodies and universities
- Network operators
- Communication service providers
- Public administrations

4.3.5 Contributions and innovations of the SELFNET self-protection use Case

The self-protection use case will lead to a new and innovative way of deploying multi-tenant security services distributed across edge and core 5G networks to counter cyber-attacks. The use case will demonstrate how the SELFNET framework will strengthen system resilience and service availability, in line with the essential requirements for the 5G systems identified by 5G-PPP. This use case will help to ensure self-protection capabilities against cyber-attacks, by providing advanced monitoring and detection algorithms to detect alleged cyber-attacks and a new way of deploying a chain of mitigation network functions. This deployment will automate the protection capabilities of the multi-tenant system by means of self-organizing procedures to dynamically and flexibly deploy actuator VNFs when and where needed.

The multi-stage protection approach proposed by this use case, where sensors and actuators of various security functions provide monitoring and mitigation capabilities at different network traffic granularities, representing a key innovation in the way security is implemented in highly distributed networks such as 5G. This allows

implementing a highly scalable security infrastructure for 5G services. In particular the proactive protection approach is crucial in the prevention of wide spreading of attacks, thus reducing the need of deploying numerous deep traffic inspections across the 5G network.

Moreover, multi-tenancy is a key aspect and concept for network and service operators in 5G. This use cases combines the concept of IT resources virtualization in cloud and network and service virtualization in telecommunications for advanced tenant-aware security management. Virtualization techniques and mechanisms are well defined and widely spread in cloud-based environments, where virtualization of IT resources allows accommodating and multiplexing multiple customers within their physical infrastructures. Network and service virtualization is also a well-defined concept for network and service operators, which allows the sharing of network infrastructures between physical network owners and virtual network or service operators, like the widely adopted Mobile Virtual Network Operator (MOVNO) model. The combination of the two in this use case, which basically allows providing multiple VNFs running in data centres and chain them within a virtualized network infrastructure, represents a key innovation and opens new business opportunities for network and service providers while enabling the sharing of 5G physical infrastructures among multiple stakeholders. This use case would advance this innovative approach by providing secure multi-tenant virtual infrastructures, where per-tenant virtual networks are secured by the combination of distributed virtual security sensors and actuators.

4.4 Self-Optimization Use Case

The aim of this use case is to demonstrate how the smart network management capabilities of the SELFNET framework can be used to meet the QoE expectations of consumers of video/multimedia in future 5G mobile networks under a wide range of network conditions.

It will highlight the benefits and positive impact of the SELFNET framework on a number of key 5G requirement areas. In terms of societal impact it will demonstrate U-HD video streaming, a new economically-viable service of high societal value and will support an optimized user experience through transparent QoE based service delivery. In terms of 5G performance requirements this use case will provide high levels of service continuity for video delivery across 10 to 100 times more devices with vastly reduced provisioning times and, through smart caching, improved service delivery speed.

4.4.1 General Background

Traffic generated by video applications has increasingly dominated 3G/4G mobile networks, thereby placing great strain on network capacity. As mobile network operators transition to 5G networks they will have to contend with both the massive increase in video traffic and heightened user expectations of service levels and quality. In the face of such challenges, and despite the expected substantially enlarged network bandwidth/capacity of 5G, it is by no means assured that the enlarged bandwidth will be able to keep pace with the ever-growing consumer demands for higher quality and resource-hungry video applications.

The emergence of Ultra-High-Definition (U-HD) video streaming applications like U-HDTV, requiring up to 16 times the bandwidth of current high definition video, and an

increasing number of 5G subscribers, when taken together, are likely to fuel continued rapid growth in video traffic. It can also be expected that the higher bandwidth of 5G networks will provide the impetus for the development of new mobile video services in M2M, IoT, and telemedicine, security/surveillance and consumer domains.

4.4.2 Storyline

User Perspective

Consumers of video content delivered over 5G networks will have high expectations of video quality, network reliability and service continuity. These expectations will be driven by new U-HD capable consumer devices and user's perception of the improvements that a generational shift in network technology should deliver. In this use case we will study several scenarios that are likely to impact on the end user's QoE and explain which autonomic behaviours and SELFNET architectural components will be used to automatically respond when QoE levels have either fallen below, or are predicted to fall below, expected levels. Additionally, in this use case, the end to end energy efficiency of the network is considered with SELFNET monitoring and proactively managing the energy use of resources across the network

This use case differs from the Self-Healing use case (Section 4.2) in that it goes beyond reaction to adverse events or network states and aims to maximise the utility of the network for the user's advantage by providing the best possible QoE for users at all times. As part of this strategy and in addition to the reactive and proactive measures described in the scenarios below, operators will be able to set QoE optimization targets (i.e. a minimum level of QoE for each service type) that the self-optimization aspect of SELFNET will seek to maintain at all times. Towards these aims, the self-optimization aspect will work in concert with other use case scenarios (Self-Healing, Self-Protection) to always maintain the QoE levels of users not directly impacted by the enforced actions of self-healing or self-protection mechanisms.

4.4.2.1 Scenario 1 - Video Streaming in Changing Network Environment using a 5G Hot Spot

In this scenario a nomadic mobile user enters a busy public location such as a cafe, arena or airport where he connects to a 5G hot spot. There are a number of other users connected to the same 5G hot spot, all of whom use Internet access for a diverse set of tasks including social media networking, video watching, e-mail and VPN access using their smartphones, tablets and laptops. It is assumed that there will be a number of adjacent hot spots, some of which offer overlapping coverage. We focus on the QoE of a single user in a realistic evolving scenario. He has requested a U-HD video stream from a content provider located out with his own network. At the outset this stream is the only significant (in terms of bandwidth) application that this user is running.

Step 1- Sparsely Populated RAN

Initially, there are few users concurrently attached to the hot spot and consequently network conditions are stable with perfect or near to perfect channel conditions. Since there is no network impairment the user's QoE expectations will be met, providing him with ultra-high resolution video without any noticeable buffering waits or visual artefacts such as blocking or blurring. The SELFNET framework is monitoring

both the network state and video application flows, continually evaluating the health of the network and estimating the QoE of users. From the user QoE perspective no autonomic behaviour is required by the SELFNET framework as expected QoE has neither dropped, nor been predicted to drop in the short term, below the user's satisfaction threshold.

Figure 4.7 shows the initial state where the user has entered the 5G hotspot.

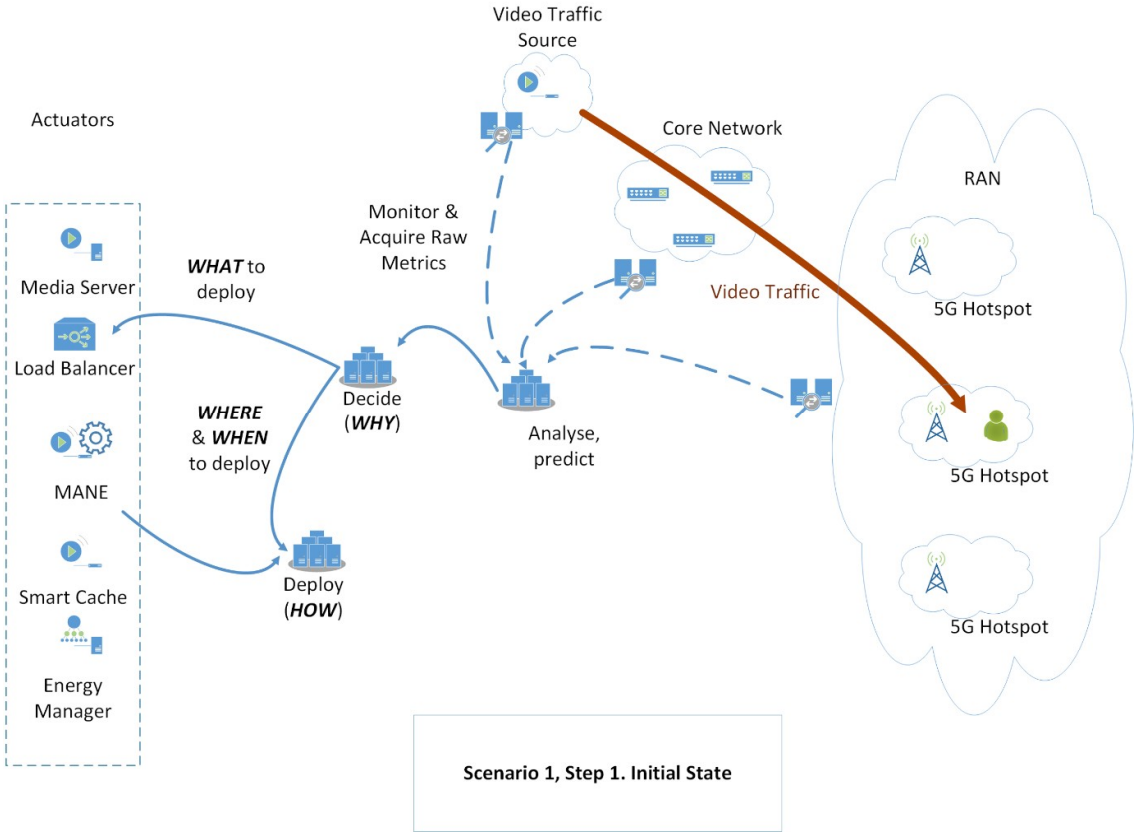


Figure 4.7 A user moves into a sparsely populated 5G hotspot and begins to receive streamed U-HD video content

From the service provider's perspective, SELFNET sensors have determined that, at a micro level, the subscriber SLA's have been met and that they have fulfilled their QoS obligations to the individual subscriber. While at a macro level the overall health of the network has been maintained and consequently no autonomic behaviour is required to ensure compliance with SLA's. However, the SELFNET framework is also monitoring the energy efficiency of operations within the RAN. In this lightly populated situation, SELFNET decides that a single 5G hot spot is sufficient to manage the traffic load and meet QoE expectations, consequently adjacent hot spots are switched off to save energy. This decision has no impact on the users.

The SELFNET framework continues to monitor the estimated QoE level of the video throughout the duration of the user's session.

Figure 4.8 shows the state after SELFNET intervention where the action performed has been to deploy an energy management actuator that places adjacent, unrequired, hotspots into sleep mode.

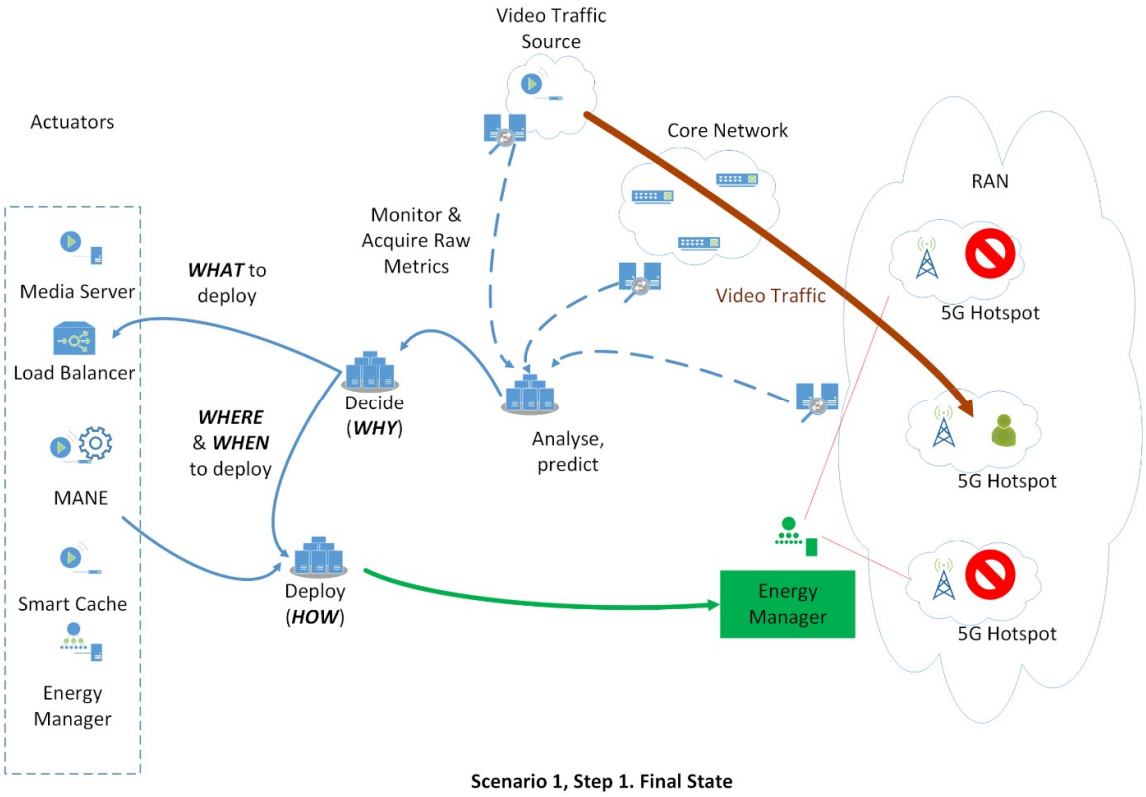


Figure 4.8 An energy management actuator has been deployed to the RAN and adjacent hotspots put into sleep mode

Step 2 -Increasingly Congested RAN

Over time more users arrive at the physical location and attach to the same hot spot. Simultaneously some users open multiple applications on their devices, each of which generates a new application flow. The immediate implication is that each user now has less bandwidth available to him as the available bandwidth is shared fairly between users attached to the hot spot. Continuous monitoring and analysis of low level metrics by the SELFNET framework determines that congestion has either been observed or predicted to occur in the immediate future and anticipates that user QoE expectations will no longer be met. The net effect of this congestion in the RAN, if not proactively mitigated, would be a reduction in user's QoE. This would be observed by the user as periods of buffering and a reduction in picture quality (visual impairments such as blocking and blurring). The reduced bandwidth available to each user also results in subscriber SLA's having been breached or predicted to be breached.

As user density at the hot spot increases SELFNET responds by performing autonomous behaviours aimed at minimizing the impact on user's QoE whilst ensuring that subscriber SLA's are met. Bearing in mind energy efficiency, SELFNET would start up the minimum number of adjacent hot spots required to offload users situated at the periphery attempting to ensure that each user had enough bandwidth to meet their subscriber SLA and that macro level health of networks metrics remained satisfactory. Where subscribers are currently running multiple applications they will have the ability to influence the SELFNET decision making process by indicating which application is most important to them. However SELFNET's autonomic responses will be transparent to the subscriber and will deploy smart

media adaptation network entities (MANE's) and smart video caching actuators to the network edges. The MANE's would intelligently adapt video streams to meet the bandwidth and delay limitations of the congested RAN in a QoE optimized manner. This would be done by considering not only network state metrics but also video metrics such as content type and the user's device capabilities.

Therefore video quality degradation likely to result from increasing congestion is mitigated in the data plane. Intelligent video adaptation using MANEs ensures that any quality degradation occurs smoothly and has limited impact on human perception of quality (QoE), even though the congestion is already measurable by detectors (QoS).

The SELFNET framework will deploy the automated responses as close to the congested area as possible. The impact of SELFNET's automatic response is the return of user QoE levels to an acceptable level which in turn results in the delivery of ultra-high resolution video without any noticeable buffering waits or visual artefacts such as blocking or blurring. The SELFNET framework continues to monitor the estimated QoE level of the video throughout the duration of the user's session. At a micro level the QoE of each user will be supported by adapting the video stream in the 'best' way to suit his needs and circumstances while at a macro level SELFNET decision making and planning will ensure fairness in the level of QoE provided to every user. Figure 4.9 and Figure 4.10 show the initial and final states respectively.

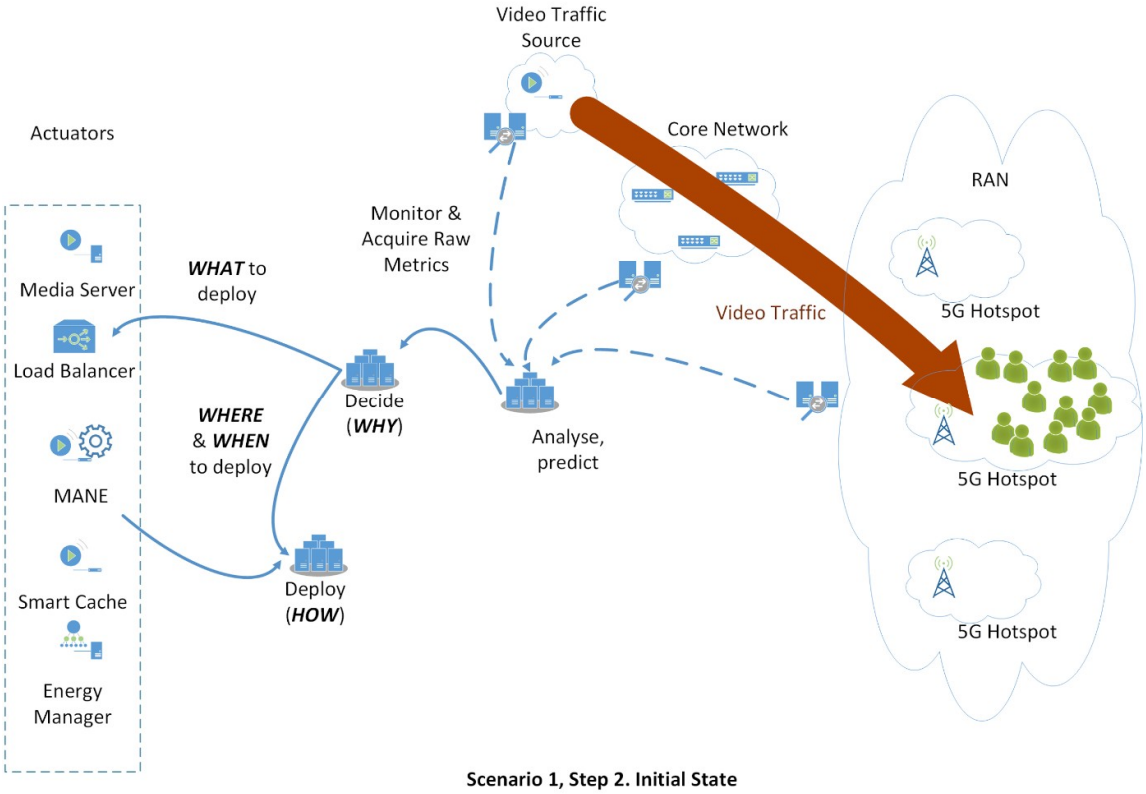


Figure 4.9 A large number of users, all streaming video traffic begin to cause congestion in the 5G hot spot

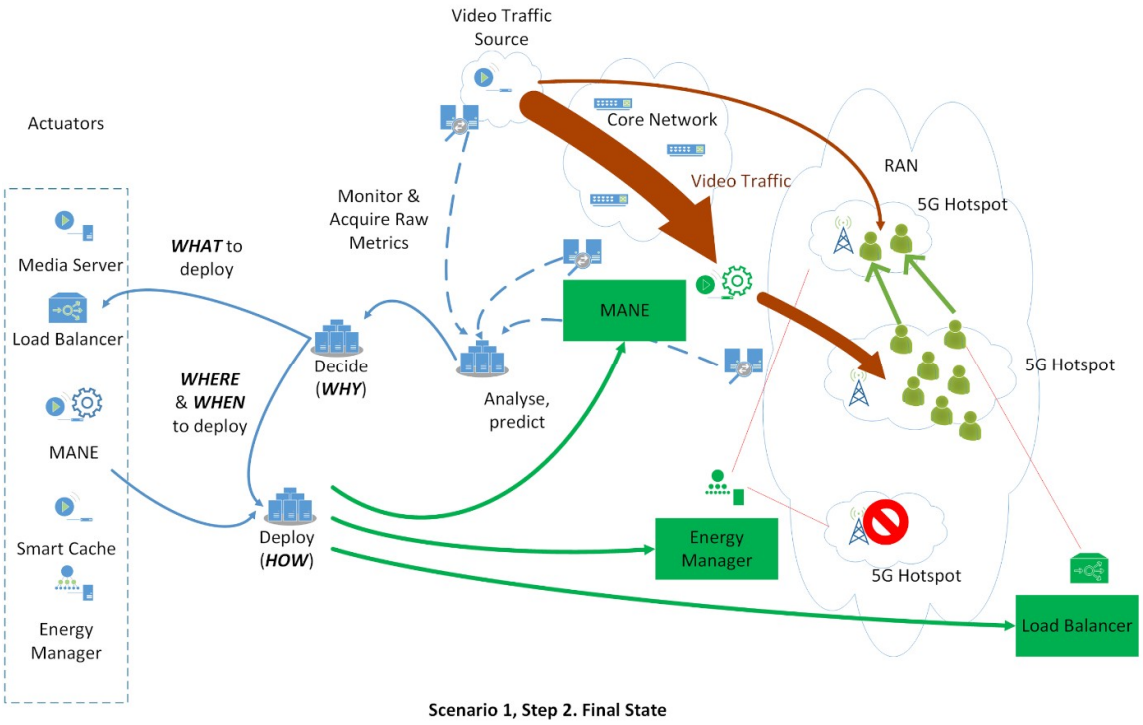


Figure 4.10 Media Adaptation, Energy Management and Load Balancing actuators deployed

Step 3-Significant Network Impairment

Whilst the RAN is densely loaded with users in the original and adjacent hot spots a significant impairment such as a network outage impacts the core network. Many users, across many RAN's are concurrently streaming U-HD video. After the Self-Healing use case reconfigures the network to restore connectivity to the best possible state, the Self Optimization algorithms will work to provide the highest possible level of QoE to the users affected by the network impairment without affecting the other users of the network.

Due to the impairment localized SLA breaches will occur as, in some cases, it will not be possible to maintain all the streams at normal throughput. As part of the self-optimizing response to such a network event, the SELFNET SON will deploy MANEs and traffic engineering resources globally across the network to reduce the resource usage of video flows in a QoE efficient manner in support of the self-healing effort. The above three steps of this scenario are summarized in Table 4.1.

Table 4.1 Steps Scenario 1 – Self-Optimization Use Case

Network State	Action	QoE
Sparsely populated	Reduce bandwidth to save energy	Perfect
Increasingly congested	Automatically adapt data plane using intelligent traffic management features in conjunction with layered video coding	Degradation almost no noticeable
Significant Impairment	Adaptation by control plane	Acceptable degradation

4.4.2.2 Scenario 2 - Video Streaming where the end user is both consumer and provider of real-time video content.

This scenario considers the case of a nomadic user who may be both the consumer and originator of ultra-high definition video content. This scenario makes the assumption that, as high bandwidth low latency 5G networks become available and U-HD capable mobile devices become common, new services will allow users participate in real-time video calling at spatial resolutions that make the full use of their device's capabilities. Similarly, it is anticipated that subscribers will not only be able to upload high frame rate U-HD videos quickly to social networking and video sharing sites but will also be able to stream videos they are currently taking in real time, or very close to real time, to other users or groups of users. Although the recipient users' QoE will be managed at the network edge close the their physical location in the same manner as scenario A, SELFNET will need to deploy and manage a different set of resources to facilitate upstream video streaming from the RAN, through the core to another, remotely located RAN. Many user mobile devices will be capable of recording U-HD video however, all but the most heavily resourced, but may not be capable of encoding highly compressed scalable video in real time. Traditionally, in today's networks the bandwidth provisioning (governed by SLA's) is asymmetrical with download links typically having over 10 times as much capacity per user as upload links. To accommodate this scenario, uplink provisioning must be sufficient to support these new applications. When SELFNET's monitoring and analysis tools either observe that upstream video delivery or U-HD video calling is taking place or predict that it may do so by observing, for example, a surge in social media use in a certain 5G hot spot or RAN the decision making planner must propose autonomic actions to support the subscriber to successfully stream in real time. Figure 4.11 shows the initial state when two remote users begin a real time video call.

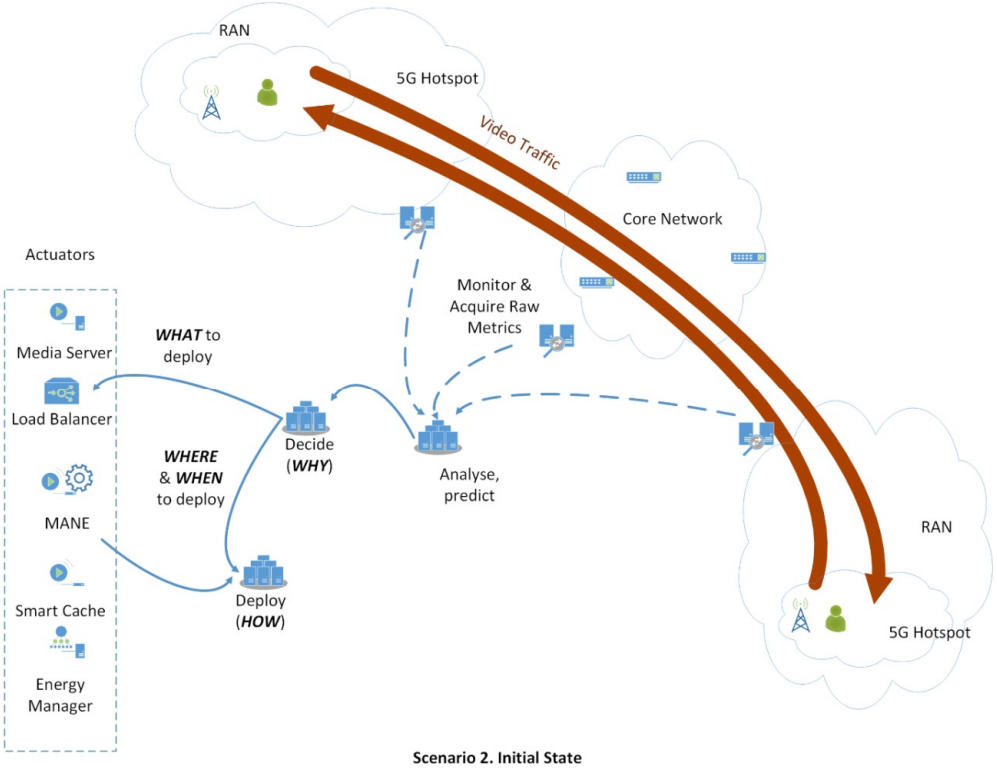


Figure 4.11 Initial state for a video calling application prior to Framework intervention

An example of SELFNET autonomic responses in this scenario is illustrated in Figure 4.12. Autonomic actions performed by SELFNET may include deployment of smart video caches and media streaming servers or video transcoders to the RAN, these new network entities would allow some of the management of the upstream video delivery away from, possibly resource constrained UE devices and reduce the energy usage (battery depletion rate) of the user devices. From a network management perspective, when large volumes of video traffic originating in the access networks are detected, SELFNET will need to deploy resources that will provision uplink SLA's for the subscriber.

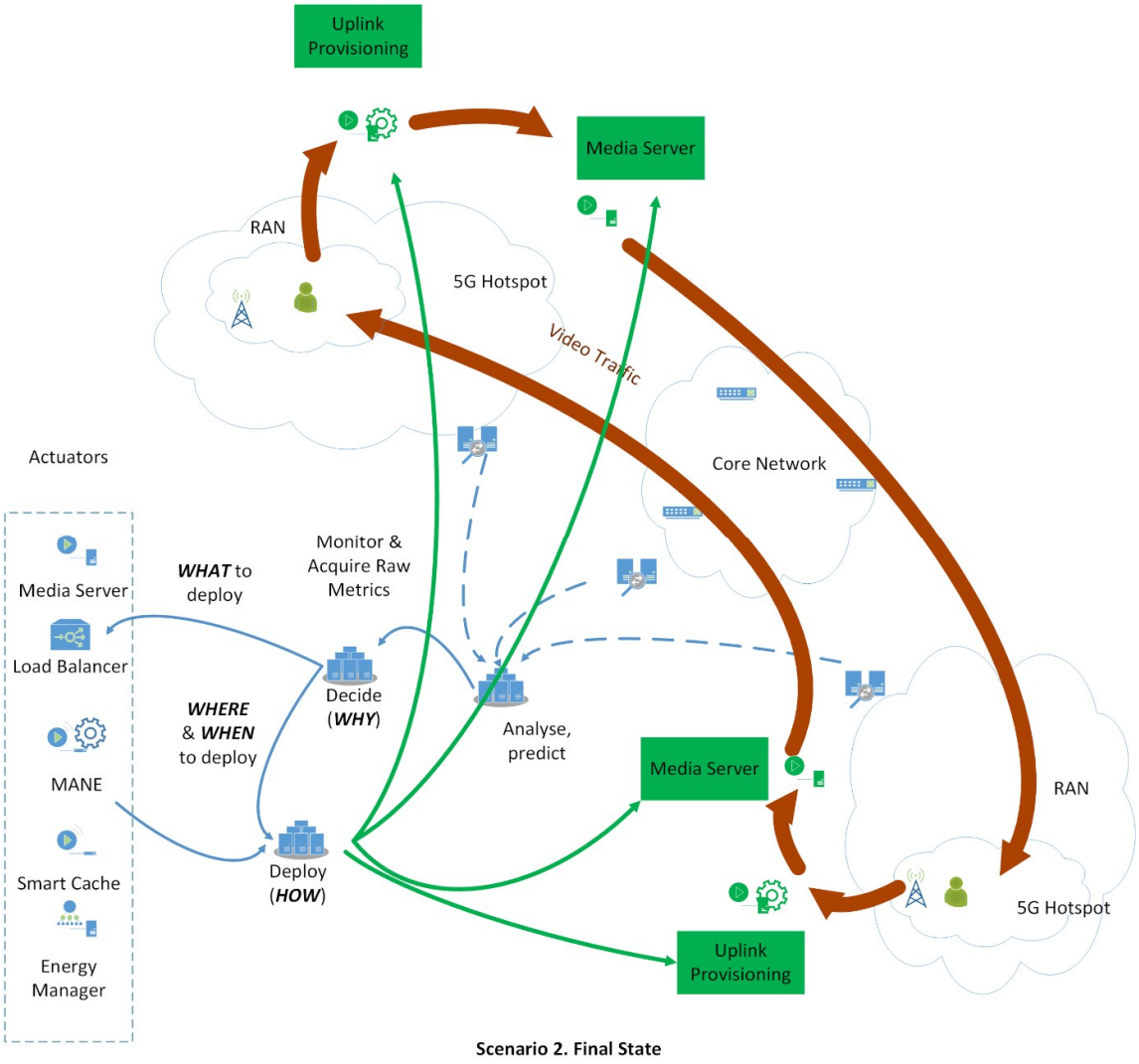


Figure 4.12 SELFNET has deployed media server and uplink provisioning actuators at both end of the video call

4.4.2.3 Scenario 3- Video Generated by Smart City Applications

In this scenario the user is defined as an M2M application for automated video surveillance or some other critical application. Where this scenario differs significantly from the consumer driven scenarios (1 and 2) is that the QoE (if such a term is actually appropriate) of such services, although potentially of vital importance in future smart cities, is an area that has been under-researched. In terms of monitoring

and analysis the video QoE high level metric must reflect the information content of a video stream and its utility in performing automated recognition or detection tasks and must support appropriate decision making rather than perceptual quality from a consumer's perspective. Smart video adaptation algorithms running on MANE's used in the core or at the edge to manage this type of traffic should adapt stream in a manner that optimizes this quality utility function rather than more traditional perceptual quality. This is made more challenging by the fact that the video stream requires real time delivery which is being adversely affected by high volumes of consumer U-HD video traffic in the core network.

The M2M system operator established an SLA with the SELFNET operator that allows both a slight degradation of the video quality and the relaxation of the real time constraints for small periods of time. The SELFNET framework will correctly identify the different characteristics of the M2M flow, apply a different policy to these flows, and if needed a MANE will modify the video stream in an attempt to reduce the required throughput while still maintaining the contracted SLA. If the network is still congested after the modification of the M2M traffic, the SELFNET framework should attempt other strategies to improve the situation, such as reconfiguring the MANEs that handle the other user's best effort traffic in an effort to allow the return of the M2M traffic to nominal conditions.

This scenario ends with the M2M traffic within the conditions that are considered nominal by the SLA and the lowest impact possible on the remaining user streams, either by severely degrading a few streams or by slightly modifying a large number.

Privacy of the content of user video streams.

Importantly, it is assumed in this use case all QoE monitoring components that inspect video streams to obtain QoE metrics, whether in the compressed on uncompressed domains, will not impact on the privacy of users or owners of content. Whilst in a great many cases the video content will come from content delivery networks that may add metadata about content type or other QoE related low level metrics, many user generated and owned videos will also need to be processed to estimate content type etc. It is anticipated that video type will be derived from the compressed bit stream using schemes similar to that proposed in [18] where video content type is estimated from the new H.265 coding tree structure and motion vector data without any inspection of the information content of the video stream.

Technical Perspective

The challenge addressed in this self-optimizing use case is that of finding autonomous methods of proactively predicting the impact of massive video traffic loads on network health, user experience and energy efficient 5G network operation and then rapidly deploying network, video and energy management resources in a co-ordinated fashion to counter potential failures and meet required health of network, user quality and energy use service levels. It is also important that network management resources be deployed at appropriate locations in the network.

This use case will demonstrate how the SELFNET framework can deliver self-adjusting traffic management mechanisms for delay reduction and loss prioritizing in the video data plane by cooperating with intelligent encoding and packet marking schemes. The overall aim being to demonstrate an ability to achieve very high QoE even when traditional QoS levels are poor. Typically this will be achieved by selective dropping of enhancement layer packets of scalable video streams and/or redundant

transmission of important video frames essential to the decoding process. In addition end-to-end QoE enhancement methods such as feedback of receive quality to the sender will be considered.

In line with the trend of user aware design, it is anticipated that users may be able to exert greater influence over the way in which services are delivered (including connection parameters and service differentiation), this use case will also consider ways of recording and utilising the preferences of users when making autonomous network management decisions. This will require a new, user-influenced, way of differentiating application flows that will; in addition to delivering a personalised approach to the user within the robust, smart and autonomous SELFNET framework; also satisfy the network management needs of service providers.

Each of the main components of this use case (self-optimized video adaptation, user-assisted approach, and energy-aware approach) is underpinned by video encoding and adaptation technologies. Among other potential adaptation schemes, a scalability-based video adaptation scheme is described here to present a specific example as a starting point.

As illustrated in Figure 4.13, flows of video data are encoded in a layered format, where the Base Layer (BL) contains the most important video packets that have the greatest impact on an end user's perceived visual quality and the Enhancement Layers (ELs) contains additional details for improved visual quality but are not essential (EL1 is more important than EL2, EL2 more important than EL3 and so on). When network congestion at the core network or insufficient bandwidth at the RAN is detected, selected higher Enhancement Layer video packets (EL2 packets in this example) will be dropped at a Media Aware Network Element (MANE) to reduce the demands on bandwidth whilst the Base Layer and the lower Enhancement Layer(s) will be delivered. Such selective packet dropping using layered video coding can result in substantial bitrate savings with little impact on the perceived quality at the end users.

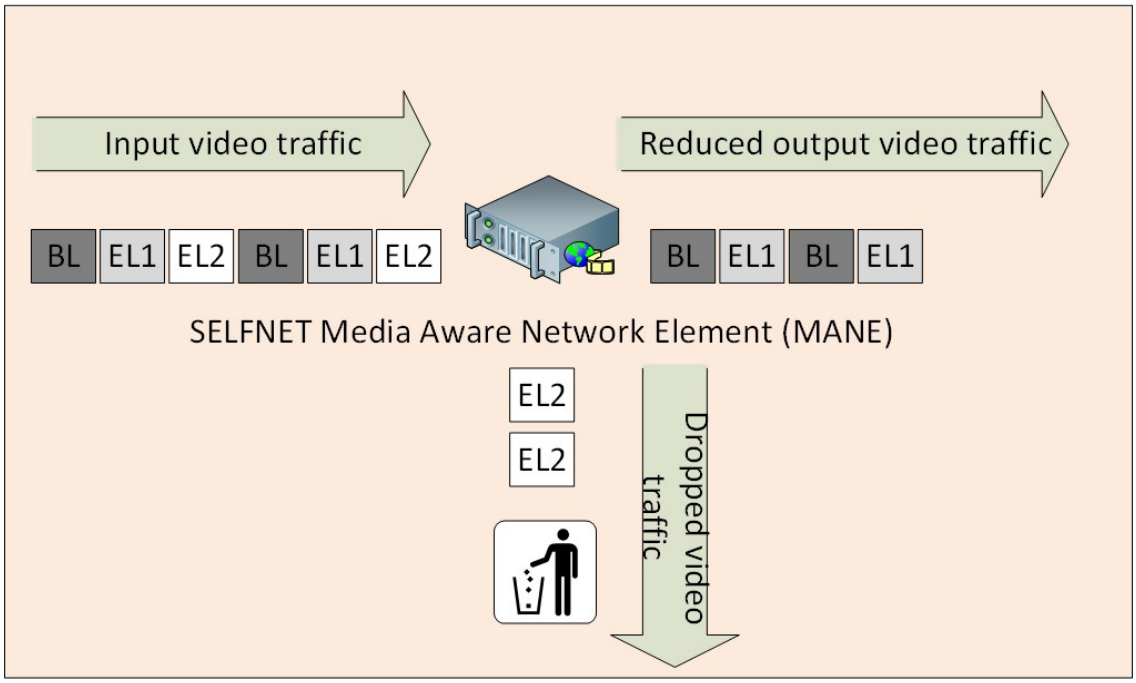


Figure 4.13 SELFNET video streaming adaptation use case scenario: data plane (example)

In this use case MANE's may be deployed to intelligently adapt scalable video streams in support of multiple objectives in network capacity management, energy management and user centric quality management. MANE's can support user-assisted 5G aims as part of an overall user-influenced QoE management strategy where both objectively measured QoE utility estimates and user preferences (as to which of his own application flows should have highest priority) form the basis of smart autonomic video adaptation schemes. Similarly MANE's might be deployed at strategic points in the RAN to adapt video traffic intelligently in order to reduce the energy consumption of 5G base stations or access points as part of a wider energy management strategy.

Previous MANE implementations have primarily adapted video streams encoded using the H.264 Scalable Video Coding (SVC) codec reactively in response to changes in available bandwidth. This use case, in addition to addressing the anticipated very large volumes of 5G U-HD video traffic encoded with new and emerging codecs, further considers a combined proactive deployment of MANEs and complementary SDN/NFV enabled smart tools for related tasks such as video caching, load balancing, traffic offloading and energy management.

This fact, combined with an efficient automated distributed deployment of MANE elements, is able to perform advanced video processing and adaptation wherever and whenever in the network, and thus will contribute to a number of ambitious KPIs envisioned in 5G. This will enable a real-time, continuous, smooth/seamless video streaming experience at the end users' side, and resolve network congestion by discarding non-essential information, which reduces the bandwidth consumed by video traffic flows.

Beyond QoS - Meeting User Expectations

As part of the ambitious SELFNET approach, new and innovative ways of measuring the health of networks that take account of user expectations of quality must be found and implemented in SELFNET SDN-Sensors and the SELFNET aggregator/analyzer module. The definitions of who or what constitutes an end user in the 5G environment must be revised in light of the expected upsurge in M2M communications (including video application for surveillance etc.) in 5G networks as must the way in which QoE is expressed for these new services.

Video Stream QoE Indicators

It is now widely recognized that the estimation of user QoE for streamed video content is dependent upon many factors, some of which relate directly to the nature of the video itself, some to the type of encoding used, some to the type of client side playback device and its resource limitations and others to traditional QoS metrics from the transmission network. Estimation of QoE is therefore a very challenging and, as yet, unresolved, area of research. From a video perspective the content type of the video is of primary importance, for example a video containing low levels of detail and motion such as a newsreader sitting at a desk is significantly less susceptible to network impairments than a high motion, highly textured sports broadcast. In order to successfully demonstrate the capabilities of the SELFNET framework to manage immense volumes of 5G video traffic, SELFNET SDN-Sensors must be able to acquire important video stream metrics such as content type in real time, either from pre-processed data inserted into the stream, from metadata files such as the MPD

file used in Adaptive HTTP streaming, or on the fly during transmission. The SELFNET aggregator/analyzer must also be able to derive high level objective QoE estimates from the monitoring data delivered by the SDN-sensors. It is therefore important that The SELFNET framework must provide a means of accessing video stream QoE indicators from encrypted video streams, either through metadata, a video stream descriptor file or by inclusion of unencrypted data in the video packet headers. The SELFNET framework should also be able to manage QoE -aware video stream management end to end across multiple service provider domains.

Two-Tier Data Centre Architecture

It is envisaged that MANE (and other traffic engineering resources) will be deployed across a two-tier data centre architecture. In access networks virtualized resources would be deployed at 'last mile data centres' located at the ISP's point of presence (PoP), while virtual resources would be deployed at the SELFNET central data centre to provide network management functionality such as traffic engineering and video adaptation within the core network. This two-tier approach will facilitate, amongst others, coordinated local energy-aware management at the PoP of 5G base stations and access points. Unlike existing MANE deployments that provide static MANE resources in the core or RAN networks, this use case considers the ability to rapidly deploy MANEs either in the core (central data centre) or at the network edge (last mile data centre) to proactively manage video traffic and to meet user QoE expectations. This requires new intelligent behaviour that is context (e.g., network topology), energy consumption, user preference, service type and video content aware.

Energy Aware

SELFNET should be an energy-aware system end to end. We can follow different approaches to get information about the energy consumed by each of SELFNET's components. Information can either be collected from the physical components presents in the RAN or from congestion mapping and prediction taken from SELFNET HoN metrics. These HoN metrics will be able to predict when congestion is about to happen in a given RAN including at any given base station or access point and the estimated energy consumption of all scalable video streams routed through that base station.

The SELFNET decision making process will then decide how to cope with this congestion which may either be by energy-aware and QoE-aware scalable video adaptation via a MANE deployed at the DCPoP or by traffic engineering solutions such as redistributing to adjacent base stations according the network load. Additionally in areas where high densities of users might be expected such as airports or sports venues/events stadia, the SELFNET decision maker will selectively activate and deactivate physical resources such as base stations and access points as and when required to manage energy consumption.

SELFNET will propose a more flexible way to optimize the number of active network elements as the traffic grows/decreases making the network more efficient in terms of energy consumption. This is especially relevant in spaces with a high density of users and time variant traffic patterns. In respect of the latter, the SELFNET platform can collect usage statistics and extract daily usage profiles per network element. The platform can extract users' location and movement patterns. This will identify heavily used locations and help to define the optimum number of NEs that should be started at a given moment of the day and location. Improvements in terms of energy

consumption can be achieved also at network element level: when high QoE is detected it is very likely that the network elements have spare bandwidth. In such a case we can reduce the link capacity to save energy. Should the system is able to use an energy-aware cloud system then SELFNET will also be aware of the energy consumed by the virtual network functions deployed in the cloud infrastructure. GreenCloud [21] is an example of system with the capability to capture details of the energy consumed by data centre components as well as packet-level communication patterns between them.

New and Emerging Video Applications

SELFNET sensors and actuators must also be able to effectively manage, at immense scale, video applications other than the current provider/subscriber models of content delivery networks that may emerge as users gain access to the expected high bandwidth and low latency 5G network environment. For example, in addition to a potentially huge rise in the use of video calling applications at very high densities within the RAN, new real-time video streaming services where individual mobile users can be either content provider or subscriber may emerge.

4.4.3 Relation to 5G requirements/ visions

The proposed use case scenario would be able to demonstrate SELFNET's contribution to the following KPIs [46] [47]:

- "New economically-viable services of high societal value (like U-HDTV and M2M applications)" (Societal KPI) in terms of supporting and optimizing U-HD video services
- "Zero perceived downtime for services provision" (Performance KPI) in terms of minimising video streaming disruptions for end users
- "10 to 100 times more connected devices" (Performance KPI) in terms of supporting more video sessions (or users) by employing the more efficient new video codec
- The implementation of the use case will contribute to the reduction of the provisioning time from "90 hours to 90 minutes" (Performance KPI) for the services involved in this use case. It would validate the feasibility of SELFNET Framework to reduce the provisioning time of other software elements.
- To improve the speed of video delivery, via smart caching and/or other techniques wherever appropriate, to make complementary contribution at the application level to the ultra-low latency envisioned in 5G (sub-1ms latency Performance KPI within 1 Km).
- To support applications and services with an optimal and consistent level of QoE anywhere and anytime.

4.4.4 Stakeholders

The Self-Optimization use case is aligned with the following 5G groups of stakeholders:

- Manufacturers
- Industry associations
- Research community
- Regulatory bodies and universities
- Network operators

- Vertical sectors like energy, health, manufacturing, robotics, environment, broadcast, content and creative industries, transport, smart cities.
- Communication service providers
- Public administrations

4.4.5 Contributions and innovations of the SELFNET self-optimisation use case

This self-optimization use case will have significant impact on major areas of 5G development and performance. Firstly, it will underpin the EU 5G vision of ubiquitous delivery of new services based on U-HD video. Secondly, it will contribute to performance improvements through faster deployment times and reduced service discontinuity. Thirdly it will place the user at the heart of network management decision making by adopting a QoE based approach to service level monitoring and delivery and finally it will reduce operational costs and help to meet carbon reduction targets by operating in an end to end energy efficient manner.

The transition from QoS to QoE aware service delivery represents a highly innovate change in how services are delivered. In QoE based video streaming the emphasis is on how users perceive of the quality of the services they receive. Any such transition will have significant societal impact. The self-optimizing use case will not only define novel methods of estimating the user's perceived QoE but will implement them as part of an end to end user centric approach to video streaming. In addition further highly innovative and challenging QoE estimation techniques for video services such as M2M and automated surveillance where quality is measured by the utility of the information contained in a video when performing a task such as object recognition, target tracking or decision making tasks. The SELFNET framework will provide sensors, actuators and the decision making logic required to realise QoE based video streaming.

The self-optimization use case will support the transition from current video encoding standards to the new H.265 standard and its scalable extension. Innovative, fast and reliable in network media adaptation NFVs will be developed for use with U-HD video encoded using these latest codecs.

SELFNET sensors must be equipped with a means of acquiring video metrics from both compressed and encrypted video streams and actuators, such as NFV-MANE's with a means of adapting those same streams. No such capability currently exists.

Another SELFNET innovation that will be developed from the YouQoS concept [48] is the introduction of receive-subscriber driven QoE optimization. It allows the consumers to influence network management decisions about their traffic. This feature will help small service providers to compete with industry giants. For example a subscriber may prefer to watch a video from a small service provider instead of e.g. YouTube and assign priorities accordingly.

In terms of energy awareness, the self-optimization use case will use novel energy monitoring sensors to develop a global view of energy usage across the network, and then optimize energy use through the deployment of Energy Manager NFVs.

4.5 Composite Use Case

In addition to the three different use cases defined above, SELFNET will also be tested and verified against a hybrid use case in which either two, or all three, of the primary use cases (self-healing, self-protection and self-optimization) are

simultaneously involved. A prerequisite for the hybrid use case will be prior successful validation of all of the elements (SDN controllers, SDN-Apps and NFV-Apps) designed and developed for the individual use cases.

The main purpose of this composite use case is to validate the integration and interworking of the three individual SDN controllers and to demonstrate how SELFNET is able to fuse their composition in more complex scenarios. Consequently, this coordinated use case tests the inter-coordination between NFV-Apps and SDN-Apps and aims to demonstrate of vertical coordination of the different apps from each individual use case. This will solve the problems inherent in each of them, but without negatively affecting the operation of the rest. The composition of individual use cases in a hybrid one will further test the robustness, expandability and adaptability of the SELFNET framework, offer insights into managing complex network problems when they are considered together for an integrated solution from a global system-wide point of view.

The storyline of this hybrid SELFNET use case will be developed by combining elements from the scenarios defined in each of the three primary use cases (self-healing, self-protection and self-optimization). An example of one possible combined scenario could be a situation in which the 5G network encounters a critical situation such as being subjected to a DDoS attack. In this scenario the self-protection functionality will be triggered first in order to combat the attack both proactively and reactively. As a consequence of the initial attack some damage has either occurred to the infrastructure (or currently running services) or is predicted imminently occur despite the self-protection actions. The self-healing functionality will then be triggered either concurrently or sequentially to provide corresponding remedies which either avoid or mitigate the detected/anticipated damage. After the system is restored to a normal operation state by self-protection and self-healing actions, the self-optimization functionality may be triggered to optimize the performance of the system according to a predefined or run-time optimization target.

5 SELFNET Requirements

Towards implementing the proposed SELFNET architecture, its components and the use cases, this section derive and summarize the requirements foreseen at this stage of the project. The complete list of the requirements identified for each reference architecture layer, each component and use cases can be found in Annex A, Annex B, and Annex C.

5.1 Requirements Methodology

In order to obtain the system requirements of SELFNET platform we will use a top-down approach starting from the global use case that includes all the technical scenarios that may be targeted by the approach proposed by the project. Then we will filter and consider use cases with a narrower scope which will be driven by different technical domains of network management (configuration, optimization, security, etc.). The idea is to focus in a limited number of use cases that will target real problems of 5G while maintaining a realistic scope that may give the partners the opportunity to verify the project's thesis. In the next stage we will do a decomposition of each technical domain and will select representative use cases in the following domains: optimization of network performance, self-healing capabilities and self-protection of the network. Next step will be extracting technical requirements that will allow the implementation of the selected use cases following SELFNET's approach. The obtained requirements will be organized to the use cases themselves and also to the system architecture that SELFNET proposes in order to tackle the consolidated scenarios based on such use cases (Figure 5.1).

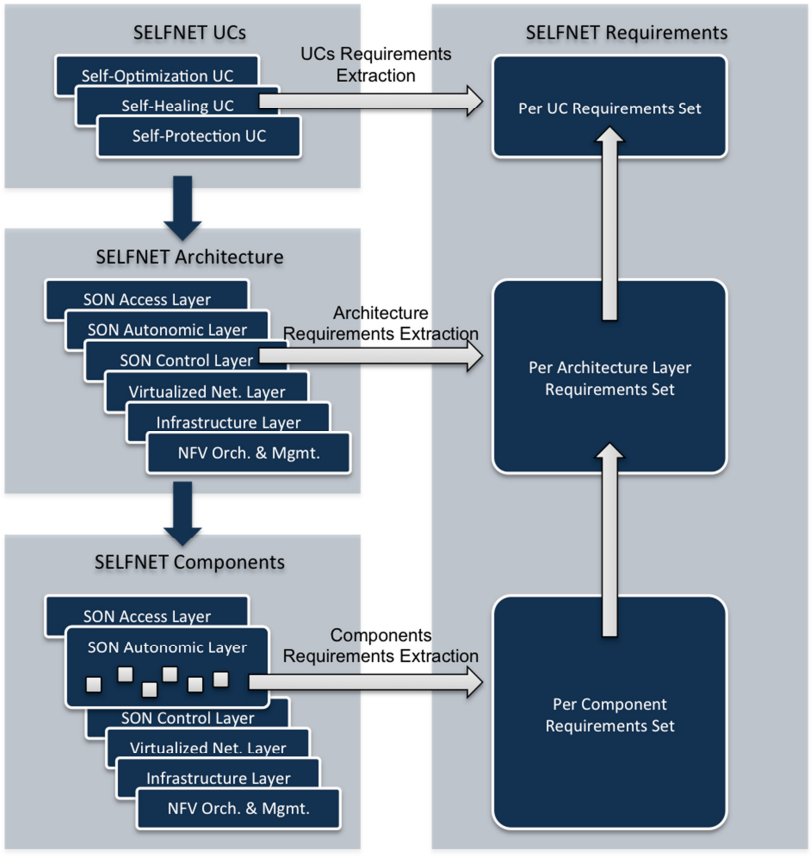


Figure 5.1 Requirements Methodology

5.2 General Requirements

Most of the general requirements of SELFNET come from the adoption of the different design principles and the convergence of similar needs on the use cases. This is intended to facilitate the development of a layered architecture, extensibility, expandability, scalability and accommodation to different standards and regulations. This cluster of requirements includes various conditions, highlighting those aspects of SDN/NFV applications, layering or monitoring, involved on the specification and deployment of SELFNET. However, in addition to these characteristic features, it is important to take into account other attributes in direct relationship with implementation and validation. They include conditions related to the operation, verification, certification and compatibility of the different SELFNET actors, underscoring those concerned with the function/elements repository, hardware or interaction with SDN/NFV technologies.

5.3 Use Case Requirements

5.3.1 Self-Healing Requirements

Addressing the various problems posed by the Self-healing Use Case implies the necessity of satisfice several conditions. The most basic requirements focus on the problem of information management, such as collecting and storing data provided by the SELFNET actors or the ability of monitoring the pre-defined levels of SLAs (network slices). Reactions led by the decision making planner are also taken into account. Because of this, SELFNET must be able to deploy sensors in order to monitor the network response to the SH actuators, and access information on the healing database in order to enhance the self-healing recovery plan. This group also includes the need of performing a fast deployment of multiple reactive/proactive recovery mechanisms, and the ability of reverse them. To take the appropriate decisions for each situation, the identification of certain events is also required. Thus, SELFNET must be able to detect vulnerabilities on the virtual execution environment, unexpected peaks on the network infrastructure and errors on the physical layer, such as link failures, hardware problems, energy output inconsistencies or misconfigurations. From these observations SELFNET must have the potential of inferring infrastructure metrics, SLAs metrics, Cyber-Footing Human dynamics correlations, and with these, predict service disruptions or network failures. Along with this, the Self-Healing Use Case could carry out its mandated activities. However it must also meet other general requirements. For example, in order to ensure its operation, the updating/modification of modules on repository must not affect the correct operation of Sensors/Actuators running on infrastructure. Another optional feature is to preserve isolated execution environment in accordance with the multi-tenancy capabilities. Finally, to in order to provide good QoE, it is required that customers obtain feedback about success/failure of different processes in SDN/NFV modules.

To achieve good results, others additional requirements should be taken into account. This is the case of secure data provided by SELFNET actors by encryption or store information about the SLA fulfilment during network operation. The last group of requirements gathers all situations that may be implemented. For example, SELFNET may verify and certify the modules published in repository. This repository may also provide rating information about such modules. In respect of interoperability, it is important to note that SELFNET may support interaction with services that does not support SDN/NFV technologies.

5.3.2 Self-Protection Requirements

The implementation of the self-protection use case described above poses a set of challenges and requirements to the SELFNET platform that can be briefly summarized with the following keywords: distribution, multi-tenancy, automated deployment and composition, multi-level and self-learning.

5G will bring much more users and interconnected devices combined with higher data rates, mobility and dynamicity than current 4G and fixed networks. When moving to network security aspects and functions, traditional security infrastructures need to evolve towards more flexible and manageable solutions able to cope with challenges posed by high density of 5G services and users. For this reasons the self-protection use case requires security functions to be distributed and spread in the 5G network, to have them located (and dynamically re-located) close to crucial and vulnerable points according to specific 5G service and user needs. Multi-tenancy is also key in 5G environments, especially for network and service providers that can have concrete new business opportunities when virtualizing their infrastructures and offering virtualized services to customers and other stakeholders in general. Security sensors and actuators functions must be therefore implemented as virtualized network functions following NFV and be part of distributed security services running over per-tenant virtualized networks and infrastructures. The combination of a distributed security service with sensors and actuators implemented as VNFs requires a high degree of automation in deployment of these security VNFs in the virtualized infrastructures to support to self-capabilities envisaged by SELFNET. In addition, SELFNET must also provide automated mechanisms for the composition of individual sensors and actuators, where multiple distributed VNFs are chained and traffic is steered across them to build security services spanning different portions of the 5G networks. A further degree of dynamicity is also required here, mostly in support of new actuator VNFs to be dynamically deployed and included in the distributed service. Upon the detection of a cyber-attack, a prompt re-configuration and re-provisioning of the service chain is required to properly switch the affected traffic to the actuator for mitigation purposes.

In addition to the above automation and dynamicity requirements, the highly distributed and virtualized approach proposed in the self-protection use case poses scalability and performance challenges, mostly when considering traffic monitoring and inspection of 5G ultra high data rates. The implementation of detection and monitoring functions at multiple granularities and levels of abstraction is therefore needed. On the one end, high-level sensor VNFs are required to provide a first stage of cyber-attacks detection, e.g. by only inspecting network flows. On the other end, low-level and deep traffic inspection virtualized functions are required to provide a second stage of cyber-attacks detection for those network traffic flows already identified as suspect to be under attack. This combined multi-level and multi-granular detection approach allows collecting heterogeneous information about detected attacks, and opening the possibility to implement self-learning techniques, which can be considered as the ultimate requirement for SELFNET to provide a full self-protection system. Indeed, SELFNET should implement learning algorithms and tools with the aim of tuning its protection procedures and decision mechanisms analysing previous attacks and evaluating success or failure of previously applied strategies.

5.3.3 Self-Optimization Requirements

In order to optimize network resource usage, while maintaining a good QoE, the Self Optimization use case must implement new functionality as well as port existing functions to the SELFNET framework. This use case takes advantage of the emerging codec H.265 that allows a layered encoding of video, as well as HD and U-HD resolutions. Codecs that allow layered encoding allow some of the layers to be dropped, reducing video quality, but keeping the video playing without artefacts or buffering pauses. This allows the video stream to be manipulated in such a way that the QoE is maintained for the end user without the need to use an expensive operation such as transcoding. The first set of requirements deals with the availability of the codec, as well as the building blocks needed to build a service chain that allows the manipulation of a single H.265 stream in a SELFNET environment.

When many streams from different sources are present, it becomes necessary to categorize them according to SLA in order to differentiate essential video streams such as telemedicine from less essential streams like a regular video call. Once this initial differentiation is accomplished, each class of stream can then be subject to the different kinds of manipulation available on the SELFNET platform. If the RAN is congested, some non-essential layers of the video can be dropped, hence consuming less resources, allowing the QoE to be maintained. If the core network and ISP peering are congested, caches can be deployed on the network, reducing the pressure on the congested links by serving the most common streams from a cache placed as close to the end user as possible. A second set of requirements deals with the co-existence of very different flows of video on the network, as well as different types of congestion and unreliability. The objective is to perform different adaptations for each situation, while attempting to maintain a good QoE for the end users.

This use case also attempts to take into account user preferences when deciding to apply any modification to a video, as well as on what kind of modifications to apply. A user can record his preferences with the SELFNET system, specify relative priorities for each type of stream and the SELFNET elements will take those preferences into account when performing traffic optimizations, for instance by dropping an extra layer of a lower priority stream to keep an extra layer on a higher priority stream for the same user. The third set of requirements attempts to reflect an user orientation, where the user is allowed to save his personal preferences, and where possible, the SELFNET framework will take those preferences into account when deciding how to handle each video stream.

The final goal of this use case is energy efficiency. The autonomic engine that manages the deployment of the components on the physical infrastructure will take among others, expected energy impact of deploying a virtual function as well as the impact of activating certain elements such as radio antennas. This is expected to allow a higher level of virtual components consolidation allowing certain physical resources to enter lower energy states when not used at all. A more aggressive possibility that will be explored is actually signalling some of the seldom used infrastructure to enter a soft off state, which would achieve a higher energy conservation not only via a direct reduction of consumed power but also via the reduction of the energy spent dissipating generated heat. The final set of requirements deals with the need to feed energy related metrics to the core of the SELFNET autonomic layer, the autonomic layer will then take these new metrics into account when deciding between similar deployments with different energy consumption requirements.

5.4 Component and Layer Requirements

5.4.1 Infrastructure Layer Requirements

The Infrastructure Layer must effectively establish the link between the SELFNET framework and the underlying 5G mobile networking system to allow 5G base stations to be connected to virtualized SELFNET services. To enable multiple mobile network operators to share the same infrastructure, multi-tenant aware virtualization and distributed locations support must be enabled in this layer. This layer must offer a logical separation between control plane and data plane, and facilitate the monitoring of both physical and logical infrastructure whilst putting all the network traffic under control.

5.4.2 Virtualized Network Layer

The Virtual Network Infrastructure must also support multi-tenancy so that the resources can be shared among multiple operators. Service continuity must be controlled through transparent and dynamic service chaining. Metrics relating to the overall operation of the infrastructure must be maintained in order to aid autonomic operation.

5.4.3 SON Control Layer Requirements

This layer may be considered the place holder to allocate all the system requirements associated to the use cases considered in SELFNET. Also, as an overall functionality to enable the provisioning of this use cases, the system must provide support for the execution of SDN, VNE and VNF Applications. These applications should provide a common way to perform their configuration and monitoring in order to enable upper layer to interact with this. This layer will also contain the SND Management Applications to control the channelling of other SDN apps. It will consider as well the adaptability of the architecture to enable the usage of different SDN Controller.

5.4.4 SON Autonomic Layer Requirements

5.4.4.1 Monitoring

Monitoring module must be able of collect and manage all data provided by the various SELFNET actors, discover new devices and sensors deployed on network and facilitate the querying of gathered information to the coming processing stages. All of this must be consistent with the current status of the network.

To bring this about, data structures involved in storing monitored information may be efficient and allow implementing different abstract data types. Finally, monitoring should be adapted to the communication protocols used by the different actors, layers and tasks of SELFNET. This implies that the gathered data must be provided by the different APIs and interfaces of SELFNET, and is accessible and understood by the coming processing stages.

5.4.4.2 Aggregation

The aggregation module will transform low-level metrics received from the monitoring module to high-level metrics that translate potential suspicious or anomalous situations in the SELFNET framework. The high-level metrics are obtained through, for example, data correlation, data processing, data mining and/or data prediction

and delivered to the analysis module. The aggregation module should be implemented in an easy configurable way, and well-defined southbound (towards the monitoring module) and northbound (towards the analysis module) APIs must be provided.

5.4.4.3 Analyzer

The analyzer module must be able of calculate the current status of SELFNET, perform identification and assessment of suspicious or anomalous situations, and provide any information required for decision making. All of this must be performed efficiently, in order to facilitate the deployment of countermeasures in real time. In addition, the assessment of detected situations should be proportional to their impact.

Data structures involved in storing monitored information may be efficient and allow implementing different abstract data types. In order to enhance the processes of analysis, they also should permit encapsulation of information.

Finally, monitoring should be adapted to the communication protocols used by the different actors, layers and components of SELFNET. This implies that the gathered data must be provided by the different APIs and interfaces of SELFNET, and is accessible and understood by the coming processing stages.

5.4.4.4 Tactical Autonomic Language

The Tactical Autonomic Language and the accompanying library provide the means for expressing autonomic policies in a way that can be integrated with the overall functionality of the rest of components of the SON Layer. The language allows for definition of several parameters that regard HoN and other metrics. The various metrics are processed according to the specified policies and every time the library is fed with the related status data it produces an configuration plan to be used by the decision making engine to provide an action plan. The language must be extensible and must support simple or complex expressiveness to describe autonomic policies.

5.4.4.5 Intelligent Network Diagnostic Algorithms

Intelligent Network Diagnostic module is capable of diagnosing the detected network problems and providing the reactive and corrective strategies based on the incoming monitoring information. Besides, Intelligent Network Diagnostic module can diagnose potential network problems and provide the proactive and preventive strategies before the problem take place or become critical. The proactive and preventive capability of network management is one of the distinct features provided by SELFNET framework. This module should recognize and process the incoming Monitoring information timely and correctly, and provide the reactive and proactive strategies to the Decision-Making module. This module should follow the semantics, data structures; strategies defined in tactical autonomic language and can directly utilize its functionality library. Intelligent Network Diagnostic module should be implemented in an open, programmable and extensible way, which facilitates the later update and evaluation.

5.4.4.6 Decision Making Planner

Decision Making Planner is capable of deciding a set of reactive and corrective actions to deal with the detected network problems based on the incoming diagnostic information. Besides, Decision Making Planner is capable of deciding a set of proactive and preventive actions to deal with the potential network problems before the problem take place or become critical. The proactive and preventive capability of

network management is one of the distinct features provided by SELFNET framework. This module should recognize and process the incoming diagnostic information timely and correctly, and provide the reactive and proactive sets of actions to the Action Enforcer module. This module should follow the semantics, data structures; strategies defined in tactical autonomic language and can directly utilize its functionality library. Decision Making Planner should be implemented in an open, programmable and extensible way, which facilitates the later update and evaluation.

5.4.4.7 Intelligent Action Enforcer

The Action Enforcer (AE) must receive and process multiple actions provided by the Decision Making Planner in order to deal with the identified and potential network problems in both reactive and proactive manners. To this end, AE must enable the definition of multiple inputs so that it can receive multiple actions. Moreover, the AE must validate the consistency and coherency of the received action plan e.g., by applying conflict detection and resolution techniques. AE must organize and provide an implementable plan with one or more actions ready to be enforced by the Orchestrator by leveraging language refining and other techniques. Furthermore, AE must interface with the DMP and the Orchestrator in an efficient way. To this end, the design of AE should take into account the data structures, semantics and strategies defined in TAL, DMP and the Orchestrator, and the communication protocols used by AE should be designed/adapted accordingly.

5.4.4.8 Orchestrator

The Orchestrator (OR) must be able implement the action plans provided by the AE from the Decision Making Planner, according to the available Apps and network resources which are administered by the NFV/SDN Application Manager. The OR must be able to query the available resources and Apps, and this data will include the features of the resources and Apps. The received features are translated into low level actions and filtered matching the provided high level actions. The OR should resolve dependencies of several instructions. The result will be a set of low level actions which can be applied directly to the Apps. The OR enforces the actions using the Actuator API. Additionally the OR should inform the DMP about the enforced Actions, so the DMP can readjust the sensors to check impact of the actions. In addition, the OR also acts as a resource broker.

5.4.4.9 NFV/SDN Application Manager

The App Manager processes orchestration requests relating to provisioning and configuration of NFV/SDN Apps that are instantiated in running computing resources (virtual or physical) as applications. A resource abstraction layer for those resources that require a resource adaptor (agent) to be instantiated for processing sensing/actuations requests may be maintained by the App Manager. The App Manager can use application deployment systems such as Chef, Puppet, Docker, etc. in order to enumerate the available data layer resources that can accommodate and execute Apps and also to perform setup and configuration actions. Support of SDN North and/or proprietary protocols may be required for the execution of simple configuration and control actions that do not require control layer artefacts to be instantiated. Finally the App Manager must be able to detect the status of the deployed Apps and optionally trigger alerts to be handled in the context of autonomous operation.

5.4.4.10 Resource Manager

The Resource Manager (RM) will provide the interaction with the virtual infrastructure manager (VIM) and with the WAN Infrastructure manager (WIM) in order to enable the implementation of the actions provided by orchestrator module. Abstraction of underlying particular technologies will be considered in order to enable the usage of different VIM and WIM implementations. .

The RM will instantiate / delete SDN-Apps and NFV-Apps over the cloud infrastructure. This component will enumerate the available resources in the NFV Layer in terms of available networking functionality in the context of the orchestration scenarios. The RM will maintain as well a list of used and available cloud resources. It will be in charge of the complete lifecycle of the associated resources emphasizing optimal resource usage.

5.4.4.11 NFV Apps and SDN Apps Encapsulation

The NFV Apps and SDN Apps encapsulation must provide a common approach for the life-cycle management of VNFs developed in SELFNET to implement heterogeneous sensors and actuators functions. Unified mechanisms, primitives and APIs must be provided to abstract the SELFNET VNFs and publish their capabilities irrespectively of the given sensor or actuator nature. The NFV Apps and SDN Apps encapsulation must therefore allow the containerization of developed sensors and actuators into standardized SELFNET NVFs for their homogeneous storage, access and management. On top of these common abstraction functionalities, the encapsulation must also provide mechanisms and tools to automate the deployment and undeployment of actuator and sensor Apps in the SELFNET virtualized infrastructure.

5.4.4.12 NFV / SDN Repository

The NFV and SDN repository must provide a storage place for all the NFVs implemented by SELFNET (and possibly external) developers. Dedicated mechanisms and tools to access stored NFVs and collect information about their capabilities must be also provided by the repository, mostly to allow other SELFNET components in the SON layer to manage the life-cycle of the SELFNET VNFs and easily deploy them leveraging on the abstraction provided by the encapsulation functionalities. The NFV & SDN repository should act as the SELFNET sensors and actuators market place, where heterogeneous information related to NFVs must be exposed in a structured way. Also, mechanisms to publish newly stored NFVs to other SELFNET SON components must be provided. The NFV & SDN repository should therefore make available new VNFs as soon as created and stored for their deployment in the virtualized infrastructure, also giving the possibility to software developers to update their NFVs and consequently support their versioning.

5.4.5 SELFNET Access Layer Requirements

5.4.5.1 Graphical User Interface

The GI will provide an appealing and intuitive interface for authorized users to monitor and check on the status of SELFNET. Using this interface, users will be able to check on the status of SELFNET and see current errors and anomalies that the system is experiencing. GI will list all the sensors and devices currently deployed in SELFNET and will also provide a view on the loggings and messages provided by these devices and sensors. By doing this, GI will allow efficient motorization of the

status and behaviour of each sensor allowing to not only have a wider view of the SELFNET status but also analysing the behaviour and pinpointing any problem to a given sensor/device.

SELFNET aims to be an independent and autonomous solution that will not only detect a strange or error behaviour/pattern on a SDN but also acting upon it and mitigating or solving it without any actions from real users. Despite this autonomous behaviour, it is expected that end users will be able to see and study actions taken by SELFNET allowing either the validation or the application of corrective measures. GI will provide a view on the actions taken by SELFNET allowing end users to audit them and validate SELFNET's autonomous workflow.

The GI will also provide the ability to support the definition and enforcing of the autonomic capabilities expressed by the tactical autonomic language.

5.4.6 NFV Orchestration and Management Layer Requirements

5.4.6.1 VIM Cloud Management

The VIM Cloud Manager must provide a central point to manage virtual infrastructures. It must support the ability to handle multiple points of presence geographically separated in order to handle data centre and edges of the network. It will provide the support for multi-tenancy in virtual infrastructure and the ability to control and manage such infrastructures.

5.4.6.2 WIM NFV Management

The Wan Infrastructure Manager (WIM) provides a central point to manage virtual network infrastructures. It should support the ability to handle multiple points of presence geographically separated in order to handle data centre and edges of the network. It will provide the support for multi-tenancy in virtual network infrastructure and the ability to control and manage such infrastructures. Each of the controlled elements of this manager should provide the ability to control of traffic flows in order to provide service channelling services along the infrastructure.

6 Conclusions

The SELFNET project aims to design and implement an autonomic network management framework, which involves a number of essential management tasks such as automated network monitoring, autonomic network maintenance, automated deployment of network tools and automated network service provisioning. To facilitate the subsequent detailed design of the whole system, this deliverable has presented the initial step to define the specification of use cases, system requirements and their components, aligned with 5G visions/requirements and following a use case driven methodology. The deliverable document will be a working document evolving along the execution of the SELFNET project and used as a guideline for the subsequent work of the project.

Firstly, this deliverable has produced an updated and detailed SELFNET reference architecture, developed significantly from the original version presented in the project proposal. A strictly layered approach was determined, comprising five main layers (bottom-up order: Infrastructure, Virtualized Network, SON Control, SON Autonomic, and SELFNET Access), which have been specifically defined in order to establish the SELFNET framework to provide the proposed self-organization and automation capabilities to the network. These layers have been proposed in line with the NFV and SDN concepts, namely on the architecture that is determined by ETSI. These concepts are widely recognized as key enabling technologies for 5G systems.

SELFNET's architecture is based on NFV and SDN standards proposed by ETSI NVF and Open Networking Foundation respectively, but it goes a step beyond by combining both. The approach for a careful integration of NFV and SDN in the SELFNET architecture has been presented to enable cost-effective SDN-controlled VNFs and other flexible SDN/NFV based deployment. Moreover, the sublayers and components in these layers have been described in details.

Secondly, the definition of the use cases has been motivated and inspired by an analysis practice of 5G requirements, visions and Key Performance Indicators (KPIs). This analysis has outlined the challenges and drivers of 5G systems and also the possible contribution of SELFNET in meeting the ambitious 5G-PPP KPIs. Consequently, three use cases have been defined: self-healing, self-protection and self-optimization. The Self-healing use case targets realizing, detecting and avoiding failures in the new virtualized networking paradigm before the pending problems occur, thereby greatly advancing the current "Break-Fix" approach and thus minimizing potential damages to the service provisioning. Self-protection offers an innovative way of deploying multi-tenant security services distributed across edge and core 5G networks to counter distributed cyber-attacks. The last use case, self-optimization, focuses on addressing the optimal delivery of resource-demanding Ultra-HD videos in mobile networks, one of the major 5G drivers and great challenges, taking into account the end users' QoE, preferences and energy efficiency.

Thirdly, based on the definition of the updated SELFNET reference architecture and the uses cases, a range of technical requirements for building the architecture and achieving the use cases have been derived. These include the general requirements for the whole system, specific requirements for each architectural layer and its components, and use case specific requirements. For this purpose, the analysis of data structures, methodologies, protocols, techniques and technologies have been

carried out and the resultant requirements are archived in a series of tables. In addition, other important issues have been discussed, such as the initial interoperability and compatibility conditions to unify the inputs/outputs of the modules or the non-functional requirements of SELFNET including data integrity, security, privacy, system performance, extensibility/expandability, and scalability.

Finally, as the foundation of the use cases and system requirements of SELFNET has been established through this deliverable (D2.1), the next step is to further define the APIs and interfaces towards creating a functional architecture and facilitating the system integration at a later stage. The result of this subsequent activity will be reflected in the following deliverable (D2.2). It is noted that this deliverable is a working reference document for the project and it is expected to undergo continuous review and adjustments during the course of the project.

7 References

[1] “5G-PPP. Advanced 5G Network Infrastructure for the Future Internet,” 2013. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/Advanced-5G-Network-Infrastructure-PPP-in-H2020_Final_November-2013.pdf

[2] FP7-ICT, “EU UNIFY Project. Unifying Cloud and Carrier Networks. Project reference: 619609. Funded under: FP7-ICT,” 2014. [Online]. Available: http://www.fp7-unify.eu/.

[3] “MCN Project. Funded under: FP7-ICT. Project reference: 318109,” [Online]. Available: http://www.mobile-cloud-networking.eu/site/.

[4] “ETSI NFV,” 2015. [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/nfv.

[5] “ONF,” 2015. [Online]. Available: https://www.opennetworking.org/about/onf-overview.

[6] “TMForum ZOOM,” [Online]. Available: https://www.tmforum.org/zoom.

[7] L. Gavrilovska, V. Rakovic y V. Atanasovski, “Visions Towards 5G: Technical Requirements and Potential Enablers,” *Wireless Personal Communications,* pp. 1-27, May 2015.

[8] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong y J. C. Zhang, “What Will 5G Be?,” *IEEE Journal on Selected Areas in Communications,* vol. 32, nº 6, pp. 1065-1082, June 2014.

[9] V. C. M. Borges, K. Vieira Cardoso, E. Cerqueira, M. Nogueira y A. Santos, “Aspirations, Challenges, and Open Issues for Software-Based 5G Networks in Extremely Dense and Heterogeneous Scenarios,” *EURASIP Journal on Wireless Communications and Networking,* vol. 164, pp. 1-13, June 2015.

[10] B. Bangerter, S. Talwar, R. Arefi y K. Stewart, “Networks and Devices for the 5G Era,” *IEEE Communications Magazine,* vol. 52, nº 2, pp. 90-96, February 2014.

[11] P. Kwadwo Agyapong, M. Iwamura, D. Staehle, W. Kiess y A. Benjebbour, “Design Considerations for a 5G Network Architecture,” *IEEE Communications Magazine,* vol. 52, nº 11, pp. 65-75, November 2014.

[12] D. Soldani y A. Manzalini, “A 5G Infrastructure for "Anything-as-a-Service"," *Telecommunications System & Management,* vol. 3, nº 2, pp. 1-10, August 2014.

[13] A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch, M. Maternia, O. Queseth, M. Schellmann, H. Schotten, H. Taoka, H. Tullberg, M. A. Uusitalo, B. Timus y M. Fallgren, “Scenarios for 5G Mobile and Wireless Communications: The Vision of the METIS Project,” *IEEE Communications Magazine,* vol. 52, nº 5, pp. 26-35, May 2014.

[14] H. Viswanathan y M. Weldon, “The Past, Present, and Future of Mobile Communications,” *Bell Labs Technical Journal,* vol. 19, pp. 8-21, August 2014.

[15] N. Alliance, “5G White Paper,” 2015. [Online]. Available:

https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf.

[16] "5G: Challenges, Research Priorities, and Recommendations," *NetWorld2020,* 2014.

[17] Nokia, "5G Use Cases and Requirements," 2014. [Online]. Available: http://networks.nokia.com/file/31121/5g-requirements.

[18] J. Nightingale, Q. Wang, C. Grecos y S. Goma, "Deriving video content type from HEVC bitstream semantics," de *SPIE Photonics Europe*, International Society for Optics and Photonics, 2014.

[19] J. Wang, Z. Lv, Z. Ma, L. Sun y Y. Sheng, "I-Net: New Network Architecture for 5G Networks," *IEEE Communications Magazine,* vol. 53, nº 6, pp. 44-51, June 2015.

[20] S. Chen, J. Zhao, M. Ai, D. Liu y Y. Peng, "Virtual RATs and a Flexible and Tailored Radio Access Network Evolving to 5G," *IEEE Communications Magazine,* vol. 53, nº 6, pp. 52-58, June 2015.

[21] D. Kliazovich, P. Bouvry y S. U. Khan, "GreenCloud: A Packet-level Simulator of Energy-aware Cloud Computing Data Centers," *The Journal of Supercomputing,* vol. 62, nº 3, pp. 1263-1283, 2012.

[22] 5G-PPP, "5G Vision," 2015. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf.

[23] U. C. Kozat, V. Yazici y O. Sunay, "A New Control Plane for 5G Network Architecture with a Case Study on Unified Handoff, Mobility, and Routing Management," *IEEE Communications Magazine,* pp. 76-85, November 2014.

[24] R. Trivisonno, R. Guerzoni, I. Vaishnavi y D. Soldani, "SDN-based 5G Mobile Networks: Architecture, Functions, Procedures and Backward Compatibility," de *Proceedings of the 1st International Conference on 5G for Ubiquitous Connectivity (5GU)*, Akaslompolo, 26-28 November 2014.

[25] H. Hawilo, A. Shami, M. Mirahmadi y R. Asal, "NFV: State of the Art, Challenges, and Implementation in Next Generation Mobile Networks (vEPC)," *IEEE Network,* vol. 28, nº 6, pp. 18-26, November 2014.

[26] A. Imran, A. Zoha y A. Abu-Dayya, "Challenges in 5G: How to Empower SON with Big Data for Enabling 5G," *IEEE Network,* vol. 28, nº 6, pp. 27-33, November 2014.

[27] N. Zhang, N. Cheng, A. T. Gamage, K. Zhang, J. W. Mark y X. Shen, "Cloud Assisted HetNets Toward 5G Wireless Networks," *IEEE Communications Magazine,* vol. 53, nº 6, pp. 59-65, June 2015.

[28] C. Harold Liu y J. Fan, "Scalable and Efficient Diagnosis for 5G Data Center Network Traffic," *IEEE Access,* vol. 2, pp. 841-855, August 2014.

[29] A. Bradai, K. Singh, T. Ahmed y T. Rasheed, "Cellular Software Defined Networking: A Framework," *IEEE Communications Magazine,* vol. 53, nº 6, pp. 36-43, June 2015.

[30] J. Sanchez, I. G. Ben Yahia, N. Crespi, T. Rasheed y D. Siracusa, "Softwarized

5G Networks Resiliency with SelfHealing," de *Proceedings of the 1st International Conference on 5G for Ubiquitous Connectivity (5GU)*, Akaslompolo, November 2014.

[31] "ITIL," [Online]. Available: https://www.axelos.com/best-practice-solutions/itil.

[32] "NETCONF Protocol," [Online]. Available: http://www.rfc-editor.org/rfc/rfc4741.txt.

[33] "OpenFlow," [Online]. Available: https://www.opennetworking.org/sdn-resources/openflow/.

[34] "Open vSwitch," [Online]. Available: http://openvswitch.org/.

[35] E. I. S. G. (ISG), "Network Function Virtualization (NFV) Architectural Framework," pp. 1-21, 2013.

[36] E. I. S. G. (ISG), "Management and Orchestration (ETSI MANO)," pp. 1-184, 2014.

[37] Cisco, "Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014–2019," 2015. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

[38] J. . M. S. Vilchez, I. G. B. Yahia y N. Crespi, "Self-healing Mechanisms for Software Defined Networks," *8th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2014),* July 2014.

[39] 5.-P. w. paper, "Specialized Services, Network Management and 5G," [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2015/06/Specialized-Services-Network-Management-and-5G.pdf.

[40] F. Boccardi, R. Heath, A. Lozano, T. Marzetta y P. Popovski, "Five disruptive technology directions for 5G," *IEEE Communications Magazine,* vol. 52, nº 2, pp. 74-80, 2014.

[41] I. Alsmadi y D. Xu, "Security of Software Defined Networks: A Survey," *Computers and Security,* vol. 53, pp. 79-108, 2015.

[42] C.-J. Chung, P. Khatkar, T. Xing, J. Lee y D. Huang, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems," *IEEE Transactions on Dependable and Secure Computing,* vol. 10, nº 4, pp. 198-211, 2013.

[43] E. w. paper, "5G Systems," [Online]. Available: http://www.ericsson.com/res/docs/whitepapers/wp-5g-security.pdf.

[44] A. w. paper, "5G is coming: Are you prepared?," [Online]. Available: http://www2.alcatel-lucent.com/landing/5g.

[45] J. Demarest, "Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks," *Statement before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism,* 2014.

[46] T. kleiner, "Why 5G research?," 5G Research in Horizon 2020 webcast, 2014. [Online]. Available: http://ec.europa.eu/digital-agenda/en/news/5g-research-

horizon-2020-webcast.

[47] 5G-PPP, “5G-PPP Key Performance Indicators (KPIs),” [Online]. Available: https://5g-ppp.eu/kpis/.

[48] C. Liss, T. Fendler, D. Gajic y A. Vensmer, “YouQoS - Combining Quality of Service with Network Neutrality,” *9th ITG Symposium in Broadband Coverage in Germany,* pp. 1-6, April 2015.

Annex A General Requirements

ID	REQ_GR_01
INVOLVED LAYERS	General Requirement
DESCRIPTION	The SELFNET framework MUST provide an expandable architecture to be able to include more SDN applications, NFV applications and computer resources in both edge and datacentre.
JUSTIFICATION	This capability will improve the extensibility and reusability of the SELFNET system.
CATEGORY	Functional
VALIDATION	To be able to add a new extension (SDN and NFV) dynamically in both data centre and edge.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_GR_02
INVOLVED LAYERS	SON Control Layer
DESCRIPTION	The SELFNET framework MUST be able to control sensors and actuators.
JUSTIFICATION	In order to optimize the network it must be possible to compare the initial with the final condition.
CATEGORY	Functional
VALIDATION	All deployed functions/elements can be controlled from the SELFNET framework.
NOVELTY	Medium
EXPLOITABILITY	High

ID	REQ_GR_03
INVOLVED LAYERS	SON Control Layer
DESCRIPTION	SELFNET MUST have a functional repository available for automatic deployment.
JUSTIFICATION	When performing automatic operations, the elements that are used will be pulled from a repository of functions.
CATEGORY	Functional
VALIDATION	To deploy network functions in a uniform way from a standard repository.
NOVELTY	Low
EXPLOITABILITY	High

ID	REQ_GR_04
INVOLVED LAYERS	General Requirement
DESCRIPTION	SELFNET MUST be able to manage services in both data centre and edges of the network.
JUSTIFICATION	When performing automatic operations, elements will be deployed, managed and controlled in different locations of the network according to their purpose.
CATEGORY	Functional
VALIDATION	To deploy network functions in different parts of the networks.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_GR_05
INVOLVED LAYERS	General Requirement
DESCRIPTION	SELFNET MUST be able to provide network traffic isolation for the network applications deployed in the system.
JUSTIFICATION	It will enable to share network components among different tenants.
CATEGORY	Functional
VALIDATION	To validate the isolation of network traffic between tenants.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_GR_06
INVOLVED LAYERS	All the layers below SON Control Layer
DESCRIPTION	SELFNET MUST be able to collect network elements information.
JUSTIFICATION	The monitoring techniques require access to low-level network elements information. The accuracy of the SELFNET HoN metrics depends on, among others, the quality of the information provided by monitoring agents on network devices.
CATEGORY	Functional
VALIDATION	The information sent by all the components of the SELFNET infrastructure is correctly received, validated and processed.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_GR_07
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	The SELFNET framework MUST be configurable to understand new use case specific metrics.
JUSTIFICATION	The framework must be flexible enough to allow service specific metrics to act as inputs to its self-management processes.
CATEGORY	Functional
VALIDATION	The relevant metrics are correctly interpreted and used when placing and/or configuring SDN-/NFV-Apps on the network.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_GR_08
INVOLVED LAYERS	SON Control Layer
DESCRIPTION	The information of NFV-Sensors and NFV-Actuators MAY be encrypted.
JUSTIFICATION	The correct operation of SELFNET Framework depends on the accuracy and integrity of the information provided of SDN Sensors. Similarly, the instructions sent to SDN-Actuators are able to modify the network behaviour. Therefore, security ensures a good SELFNET operation.
CATEGORY	Functional
VALIDATION	The information managed in NFV Sensor/Actuators is encrypted.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_GR_09
INVOLVED LAYERS	General Requirement
DESCRIPTION	SELFNET MUST be able to keep running information for statistical purposes disaggregated from personal information of the user accordance with existing legislation.
JUSTIFICATION	Safeguard privacy of users is one of the key technological challenges in the evolution of the current communication networks to 5G. Certain self-healing elements, such as DPI or other kind of sensors, must gather network information within the boundaries of legality.
CATEGORY	Functional
VALIDATION	SELFNET ensures gathering data disaggregated from user information.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_GR_10
INVOLVED LAYERS	SON Control Layer, NFV Orchestration and Management
DESCRIPTION	Updating of Repository modules MUST not affect the correct operation of running Sensors/Actuators on infrastructure.
JUSTIFICATION	SELFNET enables the creation/contribution of third party developers. Users can create, modify and update their own Sensors and Actuators. The development/update of a module must not affect the operation of the modules that are downloaded and running in the infrastructure.
CATEGORY	Functional
VALIDATION	The modification procedures of modules do not affect the normal operation of running Sensors/Actuators.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_GR_11
INVOLVED LAYERS	SON Control Layer
DESCRIPTION	SELFNET MAY verify and certify the modules published in VNFs Onboarding sublayer
JUSTIFICATION	Third party developers can update/modify/upload modules on the VNFs Onboarding Sublayer. Technical staff should verify the correct operation of the modules to guarantee the correct network behaviour. For this reason, the acceptance of a Sensor/Actuator should comply with established technical and Terms of Service conditions. This process ensures the proper functioning of the module.
CATEGORY	Functional
VALIDATION	SELFNET verify the proper functioning of modules.
NOVELTY	Medium
EXPLOITABILITY	Medium

Annex B Use Case System Requirements

B.1 Self-healing Use Case

ID	REQ_SH_01
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	SELFNET MUST be able to predict certain service disruptions or network failures based on the SLAs indicators and infrastructure metrics.
JUSTIFICATION	SELFNET based on data mining and learning algorithms must be able to predict some types of network failures, which will lead to the deployment of recovery actions before these failures occur.
CATEGORY	Functional
VALIDATION	SEFNET predicts service disruptions or network failures based on SLAs
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_SH_02
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	SELFNET MUST be able to deploy sensors in order to monitor the network response to the SH actuators
JUSTIFICATION	SELFNET must collect information about the network response to the reactive/proactive healing actions deployed in the network. This enhanced knowledge will contribute to the better design and deploy of self-healing actions.
CATEGORY	Functional
VALIDATION	SELFNET deploys sensors to monitor the network response to the SH actuators.
NOVELTY	Medium
EXPLOITABILITY	High

ID	REQ_SH_03
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	SELFNET SHOULD be able to guarantee a second redundancy link (Network Slices).
JUSTIFICATION	SELFNET should control strict levels of resilience and availability
CATEGORY	Functional
VALIDATION	SELFNET guarantees a second redundancy link
NOVELTY	Medium
EXPLOITABILITY	Medium

ID	REQ_SH_04
INVOLVED LAYERS	Infrastructure Layer, SON Autonomic Layer
DESCRIPTION	SELFNET SHOULD be able to rollback self-healing recovery mechanisms.
JUSTIFICATION	If a recovery action is unsuccessful, SELFNET should reverse the network to a previous state (rollback mechanism).
CATEGORY	Functional
VALIDATION	SELFNET can reverse the not-effective self-healing procedures.
NOVELTY	High Such “Undo” operation is very challenging in complex scenarios.
EXPLOITABILITY	High

ID	REQ_SH_05
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	SELFNET MUST be able to save the collected information from the network elements.
JUSTIFICATION	SELFNET must save the collected information on a database so that it has relevant information about the network performance on previous critical situations.
CATEGORY	Functional
VALIDATION	SELFNET is able to collect and save the relevant information about the network behaviour.
NOVELTY	Low
EXPLOITABILITY	High

ID	REQ_SH_06
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	SELFNET MUST be able to quickly deploy multiple reactive/proactive recovery mechanisms in case of a network failure.
JUSTIFICATION	“Reducing service creation reaching a complete deployment time from 90 h to 90 minutes” is a crucial KPI for 5G networks. Therefore, SELFNET must be able to do a quick diagnosis of the network problems, leading to the fast deployment of the recovery mechanisms.
CATEGORY	Non Functional
VALIDATION	SELFNET is able to deploy the recovery mechanism.
NOVELTY	High Timely service recreation/redeployment has yet to be realized in mobile networks.
EXPLOITABILITY	High

ID	REQ_SH_07
INVOLVED LAYERS	Infrastructure Layer, Virtualized Network Layer
DESCRIPTION	The deployment of self-healing measures SHOULD not lead to the emergence of new points of failure or vulnerabilities.
JUSTIFICATION	Incorporating of self-healing capabilities often carries the emergence of new points of failure or vulnerabilities. This opens the door to adversarial attacks, which may compromise the previous VNFs by exploiting new routes or network functions. Thus, SELFNET may take into account previous experiences to perform the deployment of new self-healing actions, in order to minimize vulnerabilities.
CATEGORY	Functional
VALIDATION	The execution of self-healing actions does not create new points of failures or vulnerabilities.
NOVELTY	High Predicting and minimizing the side-effect of a self-healing action is very challenging.
EXPLOITABILITY	High

ID	REQ_SH_08
INVOLVED LAYERS	Infrastructure and Virtualized Network Layer
DESCRIPTION	The network administrator MUST get feedback about success/failure of different processes in SDN/NFV modules.
JUSTIFICATION	The SELFNET SDN/NFV modules will be executed in different locations in network infrastructure. For this reason, the network administrator will be periodically notified about the success/failure of the different operations executed in modules (download/remove/change of parameters).
CATEGORY	Operational
VALIDATION	The network administrator is able to get feedback about the success/failure of the operations executed in modules.
NOVELTY	Medium
EXPLOITABILITY	Medium

ID	REQ_SH_09
INVOLVED LAYERS	NFV Orchestration and Management Layer
DESCRIPTION	SELFNET SHOULD store information about the SLA fulfilment during network operation.
JUSTIFICATION	The compensation or penalties caused by the SLA violations requires that SELFNET can register updated information about the network behaviour.
CATEGORY	Operational
VALIDATION	SELFNET registers the behaviour of the network in function of the fulfilment of SLA.
NOVELTY	Medium
EXPLOITABILITY	High

ID	REQ_SH_10
INVOLVED LAYERS	Infrastructure Layer
DESCRIPTION	SELFNET MAY support interaction with equipment that does not support SDN/NFV technologies.
JUSTIFICATION	It is desirable a certain level of coordination or interaction with equipment that does not support SDN/NFV technologies. SELFNET may use these “typical” network resources to improve the quality of the network behaviour.
CATEGORY	Functional
VALIDATION	SELFNET enables support with traditional equipment.
NOVELTY	Medium
EXPLOITABILITY	Medium

ID	REQ_SH_11
INVOLVED LAYERS	Infrastructure Layer, Virtualized Network Layer, SON Control Layer
DESCRIPTION	SELFNET SHOULD be able to detect some typical network failures, problems and misconfigurations on the physical/virtual network elements.
JUSTIFICATION	SELFNET should be able to detect a range of network failures/problems.
CATEGORY	Functional
VALIDATION	SELFNET detects a range of network failures/problems.
NOVELTY	High The capabilities of detecting pending network problems are not widely available in reality and is highly innovative and desirable.
EXPLOITABILITY	Medium

ID	REQ_SH_12
INVOLVED LAYERS	Infrastructure and Virtualized Network Layer
DESCRIPTION	SELFNET SHOULD be able to detect failures or aging on the virtual execution environment.
JUSTIFICATION	SELFNET should be able to detect network failures on the virtual machines. For instance, SELFNET must monitor the virtual resources supply to ensure that the virtualized functions, Apps (ageing) and operation environments will not fail due to the shortage or misallocation of the required resources.
CATEGORY	Functional
VALIDATION	SELFNET detects failures on virtual execution environment.
NOVELTY	Medium
EXPLOITABILITY	High

ID	REQ_SH_13
INVOLVED LAYERS	Infrastructure and Virtualized Network Layer
DESCRIPTION	SELFNET MUST be able to detect unexpected usage peaks of the network infrastructure.
JUSTIFICATION	SELFNET must be able to detect unexpected peaks on the network usage in order to infer critical mobile traffic situations.
CATEGORY	Functional
VALIDATION	SELFNET detects unexpected usage of peaks on network infrastructure
NOVELTY	Medium
EXPLOITABILITY	Medium

ID	REQ_SH_14
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	SELFNET MUST be able to infer concerned infrastructure metrics.
JUSTIFICATION	SELFNET must be able to infer interested infrastructure metrics from the information gathered by the SH sensors
CATEGORY	Functional
VALIDATION	SELFNET infers concerned infrastructure metrics.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_SH_15
INVOLVED LAYERS	SON Control Layer
DESCRIPTION	SELFNET MUST be able to monitor pre-defined levels of SLAs.
JUSTIFICATION	SELFNET should control strict levels of coverage, resilience and availability.
CATEGORY	Functional
VALIDATION	SELFNET monitors pre-defined levels of SLAs
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_SH_16
INVOLVED LAYERS	SON Autonomic Layer, SON Control Layer
DESCRIPTION	SELFNET SHOULD be able to infer SLAs metrics.
JUSTIFICATION	SELFNET should be able to infer SLAs indicators based on the information gathered by the SH sensors.
CATEGORY	Functional
VALIDATION	SELFNET infers SLAs metrics.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_SH_17
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	SELFNET SHOULD be able to deal with contextual sources of information to enable the inference of Cyber-Footing Human dynamics correlation
JUSTIFICATION	SELFNET may be able to infer Cyber-Footing Human dynamics correlation from the information collected from the networks and from contextual-information by using data mining and learning algorithms
CATEGORY	Functional
VALIDATION	SELFNET uses contextual sources of information and infers Cyber-Footing Human dynamics correlation.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_SH_18
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	SELFNET MUST be able to access information on the healing database about the network performance in previous specific situations.
JUSTIFICATION	SELFNET based on the information previously collected from the network, will enhance the self-healing recovery plan by proposing self-healing actions that were successful in previous critical situations, which will contribute to better reactive/proactive self-healing actions. SELFNET after the enforcement of any self-healing action will monitor the network performance to collect information about the impact of that action in the network infrastructure.
CATEGORY	Functional
VALIDATION	SELFNET enhances the self-healing recovery plan with information of previous situations.
NOVELTY	High
EXPLOITABILITY	High

B.2 Self-protection Use Case

ID	REQ_SP_01
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	Distribution of security functions in the 5G network. SELFNET SHOULD provide a distributed approach to security to cope with the high dynamicity, mobility and density of network services and users envisaged with 5G. Security functions SHOULD be spread in the 5G network, and located according to specific 5G service and user needs, as well as traffic and network conditions.
JUSTIFICATION	5G networks will support much more users and interconnected devices than current 4G and fixed networks. When combined with higher data rates envisaged and promised by 5G technologies, new requirements and challenges for security functions and services raise in support of this new heterogeneity and extensiveness of services offered by network operators and service providers.
CATEGORY	Non Functional
VALIDATION	SELFNET is able to deploy virtualized security functions in different locations along the network.
NOVELTY	High Currently, network security functions are mostly provided and implemented by network operators as ad-hoc services, deployed as monolithic functions to protect users and network traffic against cyber-attacks. A distributed and flexible approach, able to follow the dynamicity of 5G networks and users, would bring high novelty in the network operators service portfolio.
EXPLOITABILITY	High Solutions for a distributed approach to security and protection of 5G network connectivity services are expected to have high impact for network operators and service providers, particularly when linked to multi-tenant services. Network operators and service providers will be able to offer highly customized and personalized security services.

ID	REQ_SP_02
INVOLVED LAYERS	Virtualized Network Layer
DESCRIPTION	Implementation of security functions in software as NVFs. SELFNET MUST provide security sensors and actuators as NVFs to be easily stored, deployed, configured, and adapted following a common virtualization approach according to the dynamicity of 5G services and users.
JUSTIFICATION	Network operators have identified NFV as a new promising paradigm for a more dynamic, programmable and flexible operation of their networks. The virtualization of traditionally in-the-box network functions opens new challenges and requirements also at the network management and control level. And consequently, a number of heterogeneous virtual security sensors and actuators is required for keeping an eye on the complete life-cycle of any kind of cyber-attack.
CATEGORY	Functional
VALIDATION	SELFNET will implement a set of security sensors and actuators as virtualized network functions to be deployed in the virtual infrastructures. Candidates are: virtual IDS, virtual IPS, and virtual honey net, virtual firewall.
NOVELTY	Medium The implementation of network functions in software is the key concept of NFV, that is a well-defined virtualization solution for a more flexible and programmable operation of networks. However, NFV lacks of limited implementations and deployments in operation environments.
EXPLOITABILITY	High The SELFNET security sensors and actuators, implemented as NFVs, are expected to have high impact on the network operators business, giving them the opportunity to execute in virtual environments those security functions traditionally integrated in hardware, enabling a more dynamic and flexible management and control of security services. In addition, software vendors can have more opportunities to take a key role in the value chain of security services offered by network operators, acting as providers of NFVs to be integrated in the SELFNET system.

ID	REQ_SP_03
INVOLVED LAYERS	Virtualized Network Layer
DESCRIPTION	Distribution of security functions. SELFNET security functions MAY be split and distributed across multiple sensors and actuators NFVs aiming to significantly improve the performances of the SELFNET security infrastructure while coping with the 5G high traffic volumes.
JUSTIFICATION	The large amount of information that needs to be gathered for its analysis advises deploying parallelization techniques.
CATEGORY	Non Functional
VALIDATION	The effectiveness and load balancing of the multiple virtualized sensors and actuators is remained constant amongst them.
NOVELTY	Medium Distribution of NFV security functions is a big challenge and represents a novel approach to improve performance and scalability of network security and protection, if compared with state-of-the-art parallelization techniques for security functions implemented in dedicated hardware (or software).
EXPLOITABILITY	Medium The distribution of security functions implemented as virtualized functions promises to bring a substantial impact for network operators and service providers business. Indeed, this allows providing security services to customers and users that are easily scalable and upgradable.

ID	REQ_SP_04
INVOLVED LAYERS	SON Autonomic Layer, Virtualized Network Layer
DESCRIPTION	Automated deployment of sensor security NFVs. SELFNET MUST be able to provide dedicated management functions, tools and procedures to automate the deployment of security sensor functions as NFVs, according to the given security service requirements.
JUSTIFICATION	Automation of management and control functions is one of the top level objectives of SELFNET. The automated deployment of security NFV sensors in the SELFNET virtualized infrastructure is a key enabler for a full autonomous system able to provide programmable and flexible protection and security services.
CATEGORY	Functional
VALIDATION	The deployment of NFVs acting as security sensors is performed by SELFNET SON layer tools without the need of manual actions and configurations.
NOVELTY	High From a network management perspective, the deployment of security network functions is currently implemented by most network operators and service providers leveraging on procedures and mechanisms that are not fully automated and need lot of manual configurations and operations. The automation of NFVs deployments process, common across heterogeneous types of security sensors, provided by new tools and procedures will introduce a novel approach to network security functions management and control.
EXPLOITABILITY	High Network operators and service providers will be able to gain high benefits from full automation of deployment of sensor security NFVs in their virtualized infrastructures. Indeed, they will unlock the management complexity that currently affects the deployment of new security services.

ID	REQ_SP_05
INVOLVED LAYERS	SON Autonomic Layer, SON Control Layer
DESCRIPTION	Automated composition and chaining of security NFVs. SELFNET MUST implement automated mechanisms for the composition of security service functions, where multiple distributed VNFs are chained and traffic is steered across them to build security services spanning different portions of the 5G networks.
JUSTIFICATION	The distributed network security and protection approach envisaged by SELFNET in support of 5G high dynamicity and extensiveness requires additional automated control and management functions to chain security NFVs and compose the distributed services offered by network operators and service and providers.
CATEGORY	Functional
VALIDATION	The configuration and provisioning of the given tenant virtual network that allows to steer the traffic across the NFVs building the distributed security service is performed by SON and control layer functions without the need of manual actions and configurations.
NOVELTY	Medium The concept of chaining and composing NFVs to build end-to-end NFV services is well defined and under investigation and definition in standardization bodies like IETF, where the Service Function Chaining (SFC) working group is proposing a new approach to service delivery and operation. However, the automatisation and adaptation of these concepts to distributed and virtualized security services for 5G networks is expected to provide novel solutions and approaches to network management and control.
EXPLOITABILITY	Medium The automation of chaining of security NFVs to compose end-to-end virtualized and highly distributed security service is a substantial added value for network operators and service providers. Indeed, this is expected to reduce the burden of network management procedures while opening new business opportunities related to improved ability to offer customized security services.

ID	REQ_SP_06
INVOLVED LAYERS	SON Autonomic Layer, SON Control Layer and Virtualized Network Layer
DESCRIPTION	Automated and dynamic deployment of actuator security NFVs. SELFNET MUST provide procedures and mechanisms to automatically react to cyber-attacks with the deployment of new security actuators in the network with the aim of mitigating and block them. The deployment of a new actuator NFV also needs a proper re-configuration of the service chain to force alleged network traffic be processed by the actuator.
JUSTIFICATION	Automated reaction to potential cyber-attacks is a key feature for any kind of self-organized management system willing to implement highly efficient security and protection services.
CATEGORY	Functional
VALIDATION	The SON Layer processes the detection of the cyber-attack and autonomously manage the deployment of a new VNF actuator function to mitigate it without the need of manual actions and configuration, including dynamic re-provisioning of the VNF chain to properly switch traffic to the new actuator for isolation and mitigation of the attack.
NOVELTY	High Fully automated reaction to cyber-attacks with automated deployment of countermeasures in the form of actuator security NFVs represents a disruptive novelty in the way networks are managed and operated, overcoming current rigidness of procedures to react and mitigate a wide range of network malicious violations and intrusions.
EXPLOITABILITY	High The automatization of the reactive protection mode with deployment of dedicated NFVs to mitigate cyber-attacks is expected to provide high impact and benefits for the network operators and service providers business. Indeed, it will open the possibility to close the control and management loop for the services they offer to customers and users.

ID	REQ_SP_07
INVOLVED LAYERS	SON Autonomic Layer, SON Control Layer
DESCRIPTION	Dynamic adaptation of security services. SELFNET SHOULD orchestrate and coordinate its security services and NFV chains to follow the dynamicity of 5G services and users. Security functions and NFVs SHOULD be dynamically migrated, reconfigured, chained and adapted according to the 5G service requirements.
JUSTIFICATION	The dynamicity and automatization required in the deployment of sensor and actuator security NFVs, in support of a reactive network protection mode, must be combined with the dynamicity in the operation and maintenance of the provisioned end-to-end virtualized security service. Indeed, 5G will bring high dynamicity and mobility of users and devices, thus a planner process to orchestrate and coordinate the security NFV chains is mandatory, with the aim of dynamically and automatically (re-)configuring and migrating sensors and actuators security VNFs for efficient detection and mitigation purposes.
CATEGORY	Functional
VALIDATION	The SON Layer upon the analysis and correlation of information coming from security sensors autonomously decide to re-configure the distributed security service relocating or re-configuring certain NFVs or changing the service chain without the need of manual actions and configuration
NOVELTY	High The dynamic adaptation and re-configuration of security NFV chains is a particularization of the self-optimization capabilities provided by the SELFNET framework. Thus, it represents an innovative approach and solution for management and control of 5G networks.
EXPLOITABILITY	High The adaptive operation of the distributed NFV chains is expected to bring advantages in the way network operators will offer and run their security services, that will be actually bound to the extremely dynamic and heterogeneous 5G customer and user requirements.

ID	REQ_SP_08
INVOLVED LAYERS	SON Autonomic Layer, SON Control Layer
DESCRIPTION	High-level security sensors of 5G network traffic flows. SELFNET MUST provide high-level monitoring sensor functions able to inspect 5G network traffic and enable the detection of potential anomalies and misuses. These functions could be implemented as sensor NFVs for coarse grain monitoring and identification of cyber-attacks.
JUSTIFICATION	The highly distributed and virtualized security and protection approach envisaged by SELFNET, where multiple NFVs cooperate to secure 5G network services, open the opportunity to implement detection and monitoring functions at different granularities and at different levels of abstractions. High-level monitoring and detection sensor NFVs aim to provide a first stage of cyber-attacks detection by only inspecting network flows.
CATEGORY	Functional
VALIDATION	The SON layer is capable of monitoring all flows of the network traffic that is circulating on the physical and virtualised infrastructure
NOVELTY	High The implementation of the SELFNET highly distributed security services as multi-stage detection and reaction processes represents an innovative approach to the provisioning of secured network services, especially for the virtualized 5G scenario. This allows high-level sensor NFVs to be always up and running to inspect network traffic at a coarse granularity and detect potential sources of cyber-attacks.
EXPLOITABILITY	Medium Network operators can benefit from the separation of detection and reaction processes in multiple stages by improving and enriching their security service portfolio. Indeed, they will be able to offer highly customized and differentiated protection services according to the specific needs of customers and users (e.g. some of them might be interested to buy only high-level security services and rely on proprietary low-level security functions to be deployed in their virtual infrastructures).

ID	REQ_SP_09
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	High-level cyber-attack detection algorithms. SELFNET MUST provide high-level detection algorithms able to analyse high volumes of network traffic and identify potential cyber-attacks at a coarse level. These algorithms could correlate monitoring information gathered from multiple high-level sensor NFVs.
JUSTIFICATION	Artificial intelligence processes, such as data mining techniques, are required to analyse a large number of detection information at runtime. The definition of adequate security metrics is the main key aspect from which detection at high-level encompasses the feasibility of identifying possible potential cyber-attacks, which still are in an early stage of execution.
CATEGORY	Functional
VALIDATION	The detection rate at a coarse level is the highest possible, detecting all the alleged cyber-attacks injected on the physical and virtualised infrastructure
NOVELTY	Medium The provisioning of novel high-level detection algorithms to identify cyber-attacks in an early stage is a required feature, from which network operators and service providers will be strengthened to be informed on the actual state of security of their most important assets. In 5G networks, the monitoring and detection at high level of abstraction is the first analysis when identifying potential cyber-attacks, since the large amount of 5G subscribers' devices makes unfeasible a deeper inspection of huge number of network packages.
EXPLOITABILITY	Medium Network operators and service providers can benefit in knowing which potential cyber-attacks are being exploited in their underlying systems, as well as the possible risk levels that their organizational assets have. In any case, a low-level inspection of the network packages is a must to ensure the actual execution of a cyber-attack.

ID	REQ_SP_10
INVOLVED LAYERS	SON Autonomic Layer, SON Control Layer
DESCRIPTION	Low-level security sensors of 5G network traffic flows. SELFNET SHOULD provide low-level security sensors able to deeply monitor 5G network traffic already identified as potentially under attack. The aim of these low-level sensors is to operate on a small portion of the network traffic flows, already processed by other high-level functions. These functions could be also implemented as sensor NFVs for fine grain monitoring and identification of cyber-attacks.
JUSTIFICATION	Low-level and deep traffic inspection functions aim to provide a second stage of cyber-attacks detection for those network traffic flows already identified as suspect to be under attack. This means that once the SELFNET framework has information on an alleged cyber-attack, a low-level monitoring and detection process is needed to actually identify the cyber-attack before deploying countermeasures and react with actuator NFVs.
CATEGORY	Functional
VALIDATION	The SON layer is capable of conducting DPI monitoring on a given detection area, without losing network packages for their analysis.
NOVELTY	High The multi-stage detection and reaction process provided by the combination of coarse and fine granular monitoring functions allows the SELFNET framework to deploy the low-level security sensor NFVs and chain them in the distributed virtualized service on-demand, when actually needed and upon proper trigger from high-level sensors. This is a further step towards a highly flexible and dynamic management of virtualized security services for 5G networks and represents a key innovation for SELFNET.
EXPLOITABILITY	Medium Similarly to REQ_SP_08, network operators can benefit from the separation of detection and reaction processes in multiple stages by improving and enriching their security service portfolio. In addition, the usage of low-level sensor NFVs for suspected network traffic only allows reducing the overall set of deep network traffic inspections to be performed with a consequent expected impact on the security service performances.

ID	REQ_SP_11
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	Low-level cyber-attack detection algorithms. SELFNET SHOULD provide low-level detection algorithms able to deeply inspect 5G network traffic and identify specific signatures, virus patterns and attacks in general. These algorithms could also correlate monitoring information gathered from multiple low-level sensor VNFs.
JUSTIFICATION	The low-level detection process is carried out to confirm the existence of an actual cyber-attack, from which to boot the reaction phase for countering the detected cyber-attack as well as open the possibility of self-learning new attackers' methods for improving further detection and reaction capabilities.
CATEGORY	Functional
VALIDATION	The detection rate at low-level is the highest possible, detecting all the alleged cyber-attacks injected on the physical and virtualised infrastructure by following a deep inspection approach of the network packages.
NOVELTY	Medium It is expected the provisioning of novel distributed algorithms for identifying the actual execution of a given cyber-attack. This detection process is carried out at low level by deeply inspecting the network packages flooding the 5G core and radio access networks.
EXPLOITABILITY	Medium Similarly to REQ_SP_09, network operators and service providers can benefit from detecting the actual execution of cyber-attacks aimed at subverting the assets of their organization.

ID	REQ_SP_12
INVOLVED LAYERS	SON Autonomic Layer
DESCRIPTION	Learn cyber-attacks methods and patterns. SELFNET SHOULD be able to learn from attacks detected aiming to improve the overall security of the 5G infrastructure and system by means of automated procedures. This enables the SELFNET security infrastructure to provide self-learning capabilities.
JUSTIFICATION	Self-learning is the ultimate stage for the implementation of a full self-protection system, able to take autonomous reactions to cyber-attacks while adapting and upgrading its procedures and decision mechanisms analysing previous attacks. A set of dedicated learning functions, algorithms and tools is needed to evaluate for each attack the success or failure in deploying mitigations, reactions and actuator NFVs in general.
CATEGORY	Functional
VALIDATION	The detection and response mechanisms show better ratios (results) after deploying new procedures in managing a similar cyber-attack
NOVELTY	High A network management and control system that is able to implement self-learning functions to automatically adapt and upgrade its network security procedures, decisions and NFVs deployment strategies certainly represents an extremely innovative approach and solution to ease 5G network operation.
EXPLOITABILITY	High Network operators and service providers are more and more willing to introduce virtualized management and control functions able to reduce the burden and complexity of operating networks and services. With 5G this will be even truer, and the possibility to have self-learning virtualized security services is expected to have a high impact in new services offered.

B.3 Self-optimization Use Case

ID	REQ_SO_01
INVOLVED LAYERS	Infrastructure Layer, Virtualized Network Layer, SON Autonomic Layer, SON Control Layer
DESCRIPTION	There MUST be a way to measure the QoE of the user consuming a video.
JUSTIFICATION	This use case aims to optimize video delivery, and one of the optimization targets is users' QoE. Hence, there must be a metric to evaluate QoE quantitatively.
CATEGORY	Non Functional
VALIDATION	An objective way is defined to measure the QoE perceived by a user watching a video. QoE estimates must closely match subjectively measured opinions of quality. QoE estimates should consider both visual quality and other indicators of perceived quality such service continuity.
NOVELTY	High Fast, accurate methods of estimating QoE for streamed video (especially HD and U-HD resolution video) content "on the fly" have yet to be realized. This is especially important for real-time video services where quality estimates may need to be made in-network on the compressed domain of H.265 encoded video.
EXPLOITABILITY	High

ID	REQ_SO_02
INVOLVED LAYERS	Infrastructure Layer, Virtualized Network Layer, SON Autonomic Layer, SON Control Layer
DESCRIPTION	SELFNET framework SHOULD be able to manage video traffic delivery end to end across the network.
JUSTIFICATION	Communication between different network operators is a reality. This Use Case should not create obstacles to these communications.
CATEGORY	Functional
VALIDATION	The video adaptation should not hamper the communication between terminals on different operators.
NOVELTY	Medium
EXPLOITABILITY	High

ID	REQ_SO_03
INVOLVED LAYERS	Infrastructure Layer, Virtualized Network Layer, SON Autonomic Layer, SON Control Layer
DESCRIPTION	SELFNET MUST be able to deploy complex services on the appropriate network locations, with dependencies between elements. Specifically, the MANEs etc. should be placed at the location that maximises their efficiency.
JUSTIFICATION	The initial service deployment should be fast and automated.
CATEGORY	Functional
VALIDATION	Services deployed by SELFNET are correctly distributed among several PoP according to the function of each element.
NOVELTY	Low
EXPLOITABILITY	High

ID	REQ_SO_04
INVOLVED LAYERS	Infrastructure Layer
DESCRIPTION	A codec that allows layered adaptation at stream time MUST be made available to the consortium, such as H.265.
JUSTIFICATION	A typical video adaptation scenario revolves around dropping selected packets belonging to one or more layers of the codec in accordance with the network conditions and the user preferences.
CATEGORY	Non functional
VALIDATION	When the network conditions deteriorate, the network elements adapt/recode/drop layers of the video without needing to contact the original video source
NOVELTY	High The proposal is to use the scalable extension to the latest H.265 codec. This is a very recent standard and there are no existing implementations or publications on using this standard in and SDN/NFV environment.
EXPLOITABILITY	High

ID	REQ_SO_05
INVOLVED LAYERS	SELFNET Access Layer, SON Autonomic Layer, SON Control Layer
DESCRIPTION	SELFNET MAY allow the end user to record and configure his preferences regarding the experienced service, including service differentiation.
JUSTIFICATION	The user should be able to influence the way his traffic is handled in the core network.
CATEGORY	Functional
VALIDATION	The recorded user preferences can be retrieved and modified by the user, and can be read by the SELFNET core components
NOVELTY	Low
EXPLOITABILITY	High

ID	REQ_SO_06
INVOLVED LAYERS	Virtualized Network Layer, SON Autonomic Layer, NFV Orchestration and Management Layer
DESCRIPTION	Recorded user preferences SHOULD influence autonomous SELFNET decisions.
JUSTIFICATION	The user should be able to influence the way his/her traffic is handled in the core network.
CATEGORY	Functional
VALIDATION	The recorded user preferences are used as part as part of the decision process regarding a given user's flows
NOVELTY	High. Little existing deployment has achieved user-influenced traffic engineering.
EXPLOITABILITY	High

ID	REQ_SO_07
INVOLVED LAYERS	Virtualized Network Layer
DESCRIPTION	A Media Aware Network Element MUST be able to manipulate the chosen H.265 streams in real time. This option should take into account factors such as QoE or user preferences if applicable.
JUSTIFICATION	This is the element that performs the actual manipulation of the video streams.
CATEGORY	Functional
VALIDATION	It is possible to manipulate/transform a video stream in transit.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_SO_08
INVOLVED LAYERS	Virtualized Network Layer
DESCRIPTION	There MAY be a SELFNET compatible network function that operates on the video streams: transcoders that transcode between a legacy stream and the latest video codec (H.265).
JUSTIFICATION	The use case need this function to be created so that the framework can deploy the transcoding at the appropriate network locations.
CATEGORY	Functional
VALIDATION	Transcoding a legacy video stream to H.265 and vice versa is performed according to the application optimization requirements.
NOVELTY	High There are very few (if any so far) existing implementations or publications on exploring the H.265 standard in an SDN/NFV environment.
EXPLOITABILITY	High

ID	REQ_SO_09
INVOLVED LAYERS	Virtualized Network Layer
DESCRIPTION	There MUST be a SELFNET compatible network function that operates on the video streams: caches
JUSTIFICATION	The deployment of a smart cache can have a big impact on the overall traffic going in and out of the service provider. Also, these elements may be required as SSL terminators to implement advanced manipulation of encrypted traffic.
CATEGORY	Functional
VALIDATION	When the same video stream is requested many times, SELFNET deploys this element and the network starts behaving in a similar way to a CDN.
NOVELTY	Medium
EXPLOITABILITY	High

ID	REQ_SO_10
INVOLVED LAYERS	Infrastructure Layer, Virtualized Network Layer
DESCRIPTION	There MUST be a way to trigger varying network conditions (for testing, evaluation and validation purposes) from low bandwidth, to high error rates on the RAN and the core network.
JUSTIFICATION	In order to formulate the conditions that will trigger a use case scenario e.g. the SO video optimizations to take place, such a mechanism is necessary.
CATEGORY	Non functional
VALIDATION	It is possible to simulate/emulate network conditions including overutilization/underutilization etc. on certain network links.
NOVELTY	Low
EXPLOITABILITY	High

ID	REQ_SO_11
INVOLVED LAYERS	Infrastructure Layer, Virtualized Network Layer, SON Autonomic Layer, SON Control Layer
DESCRIPTION	A Media Aware Network Element MUST be able to load balance video streams between existing manipulation elements.
JUSTIFICATION	The use case must be scalable; there is the need to scale the number of video adaptation elements, and possibly other elements.
CATEGORY	Functional
VALIDATION	When the load of a transformation element reaches a threshold, new video streams will be redirected to another transformation element.
NOVELTY	High
EXPLOITABILITY	High

ID	REQ_SO_12
INVOLVED LAYERS	Infrastructure Layer, Virtualized Network Layer, SON Control Layer
DESCRIPTION	Video traffic MAY be differentiated in categories such as consumer, IoT/M2M, telemedicine or emergency systems.
JUSTIFICATION	This two tier approach will enable a co-ordinated management of the resources and user experience.
CATEGORY	Functional
VALIDATION	The traffic is differentiated at the network according to its category.
NOVELTY	Medium
EXPLOITABILITY	High

ID	REQ_SO_13
INVOLVED LAYERS	Infrastructure Layer
DESCRIPTION	The user traffic SHOULD be tagged according to the categories defined by the user. This tagging will be used by the core network to influence the QoE decisions regarding a specific flow.
JUSTIFICATION	These categories may later be used by the core network to prioritize flows according to the user preferences.
CATEGORY	Functional
VALIDATION	The traffic generated by the user has its category clearly marked on the headers when it reaches the core of the network. This two level categorization (together with REQ_SO_12) will ensure a better user experience.
NOVELTY	Medium
EXPLOITABILITY	High

ID	REQ_SO_14
INVOLVED LAYERS	Infrastructure Layer, Virtualized Network Layer, SON Autonomic Layer, SON Control Layer
DESCRIPTION	Given the optimization targets, the core network MUST be able to apply policies to the generated traffic.
JUSTIFICATION	This is required for an optimization operation to be applied.
CATEGORY	Functional
VALIDATION	Traffic manipulation is automatically applied to the user's traffic as self-optimization is triggered. Actions are transparent to the user.
NOVELTY	High Little work exists on optimization of U-HD video transmission in virtualized networking environment.
EXPLOITABILITY	High

ID	REQ_SO_15
INVOLVED LAYERS	Infrastructure Layer, Virtualized Network Layer, SON Autonomic Layer, SON Control Layer
DESCRIPTION	SELFNET SHOULD be able to estimate the energy consumption of an element, and use that value in the decision making process.
JUSTIFICATION	In order to achieve better energy efficiency, SELFNET should be able to take into account the impact of an action on the energy consumption.
CATEGORY	Functional
VALIDATION	Energy-aware service (esp. U-HD video) delivery is achieved.
NOVELTY	High Little existing work have considered the overall energy awareness in delivering video, esp. U-HD.
EXPLOITABILITY	High

ID	REQ_SO_16
INVOLVED LAYERS	Infrastructure Layer, Virtualized Network Layer, SON Autonomic Layer, SON Control Layer
DESCRIPTION	SELFNET SHOULD be able to set equipment's power level to an energy efficient value (standby or even off) when there is no use for said equipment.
JUSTIFICATION	By carefully managing the power state of the equipment, SELFNET can achieve even greater power efficiency on void moments, while its predictive capabilities allow the system to anticipate when more resources will be needed.
CATEGORY	Functional
VALIDATION	SELFNET is able to set some of the unused equipment to a low power state, or at least allow some equipment to enter power saving states by consolidating deployed elements as much as possible
NOVELTY	Medium
EXPLOITABILITY	High

ID	REQ_SO_17
INVOLVED LAYERS	Virtualized Network Layer, SON Autonomic Layer, SON Control Layer
DESCRIPTION	SELFNET framework SHOULD provide means of accessing QoE indicators from encrypted video streams.
JUSTIFICATION	Some of the video streams may be encrypted; this fact should not be an impediment to the video adaptations suggested by this Use Case.
CATEGORY	Functional
VALIDATION	Media Aware Network Element should be able to handle encrypted video streams and perform the required adaptations.
NOVELTY	High Most existing work assume unencrypted video traffic for QoE-related studies/deployment.
EXPLOITABILITY	High

Annex C Component and Layer System Requirements Template

C.1 Infrastructure Layer Requirements

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_IL_01	Edge nodes SHOULD allow connecting 5G base station hardware to virtualized services.	Medium	High
	REQ_IL_02	The management of both virtual and physical infrastructures SHOULD be centralized.	Medium	Medium
	REQ_IL_03	Logical separation between control and data plane MUST be in place.	Low	Low
	REQ_IL_04	Physical and virtual infrastructure MUST be able to be monitored.	Medium	Medium
	REQ_IL_05	The system MUST be able to handle multiple locations geographically distributed (edge locations and datacentre).	Medium	High
	REQ_IL_06	The system SHOULD be able to control all networks traffic within the infrastructure.	High	High
	REQ_IL_07	The Virtual Infrastructure MUST support multi-tenancy.	High	High
Technologies /	REQ_IL_08	Physical infrastructure SHOULD be able to be	Medium	High

Techniques		automatically installed and configured from bare metal to reduce service creation and provisioning time.		
	REQ_IL_09	The usage of multiple virtualization technologies MAY be enabled.	Low	Low
Component Protocols	REQ_IL_10	Security SHOULD be an integrated part of the system and protocols.	Low	Low
Data Structures	None	None		
Non Functional	REQ_IL_11	Both virtual and physical Infrastructure SHOULD support geo location aspects for accurate planning and efficient resource management.	Medium	High
Interoperability / Compatibility	REQ_IL_12	The VI MAY support any cloud management system by the integration of the appropriate plugins.	High	High

C.2 Virtualized Network Layer

REQ Type	ID	Description	Novelty	Exploitability
	REQ_VNL_01	The management of virtual network infrastructures SHOULD be centralized.	Medium	Medium
	REQ_VNL_02	Logical separation between control and data plane MUST be in place.	Low	Low
Component Design	REQ_VNL_03	The Virtualized Network Infrastructure SHOULD support multi-tenancy.	High	High
	REQ_VNL_04	The Virtualized Network Infrastructure MUST support dynamic service chaining.	High	High
	REQ_VNL_05	The Virtualized Network Infrastructure SHOULD support provision of HoN metrics related to the availability and management of the underlying resources.	Medium	High
Technologies / Techniques	None	None		
Component Protocols	None	None		
Data Structures	REQ_VNL_06	The Virtualized Network Infrastructure MAY support expandable information and data models to cater for forward compatibility.	High	High
Non Functional	REQ_VNL_07	The Virtualized Network Infrastructure SHOULD support geo location aspects for accurate planning and efficient resource management.	Medium	High
	REQ_VNL_08	The Virtualized Network Infrastructure MUST be able to execute virtualized NFV components.	Low	High
Interoperability / Compatibility	REQ_VNL_09	An SDN architecture MAY provide support for multiple pluggable SDN controller.	High	High

C.3 SON Control Layer Requirements

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SONCL_01	The System MUST be able to execute SDN Applications.	Low	High
	REQ_SONCL_02	The System MUST be able to execute VNE Applications.	High	High
	REQ_SONCL_03	The System SHOULD be able to execute VNF Applications.	High	High
Technologies / Techniques	None	None		
Component Protocols	None	None		
Data Structures	REQ_SONCL_04	The SON NFV components MAY support expandable information and data models to cater for forward compatibility.	High	High
Non Functional	None	None		
Interoperability / Compatibility	REQ_SONCL_05	A homogeneous access to SON NFV metrics SHOULD be provided.	High	High
	REQ_SONCL_06	An SDN architecture MAY provide support for multiple pluggable SDN controller.	High	High
	REQ_SONCL_07	A systematic way to control and configuration of SON NFV SHOULD be provided.	High	High

C.4 SON Autonomic Layer Requirements

C.4.1 Monitoring

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SON_MO_01	Monitoring MUST collect and manage all data provided by the different SELFNET actors and components.	Medium	High
	REQ_SON_MO_02	Monitoring MUST detect new devices and sensors deployed on SELFNET.	Medium	High
	REQ_SON_MO_03	Monitoring MUST facilitate querying of the gathered information on SELFNET.	Medium	High
	REQ_SON_MO_04	Monitoring SHOULD provide distributed monitoring capabilities over the different components of the system.	Low	High
	REQ_SON_MO_05	Monitoring MUST be able to monitoring both Virtual and Physical Infrastructures.	High	High
	REQ_SON_MO_06	Monitoring MUST be able to monitoring SDN and NFV components.	High	High
Technologies / Techniques	None	None		
Component Protocols	REQ_SON_MO_07	Monitoring SHOULD be adapted to the communication protocols used by the different actors and components, layers and tasks of SELFNET.	High	High
Data Structures	REQ_SON_MO_08	Data structures involved in storing monitored information in the database system MAY be efficient and allow to implement different abstract data types.	Low	Low
Non Functional	REQ_SON_MO_09	Data gathered SHOULD be consistent with the current SELFNET status.	Medium	Medium
Interoperability / Compatibility	REQ_SON_MO_10	The monitored data MUST be provided by the different APIs and interfaces of SELFNET.	Medium	Medium
	REQ_SON_MO_11	The monitored data MUST be accessible and understood by the coming processing stages.	Medium	Low

C.4.2 Aggregation

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SON_AG_01	Aggregator MUST collect the low-level network metrics from the “Monitoring & Detection” module.	Low	High
	REQ_SON_AG_02	Aggregator MUST produce high-level metrics, also known as indicators. Several techniques, such as data correlation, data mining, data processing, data prediction and/or others SHOULD be used.	High	High
	REQ_SON_AG_03	Aggregator MUST deliver the high-level network metrics to the analyzer module.	High	High
Technologies / Techniques	REQ_SON_AG_04	Aggregator SHOULD leverage on the existing technologies in the field of data aggregation and enhance them in support of SELFNET low-level to high-level metrics transformation.	Medium	High
Component Protocols	REQ_SON_AG_05	Aggregator SHOULD take advantage of, enhance and integrate the existing protocols in the field of data aggregation.	Medium	Medium
Data Structures	REQ_SON_AG_06	Data structures involved in data aggregation MUST be efficient and allow implementing different abstract data types.	Medium	High
Non Functional	REQ_SON_AG_07	Low-level to high-level metrics transformation MUST be fast enough to enable the analysis algorithms to detect suspicious or anomalous situations on SELFNET.	High	High
Interoperability / Compatibility	REQ_SON_AG_08	The aggregated data MUST be accessible and understood by the coming processing stages.	High	High

C.4.3 Analyzer

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SON_AN_01	Analyzer MUST be able to calculate the current status of SELFNET.	Medium	High
	REQ_SON_AN_02	Analyzer MUST perform Identification and assessment of suspicious or anomalous situations on SELFNET.	Medium	High
	REQ_SON_AN_03	Analyzer MUST provide any information about the current status of SELFNET required for decisions.	Medium	High
Technologies / Techniques	None	None		
Component Protocols	REQ_SON_AN_04	Communications between analyzer and coming data processing stages SHOULD be adapted to the communication protocols used by the different actors and components of SELFNET.	Medium	Medium
Data Structures	REQ_SON_AN_05	Data structures involved in analysing information MAY be efficient and permit to implement different abstract data types.	Low	Low
	REQ_SON_AN_06	In order to enhance the processes of analysis, the implemented data structures SHOULD permit encapsulation of meta information.	Medium	Medium
Non Functional	REQ_SON_AN_07	SELFNET status SHOULD be calculated efficiently, in order to facilitate the deployment of countermeasures in close to real time response time.	Low	Medium
	REQ_SON_AN_08	The assessment of detected situations SHOULD be proportional to their impact.	High	High
Interoperability / Compatibility	REQ_SON_AN_09	The information about the system status MUST be sent to the coming processing stages by the different APIs and interfaces of SELFNET.	Low	Medium
	REQ_SON_AN_10	The information about the system status MUST be accessible and understood by the decision making tasks.	Medium	Medium

C.4.4 Tactical Autonomic Language

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SON_TL_1	TAL MUST allow for definition of multiple input parameters.	Medium	High
	REQ_SON_TL_2	TAL MUST allow for definition of multiple output actions.	Medium	High
	REQ_SON_TL_3	TAL SHOULD allow for definition of both logical and arithmetic operators.	Medium	High
	REQ_SON_TL_4	TAL MAY allow for definition of state diagrams and execution flows to define autonomic behaviour.	Medium	High
Technologies / Techniques	REQ_SON_TL_5	TAL MAY be executable.	Medium	High
	REQ_SON_TL_6	TAL execution framework MUST be able to interface with any service endpoint by injection of the appropriate plugin (e.g. REST, SOAP, XMLRPC, etc.).	Medium	High
Component Protocols	REQ_SON_TL_7	TAL SHOULD allow for layered description/definition of network semantics so as to cover all the potential protocols and information views of interest.	High	High
Data Structures	REQ_SON_TL_8	TAL SHOULD be based on extensible data structuring techniques with no nesting limitations.	Low	High
Non Functional	REQ_SON	TAL SHOULD be abstract	High	High

	_TL_9	and not bound to specific semantics but it SHOULD allow for semantics to be definable.		
	REQ_SON_TL_10	TAL SHOULD express any operation action relating to autonomic strategies.	High	High
	REQ_SON_TL_11	TAL MAY include forward compatibility mechanisms for expressing strategies based on SDN and NFV functionalities that may emerge in the future.	High	High
	REQ_SON_TL_12	TAL SHOULD have mechanisms for definition of HoN metrics on which operators act upon during strategy execution.	High	High
Interoperability / Compatibility	REQ_SON_TL_13	TAL execution framework MUST be integrated with the rest of the components of the Decision Making Planer.	High	High
	REQ_SON_TL_14	TAL execution framework SHOULD interface with the components of the Aggregator and Analyzer.	High	High

C.4.5 Intelligent Network Diagnostic Algorithms

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SON_IN_01	Intelligent Network Diagnostic MUST allow for recognizing the incoming Monitoring information.	High	High
	REQ_SON_IN_02	Intelligent Network Diagnostic MUST allow for diagnosing existing network problems and provide the reactive and corrective strategies based on the incoming Monitoring information.	High	High
	REQ_SON_IN_03	Intelligent Network Diagnostic MUST allow for diagnosing potential network problems and provide the proactive and preventive strategies based on the incoming Monitoring information	High	High
	REQ_SON_IN_04	Intelligent Network Diagnostic MUST allow for providing the reactive strategies to the Decision-Making Planner.	High	High
	REQ_SON_IN_05	Intelligent Network Diagnostic MUST allow for providing the proactive strategies to the Decision-Making Planner.	High	High
Technologies / Techniques	REQ_SON_IN_06	Intelligent Network Diagnostic SHOULD leverage on the existing (published, standardized) technologies in the field of artificial intelligence, pattern recognition, data mining and enhance them in support of	High	High

		SELFNET intelligent diagnosis of network problems.		
Component Protocols	REQ_SON_IN_07	Intelligent Network Diagnostic SHOULD take advantage of, enhance and integrate the existing (published, standardized) protocols in the field of artificial intelligence, pattern recognition, data mining.	High	High
Data Structures	REQ_SON_IN_08	Data structures involved in Intelligent Network Diagnostic SHOULD be based on the data structure specified in TAL.	High	High
Non Functional	None	None		
Interoperability / Compatibility	REQ_SON_IN_09	Intelligent Network Diagnostic SHOULD be extensible and expandable.	High	High
	REQ_SON_IN_10	Intelligent Network Diagnostic SHOULD be open and programmable.	High	High

C.4.6 Decision Making Planner

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SON_DM_01	Decision Making Planner MUST allow for recognizing the incoming diagnostic information.	High	High
	REQ_SON_DM_02	Decision Making Planner MUST allow for deciding a set of reactive and corrective actions to deal with the existing network problems based on the incoming diagnostic information.	High	High
	REQ_SON_DM_03	Decision Making Planner MUST allow for deciding a set of proactive and preventive actions to deal with the potential network problems based on the incoming diagnostic information.	High	High
	REQ_SON_DM_04	Decision Making Planner MUST allow for providing the decided set of reactive actions to the Intelligent Action Enforcer.	High	High
	REQ_SON_DM_05	Decision Making Planner MUST allow for providing the decided set of proactive actions to the Intelligent Action Enforcer.	High	High
Technologies / Techniques	REQ_SON_DM_06	Decision Making Planner SHOULD leverage on the existing (published, standardized) technologies in the field of artificial intelligence, pattern recognition, and data mining	High	High

		and enhance them in support of SELFNET intelligent decision-making against network problems.		
Component Protocols	REQ_SON_DM_07	Decision Making Planner SHOULD take advantage of, enhance and integrate the existing (published, standardized) protocols in the field of artificial intelligence, pattern recognition, data mining.	High	High
Data Structures	REQ_SON_DM_08	Data structures involved in Decision-Making Planner SHOULD be based on the data structure specified in TAL.	High	High
Non Functional	REQ_SON_DM_09	Decision Making Planner MUST be extensible and expandable	High	High
Interoperability / Compatibility	REQ_SON_DM_10	Decision Making Planner SHOULD be open and programmable.	High	High

C.4.7 Intelligent Action Enforcer

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SON_AE_01	AE MUST allow for definition of multiple inputs so that it can receive multiple actions to be enforced.	Medium	High
	REQ_SON_AE_02	AE MUST provide an implementable plan with one or more actions ready to be enforced.	Medium	High
	REQ_SON_AE_03	AE MUST consider language refining techniques to provide an implementable plan from the multiple inputs received.	Medium	High
	REQ_SON_AE_04	AE MUST allow for definition of state diagrams and execution flows.	Medium	High
Technologies / Techniques	REQ_SON_AE_05	AE MUST consider conflict detection and resolutions techniques.	Medium	High
	REQ_SON_AE_06	AE MAY leverage on the existing (published, standardized) technologies in the field of conflict detection and resolutions techniques, language refining techniques, and enhance them in support of SELFNET intelligent plans ready to be enforced against network problems.	Medium	Medium
Component Protocols	REQ_SON_AE_07	AE MAY take advantage of, enhance and integrate the existing (published, standardized) protocols in the field of conflict detection and resolutions techniques, language refining techniques, etc. in order to provide an implementable plan ready to be enforced.	Medium	Medium
Data Structures	REQ_SON	Data structures involved in AE SHOULD be based on	High	High

	_AE_08	the data structures specified in TAL and on the Decision-Making Planner		
Non Functional	REQ_SON_AE_09	Intelligent execution MUST refine to actions that have been decided by the Decision-Making Planner framework to provide an implementable plan.	Medium	High
	REQ_SON_AE_10	A validation and organization MUST be done to the information received from the Decision-Making Planner framework	High	High
	REQ_SON_AE_11	AE MUST apply a conflict detection and resolution techniques, in order to provide an implementable plan ready to be enforced	High	High
	REQ_SON_AE_12	AE MUST enforce any operation action relating to the HoN metric reports received by the Decision-Making Planner framework	High	High
Interoperability / Compatibility	REQ_SON_AE_13	AE execution framework MUST be integrated with the rest of the components of the Decision Making Planer Module	High	High
	REQ_SON_AE_14	AE execution framework MUST interface with the components of the Decision Making Planner and the Orchestrator Module.	High	High
	REQ_SON_AE_15	AE MUST be implemented over the self-managed 5G network.	High	High
	REQ_SON_AE_16	AE SHOULD be open, programmable and extensive.	High	High

C.4.8 Orchestrator

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SON_OR_01	The Orchestrator (OR) MUST be able to receive and queue incoming actions from the Decision Making Planner (DMP) sublayer.	Low	Medium
	REQ_SON_OR_02	The OR MUST be able to query the available resources and Apps from Resource Manager and Application Manager.	Low	Medium
	REQ_SON_OR_03	The OR MUST match the high level actions against the available low level actions according to the available resources and Apps.	High	High
	REQ_SON_OR_04	The OR SHOULD be able to detect dependencies between the estimated actions.	High	High
	REQ_SON_OR_05	The OR MUST be able to enforce the actions, by calling and deploying the selected Apps, and operating on the Apps through the Application Manager.	High	High
	REQ_SON_OR_06	The OR MUST be able to provide a resource brokering service.	High	High
Technologies / Techniques	REQ_SON_OR_07	OR SHOULD leverage on the existing (published, standardized) technologies to find and resolve dependencies of the actions.	High	High

	REQ_SON_OR_08	OR SHOULD leverage on the existing (published, standardized) technologies to find matching low level actions according to the provided high level actions.	High	High
Component Protocols	REQ_SON_OR_09	The OR SHOULD be able to communicate with the connected components therefore TAL, actuator API and database query languages should be implemented.	Medium	High
Data Structures	REQ_SON_OR_10	The OR SHOULD have data structures to cache the available resources VNFs and their features.	Low	Low
Non Functional	None	None		
Interoperability / Compatibility	REQ_SON_OR_11	The OR MUST be able to query the databases of Resource Manager.	Low	Low
	REQ_SON_OR_12	The OR MUST be able to query the databases of Application Manager.	Low	Low
	REQ_SON_OR_13	The OR MUST be able to enforce the selected actions to the network using the actuator API.	Low	Medium
	REQ_SON_OR_14	The OR SHOULD be able to send the orchestrated actions back to the DMP.	Low	Medium
	REQ_SON_OR_15	The data set to specify resources SHOULD be defined minimized and orthogonal for potential standardization.	Low	Medium

C.4.9 Application Manager

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SON_AM_1	App Manager MUST process orchestration requests related to provisioning of NFV/SDN Apps.	High	High
	REQ_SON_AM_2	App Manager MUST process orchestration requests related to configuration of NFV/SDN Apps.	High	High
	REQ_SON_AM_3	App Manager MAY contain a resource abstraction layer for those resources that require a resource adaptor (agent) to be instantiated for processing generic orchestration requests and streamlining these to resource specific actions.	Medium	Medium
	REQ_SON_AM_4	App Manager MUST detect compatible resources (that can be administered by the App Manager) existing in the physical or virtualized layers.	High	High
Technologies / Techniques	REQ_SON_AM_5	App Manager MAY support, via plugins, application deployment systems such as Chef, Puppet, Docker, etc.	High	High
Component Protocols	REQ_SON_AM_6	App Manager MUST be able to use proprietary protocols and APIs in order to apply configuration actions as indicated by the orchestrator.	High	High
Data Structures	REQ_SON_AM_7	App Manager MUST support a uniform and technology agnostic data and	Medium	High

		information model that can be used by the orchestrator.		
	REQ_SON_AM_8	App Manager MUST provide a uniform API accommodating all the requests generated by the orchestrator.	High	High
Non Functional	REQ_SON_AM_9	App Manager SHOULD monitor the status of the deployed Apps.	Medium	Medium
	REQ_SON_AM_10	App Manager MAY trigger alerts relating to the status of the Apps to be processed in the context of autonomous operation (corrective actions).	Medium	Medium
Interoperability / Compatibility	REQ_SON_AM_11	App Manager SHOULD be able to interface with SDN, VNE and VNF applications.	High	High
	REQ_SON_AM_12	App Manager SHOULD support pluggable modules for communicating with the APIs of SDN Apps, VNE, and VNF.	High	High

C.4.10 Resource Manager

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SON_RM_01	Resource Manager MUST offer the means to the Orchestrator to Instantiate or delete and administer NVFs over the Virtual Infrastructure Manager.	High	High
	REQ_SON_RM_02	Resource Manager MUST enumerate the available resources in the VNL Layer in terms of available networking functionality in the context of the orchestration scenarios.	High	High
	REQ_SON_AM_03	Resource Manager MUST offer the means to the Orchestrator to Instantiate or delete and administer NVFs over the WAN Infrastructure Manager.	High	High
	REQ_SON_RM_04	Resource Manager SHOULD have the possibility to query the actual resources from physical network.	High	High
Technologies / Techniques	REQ_SON_RM_05	Resource Manager SHOULD interface with the most promising open source cloud services like Open Stack, Apache Cloud Stack, etc.	Medium	High
Component Protocols	None	None		
Data Structures	REQ_SON_RM_06	Resource Manager SHOULD support a uniform and technology agnostic data information model (e.g. independent of the cloud provider used) representing the deployed NFV & SDN resources and the available cloud resources.	High	High
Non Functional	None	None		
Interoperability / Compatibility	REQ_SON_RM_07	Resource Manager SHOULD provide the abstraction instances of the underlying virtualized infrastructure composing a uniform view.	High	High

C.4.11 NFV Apps and SDN Apps Encapsulation

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SON_NS_01	Encapsulation MUST provide a unified abstraction of life-cycle management primitives valid for any SELFNET NFVs.	Medium	Medium
	REQ_SON_NS_02	Encapsulation MUST provide mechanisms and tools to containerize the SELFNET NFVs for their homogeneous access and storage into the SDN/NFV applications repository.	Medium	Low
	REQ_SON_NS_03	Encapsulation MUST provide mechanisms and tools for automated deployment and un-deployment of SELFNET NFVs into the virtualized infrastructure.	Medium	High
	REQ_SON_NS_04	Encapsulation MUST enable automated configuration and dynamic re-configuration of SELFNET NFVs.	High	High
	REQ_SON_NS_05	A service description SHOULD contain clear identification of what plane each deployable element belongs to.	Medium	Medium
	REQ_SON_NS_06	Each deployable component MAY have a list of required hardware properties.	Low	Low
Technologies / Techniques	REQ_SON_NS_07	Encapsulation SHOULD leverage on ETSI NFV MANO components and interfaces and enhance them in support of SELFNET automated and dynamic NFVs lifecycle management.	Medium	Medium

	REQ_SON_NS_08	Encapsulation SHOULD enhance NFV management and orchestration tools to homogenize mechanisms and primitives to manage and configure the SELFNET NFVs.	Medium	High
Component Protocols	None	None		
Data Structures	REQ_SON_NS_09	Encapsulation SHOULD enhance VNFs data structures and descriptors defined in ETSI NFV MANO towards a uniform abstraction of capabilities and virtual resource requirements across heterogeneous NFVs.	Medium	High
	REQ_SON_NS_10	Encapsulation SHOULD enhance data structures and descriptors defined in ETSI NFV MANO for NFVs link to facilitate the automated SELFNET virtual service composition and chaining (coordinated by the orchestrator).	High	High
Non Functional	REQ_SON_NS_11	Encapsulation mechanisms and tools MUST enable fast deployment of SELFNET NFVs into the virtualized infrastructure.	Medium	Medium

	REQ_SON_NS_12	Encapsulation MUST provide simple and user-friendly primitives and APIs to facilitate its integration into NFVs implemented by SELFNET software developers.	Medium	Low
	REQ_SON_NS_13	Encapsulation MUST provide secure mechanisms to access the life-cycle management APIs exposed to other SELFNET components.	Low	Medium
Interoperability / Compatibility	REQ_SON_NS_14	Encapsulation MUST enable publishing and upload of SELFNET NFVs into the SDN/NFV Applications repository.	Low	Medium
	REQ_SON_NS_15	Encapsulation MUST expose dedicated APIs for its integration with the Orchestrator.	Medium	Medium
	REQ_SON_NS_16	Encapsulation MUST enable publishing an update of SELFNET NFVs capabilities into the Decision-Making Planner.	Medium	Medium

C.4.12 NFV/SDN Repository

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SON_NR_01	NFV & SDN Repository MUST provide life-cycle management primitives to enable SELFNET tools to automatically deploy and undeploy NFV Apps.	Medium	Medium
	REQ_SON_NR_02	NFV & SDN Repository MUST provide mechanisms and tools to access stored VNFs and collect information about their capabilities.	Medium	Medium
	REQ_SON_NR_03	NFV & SDN Repository MUST provide management primitives to get required virtualized infrastructure resources to deploy VNFs.	Medium	High
	REQ_SON_NR_04	NFV & SDN Repository SHOULD provide a user-friendly GUI for software developers to upload and remove SELFNET NFVs.	Low	Low
	REQ_SON_NR_05	NFV & SDN Repository SHOULD organize, store and expose SELFNET NFVs according to their capabilities (e.g. type of sensor/actuator).	Low	Medium
	REQ_SON_NR_06	NFV & SDN Repository MUST be able to provide remote deployment of components in different locations of the network.	High	High
Technologies / Techniques	None	None		
Component Protocols	None	None		

Data Structures	REQ_SON_NR_07	NFV & SDN Repository SHOULD provide a common and uniform description and representation of stored NFVs to ease their export and usage by the SELFNET platform.	Medium	Medium
Non Functional	REQ_SON_NR_08	NFV & SDN Repository MUST provide secure mechanisms to retrieve and store all the NFV-Apps and SDN-Apps.	Medium	Medium
	REQ_SON_NR_09	New NFV-Apps and SDN-Apps SHOULD be available as soon as created for their deployment.	Low	Low
	REQ_SON_NR_10	NFV & SDN Repository MAY support versioning of stored SELFNET VNF.	Low	Medium
Interoperability / Compatibility	REQ_SON_NR_11	The NFV & SDN Repository SHOULD provide management primitives for software developers to update their stored SDN-Apps and NFV-Apps.	Low	Medium
	REQ_SON_NR_12	The NFV & SDN Repository MUST enable publishing the SDN-Apps and NFV-Apps for the SELFNET Decision Making Planner and Orchestrator.	Medium	Low

C.5 SELFNET Access Layer

C.5.1 Graphical Interface

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_SAL_GI_01	GI MUST show all devices and sensors/actuator deployed on SELFNET	High	High
	REQ_SAL_GI_02	GI MUST show the current status of a given device or sensor/actuator deployed on SELFNET	High	High
	REQ_SAL_GI_03	GI MUST be able to retrieve or set devices and sensors/actuators configuration	High	High
	REQ_SAL_GI_04	GI SHOULD be able to display data collected by devices and sensors/actuator deployed on SELFNET.	High	High
	REQ_SAL_GI_05	GI SHOULD be able to display the current status of SELFNET.	High	High
	REQ_SAL_GI_06	GI MUST be able to present suspicious and anomalous situations on SELFNET.	High	High
	REQ_SAL_GI_07	GI MAY be able to display autonomous decision-making action points taken by SELFNET.	High	High
	REQ_SAL_GI_08	GI MUST provide user management features.	Low	High
	REQ_SAL_GI_09	GI MUST implement an authentication mechanism to end users in order to validate that a user has access to SELFNET's GUI and to check the correspondent role.	Low	High
	REQ_SAL_GI_10	Based on a user's role on SELFNET, GI will filter the provided features.	Low	High
	REQ_SAL_GI_11	GI MUST provide the ability to help in the description and insertion of the tactical autonomic capabilities used to configure the SELFNET framework.	High	High

Technologies / Techniques	None	None		
Component Protocols	REQ_SAL_GI_12	GI MUST be able to support SELFNET's Northbound API and protocols in order to interact with SELFNET.	Medium	High
Data Structures	REQ_SAL_GI_13	GI MUST be able to support data structures in use on SELFNET.	High	High
Non Functional	REQ_SAL_GI_14	GI SHOULD provide the most important features/actions with no more than three mouse clicks.	Medium	High
	REQ_SAL_GI_15	GI should be easy to understand and to interact with, without the need to read a complicated manual.	Medium	High
	REQ_SAL_GI_16	GI should always allow an end user to be able to identify where he is.	Medium	High
	REQ_SAL_GI_17	GI should always allow to seamlessly going back to the main screen /dashboard.	Medium	High
	REQ_SAL_GI_18	GI should be consistent. Consistency improves predictability, which increases learnability.	Medium	High
	REQ_SAL_GI_19	GI MUST provide visual feedback, especially in cases of loading and error.	Medium	High
Interoperability / Compatibility	REQ_SAL_GI_20	GI MUST be able to interact with SELFNET's Northbound API.	Medium	High

C.6 NFV Orchestration & Management Layer

C.6.1 VIM Cloud Management Sublayer

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_CML_1	VIM Cloud Management MUST be able to manage multiple zones geographically distributed (data centre and edge networks).	Low	High
	REQ_CML_2	VIM Cloud Management MUST provide management functionalities over the compute resources of the infrastructure.	Low	High
	REQ_CML_3	VIM Cloud Management MUST provide multi-tenancy support over physical infrastructures.	Low	High
Technologies / Techniques	None	None		
Component Protocols	None	None		
Data Structures	None	None		
Non Functional	None	None		
Interoperability / Compatibility	None	None		

C.6.2 VIM NFV Management Sublayer

REQ Type	ID	Description	Novelty	Exploitability
Component Design	REQ_NFVM_1	WIM MUST be able to manage multiple zones geographically distributed (data centre and edge networks).	High	High
	REQ_NFVM_2	WIM MUST provide management functionalities over the connectivity of NFV resources (service channelling).	High	High
	REQ_NFVM_3	WIM SHOULD provide multi-tenancy support over networking infrastructures	High	High
Technologies / Techniques	None	None		
Component Protocols	None	None		
Data Structures	None	None		
Non Functional	None	None		
Interoperability / Compatibility	None	None		