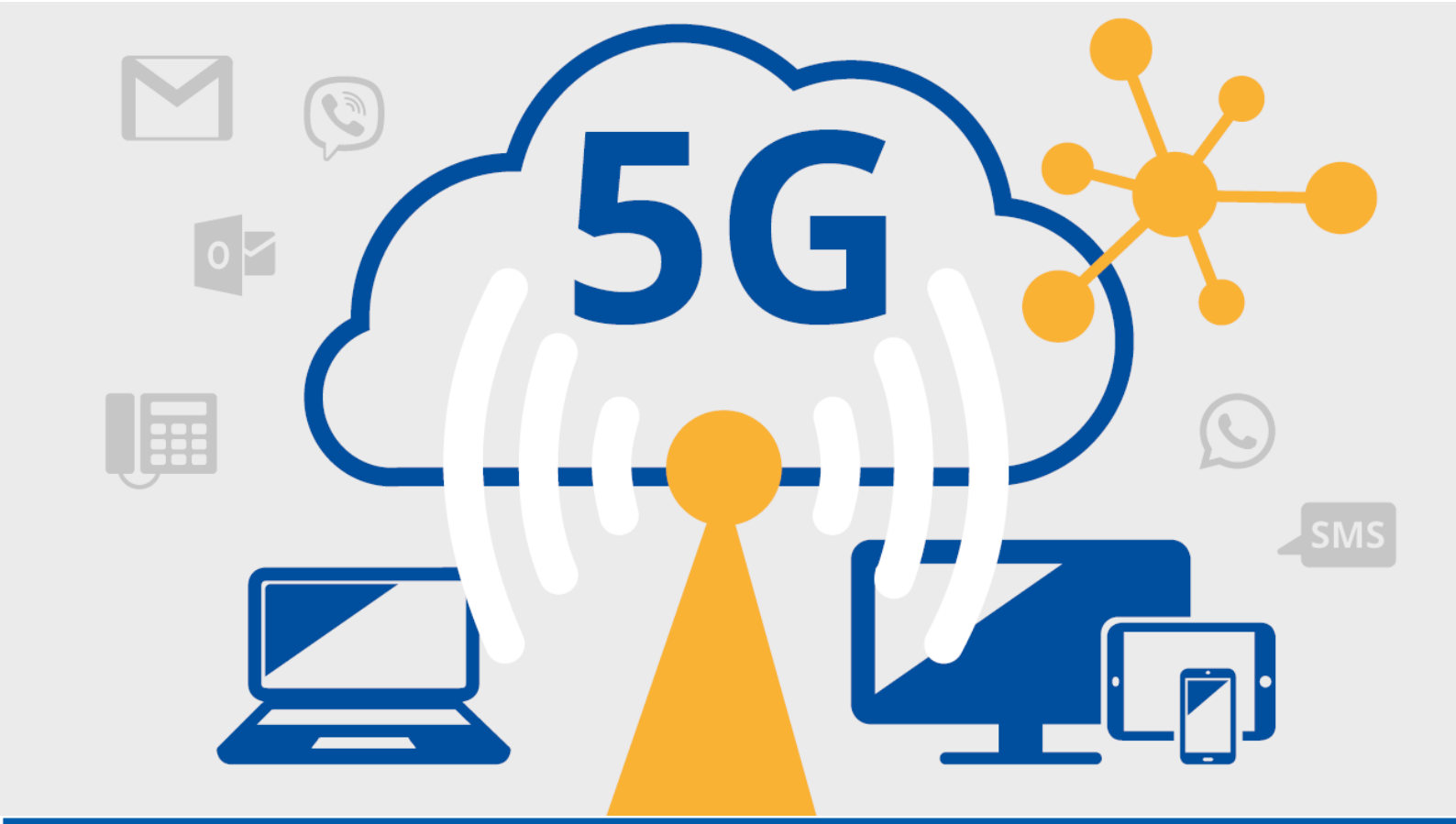
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



NFV SECURITY IN 5G

Challenges and Best Practices

FEBRUARY 2022

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use resilience@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

EDITORS

Evgenia Nikolouzou, Goran Milenkovic, Georgia Bafoutsou and Slawomir Bryska (ENISA)

CONTRIBUTORS

Mohamad Hajj, Claire Loiseaux

ACKNOWLEDGEMENTS

We are grateful for the review and valuable input received from: the experts in the ECASEC Expert Group (formerly known as Article 13a Expert Group), which comprises national telecom regulatory authorities (NRAs) from all EU and EFTA countries, from the experts from national authorities in the NIS Cooperation group, and particularly those experts contributing to the NIS CG work stream on 5G cybersecurity, from the ETSI ISG NFV Security WG that is developing specifications and reports for the virtualization of network functions, with focus on the management and orchestration of virtualized resources.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-557-9, DOI 10.2824/166009, Catalogue Number TP-06-22-045-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The advent of 5G wireless communications constitutes a new era of network connection that will not only expand technical capabilities but will also revolutionise many aspects of commerce and personal lives by driving an exponential increase in the number of connected devices in various sectors of the economy.

5G is an altogether different network technology that will introduce a virtualised, cloud-based architecture, enabling highly specialised functions and security for different network applications. This 5G revolution will also expand the attack surface for cyberthreats thus necessitating the introduction of the principles of security-by-design from the early stages of the design and deployment of 5G networks.

Towards this technological revolution, the European Commission and the Member States, with the support of ENISA, developed a single EU Coordinated Risk Assessment on Cybersecurity in 5G Networks, following on the European Commission's Recommendation on the cybersecurity of 5G networks. Subsequently, the NIS Cooperation Group published the EU toolbox of risk mitigating measures.

The objectives of this toolbox are to identify a possible common set of measures that are capable of mitigating the main cybersecurity risks of 5G networks that were identified in the EU report on coordinated risk assessment, and to provide guidance for the selection of measures that should be prioritised in mitigation plans at national and at Union level. One of the technical measures, TM04, calls on relevant authorities in EU Member States to ensure that Mobile Network Operators follow security best practices for network function virtualisation (NFV).

Network Function Virtualisation (NFV) has made a huge impact in a very short time since the use of virtualisation technologies brings various benefits such as agility, flexibility and cost efficiency. At the same time, the introduction of NFV in 5G networks also introduces new challenges and risks. NFV changes the network security environment due to resource pools based on cloud computing and open network architecture.

Thanks to the agility and the Orchestration and Management (O&M) efficiency of NFV networks, attacked networks can potentially be abandoned and resources recycled, enabling disasters to be quickly isolated, a response that's impossible in traditional networks. Network functions, network links, and even entire networks can be rapidly redeployed, enabling fast recovery from disasters. At the same time, though, security challenges have become more diverse.

In this report the relevant challenges, vulnerabilities and attacks pertaining to NFV within the 5G network are explored and security controls and best practices are put forward to address these challenges, taking into account the particularities of this highly complex, heterogeneous and volatile environment.

Accordingly, this ENISA study provides the following main information:

- The 5G NFV security framework,
- Potential 5G NFV deployment models,
- Main stakeholders involved in the 5G NFV ecosystem with their roles and responsibilities,
- Challenges, vulnerabilities, assets and attack taxonomies for 5G NFV,
- Best practices to improve the cybersecurity posture of 5G NFV,

- Full mapping of challenges, vulnerabilities, assets, attack scenarios and best practices,
- NFV Standardisation, Open-Source and initiatives from academia and industry.

Specifically, in this report sixty security challenges grouped into 7 categories have been identified and explored. These drive the report to the next steps: vulnerabilities, attack scenarios, their impact on the 5G NFV assets and 55 best practices classified under Technical, Policy and Organisational categories.

The main challenges explored in this report have shown that:

- **Resource virtualisation:** the virtualisation layer provides unified computing resources based on generalised hardware to the layers above and is the basis of all cloud-native and virtualised network functions and service software. If the virtualisation layer is breached, all network functions come under direct attack with disastrous consequences.
- **Resource sharing:** a single physical server may run several different tenants' virtual resources (e.g. virtual machines (VMs) or containers), and a single tenant's virtual resource might be distributed across several physical servers. Multi-tenancy resource sharing and the breaking of physical boundaries introduce the risks of data leaks, data residue and attacks.
- **Use of open source:** there will be increasing use of open-source software. This introduces a new set of security challenges in terms of keeping a consistent and coherent approach to security-by-design and the prevention of deliberate security flaws.
- **Multi-vendor environment**: in such an environment is it difficult to coordinate security policies and determine responsibility for security problems and requires more effective network security monitoring capabilities.
- **Supply chain**: introduces risks such as malicious software and hardware, counterfeit components, poor designs, manufacturing processes and maintenance procedures. This may result in negative consequences, such as data and intellectual property theft, loss of confidence in the integrity of the 5G network, or exploitation to cause system and network failure.
- **Lawful Interception (LI) functionality:** placing LI functions within the virtualised environment exposes them to a variety of security and visibility risks.

1. INTRODUCTION

Fifth Generation (5G) networks aim at providing value-added services with advanced performance such as low-latency communications, high reliability, high data rates and capacity to support an increasing number of connected devices. 5G aims to provide a flexible platform to integrate vertical industries and a wide range of services and applications such as autonomous driving, robotics, augmented and virtual reality, remote healthcare, and more.

For such services and use cases, security technology and architecture must be natively integrated into the overall hybrid and virtual architecture to appropriate internal and external security services. Previous iterations, such as GSM/CMDA (2G) and HSPA/eVDO (3G,) were designed to connect people to people predominantly through voice and text, while LTE/LTE-A (4G) was designed to connect people to the Internet. 5G expands upon this evolution through ubiquitous connectivity of things to people, services, the Internet and things.

To meet the requirements for scale, throughput, latency, and reliability, 5G architecture has adopted Network Function Virtualisation (NFV) and software-Defined Networking (SDN) to streamline network and service deployment, operations and management. Operators, service providers and other verticals (e.g. Connected Cars, IOT, eHealth, Industry 4.0) can leverage SDN/NFV to provide flexible and cost-effective service without compromising the end user's quality of service (QoS).

NFV and SDN open the door to flexible networks and rapid creation of services. This both offers opportunities for security and introduces additional security challenges and complexities in some cases.

With the rapid proliferation of 5G networks, operators have started the deployment of NFV. While several standardisation bodies (e.g. ETSI, 3GPP, NGMN and GSMA) have started looking into the many security issues introduced by NFV, additional work is needed with greater involvement of the security community including vendors, operators, universities and regulators.

This report will focus on various security challenges and opportunities introduced by NFV in 5G. We will present current security challenges, vulnerabilities and attacks pertaining to NFV within the 5G network and put forward security controls and best practices to address these challenges taking into account the particularities of this highly complex, heterogeneous and volatile environment.

1.1 OBJECTIVES

This ENISA study aims at underlining and analysing the security challenges related to 5G NFV. The main objectives are to identify challenges and best practices to ensure the security of 5G NFV, while mapping the relevant security challenges, vulnerabilities, attacks scenarios, assets and best practices.

Note: '5G NFV' in this report means the 'NFV as applicable to 5G'.

This study indicates how challenges and vulnerabilities can be exploited through cyberthreats and how this exploitation can be mitigated through security controls and best practices.

The following objectives have been set:

- identify 5G NFV sensitive assets,
- identify potential and main cyber challenges, vulnerabilities and attack scenarios targeting 5G NFV,
- map identified challenges, vulnerabilities and attack scenarios to assets,
- identify relevant security measures and best practices, and map them to the security challenges.

Identified challenges, vulnerabilities, attack scenarios and best practices are consolidated from various publicly available resources including:

- main 5G standardisation documents and telecommunication best practices (3GPP, ETSI, NIST, FFT, FCC and GSMA),
- EU-funded research projects (5GPPP),
- industrial white papers,
- research articles,
- guidance and recommendations for organisations such as CIS and CSA,
- interviews and contributions from 5G security experts and Member States

1.2 SCOPE

Towards this technological revolution, the European Commission and the Member States (MS), with the support of ENISA, developed a single EU Coordinated Risk Assessment on Cybersecurity in 5G Networks[1], following on the European Commission's Recommendation on the cybersecurity of 5G networks[2] (published on 26 March, 2019).

This coordinated risk assessment is based on individual national risk assessments and identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities and the main risks.

To complement this report and as a further input for the toolbox, ENISA carried out a dedicated threat landscape mapping, consisting of a detailed analysis of certain technical aspects, in particular the identification of network assets and of threats affecting these.

Subsequently, on 29 January 2020, the NIS Cooperation Group published the EU toolbox of risk mitigating measures[3]. The objectives of this toolbox are to identify a possible common set of measures that are capable of mitigating the main cybersecurity risks of 5G networks as have been identified in the EU coordinated risk assessment report, and to provide guidance for the selection of measures, which should be prioritised in mitigation plans at national and at Union level.

The toolbox identifies two groups of measures MS can take: strategic and technical measures. In addition, it identifies a number of supporting actions that can assist, enable or support the implementation of strategic and technical measures.

One of the technical measures, TM04, calls on relevant authorities in EU Member States to ensure that mobile network operators follow best practices in security for network function virtualisation (NFV). To support implementation of this technical measure, the Toolbox also defines the supporting action SA01, calling for reviews or the development of guidelines and best practices on network security, and identifying ENISA and the relevant authorities in MSs as relevant actors for these regards. NFV Security in 5G is one of the key issues that needs to be

[1] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security
[2] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154
[3] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

addressed comprehensively in order to take advantage of the business opportunities arising from 5G Networks.

This ENISA study outlines best practices for the security of 5G NFV. It is building on several previous ENISA studies on 5G[4][5] and virtualisation[6] and mainly focuses on 5G NFV.

The purpose of the report is to explain the security challenges associated with NFV in 5G and make practical best practices and recommendations for addressing those challenges when planning for, implementing and maintaining NFV.

Within NFV, a Network Function is implemented in a virtualised form of NF or cloud Native NF. In this report the term 'VNF' Virtual Network Function is used to designate both virtualised NF and cloud Native NF. The VNF is defined in this report as a software implementation of a Network Function, capable of running on the Cloud Infrastructure. VNFs are built from one or more VNF components (VNFC) and, in most cases, the VNFC is hosted on a single VM or container.

Virtualised NF and Cloud Native NF are similar in that they both virtualise network functions to build an agile 5G NFV infrastructure. Both use an underlying physical server to readily expand and adapt whenever and wherever the user needs to deploy network capabilities. The difference mainly lies in how those network functions are abstracted from the underlying physical server infrastructure.

- Virtualised NF uses a hypervisor to provide a single layer of abstraction that enables networking and network security functions to run as dedicated appliances (e.g. routers, firewalls, etc.) in the form of virtual machines (VMs), which can quickly be deployed on generic hardware.
- Cloud native NF reduces each discrete network and network security function into a microservice, packaged in its own container, and deployed on generic hardware resources on a cloud platform.

Consequently, some aspects of NFV may vary among technologies (e.g. VM, container), but the most security challenges and best practices in this report are intended to apply to most or all NFV technologies, unless otherwise specified.

1.3 TARGET AUDIENCE

The main purpose of this report is to provide knowledge and information on 5G NFV challenges and best practices to the relevant community. This information may be useful to a variety of target groups.

- **Non-technical stakeholders such as policy-makers, regulators and law enforcement**: this target group may find this report useful for understanding the emerging challenges, vulnerabilities, threats and respective practices and measures for mitigation.
- **Experts working in the telecommunication sector, such as operators, vendors, and service providers**: this target group may find this report useful for carrying out detailed threat analyses and risk assessments in accordance with their particular needs and mandate (e.g. to protect a specific number of components based on asset impact analysis, respond to specific vulnerabilities with customised mitigation measures among others).

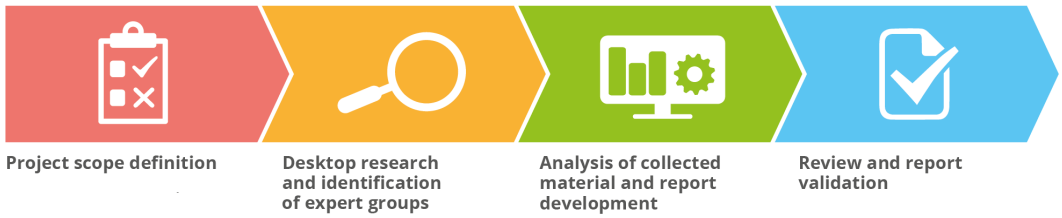
[4] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks
[5] https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc
[6] https://www.enisa.europa.eu/publications/security-aspects-of-virtualization

- **Businesses, consultants and product developers**: this target group can draw valuable conclusions from the developed analysis and material for their offerings (products, services). This can take the form of demonstrating how vulnerabilities have been eliminated by using developed defences, use of the material within customer projects, or use of the material as a benchmark for defining cybersecurity protection policies for such infrastructures (e.g. for the development of verticals). Moreover, the developed material can be used in developing security audits for 5G NFV infrastructures.
- **Experts in research and innovation**: the material presented provides a detailed view of security issues for 5G NFV. This target group may use this material as a basis for gap analysis, as material to evaluate the impact of research and as a source for innovative actions with regard to its further development and implementation. Finally, this target group may use this material as a useful resource for numerous academic activities, such as teaching, research, support of scholars, etc.

1.4 METHODOLOGY

ENISA has developed this study by following a four-step methodological approach.

Figure 1: Methodology



(1) **Project scope definition**: the first step consisted in establishing the scope of the project and identifying the main topics to be considered during the study.
(2) **Desktop research and identification of expert groups**: extensive research of relevant documents to gather as much information as possible about 5G NFV security challenges and best practices. The identified documents and standards were used as references for the development of this report. During this step, subject matter experts were also invited to validate scope and provide feedback.
(3) **Analysis of collected material and report development**: all the information collected, whether through desktop research or directly from the experts identified, was thoroughly analysed.
(4) **Review and report validation**: ENISA shared the draft of the report with its relevant stakeholder communities and reference groups for review. Taking the feedback from the stakeholders into account, the proposed final version of the report was issued.

1.5 STRUCTURE OF THE REPORT

The study is structured as follows.

1. **Chapter 1 - Introduction**: provides introductory information on the objectives, scope, target audience, methodology followed and the structure of this study.
2. **Chapter 2 - 5G NFV security framework**: describes the architecture of 5G from the core to the far edge with a focus on the roles of NFV and SDN. It explores the main opportunities in NFV when it comes to security and illustrates some deployment models with varying risks that may be considered in a virtualised environment.
3. **Chapter 3 – 5G NFV: Assets, challenges, vulnerabilities and attack scenarios**: lists sensitive assets that need to be protected. It identifies the main security

challenges to be resolved. Moreover, it illustrates the list of potential vulnerabilities related to NFV challenges and sorts the main attacks into categories and their impacts.

4. **Chapter 4 – 5G NFV security best practices**: presents a brief description of the security measures and best practices to mitigate and solve the challenges identified. It describes the high-level interrelations at the category level between the categories of challenges, categories of vulnerabilities, attacks, affected assets and best practices.
5. **Chapter 5 - Open and future security challenges**: provides some of the research challenges and future directions for NFV security.

The full details, taxonomies and coverage mappings are provided in the annexes as follows.

A. **Annex A – Roles and Responsibilities**: presents the various administrative roles and responsibilities belonging to 5G stakeholders.
B. **Annex B – Assets Maps**: provides mind maps of the assets already described in Chapter 3.
C. **Annex C - Vulnerability Taxonomy**: presents a description of the various NFV vulnerabilities illustrated in Chapter 3 that can be exploited to perform attacks impacting the confidentiality, integrity and availability of NFV systems.
D. **Annex D - Attack Taxonomy**: provides for each attack listed in Chapter 3.
E. **Annex E - Best practices register**: provides a full description of best practices from Chapter 4 with references.
F. **Annex F - Mapping of challenges, vulnerabilities, attacks scenarios, affected assets and best practices**: illustrates the detailed mapping of security challenges to vulnerabilities, attacks scenarios, affected assets and best practices.
G. **Annex G - Challenges references**: lists the documents used as references for the development of security challenges in Chapter 3.
H. **Annex H – NFV MANO Platforms**: details the main MANO (management and orchestration) platforms for both VMs and/or containers.
I. **Annex I – NFV standardisation, open source and academic or industrial initiatives:** provides the main NFV standardisation, open-source and initiatives by academia and industry.

2. 5G NFV SECURITY FRAMEWORK

2.1 5G END-TO-END ARCHITECTURE

Figure 2 presents an NFV/SDN-enabled 5G architecture. It illustrates the various components from the core to the far edge. As defined by the 3rd Generation Partnership Project (3GPP), the 5G network is a Service-Based Architecture (SBA) which is a set of interconnected network functions (NFs) that deliver the control plane functionality and common data repositories of a 5G network [1], [2], [3], [4].

Supporting an SBA brings new requirements for the control, coordination and orchestration of disaggregated network functions that are distributed across the network. These network functions are virtualised or containerised microservices that can support the 5G core, the Radio Access Network (RAN), and the MEC (Multi-access Edge Computing).

Cloud RAN (CRAN), Virtualised RAN (VRAN) and Open RAN (ORAN) are all concepts that have emerged in the last few years to run baseband functions on commodity server hardware, based on the principles of Network Functions Virtualisation (NFV). The MEC takes advantage of the existing NFV infrastructure to provide services characterised by low latency, proximity, location awareness, high bandwidth and real-time insight into radio network information.

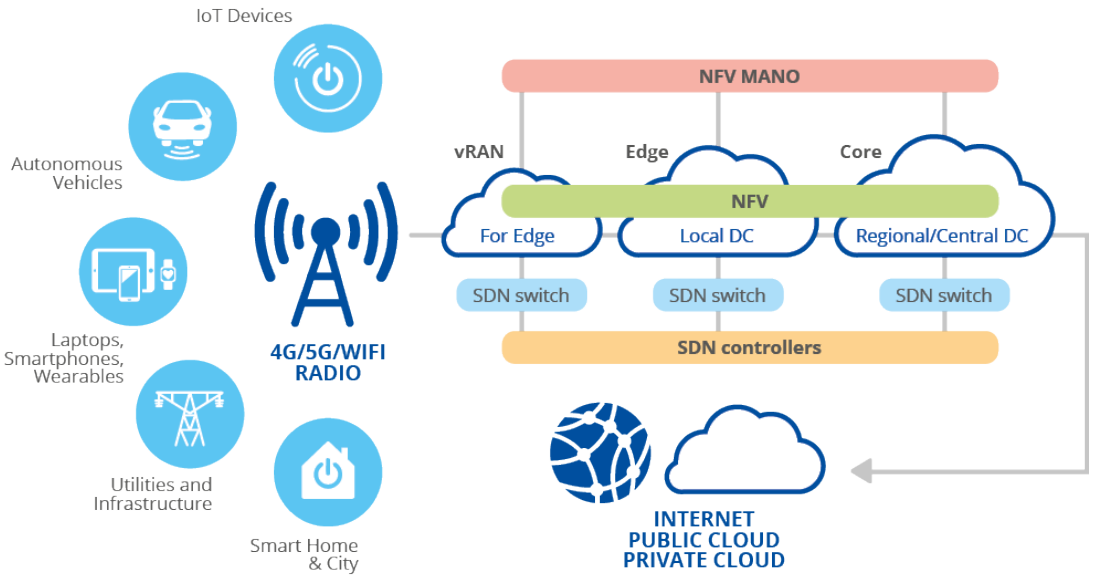
In order to support CRAN/ORAN/VRAN and MEC, operators will deploy small datacentres at the edge. These infrastructures will make it possible to deploy applications and VNFs at the edge without investing additional resources. The MEC (edge) platform at each datacentre will allow third party applications to activate traffic offloading at the edge while also enabling access to other information provided by the operator.

The core network is the central part of the 5G infrastructure. It enables all functions related to multi-access technologies. Its main purpose is to deliver services over all kinds of networks (wireless, fixed, converged). The target of SDN is to use programmable software-driven devices to control the behaviour of the infrastructure. With SDN, user services can be delivered faster, and the efficiency of network resources increases. SDN is based on three principles:

1. decoupling of control from traffic forwarding and processing,
2. logically centralised control,
3. programmability of network services.

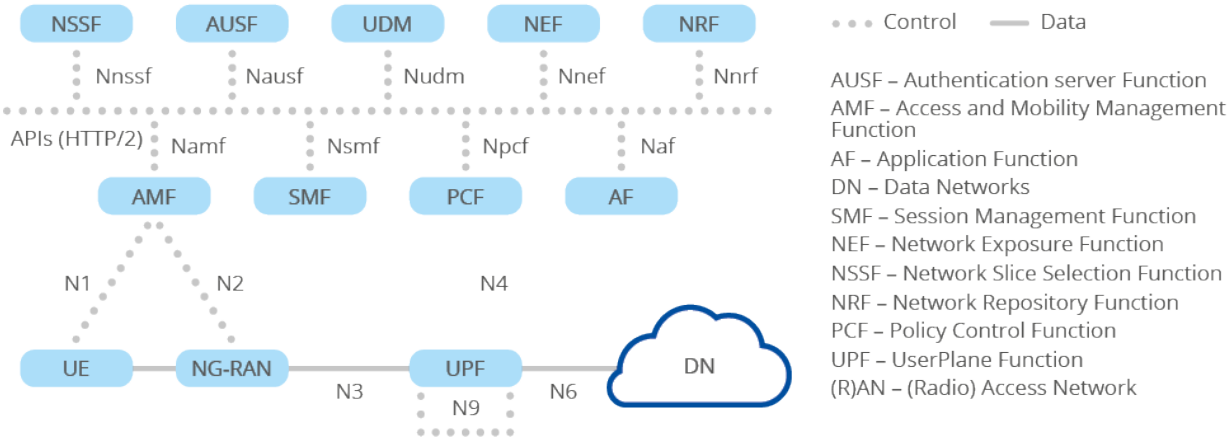
A fully virtualised 5G network could bring significant benefits of harmonisation: one single uniform hardware platform across the core network, RAN and edge. This could simplify the management of the complete network, reducing operations and maintenance costs.

The following two sections give more details on the co-dependent technologies of NFV and SDN. Where NFV is in charge of dynamically creating and managing the network functions and provisioning various network services, SDN provides the capabilities to manage and orchestrate the virtual networks among these services. While both SDN and NFV make networking architectures more flexible and dynamic, they perform different roles.



2.1.1 Service based architecture

Compared to previous generations the 3GPP 5G system architecture is service based (SBA) (Figure 3) [2], [3], [4]. That means wherever suitable the architectural elements are defined as network functions that offer their services via interfaces of a common framework to any network functions that are permitted to make use of these provided services. The SBA specifies flat peer to peer relationships between Network Functions (NFs) via the HTTP/2-based Service Based Interface (SBI). Network Repository Functions (NRF) allow every network function to discover the services offered by other network functions.



This architectural model, which further adopts principles like modularity, reusability and self-containment of network functions, is chosen to enable deployments to take advantage of the latest virtualisation and software technologies [5]. Instead of specifying network entities, a more modular design is achieved by specifying a set of NFs which allows stronger decoupling between logical and physical architecture, facilitating the virtualisation of the different NFs running on generic computer hardware. Furthermore, NFs can be physically implemented in different ways (e.g. all of them in a single physical node, distributed across multiple nodes or running on a cloud platform).

With the split of control plane and user plane, NFs responsible of the control plane are different from those responsible of the user plane allowing independent scalability and evolution (e.g. allocating more capacity to the control plane without affecting the user plane). Moreover, it allows flexible deployments, e.g. centralised location for control plane or distributed (remote) location for user plane.

2.1.2 5G Network Functions

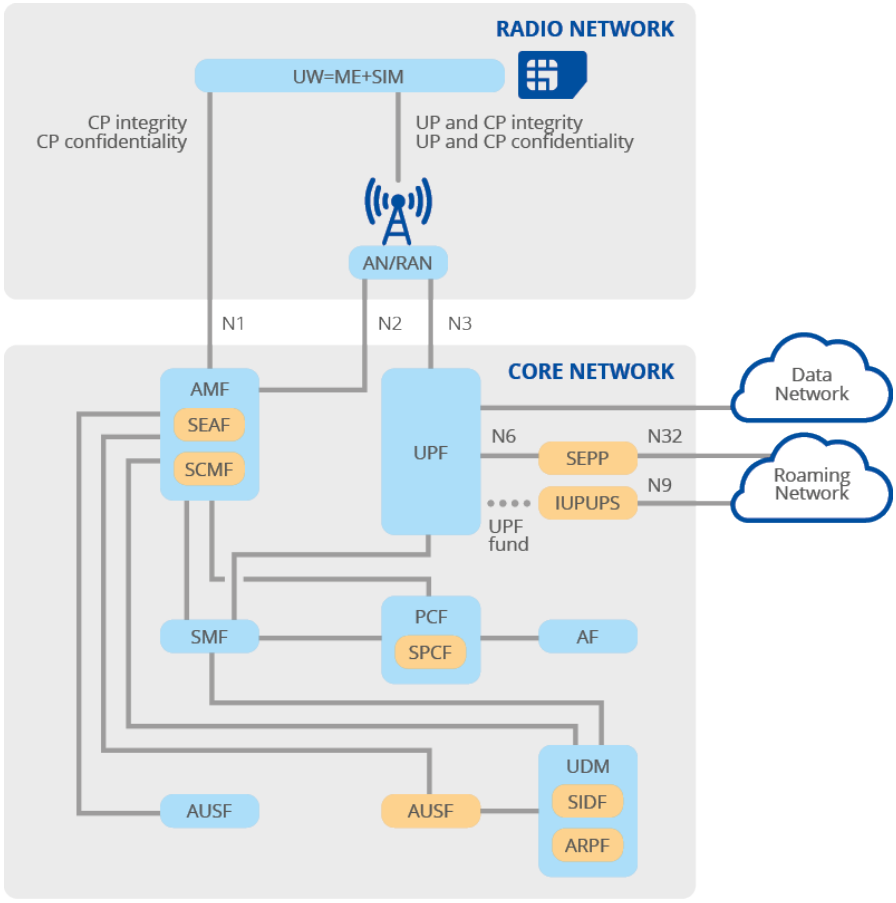
The 5G core is a mesh of interconnected services as shown in Figure 3. In addition, the 5G system architecture introduces several security-related 5G network functions [2], [3], [4], [6] as shown in Figure 4. Table 1 gives a brief explanation of each network function.

Table 1: 5G network functions

Network Function	Description
User Plane	
User Plane Function (UPF)	The User Plane Function deals with the user plane communication in the 5GC, acting as a gateway between the RAN and the external Data Network (DN) (e.g. Internet). The main functionalities are: packet routing and forwarding, downlink packet buffering and downlink data notification triggering, QoS handling and traffic measurements.
Control Plane	
Access and Mobility Management Function (AMF)	The Access and Mobility Management Function is a control plane function in charge of handling the control signalling between the UE and the 5GC. The main functionalities are: registration management, connection management to establish the control plane signalling with the UE, mobility management (e.g. idle mode UE reachability), control and execution of paging and support of infra-system and inter-system mobility.
Session Management Function (SMF)	The Session Management Function is a control plane function in charge of the following main functionalities: session establishment, modification and release, UE IP address allocation and management, control of policy enforcement and QoS and configuration of traffic steering at UPF to route traffic to proper destination.
Policy Control Function (PCF)	The Policy Control Function provides policy rules (e.g. authorised QoS for each service data flow) to the network functions in charge of enforcing them (e.g. SMF).
Application Function (AF)	The Application Function allows interacting with the applications making use of the network. This can be used for applications that require dynamic policy control, e.g. for dynamically modifying the bit rate to be provided. Based on interactions with these applications, policy requirements are provided to the PCF.
Unified Data Management (UDM)	The function of Unified Data Management is to provide the handling of user identification, subscription management, access authorisation based on subscription data (e.g. roaming restrictions), and generation of authentication credentials. It uses subscription data that may be stored in the UDR (Unified Data Repository).
Network Exposure Function (NEF)	The Network Exposure Function is used to expose services of the 5G core towards other networks (e.g. third party providers, verticals, etc.). This allows the fast creation of new services making use of the 5G core.
Network Repository Function (NRF)	The Network Repository, with the profile of the available NF instances (id, PLMN ID, network slice identifiers, capacity information, etc.) and their supported services, allows an NF to discover the services offered by the other NFs of the core network. This provides a lot of flexibility for defining the interactions between NFs and allows that any NF can directly interact with another one.
Security-related Network Function	
Authentication Server Function (AUSF)	The AUSF provides the UE authentication service. AUSF shall handle authentication requests for both, 3GPP access and non-3GPP access. The AUSF shall provide SUPI to the VPLMN (core network or serving network) only after authentication confirmation if authentication request with SUCI was sent by VPLMN. The AUSF shall inform the UDM that a successful or unsuccessful authentication of a subscriber has occurred.
Authentication Credential Repository and Processing Function (ARPF)	The ARPF is a functional element of the UDM (Unified Data Management), responsible for generating 5G HE AV (5G Home Environment Authentication Vectors) based on the subscriber's shared secret key. It selects an authentication method based on subscriber identity and configured policy and computes the authentication data and keying materials.

Network Function	Description
Inter-PLMN UP Security (IPUPS)	The 5G System architecture introduces Inter-PLMN UP Security (IPUPS) at the perimeter of the PLMN for protecting user plane messages. The IPUPS is a functionality of the UPF that enforces GTP-U security on the N9 interface between UPFs of the visited and home PLMNs.
Security Context Management Function (SCMF)	The SCMF retrieves the key from the SEAF, which is used to derive further keys.
Subscription Identifier De-concealing Function (SIDF)	The SIDF is a functional element of the UDM (Unified Data Management), responsible for decrypting a SUCI (Subscription Concealed Identifier) to reveal the subscriber's SUPI (Subscription Permanent Identifier).
Security Anchor Function (SEAF)	The SEAF forms, as an outcome of the primary authentication, the unified, common anchor key KSEAF for all the access scenarios. The unified anchor key KSEAF can be used by the UE and the serving network to protect the subsequent communication[7].
Security Edge Protection Proxy (SEPP)	The 5G System architecture introduces a Security Edge Protection Proxy (SEPP) as an entity sitting at the perimeter of the PLMN for protecting control plane messages. The SEPP enforces inter-PLMN security on the N32 interface. The SEPP shall act as a non-transparent proxy node.
Security Policy Control Function (SPCF)	The SPCF provides policies related to the security of network functions such as AMF, SMF and UE.
Network Slice Selection Function (NSSF)	The NSSF supports the selection of the Network Slice instance(s) serving a UE. It offers services to the AMF and NSSF in a different PLMN via the Nnssf service-based interface (see 3GPP TS 23.501 [3] and 3GPP TS 23.502 [4]).

Figure 4: Security-related 5G network functions[8]



[7] https://www.researchgate.net/profile/Andreas_Kunz2/publication/319527681_Overview_of_5G_security_in_3GPP/links/59b116d80f7e9b37434a8248/Overview-of-5G-security-in-3GPP.pdf
[8] https://www.gsma.com/security/wp-content/uploads/2021/06/T-ISAC_5G-Security_PenttinenJ-GSMA-public.pdf

2.1.3 Support of network slicing

A distinct key feature of the 5G system architecture is network slicing. Within the scope of the 3GPP 5G system architecture a network slice refers to the set of 3GPP defined features and functionalities that together form a complete Public Land Mobile Network (PLMN) for providing services to UEs.

Network slicing allows for controlled composition of a PLMN from the specified network functions with their specific, provided services that are required for a specific usage scenario. Each PLMNs is customised by instantiating only the features, capabilities and services required to satisfy the subset of the served users/UEs or related business customer needs [5]. With 5G, NFs can be individually instantiated for each network slice and placed where appropriate. In this way, multiple network slices can be created, each one composed of a collection of control plane and user plane NFs customised to the needs of the slice. For example, one network slice can include the NFs to support mobile broadband services with full mobility support, and another one to support non-mobile, latency-critical industry applications.

2.1.4 Support of multi-access edge computing (MEC)

MEC uses the wireless access network to provide services and cloud computing functions required by telecom users, and to construct a carrier class service environment with high performance, low latency and high bandwidth to improve the communication experience of mobile users.

Edge computing is an evolution of cloud computing that brings application hosting from centralised datacentres down to the network edge, close to the consumers and the data generated by applications. The main advantages are the computation offloading, distributed content delivery and caching, and low latency services.

In order to profit from the advantages provided by edge computing in 5G, the technology needs to support connecting the 5G core to a local area data network (LADN) where the applications are implemented and the UPF must be able to perform the local routing of certain traffic to the LADN.

In terms of physical deployment of MEC hosts, there are multiple options available based on various operational, performance or security related requirements. The following list gives an outline of some of the feasible options for the physical location of MEC:

1. MEC and the local UPF collocated with the base station,
2. MEC collocated with a transmission node, possibly with a local UPF,
3. MEC and the local UPF collocated with a network aggregation point,
4. MEC collocated with the core network functions (i.e. in the same datacentre).

The options presented above show that MEC can be flexibly deployed in different locations from near the base station to the central data network. Common for all deployments is the UPF which is deployed and used to steer the traffic towards the targeted MEC applications and towards the network.

2.2 NFV ARCHITECTURE

The virtualisation of network elements, NFV, is a concept that virtualises the main elements of a network. In this sense, instead of having a dedicated hardware element to provide a function of the network, software running on general hardware is used. In this way, entire classes of network node functions can be set up as building blocks that can be connected to create overall telecommunications networks. Examples of the virtualised functions that can be provided include virtualised load balancers, firewalls, intrusion detection devices, WAN accelerators, routers, access control and billing.

As a standard specification, ETSI focuses on high-level architecture, development guidelines, and interoperability enabled by open interfaces. ETSI describes the high-level NFV functional architectural framework and the design of virtualised network functions and of the supporting infrastructure. It identifies three main working domains in NFV:

1. Virtualised network function is the software implementation of a network function which can run over the NFVI.
2. NFV infrastructure (NFVI) includes the diversity of physical resources and how these can be virtualised. NFVI supports the execution of the VNFs.
3. NFV management and orchestration (MANO) covers the orchestration and lifecycle management of physical and/or software resources that support the virtualisation of the infrastructure, and the lifecycle management of VNFs.

The initial release of the ETSI NFV specification was predominantly dependent on hypervisor-based virtual machines (VMs) for virtualisation. Most of the specifications in ETSI NFV continue serving that purpose when being applied to the cloud native NFV. Nevertheless, an adaption is needed in some areas because of the differences between the VM based and cloud native solutions. Thus, the ETSI NFV group has published containerised VNF specifications enabling containerised VNFs to be managed in an NFV framework.

The ETSI NFV group has published ETSI GS NFV-IFA 040[9], which specifies the requirements for service interfaces and is an object model for operating system (OS) container management and orchestration. These specifications provide a baseline for the integration of OS container management and orchestration into the NFV framework.

ETSI GS NFV-IFA 040 also specifies requirements on the list of services to be offered by architectural elements providing the Container Infrastructure Service Management (CISM) and Container Image Registry (CIR) functions described in ETSI GR NFV-IFA 029[10] and on the interfaces for exposing these services to NFV-MANO and other consuming entities.

The CISM is responsible for maintaining the containerised workloads and manages the OS container, computation storage, network resources and their configuration. The CIR is responsible for storing and maintaining information on OS container software images.

ETSI GS NFV-IFA 040 is supplemented by the NFV Release 4 specifications ETSI GS NFV-IFA 010[11] and ETSI GS NFV-IFA 011[12]. These provide enhancements for the specification of the management and orchestration functional requirements, and extensions to the VNF package and VNF descriptor specifications respectively.

The considerably high level NFV architecture for 5G is in line with the ETSI NFV reference architecture [7], the NFV-MANO architectural framework [8], the ETSI NFV Adaptation to the Cloud Native Architecture [9] [10], and the ENISA 5G threat landscape [6] (section 3.7) (Figure 5). Table 2 describes the main NFV [7] and MANO [8] components of this architecture. In Figure 5, the main NFV components covering both VM-based and cloud native (container based) are highlighted.

In this report, it is assumed that the VIM supports the CISM to be able to manage both VMs and containers virtualisation technologies. As explained in ETSI GR NFV-IFA 029, there are multiple options to integrate the CISM within the NFV MANO. Only option #1 (CISM embedded in the VIM) is highlighted for reasons of simplicity since the aim is to give a big picture of the NFV

[9] https://docbox.etsi.org/isg/nfv/open/Publications_pdf/Specs-Reports/NFV-IFA%20040v4.2.1%20-%20GS%20-%20OS%20Container%20MANO%20service%20interfaces.pdf
[10] https://www.etsi.org/deliver/etsi_gr/NFV-IFA/001_099/029/03.03.01_60/gr_NFV-IFA029v030301p.pdf
[11] https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/010/04.01.01_60/gs_NFV-IFA010v040101p.pdf
[12] https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/011/04.02.01_60/gs_NFV-IFA011v040201p.pdf

architecture without going into the details of all these options already explained in ETSI GR NFV-IFA 029.

More details about the 5G NFV architecture can be found in [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16]. More details about the different MANO solutions are given in Annexes H and I.

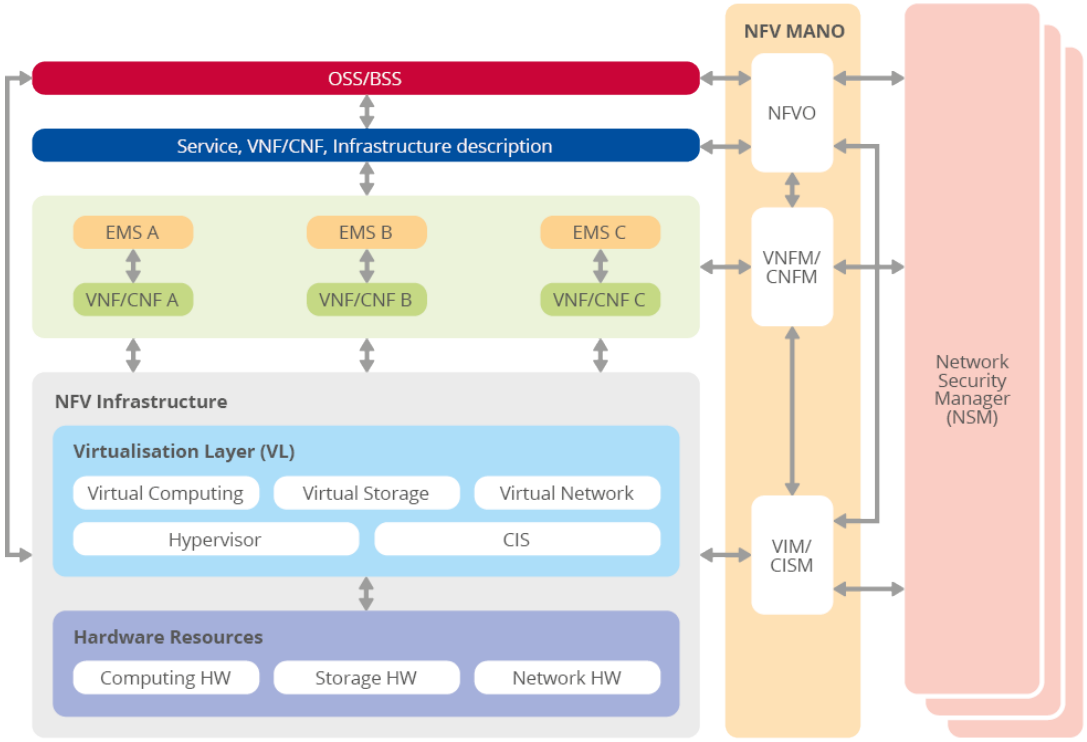


Table 2: NFV and MANO main components

Security-related Network Function	Description
NFV (Network Functions Virtualisation)	
Common components between VM-based and cloud native NFV (network functions virtualisation)	• **NFV Infrastructure (NFVI)**: The NFVI consists of all the hardware and software components that are contained within the environment in which VNFs are deployed. It provides virtualised computing, storage, and networking. One of the advantages of NFV is that the NFV-Infrastructure can be located across several physical locations, allowing operators to typically place their centres at the most convenient locations. The network providing connectivity between these locations is part of the NFV-Infrastructure. • **Operations Support System/Business Support System (OSS/BSS):** includes the collection of applications that a service provider uses to operate its business. While OSS deals with network management, fault management, configuration management and service management, BSS deals with customer management, product management, order management and billing. • **Element Management System (EMS)**: is responsible for the configuration, fault management, accounting and collection of performance measurement results for the network functions provided by the VNF. An example of management function is fault, configuration, accounting, performance and security management (FCAPS). • **Hardware Resources**: in NFV, the physical hardware resources include computing, storage and networks that provide processing, storage and connectivity to VNFs through the virtualisation layer (Host OS, Hypervisor, CIS). • **Virtualised Network Function (VNF):** an implementation of an NF that can be deployed on a network function virtualisation infrastructure (NFVI). VNFs are built from one or more VNF components (VNFC) and, in most cases, the VNFC is hosted on a single VM or container.

Security-related Network Function	Description
	• **Virtualised Network Function Component (VNFC):** is an internal component of a VNF that provides a VNF provider with a defined sub-set of that VNF's functionality. Its main characteristic is that a single instance of this component maps 1:1 against a single instance of an atomic deployable unit. An instance of an atomic deployable unit is represented by a single VM for hypervisor-based virtualisation or represented by one or a set of OS containers for CIS (Container Infrastructure Service) based virtualisation. • **Virtualisation layer:** it consists of two sub layers: a host OS and hypervisor (for VMs) and CIS (for containers).
Cloud native components within NFV	• **Container Infrastructure Service (CIS):** the cloud-native equivalent of hypervisor is container infrastructure service (CIS), which provides all the runtime infrastructural dependencies for one or more container virtualisation technologies. It can run on top of a bare metal or hypervisor-based virtualisation. It is used to create, destroy and manage containers on top of an operating system. • **Container:** is a virtualisation container using a shared operating system (OS) kernel of its host. Containers can host a VNF component (VNFC) for instance.
VM-based components within NFV	• **Hypervisor:** is a piece of software which partitions the underlying physical resources and creates virtual machines, and isolates the VMs from each other. It is running either directly on top of the hardware (bare metal hypervisor type 1) or running on top of a hosting operating system (hosted hypervisor type 2). The abstraction of resources comprises all those entities inside a computer or server which are accessible, such as processor, memory/storage, NICs. The hypervisor enables the portability of VMs to different Hardware. • **Virtual Machine (VM):** has all the ingredients (processor, memory/storage, interfaces/ports) of a physical computer or server and is generated by a hypervisor, which partitions the underlying physical resources and allocates them to VMs. Virtual machines can host a VNF component (VNFC) for instance.
NFV MANO (Management and Orchestration)	

Common components between VM-based and cloud native NFV MANO	• **Network Function Virtualisation Orchestrator (NFVO):** is responsible for coordinating the VNFM and VIM according to the requirements of the OSS/BSS to orchestrate a specific service such as a firewall or to detect intrusions. It implements resource and service orchestration in the network. NFVO is split up into resource orchestrator (RO) and network service orchestrator (NSO).
	• First, RO collects the current information regarding possible physical and virtual resources of NFVI through the VIM. Second, NSO applies a complete lifecycle management of multiple network services. In this way, NFVO keeps updating the information about the available VNFs running on top of NFVI. As a result, NFVO can initiate multiple network services. As part of the lifecycle management, NFVO can also terminate a network service whenever a service request is no longer being received for that specific service.
	• In several solutions, NFVO and VNFM are integrated into MANO. Open Source MANO (OSM)[13], Open Networking Automation Platform (ONAP)[14], OpenBaton[15], Cloudify[16], SONATA[17], and Katana Slice Manager[18] are considered as the leading integrated solutions for MANO. Note that OSM can also perform management and orchestration tasks on PNFs.
	• **VNF Manager (VNFM):** is responsible for managing the lifecycle of VNFs. VNFM operations include:
	  ○ instantiation of VNFs
	  ○ scaling of VNFs
	  ○ updating and/or upgrading
	  ○ VNFs Termination of VNFs.

VM-based components within NFV MANO	• **Virtual Infrastructure Manager (VIM):** is the management system for NFVI. It is responsible for controlling and managing the interaction of a VNF with the underlying computing, storage and networking resources and their virtualisation. It performs resource management tasks such as inventory of hypervisors, allocation of VMs onto hypervisors or increasing resources to VMs. Moreover, it performs operations on the visibility of the NFVI, analysis of data on the performance of the

[13] Open Source MANO (OSM), "OSM Open Source NFV Management and Orchestration (MANO) software stack aligned with ETSI NFV," April 2021, https://osm.etsi.org
[14] ONAP, "ONAP Open Networking Automation Platform," April 2021, https://www.onap.org/
[15] OpenBaton, "OpenBaton An extensible and customizable NFV MANO-compliant framework," April 2021, http://openbaton.org
[16] Cloudify, "Cloudify Multi Cloud Orchestration," April 2021, https://cloudify.co/
[17] SONATA, "Sonata agile development. testing and orchestration of services in 5g virtualized networks," April 2021, https://www.sonata-nfv.eu
[18] Katana Wiki Home, "MediaNetworks Laboratory," April 2021, https://github.com/medianetlab/katana-slice_manager/wiki

Security-related Network Function	Description
	infrastructure and collection of information for capacity planning, monitoring and optimisation. Consequently, VIM can supervise the allocation of NFVI resources to the available VNFs. OpenStack[19] and OpenVIM[20] (for VNFs) are possible solutions for VIM.
Cloud native components within NFV MANO	• **Container Infrastructure Service Management (CISM):** is a functional block that manages one or more container infrastructure services. The CISM provides mechanisms for lifecycle management of the managed container infrastructure objects, which are hosting application components as services or functions. It is a cloud-native equivalent of virtualised infrastructure manager (VIM). • CISM is responsible for controlling and managing the NFVI compute, storage and network resources, as well as scheduling the microservice containers in the cloud. CISM also collects performance measurements in the infrastructure including container level and makes the data available for other functional blocks for monitoring purposes. Other responsibilities of CISM include virtual networking control and management, as well as the southbound integration with various network controllers to achieve the physical network control and management capabilities. • Kubernetes[21] (for cloud native NFs) is a possible solution for CISM. Multiple options can be envisioned for mapping the CISM functionality to NFV-MANO as outlined in ETSI GR NFV-IFA 029 and ETSI GS NFV-IFA 040. Each option has it is pros and cons. Such options include: o Option#1: CISM embedded in the VIM, o Option#2: CISM distributed across VNFM and VIM, o Option#3: CISM as a stand-alone functional block, o Option#4: CISM-only replacing VIM and VNFM, o Option#5: CISM embedded into VNF with support for shared container service, o Option#6: CISM embedded into VNF without support for shared container service.
Other	
NFV Security Managers (SM)	NFV SM is a function that applies security policy to a virtualised network based on both predefined default policy and active analysis of information provided through security monitoring. It is responsible for enforcing security policy for VNFs and for instructing NFV-MANO to take VNF specific or system wide security actions [17], [18]. The security manager is a logical subcomponent of a CSP's overall network security management and monitoring systems. A CSP security management platform may require one or more security managers (SMs) depending on the security isolation and role separation required between different trust domains. In cooperation with MANO blocks dedicated to managing the virtualised network, the policy driven SM is specialised to manage the security on a network service over its entire lifecycle. It covers the following functionalities: • Security Policy Planning designs and optimises security policies for specific targets of protection (e.g. network services); • Security Policy Enforcement & Validation automates the deployment and supports the lifecycle management of security functions as defined in the design phase, then configures security policies on the security functions. In addition, during the lifetime of a network service, the validation and re-configuration or remediation of associated security policies is supported, also in an automated manner.

2.3 NFV WITH SDN ROLES

Besides the NFV technology, management and deployment of 5G technology is simplified by the adoption of complementary technologies enabling flexible usage of deployed hardware and fast provisioning of new functions and services, namely the SDN.

The core similarity between software-defined networking (SDN) and network functions virtualisation (NFV) is that they both use network abstraction. SDN seeks to separate network control functions from network forwarding functions, while NFV seeks to abstract network forwarding and other networking functions from the hardware on which it runs.

[19] OpenStack, "OpenStack The Most Widely Deployed Open Source Cloud Software in the World," April 2021, https://www.openstack.org/
[20] OpenVIM, "Telefónica NFV reference lab," April 2021, https://github.com/nfvlabs/openvim
[21] Kubernetes, "Kubernetes Production-Grade Container Orchestration," April 2021, https://kubernetes.io

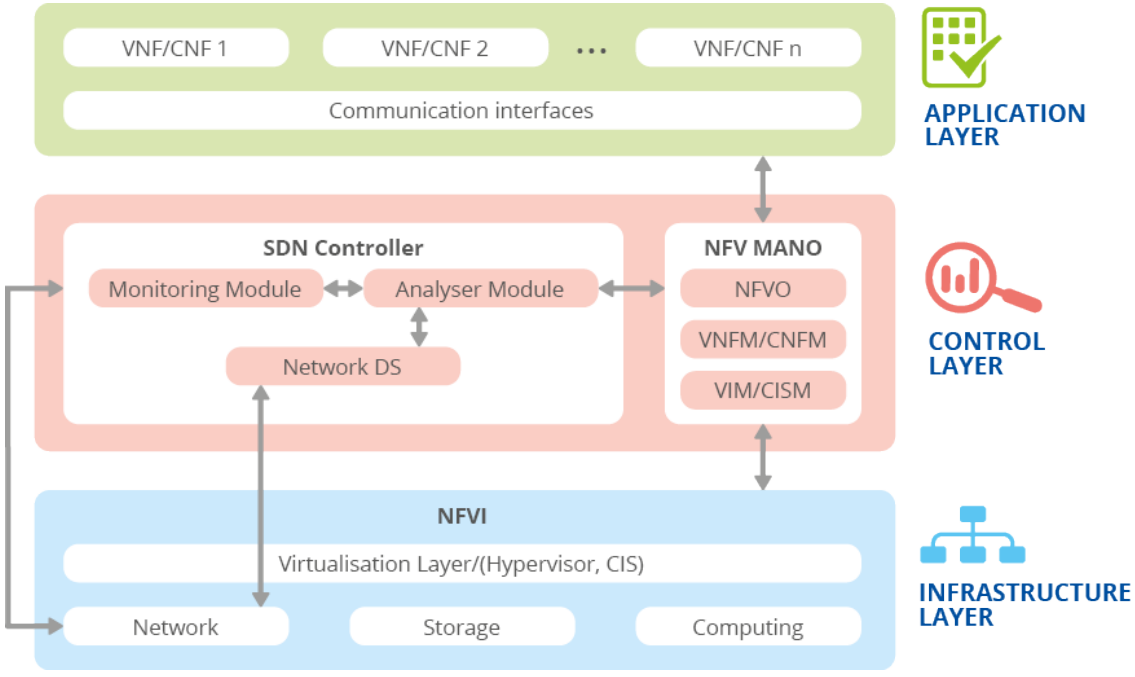
Thus, both depend heavily on virtualisation to enable network design and infrastructure to be abstracted in software and then implemented by underlying software across hardware platforms and devices [19].

When SDN executes on an NFV infrastructure, SDN forwards data packets from one network device to another. At the same time, SDN's networking control functions for routing, policy definition and applications run in a VM or container somewhere on the network. Thus, NFV provides basic networking functions, while SDN controls and orchestrates them for specific uses. SDN further allows configuration and behaviour to be programmatically defined and modified [19].

SDN and NFV differ in how they separate functions and abstract resources. SDN abstracts physical networking resources – switches, routers and so on – and moves decision making to a virtual network control plane. In this approach, the control plane decides where to send traffic, while the hardware continues to direct and handle the traffic. NFV aims to virtualise all physical network resources beneath a hypervisor, which allows the network to grow without the addition of more devices [19]. While both SDN and NFV make networking architectures more flexible and dynamic, they perform different roles in defining those architectures and the infrastructure they support [19].

A whole overview of the NFV/SDN architecture is shown Figure 6. This architecture takes into account SDN and NFV technologies. On one hand, the framework presents a layered structure: infrastructure, control and application layers, in the same way as SDN architecture. Moreover, it takes advantage of the NFV concept to allow the easy implementation and management of network functions, without the need to increase the hardware devices [20], [21].

Figure 6: Integrating SDN Controller into the reference NFV architecture



The SDN controller centralises the control plane functionalities and provides an abstract view of all the connectivity-related components it manages. The SDN Controller sets up and manages the underlying networking resources to provide the required connectivity for communicating the VNFs. Managed by the VIM, this controller may change infrastructure behaviour on-demand according to VIM specifications, adapted from the requests of tenants.

In the infrastructure layer, we have the current mobile infrastructure of the network operator providing support to a wide range of wireless and cellular technologies such as WiFi, LTE, UTMS, GSM, among others. On top of the hardware layer, there is a virtualisation layer to enable the virtualisation of hardware devices. The resources could be in different locations and datacentres and this takes three components into account:

- networking: these devices incorporate mobile technologies and OpenFlow protocol;
- storage: this element can include object storage or block storage (Swift and Cinder OpenStack) or another novel technique;
- computing: this includes high volume servers.

The control layer is in charge of monitoring, analysis, management and orchestration of devices. It consists of four modules: monitoring, analyser, network OS and NFV MANO.

- Monitoring Module: this module is able to provide the complete low-level overview of the managed systems by means of gathering metrics coming from different network devices.
- Analyser Module: this module could give a deep analysis of the data in order to determine the behaviour that suits the network. This module also can infer the recommended behaviour of the network. The techniques used in the analysis can include data mining, learning algorithms and pattern recognition, among others.
- Network OS: this uses the OpenFlow or similar protocols to send instructions to the infrastructure layer elements. Its functionality is similar to an operating system (OS) in computing.
- NFV MANO: this module determines and organises the actions to be executed in the system, the orchestration, the management of the resources and the control functions.

SDN/NFV control layer can adapt the network resources depending on the actual situation of the network and dynamically respond to failures or degradation of network performance. On the top of the architecture is located the application layer, which consists of two basic modules:

- Communication Interface: this module enables an open API for programmers to facilitate the development of new services.
- Network Functions: this module presents a scalable structure to create customised network functions or control applications.

2.4 5G NFV STAKEHOLDERS

Table 3 illustrates the actors that hold stakes in the 5G NFV markets, forming different clusters who would be active in 5G ecosystems.

First, the stakeholders from the traditional 5G industry are those who provide connectivity solutions, equipment, SW and cloud providers. They are the actors who take part in developing, delivering and providing 5G services. Second, policy makers and standard setting organisations have defined 5G as we know it today. Third, vertical industries are important stakeholders providing different services to third parties. [22], [23], [24], [25], [26] were used as references for the development of this chapter.

The 5G NFV network architecture implies the introduction of new processes, activities and operations thus defining new technical roles (e.g. administrators, integrators) and responsibilities involved in the operation, administration and maintenance of the 5G NFV. The operation, administration and maintenance of 5G NFV infrastructure requires much effort and particular skill profiles need to be employed. Listings of the roles, responsibilities and the corresponding technical processes and activities are provided in Annex A. Each role can belong to multiple stakeholders.

Table 3: 5G NFV stakeholders

5G stakeholders	Description
Mobile Network Operator (MNO)	The MNO operates its mobile network infrastructure to provide connectivity and network services to end-users.
Network Equipment Vendors	These vendors provide the network infrastructure including servers to run SDN controllers, switches, routers, gateways, radio hardware, etc. In addition, they are in charge of: • providing capability and procedures to securely configure the network device; • providing a process for users, including security researchers, to submit bug reports (e.g. using an issue tracker or a mailing list); • testing according to 3GPP test plans and this testing should include security tests of the device and its interfaces; • setting up a vulnerability management process of monitoring, identifying, evaluating, treating and reporting on security vulnerabilities in the network device including firmware; • maintenance of the firmware that includes providing patches for bugs and vulnerabilities.
NFs Vendors	They develop and provides NFs (e.g. VNF, PNF). In addition, they are in charge of: • providing capability and procedures to securely configure NFs; • providing a process for users, including security researchers, to submit bug reports (e.g. using an issue tracker or a mailing list); • testing according to 3GPP test plans and this testing should include security tests of NFs and its interfaces; • setting up a vulnerability management process for monitoring, identifying, evaluating, treating and reporting on security vulnerabilities; • maintenance of NFs that includes providing patches for bugs and vulnerabilities.
Virtualisation Hardware Infrastructure Providers	They provide the virtualised infrastructure comprising computing resources (e.g. from computing platforms) and storage nodes. In addition, they are in charge of: • setting up a vulnerability management process for monitoring, identifying, evaluating, treating and reporting on security vulnerabilities in the virtualisation hardware infrastructure; • setting up a patch development, testing and delivery processes; • maintenance of the hardware infrastructure that includes providing patches for bugs and vulnerabilities; • providing a process for users, including security researchers, to submit bug reports (e.g. using an issue tracker or a mailing list).
Vendors of Security Hardware Modules	They provide the security hardware technologies used within servers such as trusted platform modules (TPM), trusted execution environment (TEE), hardware security modules (HSM) and secure enclaves in CPUs. In addition, they are in charge of: • setting up a vulnerability management process for monitoring, identifying, evaluating, treating and reporting on security vulnerabilities; • setting up a patch development, testing and delivery processes; • maintenance that includes providing patches for bugs and vulnerabilities; • providing a process for users, including security researchers, to submit bug reports (e.g. using an issue tracker or a mailing list); • certification according to a recognised scheme such as Common Criteria[22].

[22] https://www.commoncriteriaportal.org

5G stakeholders	Description
Virtualisation Software Infrastructure Providers	They provide the virtualised infrastructure services that designs, builds, and operates virtualisation infrastructure(s). The infrastructure comprises software for compute nodes such as hypervisors, host operating systems and CISs. In addition, they are in charge of: • setting up a vulnerability management process for monitoring, identifying, evaluating, treating and reporting on security vulnerabilities in the virtualisation software infrastructure; • setting up a patch development, testing and delivery processes; • maintenance of the software infrastructure that includes providing patches for bugs and vulnerabilities; • providing a process for users, including security researchers, to submit bug reports (e.g. using an issue tracker or a mailing list).
Mobile Virtual Network Operators (MVNO)	MVNOs work with MNOs to offer their telecom services by acquiring the required network capacity for customers.
Cloud Providers	They provide computation and storage resources to third parties.
Over-The-Top (OTT) Content And Service Providers	These providers offer different applications and services to end users based on their demands and quality requirements.
Communications Service Providers (CSPs)	Communications Service Providers (CSPs) include service providers such as Mobile Network Operators (MNO) and Mobile Virtual Network Operators (MVNO).
Law Enforcement Organisations and Governmental Agencies	They should have access to control and sometimes intercept user data in 5G networks in the regulated framework of Lawful Interception.
Regulators and Policymakers	Government regulators or regulatory agencies include bodies such as the Federal Communications Commission (US), European Commission (EU), etc.
Standardisation Bodies	These include international associations, alliances with a geographical, thematic or sectorial focus, such as the International Telecommunication Union, GSMA, 3GPP, etc.
Vertical Markets	These provide various services to third parties that exploit resources (network and cloud) specifically from operators and cloud service providers.
End Users or Subscribers	These users have a subscription and can therefore access virtualised services. When they access a service, they directly or indirectly generate a data flow within the control plan, then the user plan. Their communications are transported by the user plan.

2.5 NFV SECURITY OPPORTUNITIES

Despite potential challenges due to the use of recent technologies such as NFV and SDN in 5G networks, these same technologies also open new opportunities. The main opportunities for NFV to improve the 5G security and trustworthiness are provided in Table 4 ([22], [27]).

Table 4: NFV security opportunities

NFV security opportunities	Description
Increased automation	This is provided by the management and orchestration (MANO) layer. NFV MANO provides the opportunity to automate the creation, reconfiguration and scaling in and out of network functions, and to do it in real time on the fly, based on workload needs. The automation feature provided by NFV MANO allows the security controls and mitigations to be automated. For instance, the logging of security events, monitoring, detection, prevention, verification of integrity, patch management and others can be instantiated and provided as a service to network functions and applications.
Security zoning and segmentation	In the 5G network, multi-tenancy drives the need for the logical separation of virtual resources among tenants. Through orchestration, certain VNFs can be deployed on separate VMs or containers and compute nodes, and they can be further segregated by using separate networks. In addition, the use of security zones allows VNFs to be deployed on or migrated to hosts that satisfy security-pertinent criteria such as location and level of hardening (for example, some hosts may employ the trusted computing technology).

NFV security opportunities	Description
Distributed security services	The NFV allows for the dynamic distribution not only of the instantiated VNFs throughout the virtualised infrastructure at the edge, at the core or at the RAN, but also for security. 5G network services are deployed across multiple administrative domains. NFV admins can instantiate new monitoring instances, reconfigure or modify the existing ones at the right location in the network according to available resources or security contexts.
Patch management	NFV eases the deployment of security updates. An upgraded instance of the VNF can be launched and tested while the previous instance remains active. Services and customers can then be migrated to the upgraded instance over a period of time (shorter or longer as dictated by operational needs). The older instance with the un-patched security flaw can be retired once the process is complete.
Incident response	NFV opens up the possibility to automate and improve the incident response. This automated incident response provides rapid and flexible re-configuration of virtual resources. In addition, it eases the decommissioning and re-commissioning of VNFs. If a VNF is compromised (for example, through unauthorised access via a back door), an uncompromised version can be instantiated to replace it and the compromised version can be decommissioned and a copy of it made for forensic analysis.
Programmability	Programmability offers the flexibility and dynamicity needed to have adaptable security mechanisms such as logging, policy monitoring, and verification mechanisms.
Centralised control and traffic steering	In SDN, forwarding elements are directly connected to and controlled by controller software (e.g. Ryu[23] or OpenDaylight[24]). This centralisation of the control plane enables a defence system to rapidly respond to network changes from a central controller through updating the forwarding rules of the entire network infrastructure, e.g. suspicious traffic can be dynamically detected and re-directed to security appliances.
Network slicing	Network slicing is released by virtualisation using SDN, NFV and cloud computing technologies. The E2E multi-domain and multi-tenancy support in 5G network slicing promises to enable vertical industries with a diverse set of performance, service and security requirements. Network slicing will give operators capabilities of creating different level of services for different verticals, enabling them to customise their operations.

2.6 NFV KEY TECHNOLOGIES

This section presents an overview on different virtualisation, containerisation and MANO technologies [28] currently being used in 5G to run and orchestrate multiple VNFs at the core, edge and RAN. It examines the differences between using virtual machines (VMs) vs containers vs unikernel vs cloud native microservices in the context of 5G.

2.6.1 Virtualisation

2.6.1.1 Hypervisor

Hypervisor-based virtualisation provides isolated environments on top of a shared pool of resources [29], [30]. Hypervisor is a software layer that abstracts the underlying physical resources and provides virtual machines with the full functionalities of a real system. Moreover, a hypervisor is responsible for resource allocation to the VM as well as being responsible for monitoring and managing VMs through coordination with the primary OS of the underlying hardware.

There are two types of hypervisors known as Type 1 and Type 2.

- **Based on Type I – Bare Metal Hypervisor:** a type 1 hypervisor runs directly on the host machine's physical hardware, and it's referred to as a bare-metal or native hypervisor. The type I hypervisor doesn't have to load an underlying OS. It does not need any host OS because the communication to hardware resources is direct with full visibility of hardware resources [30].
- **Based on Type II - Hosted Hypervisor:** a type 2 hypervisor is typically installed on top of an existing OS. It is sometimes called a hosted hypervisor because it relies on

[23] https://ryu-sdn.org
[24] https://www.opendaylight.org

the host machine's pre-existing OS to manage calls to CPU, memory, storage and network resources.

The bare-metal hypervisors (type I) are a more secure option. Unlike the hosted hypervisor, they do not depend on the underlying OS. Table 5 summarises the features of Type I and Type II hypervisors [31].

Table 5: Features of type I and type II hypervisors

Criteria	Type I	Type II
AKA	Bare metal	Hosted
Definition	Runs directly on server hardware	Runs on top of the supported OS
Scalability	Better scalability	Not so much, because of its reliance on the underlying OS
System independence	Has direct access to hardware along with VMs, its hosts	Is not allowed to directly access the host hardware and its resources
Performance	Provides better hardware resource utilisation	Provides less hardware resource utilisation.
Security	More secure as it is a hardware-based hypervisor	Less secure as it is a software-based hypervisor. Any problem in the OS may affect the entire system including the protected hypervisor.
Setup or installation	In many such hypervisors, setup is hard and hardware support is needed.	In many such hypervisors, setup is easy as there is already an OS.
Examples	VMware vSphere, Microsoft Hyper-V, KVM, Xen Hypervisor, Oracle VM, Citrix Hypervisor	Oracle VM VirtualBox, VMware Workstation Pro and VMware Fusion, QEMU, Parallels Desktop, KVM[25]

2.6.1.2 Virtual machines

A VM is a type of virtualisation that splits bare metal servers into multiple independent instances with separate operating systems inside. The operating system, applications and services are all bundled into a single image that is accessed via a hypervisor, built on virtualised hardware.

Such virtualisation allows us to move away from the approach of running one application or service per physical server and achieve better utilisation of capacity. The sizing of the VM will depend on the resources available and the characteristics of the application that is going to be executed on this machine. Within the VM, it is possible to run different OS depending on the necessities or requirements of the application running on top of it.

A VM consists of several files that are stored on a storage device. The key files are the configuration file, virtual disk file, NVRAM setting file and log file [28]. Some of the most interesting functions that VMs enable are Snapshots[26], Migration[27] and Failover[28] [32].

2.6.2 Cloud native

[25] Kernel-based Virtual Machine (KVM) has qualities of both a hosted and a bare-metal virtualisation hypervisor. It can turn the Linux kernel itself into a hypervisor so the VMs have direct access to the physical hardware.
[26] Snapshots: A snapshot is a state of a VM, and generally its storage devices, at an exact point in time. A snapshot enables the VM's state at the time of the snapshot to be restored later, effectively undoing any changes that occurred afterwards. This capability is useful as a backup technique, for example, prior to performing a risky operation.
[27] Migration: The snapshots can be moved to another host machine with its own hypervisor; when the VM is temporarily stopped, snapshotted, moved, and then resumed on the new host, this is known as migration. If the older snapshots are kept in synchronisation regularly, this operation can be quite fast, and allow the VM to provide uninterrupted service while its prior physical host is, for example, taken down for physical maintenance.
[28] Failover: Similar to the migration mechanism, failover allows the VM to continue operations if the host fails. Generally, it occurs if the migration has stopped working. However, in this case, the VM continues operation from the last-known coherent state, rather than the current state, based on whatever materials the backup server was last provided with.

Cloud-native is an approach to building and running applications that fully exploits the benefits of the cloud computing model. Applications are cloud-native network functions. 5G NFs, as a cloud native NF, is designed using the following important cloud-native principles.

2.6.2.1 Containerisation

OS-level virtualisation represents the containerisation model, which envisages that only the applications and their dependencies are integrated into a container. Each container shares the host OS kernel operating on bare metal, as well as its binaries and libraries so the applications run quickly and reliably from one computing environment to another[29].

As a result, containers are exceptionally lightweight and fast to start. Containers allow for more efficient implementation of microservices principles due to their elasticity and ease of provisioning. Containers are more commonly adopted by cloud-native applications, as each service component becomes a separate element in a microservices architecture.

Many types of containerisation technologies are available, for instance:

- **Docker containers:** this is a popular open-source project based on Linux containers. Docker is written in GO and developed by Dotcloud. Docker is basically a container engine (ETSI CIS) which uses the Linux kernel features like namespaces and control groups to create containers on top of an operating system and automates application deployment on the container.
- **Java containers**: these types of software packages enable standalone functioning of Java applications or parts of them. Examples: Springboot, Jetty, Tomcat.
- **LXD containers**: represent Linux containers software technology that is very similar to various Linux distributions. These are integrated with the OpenNebula EDGE platform.
- **OpenVZ containers**[30]: Open Virtuozzo is a dedicated container-based virtualisation technology specially created for Linux operating systems.
- **RKT containers**: rocket containers and RKT container engine were developed by CoreOS for the majority of Linux distributions in a cloud-native environment. This type of container is composed of a pod (like in the Kubernetes model and concept) with one or more applications inside.
- **Hyper-V containers**: they constitute a different type of container because they create their own copy of the Windows OS kernel and are completely isolated, having incorporated both kernel space and user modes. They can be easily associated with a VM.

2.6.2.2 Microservices

A 5G NF, as a cloud native NF, is composed of cloud-native network functions components that combine to enable 5G-specific features. The basic components of a cloud native NF are microservices, which can be executed independently in separate containers, be deployed independently, and be re-composed when creating a new cloud native NF. These microservice-based cloud native NFs are highly scalable and can enable the deployment of new features quickly.

A microservices architecture develops a single application as a suite of small services, each of which run their own process and communicate with lightweight mechanisms. Applications designed from the beginning as a microservice may have the innovation needed for the new telecom service environment.

The microservices architecture requires a high degree of orchestration. Moreover, consideration must be given to whether decomposing into a microservice can actually be counterproductive.

[29] https://www.docker.com/resources/what-container
[30] https://openvz.org/

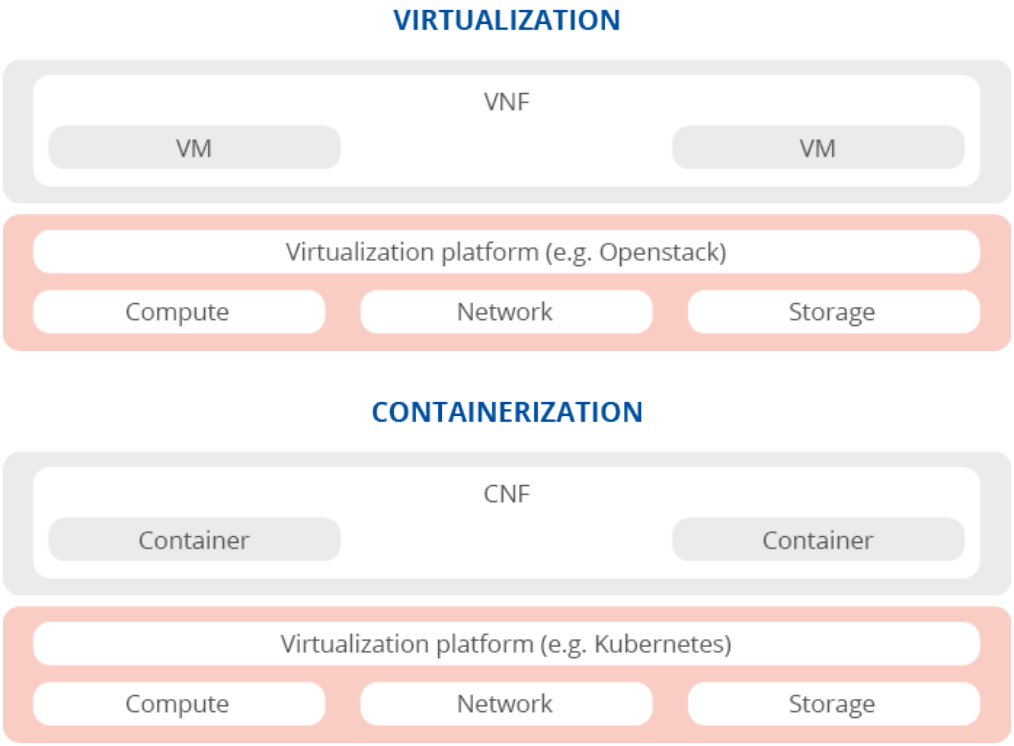
Because microservicing supports cloud-native architecture, it can create problems with latency, which is the death knell for 5G applications and services.

While mobile operators stand to benefit tremendously from fully deployed 5G networks, the reality is that there are a number of foundational issues that must be addressed to ensure those networks provide the speed, latency and reliability that 5G applications demand.

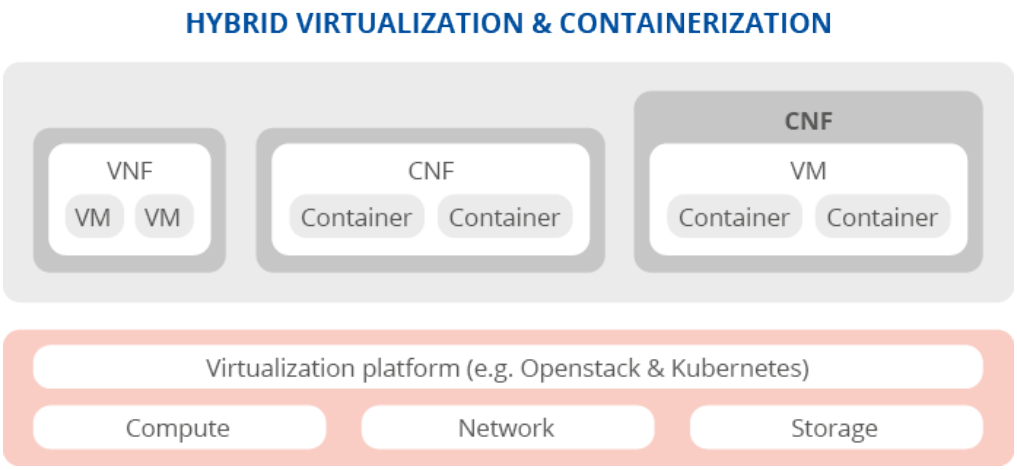
As is generally true in technology, a hybrid approach to developing VM, container and microservices technologies is likely the best pragmatic path forward for operators[31]. By combining the main principles 'containerisation' and 'microservices' operators can build a 5G network with cloud-native network functions.

2.6.3 Hybrid virtualisation and containerisation

With the development of cloud native technology, the telco infrastructure is on a path to leveraging the container-based architecture. But until then, solutions will incorporate a mixture of VMs and containers. In virtualised legacy networks like the EPC and 5G Non-Standalone (NSA) core, network functions that create real-time services and manage the user plane traffic typically run on VMs, which is appropriate for supporting services that do not have strict latency requirements or network configurations. Meanwhile, operators use containers for broadband services that need scalability or services that are not susceptible to failures. Therefore, to support interworking with existing networks, the 5G network requires virtualisation and cloud native technology that can support both VMs and containers at the same time. Typical VMs, containers and hybrid architectures are depicted in Figure 7.



[31] https://www.rcrwireless.com/20190411/5g/cloud-native-5g-reader-forum



2.6.4 Unikernels

Unikernel is an alternative to both VMs and containers for lightweight virtualisation of resources. It can embed only one application and a limited set of its dependencies which, differently from containers, also includes the libraries for hardware resource management [33]. It emerged due to the idea that the majority of the functions running either in the cloud or at the edge do not require many of the services inherent to OSs, and thus those services can be excluded.

Unikernels are single-purpose appliances that are specialised at compile time into standalone kernels[32]. They are constructed with the minimal necessary libraries, modularly, compiled together with the application code into an image (no division between kernel and user spaces) that can be run on top of a hypervisor or directly on a hardware layer. Different library OSs (e.g. IncludeOS, UKL, MirageOS, OSv, Rumprun, runtime.js) can be used to develop unikernels, with slightly different security profiles, programming languages (some of them aiming to avoid programming directly in C), and legacy compatibility.

Among other advantages, unikernels improve security over other virtualisation paradigms since (i) they have no other functions or ports apart from the specific application they were built for, thus the attack surface is minimal, and (ii) they achieve a degree of isolation similar to VMs and much higher than containers, since the latter share a common kernel. Besides, due to their specialisation, unikernels come with the benefit of faster boot times and lower image sizes than containers, as well as a similar degree of memory consumption when running.

Still, unikernels have some drawbacks that come mainly from their immaturity. The most critical one is related to the high development times as (i) kernel functionalities have to be carefully selected and configured for the specific application, (ii) there is a lack of tools designed for debugging unikernels, and (iii) to be updated they have to be shut down, updated, recompiled and instantiated, a set of operations that is not possible to run on the fly.

The nature of unikernels[33] make them suitable for deploying stateless, high-response, low-latency VNFs located at Edge nodes. General algorithms (e.g. compression, encryption, data

[32] A. Madhavapeddy et al., 'Unikernels: Library Operating Systems for the Cloud', ACM SIGPLAN Notices, vol. 48, no. 4. 2013, pp. 461–72.
[33] http://unikernel.org/projects/

aggregation) and specific functions for vehicular edge computing (VEC), edge computing for smart cities and augmented reality (AR)[34] are use cases in which unikernels can be of utility.

The UNICORE project[35], which aims at providing a toolchain for facilitating the development of secure, portable, scalable, lightweight and high performance unikernels, foresees their potential application in 5G-RAN, vCPE and serverless computing, among other fields. As current virtualised infrastructure managers (VIMs) support unikernels, some H2020 5G-PPP projects (such as 5G-MEDIA[36], 5GCity[37], Superfluidity[38], 5G-Complete[39], etc.) are using them jointly with VMs and containers within their 5G deployments, being leveraged in tandem with conforming services thus benefiting from their respective advantages.

2.6.5 VMs vs containers vs unikernels

Operators have been deploying VNFs for several years to replace hardware-based appliances. Operators deploy network functions virtualisation (NFV) in one of three ways: on virtual machines (VMs) with hypervisors; in containers; or using a hybrid approach. VMs have their own operating system (OS), while containers share an OS. As such, containers are more efficient because they don't require multiple operating systems per host.

However, containers present several challenges for telecom-grade environments. The first challenge is that sharing the OS creates the potential for applications and their containers to interfere with each other or create resource contention. For mobile operators in particular, this approach creates difficulties in both the control and data planes for a 5G environment, where latency, efficiency, security and a high level of distribution are needed.

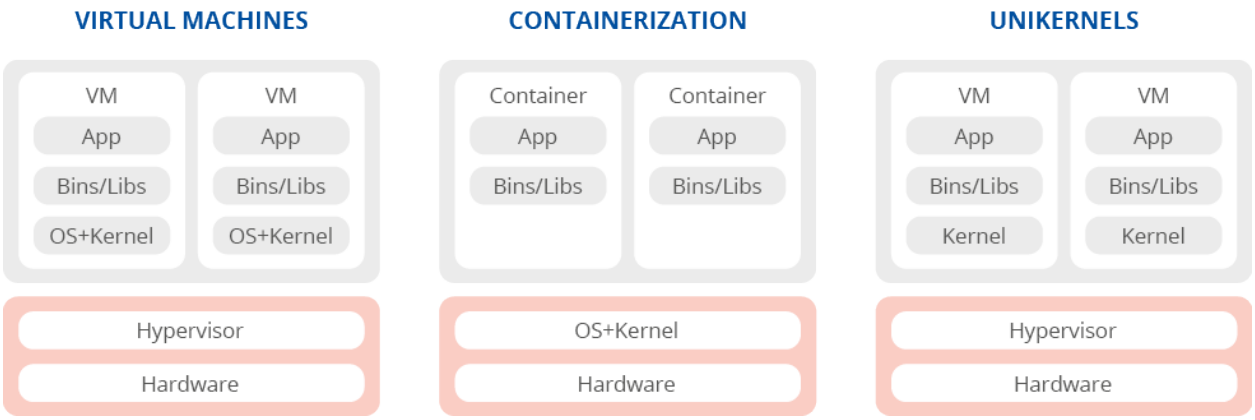
Unikernels, as a third option, primarily target the drawbacks of legacy VMs by compressing the kernel and shared libraries to the bare minimum while maintaining compatibility with the traditional cloud virtualisation stacks (hypervisors, controllers, MANO). Differently from containers, which have a shared kernel, each unikernel has its own kernel. This allows better isolation than containers. Table 6 provides a comparison of virtualisation technologies. In addition, Figure 8 illustrates the main differences between the architecture of VMs, containers and unikernels [33].

Table 6: Virtualisation technologies comparison

Feature	Virtual Machines	Containers	Unikernels
Isolation	Strong	Weak	Strong
Image size	Large	Small	Small
Instantiation (boot time)	Slow	Fast	Fast
Memory consumption (resource overhead)	High	Low	Medium
Toolset	Strong	Strong	Weak

Figure 8: Comparison of the architecture of VMs, containers and unikernels

[34] R. Morabito, V. Cozzolino, A. Y. Ding, N. Beijar and J. Ott, "Consolidate IoT EDGE Computing with Lightweight Virtualization," in IEEE Network, vol. 32, no. 1, pp. 102-111, Jan.-Feb. 2018.
[35] http://unicore-project.eu
[36] http://www.5gmedia.eu
[37] https://www.5gcity.eu
[38] http://superfluidity.eu
[39] https://5gcomplete.eu



2.7 NFV DEPLOYMENT MODELS

In a virtualised environment the underlying hardware, as well as the virtual dynamic network where the NFVs reside, may be shared by multiple tenants and there are a number of different deployment scenarios with varying risks. Such shared resources may expose security risks on several different levels and the severity of the risk may depend on the nature of such tenants. Below are the main NFV deployment models with varying risks that may be considered in a virtualised environment. Main references used to develop this section are: [32], [23], [34], [35].

2.7.1 Single operator environment

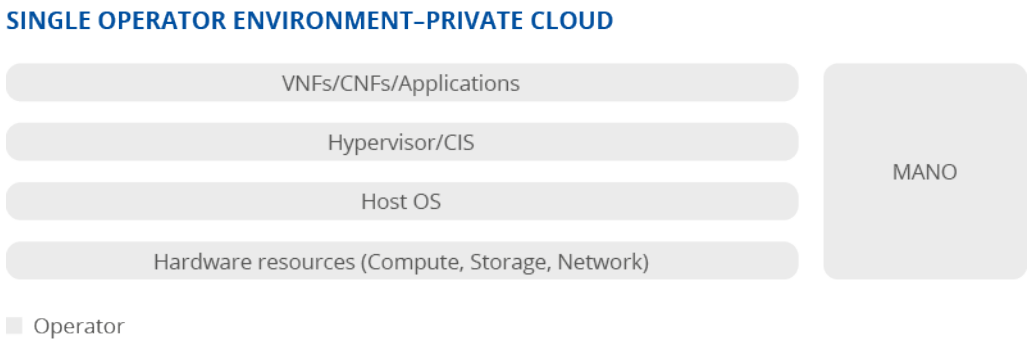
The same operator owns, operates and controls completely the VNFs, the virtualisation layer and the hardware and the premises in which they are located (see Figure 9). In this model, the operator is only exposed to its own network elements and functions. In this model, the operator must cater for most of the risks, since it has to implement security measures to protect the different layer of NFV including VNFs, virtual resources, and physical infrastructure.

The operator must also implement robust Identity, credential and access management policies to protect its assets and prevent attacks such as man-in-the-middle, whereby an attacker (e.g. a malicious or compromised tenant) can illegitimately access the offered service. Malicious insiders in the operator's system administration represent a further risk of compromising the operator's reputation and exposing security risks to the tenant, which may receive compromised services that may violate its data.

In this model, the tenant has no control over the infrastructure. Tenant data are stored within the operator infrastructure and, thus, it is of paramount importance that strong security measures necessary to protect these data are applied. Such measures include the prevention of data loss and strong isolation when data belonging to different tenants share the same server (or resources). Data breaches can also happen when a malicious tenant violates someone's data.

With this model, consumers usually access the services offered through web browsers, thus the operator must not overlook vulnerabilities in the software offered and in the protocols used (e.g. HTTP) in order to protect its network from attacks. A typical category of attack is the abuse and nefarious use of services performed, for example, by a consumer who executes a malware injection or DoS attack on the operator's server, profiting from the services offered.

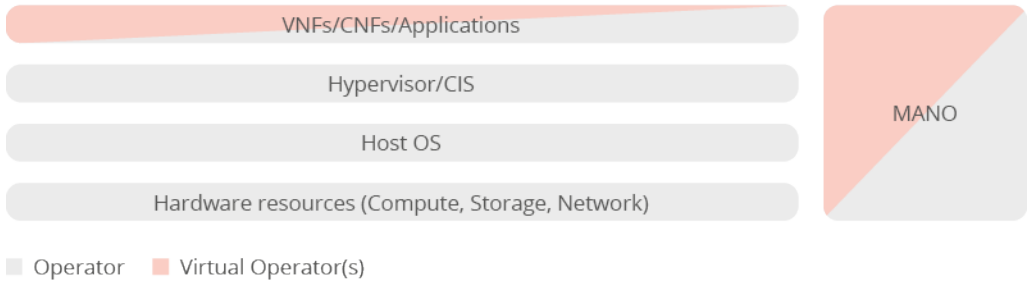
Figure 9: Single operator environment model



2.7.2 Operator hosting virtual network operators

This is based on the single operator environment model. In this model, the network operator hosts other virtual network operators within the same facility. It would probably isolate each virtual operator on separate hardware. However, in theory, the VMs or containers of different virtual network operators could run alongside each other over the same virtualisation layer (see Figure 10). In this model, the operator is exposed to its own network elements and functions, as well as the network elements and functions of the other virtual operators.

Figure 10: Operator hosting virtual network operators model



2.7.3 Third party hosting

A third-party cloud provider operates the computer hardware, infrastructure network and the virtualisation layer on which VNFs are running. The premises, including cable chambers, patch panels, etc., are physically secured by the third-party cloud provider. There are three scenarios in this model (see Figure 11):

- scenario 1 – separate cloud for a single operator: in this scenario, the platform runs the VNFs of a single operator;
- scenario 2 – community cloud for multiple operators: in this scenario, the platform runs the VNFs of multiple operators;
- scenario 3 – public cloud for operators and other service providers: in this scenario, the platform runs operator's VNFs or other non-network related services.

In all scenarios, the operators are always accountable and responsible for the protection of VNFs and data. In all scenarios, the operator is exposed to its own network elements and functions as well as to the third-party hosting service that may not be accountable and that may be able to transparently gather information emitted from the network infrastructure.

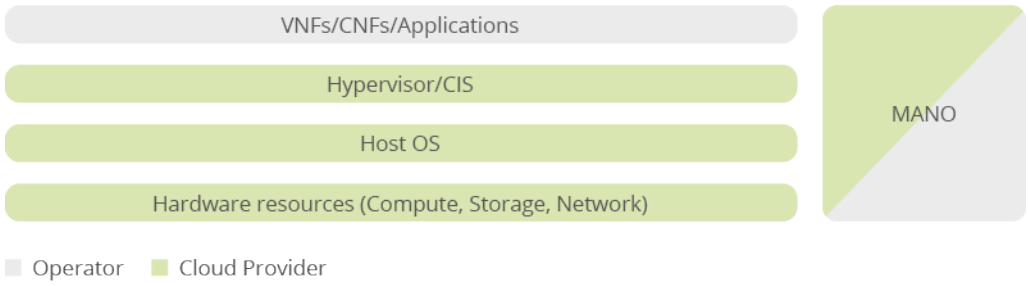
In scenario 2, the operator may also be exposed to network traffic from other operators. In scenario 3, the operator may also be exposed to network traffic from other operators as well as

traffic from other services that may have lesser security and/or integrity requirements than the operator.

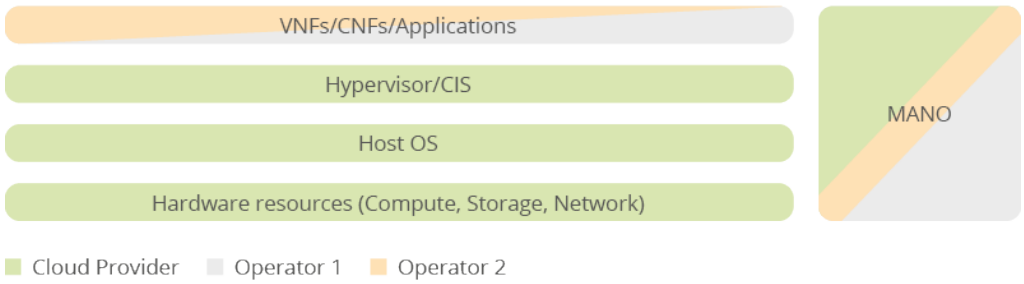
In this model, the operator must avoid software VNF vulnerabilities to prevent an attacker from making a nefarious use of services. For its part, the cloud provider must avoid software flaws in the operating system, in the virtual resources and servers offered to the operator(s) while guaranteeing them access to the platform through secure APIs to prevent malware Injections.

Due to weak isolation among resources of the platform assigned to different VNFs belonging to diverse operators or to the non-network services of other service providers, attacks such as side channel or VM or container data theft may occur. At the same time, applications or non-network related services from other service providers that are not necessarily all trusted may run on the same platform in different VMs or containers, so the operator can be damaged by an attacker that manages to exploit a lack of isolation between a vulnerable VM or container and other VMs or containers or the host machine, thus having illegitimate access to other VNFs belonging to other operators or the cloud provider's platform.

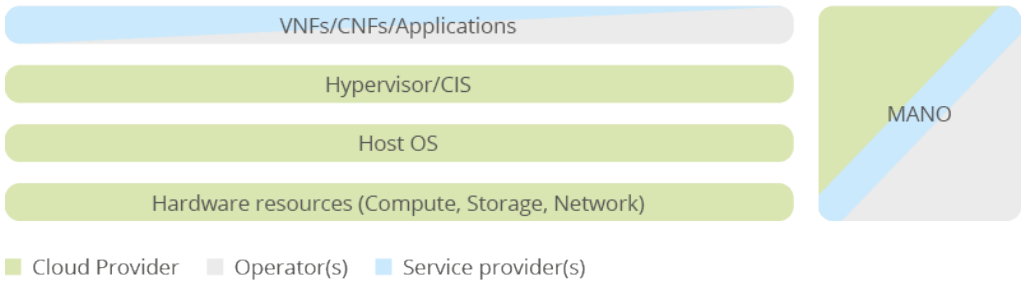
THIRD PARTY HOSTING SCENARIO 1–HYBRID CLOUD



THIRD PARTY HOSTING SCENARIO 2–COMMUNITY CLOUD



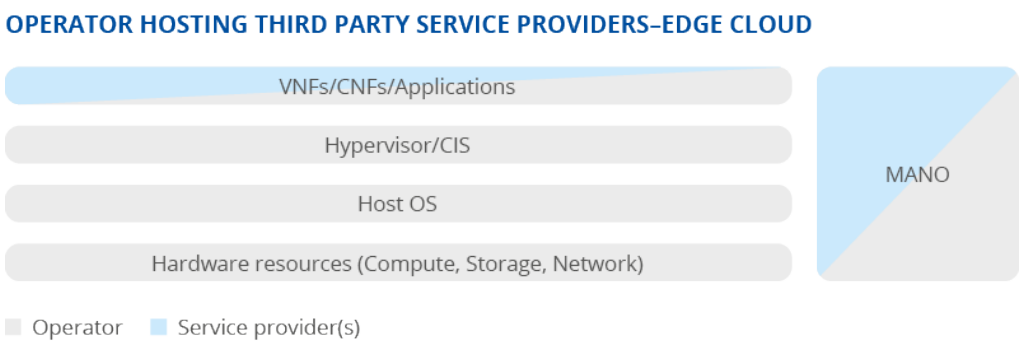
THIRD PARTY HOSTING SCENARIO 3–PUBLIC CLOUD



2.7.4 Operator hosting third party service providers

In this model, the operator leaves to the service provider the task of deploying its own applications, thus executing arbitrary software on the operator infrastructure (see Figure 12). In this case the operator is in charge of protecting its assets, which include data and servers underlying virtual resources offered as MEC services.

For the operator, potential threats can be caused in the following situations: (i) elevated privileges are given to a service provider on storage access (data breach risks), (ii) the service provider is able to control the infrastructure offered by the operator through insecure APIs (insecure APIs risks) and execute arbitrary code (higher risk of hijacking of the elements of the infrastructure by malicious service providers), and (iii) a service provider could run malicious code through the operating system of its VM, thus penetrating the operator's infrastructure, or could, intentionally or accidentally, fail in updating its VM, thus exposing it to attacks.



2.7.5 Summary

The different deployment models described above are summarised in Table 7. It shows the actor(s) involved on the management and operation at each layer of the NFV system for each deployment model. The column 'Location' states the location where the infrastructure is deployed. The column 'Cloud Type' identifies which NFV deployment scenarios are similar to the common deployment models used in cloud computing. The right-most column 'Suitable for' also provides the suitability of each deployment model for the core, MEC and/or RAN.

Table 7: Virtualisation technologies comparison

Deployment model	Hardware	Virtualisation layer (Host OS, Hypervisor, CIS)	VNFs/Applications	MANO	Location	Cloud Type	Suitable for
Single operator environment	Operator	Operator	Operator	Operator	On premise	Private Cloud	Core
Operator hosting virtual network operators	Operator	Operator	Operator, Virtual Operator (s)	Operator, Virtual Operator (s)	On premise	Private Cloud	Core, MEC, RAN
Third party hosting – scenario 1	Cloud Provider	Cloud Provider	Operator	Cloud Provider, Operator	Vendor Locations	Hybrid Cloud	Core, MEC, RAN
Third party hosting – scenario 2	Cloud Provider	Cloud Provider	Operators	Cloud Provider, Operators	Vendor Locations	Community Cloud	MEC, RAN

Deployment model	Hardware	Virtualisation layer (Host OS, Hypervisor, CIS)	VNFs/Applications	MANO	Location	Cloud Type	Suitable for
Third party hosting – scenario 3	Cloud Provider	Cloud Provider	Operators, Service Providers	Cloud Provider, Operators, Service Providers	Vendor Locations	Public Cloud	MEC
Operator hosting third party service providers	Operator	Operator	Operator, Service Providers	Operator, Service Providers	On Premise	Edge Cloud	MEC

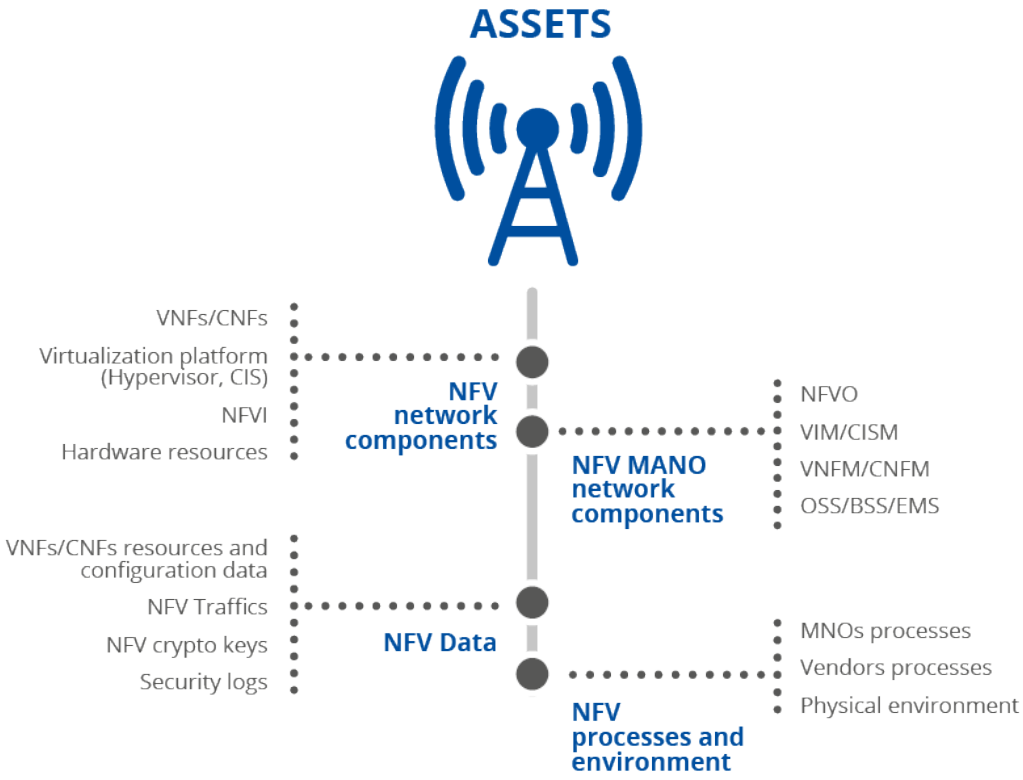
3. 5G NFV: ASSETS, CHALLENGES, VULNERABILITIES AND ATTACK SCENARIOS

In this chapter, we identify and describe 5G NFV assets, challenges, vulnerabilities and attack scenarios. This initial step will guide us to identify the best practices and provide recommendations.

3.1 ASSETS

To address NFV challenges in a 5G ecosystem, it is essential to identify the assets of such a complex ecosystem. The main asset categories introduced in this report are inspired from the ENISA Threat Landscape for 5G Networks [6] (December 2020), [36] (November 2019) and derived from the 5G NFV architecture described at the beginning of this report. These main categories include components and entities from network products, management and orchestration, data, processes and environment. A complete diagram of the asset mind maps is present in Annex B.

Figure 13: 5G NFV asset categories



An assessment of the asset categories in maintaining security-related protection properties in terms of CIA (confidentiality, integrity and availability) for each category is provided in Annex A. The critical asset categories of 5G NFV to be protected are as follows (see Figure 13).

- The **NFV network components** category includes NFV components network planes, functions, and elements. These divide into multiple asset groups such as core functions, virtualisation infrastructure, network function virtualisation (NFV), physical infrastructure, security, software-defined networking (SDN), Multi-Edge Computing (MEC), among others.
- The **NFV MANO network components** category includes the management of network functions (NFVO, VIM, VNFM), network slicing, operations support system, network/element (EMS/NMS) and SDN Controller. MANO is the most vital part of the 5G infrastructure since it is responsible for controlling the entire set of network functions, their virtualisation and the entire related software lifecycle.
- The **NFV Data** category includes users, applications, VNFs, NS, system, network, SDN, configuration and security-related data.
- The **NFV processes and environment** category includes processes and facilities related to MNOs and vendors.

3.2 SECURITY CHALLENGES

While NFV opens the door for flexible networks and rapid service creation, these offer both security opportunities while also introducing additional security challenges and complexities.

The 5G networks would essentially promote the use of NFV technologies. NFV, like many new technologies, presents new security challenges and these extend many of the security challenges applicable to NFV to 5G networks. Thus, it is important to address the security challenges appropriately and to focus on instilling stronger security and privacy settings in 5G NFV systems.

In this chapter, we identify and describe the security challenges that the 5G NFV may face. Documents used as references for the development of this chapter are provided in Annex G. The challenges have been grouped into categories to make them more understandable. The resulting list consists of seven categories (see Figure 14).

Figure 14: Categories of security challenges

Each category is provided in one section. Each section starts with an overview of the challenge category followed by a table describing the associated challenges. A high-level mapping table showing the relationship at the category level between challenge categories, vulnerabilities, attacks, affected assets and best practices is provided in section 4.4. A detailed mapping is provided in Annex F.

3.2.1 Virtualisation or containerisation

Cloud, virtualisation, containerisation, edge computing and SDN play additional roles in the era of 5G. The scale, elasticity, agility, responsiveness and rich software functionality required for 5G applications and microservices can only be achieved in the cloud. Today NFV is carried out on VMs and containers, and they'll continue to be utilised in a 5G environment.

As with any new technology, the benefits may also present potential security challenges if proper security measures are not considered. NFV enables network slicing by replacing network functions on appliances such as routers, load balancers and firewalls with instances of virtualised software that run on commodity hardware.

Virtual network functions and/or cloud-native network functions are used to run these functions as packaged software which also means a much wider attack area. Moreover, SDNs enable programmable network controls and abstract the underlying infrastructure from the apps and network services. Centralised and controllable, SDNs provide the agility required to adapt to the evolving needs of 5G microservices. However, SDNs are susceptible to attacks such as forwarding device attacks, control pane threats, API vulnerabilities, counterfeit traffic flows and more.

In the edge and far edge, operators are introducing VNFs which causes a new set of security challenges. VMs or containers may require elevated privileges to support certain network functions that could cause security vulnerabilities for the host system as well as peer VMs or containers. Due to the unique characteristic of the NFV environment, different network functions can be created and terminated dynamically on different and distributed entities.

The NFV approach allows for the dynamic distribution of the instantiated VNFs throughout the virtualised infrastructure at the edge, at the core or at the operator's datacentre. In the same way, monitoring can also be distributed and take place at different locations in the operator's network covering different parts of the network. Dynamic distribution of NFV architectures pose major security challenges that need to be considered.

A unique aspect of co-residency in NFV is that, in an NFV stack, co-residency can happen between more layers, such as between VNFs and the virtualisation layer or between the virtualisation layer and physical hosts. The co-residency of VNFs on the same physical host can occur due to placement or migration, which is known to lead to side-channel or resource depletion attacks due to the shared physical resources such as CPU, memory, or cache. The co-residency of VNFs on the host can also occur when different tenants employ the same host to run similar network functions, such as virtual firewall or virtual IDS. The fact that multiple tenants are sharing both virtual and physical resources in the same NFV stack poses additional security challenges. Table 8 illustrates the main security challenges raised by the virtualisation or containerisation technologies.

Table 8: Main security challenges facing 'virtualisation or containerisation'

ID	Challenge title	Challenge description
CH-V1	Challenges within the runtime software	Virtualisation of network functions will increase the network's vulnerability to attackers due to the increased reliance on software. A NFV software component may contain potential software vulnerabilities or it can be a malware itself. In virtualised implementations all VNFs are implemented using a common software platform such as OpenStack, Kubernetes. While vendors may produce tweaked variants, the code core will be largely identical. Similarly, host OS, hypervisor, CIS and VNFs software will be identical or from a limited set of variants. What this means is that if an attacker is able to identify a software vulnerability in one VNF, that vulnerability will likely exist in many other VNFs making the attackers job much easier and increases the risk of a cascading security failure in the network. If network security functions (e.g. SEPP) use the same software core or are in the same virtualisation layer trust domain as the functions they are protecting, the risk increases further if a software vulnerability occurs.

ID	Challenge title	Challenge description
		Note: the term 'trust domain' is defined by ETSI in [17]. It is a collection of entities that share a set of security policies. In NFV networks, multiple trust domains should be considered by CSPs during the deployment phase where a CSP wishes to achieve security role and management separation, security isolation, separation between sensitive and non-sensitive components, etc.
CH-V2	Flexibility and openness of service environment	Virtualisation technologies such as software-defined networking (SDN) and network functions virtualisation (NFV) are thriving in anticipation of 5G networks. However, they too come with new security concerns. Because of their open, flexible, programmable nature, SDN and NFV open a new avenue of security threats. The promised flexibility and openness of service environments via VNFs raises security concerns since data and NFV software are not directly controlled by the more risk-aware enterprises due to the risk of introspection by a malicious actor with total control on the execution environment entailing memory, storage and processing elements.
CH-V3	Challenges within the hypervisor	Hypervisor security mean ensuring that virtualised network elements are protected from exfiltration and VM-based attacks that come from east-west and north-south traffic. The most important software in a NFV is the hypervisor. Any security vulnerability in the hypervisor and associated infrastructure and management software or tools puts VNFs at risk. The hypervisor is fully aware of the current state of each guest OS it controls. Hypervisor introspection can enable the ability to view, inject, and/or modify information on the operational status associated with NFV through direct or indirect methods. Access to status information can result in the ability to arbitrarily read and/or write the contents of memory, storage, key storage and other NFV operational aspects.
CH-V4	Time manipulation	The virtualisation infrastructure provides a flexible environment for hosting several applications and telecommunication services. Precise and secure timing services and time-stamping of events are critical to many of those services (e.g. mobile wireless) and applications (e.g. high frequency trading, financial transactions, banking systems, billing, etc.). The virtualisation infrastructure itself requires timing and synchronisation for fault management (through logging of events) and security management (through identity and access management). A fundamental problem with all virtualised implementations is that VNFs have trouble accurately telling the time and generating entropy. Unlike a PNF which can easily be designed to have direct access to a physical clock, a VNF's view of time is only virtual. If an attacker or, in some scenarios, a malicious VM or container on the same host is able to manipulate the virtual CPU clock then is it possible to affect management or service functions such as manipulating cryptographic algorithms, key generation or other processes which are highly time dependent or may also impact the synchronisation between UEs and the network. Such manipulation may involve stretching the shape of clock cycles rather than simply increasing or decreasing their frequency. ETSI GR NFV-SEC 016[40] (draft specification - work in progress) provides more detailed discussion on timing issues with virtualised environments.
CH-V5	Entropy generation	Entropy is used across VNFs. When VNFs do not have access to high quality entropy it can negatively affect security due to weak cryptographic keys. The key point of cryptography is cryptographic algorithms and keys. The random number generator is used to generate seeds and keys randomly in many cryptographic operations. The strength and security of keys depends on their randomness. For this reason it is essential to use keys, for instance, to encrypt and decrypt information, and the security of these keys is closely related to the quality of entropy. If not enough quality entropy is available predictable keys may be produced, which are susceptible to a breach. For these reasons, a reliable source of entropy ensuring strong and random key generation is required to be used by the cryptographic operations (e.g. encryption).
CH-V6	Encrypted data processing	In a virtualised environment it is necessary to explicitly consider the risk to cryptographic processing of data within a VNF where a fully hardened HSM or HMEE (hardware mediated execution environment) is not used to perform the cryptographic function. Most software manipulating data with cryptographic operations will perform modification actions on encrypted data by first unencrypting the data either in general memory (less than ideal) or CPU cache (better but vulnerabilities exist). Following the necessary processing, the data will be encrypted again. Within existing SA3 specifications, while some specialist operations are performed in tamper resistant hardware (e.g. UICC), the bulk of cryptographic processing (e.g. user plane protection) will be performed using general X86 (or similar) servers within the core network. In a virtualised environment there are various ways in which unencrypted data can be captured: through the virtualisation layer, server management hardware, modification of VNF images, instantiating a parallel VM or container on the same physical CPU, or any number of other options. The risks of being able to capture encrypted data in an unencrypted form due to the processing of that data, increases significantly. If that processing is highly sensitive (e.g. AUC (authentication centre) or LI functions) then the risk may not be

[40] https://docbox.etsi.org/ISG/NFV/Open/Drafts/SEC016_Location_Locstamp_Timestamp/NFV-SEC016v007.zip

ID	Challenge title	Challenge description
		acceptable. Placing entire VMs into HMEE(s) is unlikely to be needed as it is more appropriate to place specific sub-functions, processes or containers into a HMEE which current CPU based HMEE(s) can support. However, in most cases this support is not currently OS kernel native.
CH-V7	Challenges within IP layer vs application layer	In a PNF implementation there are significant differences (pros and cons) between using security protocols such as IPSec designed to protect IP traffic over 3GPP reference points and over the top end to end application layer security (typically using TLS). Both are good at providing protection again a physical attacker trying to attack a physical cable or optical fibre but their characteristics vary in terms of where the encryption terminates in relation to where the data is processed or stored. TLS is considered to terminate closer to the point where a function processes or manages data, whereas IPSec may terminate at a PNF closer to the edge of the network. In flat virtualised deployments with a common virtualisation layer and resources, there is very little difference between IPSec and TLS with neither offering, by default, protection from virtualisation layer (host OS, hypervisor, CIS) attacks. In this scenario, both IPSec and TLS tunnels terminate in arbitrary memory locations which will be in the same accessible range as the plain text data they are intended to protect. Unless the IPSec or TLS tunnels transverse a physical network linked externally to the datacentres, the threats they mitigate can largely become irrelevant. Using HMEEs massively improves security (see ETSI TS NFVSEC 012[41]). However, it is clearly impractical for all TLS or IPSec endpoints for all control plane or user plane traffic to be terminated in HMEEs.
CH-V8	Default deployment or configuration	If a new, or a modification of, an existing VNF is deployed or instantiated into the production environment where it is connected to traffic and signalling interfaces, there is a risk that the VNF may become compromised before the element management EMS) has successfully configured the interface security controls. This may be caused by default or due to minimal security controls existing in the VNFD (virtual network function descriptor) or image. A common VNFD instance or image may be used to deploy multiple images of the same VNF. It is probable that each VNFD image will contain the same default security credentials and configuration. Between deployment and configuration these default security credentials may increase the exposure of the NFV elements to compromise, due to, for example, the same guest 'root' password, crypto private keys, and TLS/IPsec certificates.
CH-V9	Network traffic exposure	Existing monitoring systems need to be adapted and correctly controlled since they were meant mostly for physical and not virtual systems and boundaries, and do not allow fine-grained analysis adapted to the needs of SDN/NFV based 5G network management. The lack of visibility and controls on internal virtual networks that are created, coupled with the heterogeneity of devices used, make many performance assessment applications ineffective. For instance, existing security monitoring applications cannot monitor virtual connections in 5G network elements. Increased virtualisation introduces challenges for network monitoring. Due to the virtualised architecture of 5G networks and deployment of network functions closer to the radio access network or network access edge, it will be more difficult to detect and recognise the types of traffic inside and between VNFs crossing these networks and mitigate against any new threats. This could lead to difficulty in diagnosing network performance issues or failure to spot attackers. Traffic routed through a virtualised network may not be completely accessible for physical firewall controls or visible to traditional security inspections as previously applied on physical networks.
CH-V10	Security logs troubleshooting failure	NFV should be able to determine the source of attacks and recover, and protect against that source in the future. It should be verified that every security event is logged. NFV components may generate a huge number of logs on the virtualisation platform, therefore log analysis and event correlation in NFV will quickly become a 'big data' issue. Tools also are needed that can address all the forensics and compliance requirements. Compromised VNFs can generate a huge number of logs on the virtualisation platform, making it difficult to analyse logs from other VNFs, especially when the initial entries in the log files are deleted. There is also a risk when the infrastructure logs are leaked, as this consequently enables cross relating logs from one VNF operator to another in order to extract sensitive information.
CH-V11	Container acceleration capabilities	Container acceleration capabilities, such as container caching, present security challenges as otherwise encrypted VM equivalent image artefacts may be available in their unencrypted form in the cache to allow for fast container re-instantiation. The fast cycle times of containers also make traditional security monitoring and policy enforcement more challenging as network security enforcement decision engines cannot so easily make real-time decisions on access permission as is possible for longer lifetime VMs. Techniques using both containers and VMs provide some mitigation (e.g. running all containers for a specific VNF with a large VM, or using VMs for VNF security sensitive components such as TLS end points). Using this approach, however, restricts the flexibility of containers and introduces additional complexity or cost.

[41] https://www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/012/03.01.01_60/gs_nfv-sec012v030101p.pdf

ID	Challenge title	Challenge description
CH-V12	Container isolation failure	From a security and isolation perspective, in the container deployment scenario the VM hypervisor is replaced by a CIS which manages the life-cycle of a container within a given group of containers (e.g. pod or cluster). However, the CIS does not provide equivalent VM security memory isolation or breakout protection. The container application usually runs on 'bare metal' with no OS equivalent to the guest OS used in VM based implementations. The newer generation of NFV implementations have chosen to deploy NF as a group of containers due, especially, to the benefits associated with containers and aspects of their deployment over traditional VM deployment. Such deployments can be highly flexible by allowing the operators to deploy multiple NFs as a collection of small microservices on the same physical machines and/or even deploy NF containers within VMs. Containers co-hosted on the same physical machine as tenants share the same kernel and OS resources. This allows for a potential risk that a rogue container could escape the confinement of the container and have an impact on other co-hosted containers. There are multiple ways for attackers to escape isolation in the container. There have been reports that a number of CVEs have documented known vulnerabilities that have been identified in the past. One way to escape containers is to exploit vulnerabilities in the Linux kernel. The Linux kernel enforces container isolation by employing namespaces and cgroups. However, if attackers gain kernel level privileges through privilege escalation, they can circumvent isolation as reported in CVEs (e.g. CVE-2019-5736, CVE-2020-15257and CVE-2021-31440). There are CVEs that have reported vulnerabilities in container runtimes that allow container breakouts.
CH-V13	Sensitive data in NF container images	There are scenarios which benefit from including configuration and secrets, such as passwords or credentials, in NF container images. For example, containers need to be able to connect to other containers within the deployment as well as with external entities. All these connections need to be authenticated and secured. One way of achieving this is to provide the requisite secrets or keys to the containers which allow them to authenticate and be authenticated and secure the communication channel. A common but in-secure means of providing secrets to the containers is by packaging the secrets or the keys with the image itself. But there is the risk that the same can be extracted, read or manipulated before the container is deployed and the secret used. With a long supply chain, container images are vulnerable to outside scrutiny. With container images containing secrets or keys, this becomes a serious threat vector. Adversaries can extract them by obtaining a copy of the image and they can be potentially shared with third parties for illicit gain. • Secrets embedded within a container image can be stolen • Secrets embedded within a container image can be modified
CH-V14	Core network functions in the MEC	Multi-access edge computing (MEC) transforms the way data is processed and stored by moving some core network functions closer to the end user at the network edge, rather than relying on a central location that may be hundreds of miles away. The introduction of untrusted 5G components into the MEC could expose core network elements to risks introduced by software and hardware vulnerabilities, counterfeit components and component flaws caused by poor manufacturing processes or maintenance procedures. The presence of system components, such as hypervisors, CISs, operating systems and applications in the MEC, may provide malicious actors with additional attack vectors to intercept, manipulate and destroy critical data. Untrusted components or malware inserted within the MEC may impact user privacy by providing malicious actors the capability to clone devices and impersonate end-users to make calls, send texts, and use data. Malicious actors can use untrusted components or malware to gain access to the MEC and end-user components, leveraging them to gain access to the wider radio access network (RAN).
CH-V15	Wide geographical distribution of MEC infrastructures	As MEC Infrastructures can span a wide geographical distribution and be located in challenging environments, maintaining a uniform datacentre level of physical security is a significant challenge. A potential flaw in the physical security of any MEC hardware may result in physical attack on the infrastructure. Physical security and environmental vulnerabilities of MEC hosts may arise due to improper physical and environmental security of edge computing facilities, improper security monitoring of edge computing facilities, etc.
CH-V16	Insecure API/improper authentication of MEC components	APIs are a well-known subject of multiple attack types, as they are exposed to external access. The common API framework CAPIF is used by 3GPP as the standardised means to support providing and accessing APIs (and ETSI MEC is fully aligned with CAPIF). From a software development point of view, compliance with CAPIF should be ensured during API design and implementation phases. Further, the vulnerabilities in the service-based interface (SBI) of MEC components can include improper transport layer protection of data transferred over internal interfaces and improper verification of identity and access control to authorised MEC applications.
CH-V17	Insufficient/improper Monitoring Mechanisms of MEC components	Since MEC is based on virtualised infrastructure, it needs to include real-time security management based on NFV specifications (see ETSI GS NFV-SEC 013) [38]. Especially when deploying MEC in NFV environments, MEC should be considered as part of a whole system real-time security monitoring and management strategy. Insufficient or improper monitoring mechanisms of MEC components can result from insufficient logging of security events for MEC App and MEC host.

ID	Challenge title	Challenge description
CH-V18	Centralisation of the SDN control platforms	SDN centralises the network control platforms and enables programmability in communication networks. These two disruptive features, however, create opportunities for cracking and hacking the network. For example, the centralised control will be a favourable choice for DoS attacks and exposing the critical application programming interfaces (APIs) to unintended software can bring the whole network down [39]. The SDN controller modifies flow rules in the data path, hence the controller traffic can be easily identified. This makes the controller a visible entity in the network rendering it a favourite choice for DoS attacks. The centralisation of network control can also make the controller a bottleneck for the whole network due to saturation attacks as presented in [40],[41].
CH-V19	Malicious SDN applications	Since most network functions can be implemented as SDN applications, malicious applications if granted access can spread havoc across a network and constrict bandwidth and negatively affect operations.
CH-V20	Common SDN interfaces	Before 5G networks, mobile networks had dedicated communication channels based on GTP (GPRS tunnelling protocol) and IPsec tunnels. A significant level of expertise is required to attack communication interfaces, such as X2, S1, S6, S7, which are used only in mobile networks. However, SDN-based 5G networks will not have such dedicated interfaces but rather common SDN interfaces. The openness of these interfaces will increase the possible set of attackers. The communication in SDN based 5G mobile networks can be categorised into three communication channels, i.e. data channel, control channel and inter-controller channel [42]. In current SDN system, these channels are protected by using TLS (transport layer security) sessions [43]. However, TLS sessions are highly vulnerable to IP layer attacks [44], SDN scanner attacks [45] and lack strong authentication mechanisms [46].
CH-V21	Isolation failure between VNFs	The execution of diverse VNFs over the same NFV infrastructure sharing computing resources (e.g. CPU, memory) and networking (e.g. vSwitches, physical NICs) can create security issues, if VNFs are not properly isolated from other VNFs, from the virtualisation platform, from the host and from the network infrastructure. Security measures enforcing the isolation shall be implemented in a hypervisor hosting multiple VMs or a CIS hosting multiple containers with different security levels, for example, between VNFs supporting lawful interception (LI) with non-critical VNFs. There are various approaches to isolating VNFs, ranging from using physically separate hardware to using separate VMs or containers. There are several security threats if VNFs are not appropriately isolated, and resources are not shared effectively. These include the noisy neighbour problem and potential side-channel attacks. Note: • *Noisy neighbour* is a term commonly used to describe situations in NFV infrastructure where an application experiences degradation in performance due to the fact that some of the resources it needs are occupied by other applications in the same cloud node. These situations cannot be easily identified using straightforward approaches, which calls for the use of sophisticated methods for the management of NFV infrastructure. • *Side channel* attacks occur when an attacker is capable of gathering actionable information about cryptographic secrets by observing the implementation of a platform (for example, power consumption, run time, etcetera) and use that information to induce faults or modify the cache. Side channel attacks do not necessarily require detailed information on the platform or system being attacked. Many side channel attacks rely on statistical analysis of platform metadata that is typically exchanged (or available) in the clear. NFV platform is susceptible to side channel attacks just like regular (non-virtual) platforms.
CH-V22	Memory introspection	In a virtual environment while the virtualisation layer plays a role in preventing one VM or container from accessing the memory of another (except through declared VM or container shared memory locations), the virtualisation layer is also able to inspect any memory which is directly under its control. The virtualisation layer access to memory or other VM or container resources cannot be detected by VM or container or 3GPP security mechanisms. Encrypting memory provides some resistance but if the keys used to encrypt the memory are also under hypervisor or CIS control (including hypervisor or CIS resource controlled TPM / HSMs) then this does not prevent introspection. In addition to reading memory, the hypervisor or CIS is also in many cases able to write directly to memory, bypassing normal memory access controls and security within the VM or container. This allows an attacker with access to the hypervisor or CIS to change data within a VNF at run-time or indeed change the operation of the VNF itself. Container based NFV environments are subject to similar memory introspection risks, with the container (or cluster) management engine providing similar functionality to the hypervisor in VM based implementations.

ID	Challenge title	Challenge description
CH-V23	Trusted domains segmentation	5G network functions can be grouped into different trust domains which have varying security requirements. For example, trust in functions which contain long-term cryptographic keys might require different levels of trust to functions which only hold session keys or those which do not contain cryptographic values at all. However, this classification is too simplistic. Nearly all 3GPP NFs will contain some sensitive private information for billing purposes or cryptographic material. Applying the same security policies to NFs in different trust domains could lead to reduced security and/or reduced functionality. Security domains based on grouping whole NFs may not be sufficient. In some scenarios (e.g. LI), sub-functions of NFs (e.g. LI POIs) may need to belong to different trust domains to the rest of the NF functionality. The definition of appropriate segregation and security policies for NFs in different trust domains requires the establishment of trust domains for 3GPP NFs. It is up to 3GPP to define what a sensitive function or sub-function is and how they must be handled to protect privacy or security sensitive data, within a virtualised environment. While 3GPP TS 33.501[42] provides some consideration for 5G network functions, CSPs are also in the process of virtualising IMS or 3G/4G networks, for which similar consideration has not yet been given.
CH-V24	Access to storage resources	NFV environments run on server hardware (blade). In some use cases, there may be a need for using local storage. The common deployment is to use a SAN. The deployment of SANs within the NFV environments may have various risks, including copying an image or removing the local storage device to gain access and obtain sensitive information. A compromised VM or container can launch an attack on the SAN to obtain access to a storage area containing critical images and data The availability of the SAN is essential in a virtualised environment and any DoS attacks would affect the entire NFV.
CH-V25	Sharing of private keys between VNFs and confidentiality of sensitive data	In the 5G core network, NF communications are secured using TLS, according to the profiles in TS 33.210. ECDSA and RSA are used to authenticate these communications. Therefore, a VNF must contain private keys to authenticate these exchanges. These keys need to be provisioned to VMs or containers securely on first boot or need to be stored securely on the image in some fashion. A decision also needs to be made as to whether two NF instances may share the same key pair, for example if the second instance is to be deployed in case the first fails. Certain VNFs will hold sensitive data, which should not be available to other VNFs or which should only be made available in a specific set of circumstances. For example, the 3GPP TS 33.501 includes the requirement that long-term keys shall never leave the secure environment of the UDM/ARPF. To have the same level of confidence in the confidentiality of sensitive data when stored in a VNF as when it is stored on physically separated hardware, it is necessary to consider new threat vectors. For example, the long-term keys in a virtual UDM/ARPF could be stolen by an attacker with root access to the virtualisation layer. Alternatively, cache side-channel attacks might allow the operator of a VNF sharing resources to recover data.
CH-V26	Availability of network functions	One of the advantages of virtualisation is that a network can scale and transform to meet demand. In general, it is likely that the availability of required VNFs is less of a concern than in a physical deployment. However, virtualisation does introduce new availability risks. For example, shared resources might be monopolised by a neighbouring VM or container (the noisy neighbour problem). Many VNFs are essential for the 5G core network to function. For example, if a UDM/ARPF is not available then a user cannot complete primary authentication. Similarly, if an AMF is not available then a connection cannot be managed. Therefore, it is important that the VNF is guaranteed to be available in the same way as a physical network function would be.
CH-V27	Software catalogue image exposure	Virtualised networks define convenient software onboarding APIs and use central software catalogues to hold the VNF images prior to instantiation. There has been significant resistance in ETSI ISG NFV and open-source communities to mandate full mandatory integrity checking of software images at both the overall package and sub-component (artefact) level. Current implementations offer minimal if any mandatory signing and where they do, this is based purely on vendor signatures. Therefore, in theory at least, any image from the same vendor would pass verification checks if loaded into the wrong CSP software catalogue. Furthermore, the software catalogues with or without integrity protection provide a standardised description of the VNFs, their resource requirements, their configuration and ultimately the compiled executables that make up the VNF. If an attacker can access the catalogue then they will be able to gain directly a lot of information which can then be used to attack running instances of the VNF. Where those VNFs contain cryptographic functions or sensitive information, this increases the risk further.

[42] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

ID	Challenge title	Challenge description
		Based on current virtualisation standards in ETSI and Open Source, the protection of the confidentiality of whole images or artefacts during run-time, on-boarding, storage, and instantiation is not supported, although for LI purposes this was recommended in ETSI TS NFV-SEC 011.
CH-V28	Multi-vendors integration	At the integration and deployment stage of the NFV, the major challenges are related to interoperability between different vendors and how to integrate the software components, hardware, and security solutions of multiple vendors into a stable and efficient system, and how to assign SLA agreements between different components. Hardware, the virtualisation layer, VNFs and control solutions for cloud resources may be provided by different vendors, increasing the risk of security holes due to mismatched assumptions and expectations. Security solutions within NFV could be provided by different vendors, which may be complex to manage and monitor, resulting in the operator not using these security solutions.
CH-V29	Multi-tenants Co-residency	As an NFV stack is multi-tenant in nature, placing and migrating a VNF can be a challenging task for the provider due to the issue of co-residency. It is well known that co-residency may lead to various security issues, such as side-channel attacks, and additionally the tenant may have specific requirements in terms of (the lack of) co-residency. Co-residency may occur in an NFV environment when a VNF is first placed or when an existing VNF is migrated. The tenant requirements may specify that certain VNFs are to be placed on a dedicated host or a VM or container needs to have an auto-scaling feature such that its need for more space can be quickly fulfilled. In terms of security, co-resident VNFs may belong to tenants with conflicting interests, and the co-residency may enable an insider attack with increased privileges and connectivity not available to regular attackers. The co-residency of VNFs on the same VM or container can also occur when different tenants employ the same VM or container to run similar network functions, such as a virtual firewall or virtual IDS. Lack of multi-tenant controls in an operator's NFV infrastructure or MANO, where multiple tenants are supported, increases the opportunity for the compromise of a VNF and the underlying NFV infrastructure (e.g. supporting network, host OS, hypervisor, CIS, storage, hardware IO, compute and memory).
CH-V30	Elastic nature of NFVI-migration of VNFs	Due to the dispersion of VMs or containers that belong to a VNF across racks and datacentres within the NFVI PoP in the core, MEC and RAN, and due to the migration of VMs or containers for optimisation or maintenance purposes, the physical perimeters of the network functions become blurred and 'fluid' making it practically impossible to manually define and manage security zones. If a VM or container is migrated to another cluster where the security level is different or security measures are lacking, the VNFs may be exposed to untrusted network traffic. 5G involves the active use of mobile edge computing technology (MEC). These can be corporate applications running on service providers' networks: intelligent services, financial services, multimedia, etc. It should be noted that in this case, a 5G provider's networks are integrated into the corporate infrastructure. This gives the attacker new opportunities for entering corporate networks, as the MEC equipment is placed outside the protected perimeter of an organisation.
CH-V31	Geographical location	Using NFV, the violation of regulatory policies and laws becomes possible by moving one VNF from a legal location to another illegal location. The consequences of violating regulatory policies can be a complete banning of the service and/or the imposition of a financial penalty, which may be the original intention of the attacker in order to harm the service provider. For some VNFs (or subcomponents) it is necessary to know exactly where a VNF is (or at least in which datacentre it resides). By default, cloud hosting environments do not by nature provide an attestable guarantee of physical location of a host or VNF. It is possible to indirectly attest location through host IDs but it is also possible to move a host from one location to another. 3GPP functions such as AUC, UDM or LI functions need to be attestable within the boundaries of a specific physical location (ETSI TR NFV-SEC 016 discusses some of these issues). Furthermore, if functions such as SEPP are supposed to be the physical boundary of a network then it may be necessary to be able to constrain them, and the SDN routing to them, to specific physical locations.
CH-V32	Data life cycle and location	In virtualised environments, it is necessary to consider where data has been and whether that data is sensitive as regards privacy. If a VNF moves from one host to another or is terminated, and the previous resources are allocated to another VNF without being fully cleared, this risks compromising privacy sensitive data or keys. OSs are not unknown to proliferate temp files, which in a PNF is much easier to contain (ignoring PNFs with external storage). In a VNF, if storage or memory is not fully erased before reuse there is a significant risk of data loss between VNFs. By extension, software is not unknown to crash or experience abnormal behaviour, increasing the risk of data remaining in undesirable locations. If a VNF cannot securely attest what host it is running on then high security functions could be deployed on vulnerable hosts.

ID	Challenge title	Challenge description
CH-V33	VNF host spanning	VNFs are large complex lumps of functionality which span multiple physical hardware hosts in a virtualised implementation. In a virtualised environment, access to the interconnections between servers making up a single VNF can be gained much more easily. While there is a risk of an attacker gaining physical access to the interconnections between servers making up a single PNF, this generally requires physical access to the hardware. In a virtualised environment, however, access can be gained much more easily as the servers making up a function are more likely to be physically distributed and the SDN v-switch would allow an attacker to fork IP packets flowing much more easily between remote hosts Such forking is very difficult to detect or prevent from within a VNF unless specific mitigation during design is taken to minimise the risk. While TLS automatically applied by the NFV or SDN layer between VMs or containers reduces threats from external attackers, it is much less effective against attackers who have (or have gained) access to NFV MANO, etc.
CH-V34	Dynamic nature of network functions	One of the main persistent challenges to the use of NFV in mobile networks is the dynamic nature of VNFs that leads to configuration errors and thus security lapses. For instance, using NFV, virtual networking components (e.g. virtual routers and virtual networks) can be easily created. Quick and dynamic service decisions can result in human error when a virtual router is created and used to interconnect virtual networks without the use of any firewall. Compared to physical network appliance deployments, the dynamicity of virtual network appliances and its connectivity can lead to improper separation between the network and its subnets.

3.2.2 Orchestration and management

The MANO layer is considered as the brains of all operations for the creation, configuration, provision and monitoring of network services and their related components. In contrast, it can be seen as a single point of failure and an attractive target for attack, as any compromised operations may lead to the failure of an entire system.

The main function of MANO is to control the connectivity between VNFs, create the relationships between VNFs and virtual infrastructure resources, maintain a sequence of network forwarding paths, and address all the service chaining processes. However, a lack of consistency on how to manage and orchestrate the network services can incur security challenges. Table 9 illustrates the main security challenges raised by the orchestration and management of the 5G NFV.

Table 9: Main security challenges facing 'orchestration and management'

ID	Challenge title	Challenge description
CH-OM1	MANO single point of failure	MANO is the control node of an NFV. It controls all VNFs and indirectly (via the virtualisation layer) it can access all data within those VNFs. Compromising MANO would effectively compromise all VNFs. MANO are responsible for on-boarding, instantiation, termination and lifecycle management of all VNF within a virtualised network. Combined with 3GPP layer OSS/BSS functions they control all VNFs and indirectly (via the virtualisation layer) can access all data within those VNFs, unless specially protected. Compromising MANO would effectively compromise all VNFs (to a much lesser extent the same applies to the OSS/BSS). Therefore, for VNFs to be secure, NFs need to have minimum security guarantees from MANO and be designed to be resistant to compromise of the underlying MANO system. Communications with and within NFV MANO: attackers may try to eavesdrop or modify the traffic that transits between the NFVI and the NFV MANO, as well as traffic within the NFV MANO. NFVO and/or VNFM: attackers may attempt to exploit these two components to disrupt the lifecycle management of the network services (purpose of the orchestrator) or of individual VNFs (main role of the VNFM). In case of a DoS attack or a failure, the NFVO may be reliant on other elements (e.g. SDN controller or VIM) under its configuration control to enable them to boot, reallocate resources and reload their configuration. There is a risk that, should a major event occur, parts of the NFV infrastructure may remain out of service causing major service issues.

ID	Challenge title	Challenge description
		In addition, any change, termination, or re-instantiation of security critical NFV elements, by the NFVO and VNFM, where the critical data is overwritten, may compromise the integrity of the network; for example, deletion of customer specific profiles, LEA target information or AuC keys. The VIM is responsible for the management of the NFVI resources used by the VNFs (compute, network and storage) and attacking it could, for example, allow denial of service (DoS) or data theft, bypassing the isolation of the hypervisor or CIS.
CH-OM2	Orchestration compromise and policy violations	There are risks that: • new, or changes to existing, MANO descriptor files [43] [44] (e.g. network service templates, VNF forwarding graph descriptor, VNF descriptor) could be made without applying the correct security and affinity/anti-affinity policy rules[45] between VMs or containers leading to local legal and regulatory issues, increased risks of fraud and SDN and NFV elements exposed to additional security vulnerabilities; • an existing virtualised element (e.g. VNF, SDN Controller) managed by the NFVO may be removed while there is still an existing operational service dependency from another network element or system, causing a service outage and loss of availability. If the NFVO user interface allows for the editing, importing or generation of such provisioning or instantiation of script files (yml or other) that are used to manage VNFs (e.g. initiation and termination, description of internal and external connectivity, dependencies between VNFCs), several attack vectors may be exploited by an attacker.
CH-OM3	Resource integrity caused by manual changes or failure to update resource inventory	There could be a loss of integrity on the orchestration resource inventory with the SDN controllers, VNFM service configuration caused by direct manual configuration at the SDN/NFV layer. During the service management processes, commands may be correctly initiated from the NFVO to the SDN controller and/or VIM, VNFM; however, the success or failure of these commands may not be reflected in the service and resource inventories which could cause issues for data integrity.
CH-OM4	Vulnerabilities within orchestration protocols	The protocols used by the NFVO to communicate with the components needed to manage the virtualised environment may be vulnerable and attacks could be realised in several ways: • Spoofing of the NFVO's service requests may result in an attacker being able to generate service requests to cause a DoS by: o provisioning new instances in order to delete the number of resources available to the NFV or SDN components; o retiring NFV instances or SDN elements that are in use by the operational network; o changing the SDN configuration. This risk could impact a single element or the whole mobile network. • Spoofing as an SDN controller, VIM or VNFM to send service management requests to the NFVO on the resource performance could cause the NFVO to initiate changes on the infrastructure. This exploit could be used by an attacker who wants to force the NFVO to move a NFV component to another datacentre where the attacker may have physical access or has compromised the virtualisation layer and wants to monitor customer traffic.

3.2.3 Administration and access control

Much of the openness and programmability offered by the 5G NFV network architecture relies on the expanded use of APIs. The exploitation can target different types of API namely internal network functions, internetworking interfaces, roaming interfaces, etc. exposed in different layers of the network. A poorly designed or configured API with inaccurate access control rules may expose network functions and sensitive parameters. Table 10 illustrates the main security challenges raised by the administration of and access control to the 5G NFV.

Table 10: Main security challenges facing 'administration and access control'

[43] https://docbox.etsi.org/isg/nfv/open/Publications_pdf/Specs-Reports/NFV-IFA%20014v3.3.1%20-%20GS%20-%20Network%20Service%20Templates%20Spec.pdf
[44] https://datatracker.ietf.org/meeting/88/materials/slides-88-opsawg-6.pdf
[45] https://www.etsi.org/deliver/etsi_gs/nfv-ifa/001_099/011/02.03.01_60/gs_nfv-ifa011v020301p.pdf

ID	Challenge title	Challenge description
CH-AC1	Malicious insiders	Whoever commits a malicious action is not necessarily an outsider to the virtualised system. Accidentally or intentionally, even an insider, such as a system administrator (e.g. hypervisor or CIS administrator), could behave incorrectly. Administration roles can be used to manage the NFV environment. This environment can be used by the hypervisor or CIS administrator to eavesdrop or modify sensitive data running on a VM or container or transferring between NFV components. Moreover, this administrator may be able to change or stop processes running in the VM or container, give other applications access to the VM or container or steal critical security data.
CH-AC2	Single administrator domain	NFV deployments usually rely on a single administration domain, with a global administrator who is able to manage the hosts and NFV environment. As such, at some level, all VNFs regardless of their sensitivity are potentially reduced to the same security level of the single administration domain. Therefore, if an attacker is able to gain global administrator privileges, they will be able to control and manage all network functions, regardless of their sensitivity and trust domain.
CH-AC3	Lack of staff with the skillsets needed to operate virtualised networks	The virtualisation of network functions introduces a new risk because virtualisation is still a comparatively new architecture and carriers may still be unfamiliar with the risks inherent in networks that are more defined by software than hardware. A lack of staff with the skillsets needed to operate virtualised networks may represent the greatest threat in telecommunication networks utilising this new architecture.
CH-AC4	Insecure management, configuration, and monitoring interfaces	The interconnectivity among the virtualised end-to-end architectural components exposes new interfaces that, unless protected, can create new security threats. Through management interfaces users can access and interact with services offered by NFV. A management interface is easily hackable if it is not adequately protected because it is exposed to any external entity, which could abuse the privileges granted to it. APIs play an integral part during provisioning, management, orchestration and monitoring of the services running in the NFV framework, which makes them a perfect target for attackers. API abuse is the most-frequent attack vector. An attacker may try to exploit insecure APIs in order to access or tamper with NFV's services and/or databases. APIs-based attacks can lead to data loss or leakage, identity theft, system compromise, as well as service unavailability. Potential API-based attacks against NFV framework include parameter attacks, identity attacks, man-in-the-middle attacks and (distributed) denial of service attacks.
CH-AC5	Compromise of orchestration access control	One of the core features of NFV is management and orchestration which is, in essence, the ability to dynamically scale network capacity up or down and continuously adapt to shifting requirements. This may be realised through automated provisioning of network elements and or services. The provisioning framework itself provides several attack vectors that may be exploited by an attacker. These two features are highly centralised, which means the safe and stable operation of the entire system will be jeopardised if the functions fail or are illegally controlled. A poor authentication mechanism, weak access control and feeble authorisation rules may allow the attacker to impersonate or appear as a legitimate authenticated and authorised user. The attacker could then compromise the network and the NFV elements to influence their performance, behaviour and services.
CH-AC6	Weak or insecure authentication or access control authorisation to VIM	Attackers may be able to connect to VIM and break the administration password allowing them access into VIM management features, which would allow them to modify the existing configuration causing a DoS attack or to install unauthorised applications to facilitate fraud or eavesdropping. VIM may accept all commands sent from the NFVO. Received Commands may cause changes to the virtual environment that have a major service impact or cause a DoS. Poor segregation between vendors within a VIM may allow a vendor access to the NFV configuration of other vendors. The unauthorised access could cause knowingly or accidentally a DoS attack on a competitor's NFV by removing their VM or container resources.

3.2.4 New and legacy technologies

In the current NFV deployment, operators are incorporating NFV components into legacy devices. In this hybrid architecture, the complete network management system is be divided into two parts. The first part is a sub-system managing VNFs. The second part is the legacy OSS.

In order to avoid having to reconstruct the existing sub-system, the legacy OSS will stay unchanged and will continue to manage existing PNFs. An interface between legacy OSS and the virtualised environment is not precluded and could be a proprietary interface, based on the operators' requirements.

Given that legacy or physical network function or devices will continue to be used for the foreseeable future, operators will have to manage hybrid (part physical, part virtualised) networks. Hence, existing OSS will need to be extended (in some way) to work together with the new management and orchestration systems that support NFV.

There are also security challenges that should be considered for LI. The security challenges raised by these hybrid physical and virtual network environments should be considered when deploying the 5G telco management and orchestration architecture. Table 11 illustrates the main security challenges raised by the mix of new and legacy technologies within a 5G NFV.

Table 11: Main security challenges facing 'new and legacy technologies'

ID	Challenge title	Challenge description
CH-LG1	Mixed virtual and legacy PNF deployments	Most virtualised deployments will commence with adding VNFs to an existing PNF based network. Over time the number of VNFs will increase but mixed network deployments will be the default for the next 10+ years. Similarly, mixed SDN and non-SDN linked NFs will also co-exist. By default, PNFs and VNFs have to be able to implicitly trust each other in mixed deployments, given that 3GPP SA3 currently does not specify different handling or trust relationships based on PNF or VNF implementation. In mixed deployments, especially where older 3G CS NFs share common NFs (e.g. virtualised HSS, UDM) with 4G or 5G higher security level VNFs, additional 3GPP security mechanisms may be required to prevent attackers using insecure interfaces as the injection points against the otherwise secure VNFs (i.e. VNF implicitly accepts messages from legacy PNF with lower security). However, the reverse attack also exists where an attacker uses the much larger attack surface offered by VNFs to attack PNFs. VNFs would ignore the messages but may well forward them to the less secure PNFs. Attacks are also possible depending on the chain of VNF and PNFs, where an attacker injects messages towards a VNF, which is forwarded to a PNF and finally to another VNF. While the first VNF and PNF are unharmed by the attack, the second VNF falls foul of the implicit trust of PNF and VNF communications. It is possible to conceive other similar chained attack scenarios where PNFs and VNFs exist together without knowledge of each other's implementation or trust domain segregation.
CH-LG2	Vulnerabilities of physical hosts	X86 and similar server architectures have a number of physical security weaknesses from the perspective of a critical national infrastructure. Plug and play interfaces (e.g. USB and removal RAID discs) unless disabled or tightly controlled represent a risk to 3GPP NF security. However, more difficult to control attack vectors such as PCI Express bus direct memory access (DMA) or use of OS swap or page files represent risks if physical access to the server(s) hosting a 3GPP NF becomes possible. Similarly, most server firmware would detect hardware changes (e.g. adding an extra copy of a physical network port which is visible to the host firmware), but if the replacement hardware uses the same IDs and declared interfaces, this is much more difficult to detect. In legacy PNF implementations, such risks are better understood with physical constraints including secured racks, physical testing of interfaces to confirm they are disabled and careful placement of more sensitive functions (e.g. AUC) within CSP datacentres. However, for virtualised implements using large pools of common hosts, physically securing all hosts (rather than those dedicated to a specific function) so that any 3GPP function can run on any host, while controlling physical access attacks is difficult to achieve. This threat potentially increases with IAAS and NAAS deployments. Furthermore, many datacentre hosts are equipped with baseband management controllers and intelligent management interface protocol. If an attacker is able to access these controllers, they effectively have direct control over all hosts and all VNFs running on them. Over recent years a number of such vulnerabilities have occurred. For sensitive functions such as the AUC or LI functions, the risks would obviously be increased. Almost all virtualised environments (e.g. NFV servers) rely on x86/64 architecture and common off-the-shelf server hardware. Microprocessor side-channel security vulnerabilities such as CVE-2017-5753, CVE-2017-5715, CVE-2017-5754 (aka Spectre and Meltdown) can make NFV infrastructure a very valuable asset for attackers. These vulnerabilities may lead to information disclosure and elevation of privilege. Mitigation and resolution of these vulnerabilities are difficult and may call for both software (OS) and hardware (microcode) updates.
CH-LG3	Transformation of legacy OSS/BSS	Today's OSS/BSS architectures are built on a solid but aging foundation, developed over several decades, for telecom services that were relatively static and predictable. OSS/BSS systems are undergoing significant changes in order to benefit from, and keep up with, the pace of innovation ushered in by SDN and NFV. Operators seeking to take advantage of SDN and NFV to optimise their networks and improve agility can only do so when a new generation of OSS/BSS processes is enhanced to cope with this new virtualised and cloud-based world. Migration will take time, as operators must adapt and upgrade complex and proprietary legacy systems[46].

[46] https://opennetworking.org/wp-content/uploads/2014/10/sb-OSS-BSS.pdf

ID	Challenge title	Challenge description
CH-LG4	Integration with existing legacy OSS/BSS	Most core legacy systems cannot support end-to-end functionality. It's difficult for operators to deliver and charge for low latency and high reliability, as well as assure it and provide an appropriate SLA because the required billing integration may not be in place. Instead, they continue to use standalone solutions because of the integration costs involved[47]. The NFV infrastructure must dynamically reallocate its resources between different virtual network functions to meet variations in traffic composition. Current OSS/BSS systems cannot support this level of real-time dynamics and policy driven real-time service variation[48]. SDN and NFV are poised to reduce the cost of capacity and in turn improve service density. The knock-on effect will be an increase in service management overhead, which will create a greater workload for OSS/BSS. OSS and BSS systems will need to adapt to avoid becoming a bottleneck. For instance, billing systems will need to support more billing events as service instances grow significantly. The traffic of multiple customers traffic must be aggregated efficiently, with unique subscriber profiles, many application types and distinct policies[49].

3.2.5 Adoption of open source or COTS

Use of open source within 5G NFV will continue to increase as vendors rely on open source software to speed the delivery of new solutions. Open source software can be viewed as being analogous to corporations outsourcing functions not related to their core competencies. This introduces a new set of security challenges in terms of keeping a consistent and coherent assurance of security-by-design, and the prevention of resulting security flaws. To compound this issue, asking vendors to disclose the open source components used in their products may disclose more vulnerabilities and add to the risk.

Another security challenge is that NFs based on NFV technologies can now run on lower cost, commercial off-the-shelf (COTS) hardware, eliminating the need for more expensive, purpose-built hardware. When using COTS for the NFVI, security and performance may be impacted, and security measures must be implemented to reduce the related risks. Table 12 illustrates the main security challenges raised by the adoption of open source or COTS within the 5G NFV.

Table 12: Main security challenges facing 'adoption of open source or COTS'

ID	Challenge title	Challenge description
CH-OC1	Adoption of open source software	Many 5G vendors and operators rely on open-source software to accelerate delivery of digital innovation. Both traditional and agile development processes frequently incorporate the use of prebuilt, reusable open-source software components. As a result, some organisations may not have accurate inventories of open-source software dependencies used by their different applications, or a process to receive and manage notifications concerning discovered vulnerabilities or available patches from the community supporting the open-source. Open-source software provides attackers with a target-rich environment because of its widespread use (e.g. GitHub security breaches[50] [51]). Open-source software is incorporated into applications in many ways, and often 5G operators or vendors will not know where open-source is used. When open-source is used as the foundation for a vendor's product, any vulnerabilities could threaten the integrity of the vendor's solution. Asking vendors to disclose the open-source components used in their products may disclose more vulnerabilities and add to the risk. In 2020 we saw the Boot Hole vulnerability for GRUB2 bootloader (CVE-2020-10713), seven other GRUB2 vulnerabilities, and the critical HAProxy vulnerability with malformed HTTP/2 requests (CVE-2020-11100). Since June 2017, the Linux kernel has had 12 CVEs with a CVSS score of 10.0 (critical). Prevasio's recently completed Operation Red Kangaroo scanned the entire Docker Hub and found 51 percent of all containers had 'critical' vulnerabilities. As new open-source software vulnerabilities continue to be introduced into

[47] https://blogs.oracle.com/oracle-communications/post/without-modern-ossbss-5g-network-investments-may-be-throwing-good-money-after-bad
[48] https://opennetworking.org/wp-content/uploads/2014/10/sb-OSS-BSS.pdf
[49] https://opennetworking.org/wp-content/uploads/2014/10/sb-OSS-BSS.pdf
[50] https://www.perforce.com/blog/vcs/how-secure-git
[51] Hackers target GitHub (and other popular Git hosting tools) for many reasons. But the biggest is the potential they see in hacking into repositories on GitHub and stealing (and potentially selling) intellectual property. Hardworking developers from companies all over the world use GitHub for personal and business needs, often on an ad hoc basis. And developers in the heat of battle can often overlook security concerns. Hackers know this — and exploit it.

		development projects, it has become clear that software vendors and operators need to implement secure software development best practices and cannot rely exclusively upon the open-source community to build secure software[52].
CH-OC2	Adoption of COTS hardware	Generally, hardware design and manufacturing occur prior to software development, so it is extremely important to address hardware security in product lifecycles, because once attackers compromise hardware modules, software security mechanisms running on these devices will be compromised as well. For example, manufacturing backdoors eavesdropping, inducing faults, and hardware modification tampering through jailbroken software. Almost all virtualised environments rely on x86/64 architecture and common off-the-shelf (COTS) server hardware. This makes telecom virtual appliances (NFV firmware) a very valuable asset for security researchers and attackers alike. An attacker with physical access to the hardware resources may be able to tamper with or remove the TPM, disabling the trusted computing platform function and facilitating other attacks; for example, allowing an untrusted host OS, hypervisor or CIS to be installed.

3.2.6 Supply chain

The 5G NFV supply chain is similarly susceptible to the introduction of risks such as malicious software and hardware, counterfeit components, poor designs, manufacturing processes, and maintenance procedures. The exposure to these risks is heightened by the broad appeal of 5G technologies and the resulting rush to deployment. This may result in negative consequences, such as data and intellectual property theft, loss of confidence in the integrity of the 5G network, or exploitation to cause system and network failure. Table 13 illustrates the main security challenges facing the supply chain of the 5G NFV.

Table 13: Main security challenges facing 'the supply chain'

ID	Challenge title	Challenge description
CH-SC1	Separation of test and production environments	A significant risk is formed if the separation between test and production environment is neglected. The reason is that the security configurations of the two different environments may vary. In addition, the test configurations are updated more frequently. Moreover, the test environment is also more likely to support remote vendor access.
CH-SC2	Untrusted partners	Carriers and equipment vendors may use components within the NFV manufactured by untrusted companies, likely, in part, because of their relatively low costs or the components may already exist as part of the current LTE infrastructure. The use of components manufactured by untrusted companies could expose entities to risks introduced by malicious software and hardware, counterfeit components, and component flaws caused by poor manufacturing processes and maintenance procedures.
CH-SC3	Infected/untested/ unauthorized patches or upgrades	When updates are available, they are likely to be retrieved from a centralised server and then applied by a script or automated update process. If such a server or the applied script has been compromised, spoofed or subject to some type of malfunction there is a risk that updates have been compromised or damaged. Deploying untested or unvalidated NFV components on the NFV network poses a significant risk. This risk may result in anything ranging from minor inconveniences such as missing functionality to more dangerous issues such as signalling loops or, in the worst case, complete network failure.
CH-SC4	Test isolation and assurance	In legacy hardware deployments, 3GPP, GSMA or other testing schemes generally involve testing 3GPP functions as opaque boxes or pentesting them in isolation from other network functions. While it is possible to test virtual functions in this way, the level of assurance gained is different. Such stand-alone testing relies on the underlying virtualisation and hardware layers being 100% secure and that no future vulnerabilities are found in those underlying components. Testing functions in isolation does not guarantee that when a VNF is instantiated on a different host virtualisation environment or is instantiated in a larger virtualisation environment containing multiple VNFs that a 3GPP function tested in isolation remains secure. Isolation in testing refers to VNF to VNF isolation as well as platform to VNF isolation. In general, it means that the VNF is firstly tested on its own in a dedicated NFVI and then tested with other VNFs in a shared NFVI.
CH-SC5	Use of counterfeit components	Counterfeit NFV components are more susceptible to cyber-attack and are more likely to break because of their poor quality. Compromised counterfeit components could enable a malicious actor to impact the confidentiality, integrity or availability of data that travels through NFV and to move laterally to other more sensitive parts of the 5G network. Counterfeit components are inserted at the component manufacturing or

[52] https://www.ericsson.com/en/blog/2021/1/open-source-security-software

		distribution stage in the supply chain in order to impact components delivered to a subset (potentially a targeted subset) of downstream customers. Counterfeit parts look like regular parts and are a form of fraud. Scenario: a malicious actor identifies a government contractor that provides NFV components and attempts to sell modified or counterfeit products to them at discounted prices. While the contractor is legitimate and has the most to lose from counterfeit products, they are unaware that there is a potential problem and do not conduct an initial analysis of possible counterfeiting risks that exist within its industry. To save money, the contractor purchases the counterfeit components from the malicious actor and inserts them into their product. The counterfeit part has gone undetected in usability and functional testing and is placed into production. The resulting effect on the overall 5G system can take a variety of forms, such as impacting system performance, the availability of critical services, or loss of data.
CH-SC6	Use of inherited components	Inherited NFV components may come from extended supply chains consisting of third-party suppliers, vendors, and service providers. Supply chains may be compromised via attacks on suppliers, including suppliers of suppliers, who may have weaker security controls and audits on their development, production, or delivery channels. Flaws or malicious code inserted early in the development phases are more difficult to detect and could lead to the developer marking the component as legitimate through digital signatures or other approvals. Malicious actors could then later exploit these vulnerabilities. The malicious code may be introduced to the component in several different ways, such as via compromise of the source code repository, theft of signing keys, or penetration of distribution sites and channels. As a part of an authorised and normal distribution channel, operators unknowingly acquire and deploy these compromised components on their 5G systems and networks. Advanced malicious code typically does not disrupt normal operations and may not activate for several days or weeks, thereby remaining hidden from typical application and software testing practices. Scenario: a telecommunications company buys core network systems management software from a trusted provider. However, unbeknownst to the trusted provider, one of the components it uses in the product has been compromised and now contains malicious code. This is a threat that results from inheriting risk decisions made by a supplier within the supply chain. The deeper into the supply chain it occurs, the more difficult it is to identify in advance. This inserted vulnerability may be used by the malicious actor as a part of a larger attack chain that uses the malicious code to gain access within the core network of the telecom and then pivot towards other attack vectors.

3.2.7 Lawful interception (LI)

Securing and hiding LI functionality from other functions in an NFV environment is by far the largest security challenge. Placing LI functions within the VNF environment exposes them to a variety of security and visibility risks. Placing them outside of the NFV environment comes with a different set of visibility risks, places significant constraints on VNF mobility, makes LI fragile to dynamic changes in the NFV environment and will only be possible in scenarios where the mandatory intra-VNF and inter-VNF encryption has been disabled. Disabling intra or inter VNF encryption will expose the NFV platform to considerable cyber risks and is therefore unlikely to be acceptable.

Specific consideration of LI security challenges in hybrid part legacy scenarios must be considered. In real deployments, legacy nodes and VNF need to co-exist and be interconnected with implicit trust. This implicit trust is required as VNFs are not supposed to know they have been virtualised. This therefore means that the VNFs are connected to management and service control plane links which include legacy nodes that do not implement the same level of security as the VNF. Table 14 illustrates the main security challenges for Lawful Interception (LI).

Table 14: Main security challenges facing 'lawful interception (LI)'

ID	Challenge title	Challenge description
CH-LI1	Encryption of communications[53]	5G offers very high security standards. Although end-to-end encryption is not yet set out as mandatory in the 5G standards, it cannot be ruled out that it will be included in the standardisation process. End-to-end encryption would make it impossible to access content in electronic communications, even through lawful interception. In addition, encryption of an IMSI number (it is the individual number of the mobile phone card) would make it impossible for law enforcement and judicial authorities to identify the mobile devices or location of criminals or persons who pose a serious threat, as well as potential victims or persons facing a threat. Without access to the IMSI number, certain lawful interceptions are not possible. Therefore, metadata normally available via interception (such as location, date, time, call duration, calling and contacted party)

[53] https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf

		would be lost to law enforcement and judicial authorities. In addition, 5G will have strict authentication processes (in order to identify a user before access is granted) such as false-base detection that will make it harder for law enforcement to investigate via lawful interception without being detected. (IMSI catchers which are necessary for interception of mobile devices and location of suspects or victims would be detected.)
CH-LI2	Cooperation of numerous network providers	Up to now, when carrying out a lawful interception, the authorities deal with a limited number of network providers. With 5G network slicing technology[54], network and service providers may not – unless they are obliged to do so – have a complete copy of the information available, which would make lawful interception impossible. 5G architecture means that in order to monitor communications, one could require the cooperation of numerous network providers both at home and abroad, under different jurisdictions. While law enforcement authorities currently make requests to a single network provider operating from national territory, in the future with 5G, they may have to deal with multiple service and network providers, including from abroad. The cross-border dimension of 5G technology may increase the need for international cooperation, which may increase the time between request and implementation of the interception, with a non-negligible risk of losing a complete copy of the technical information.
CH-LI3	Availability of data at the LI central nodes	In order to improve timely response, MEC will allow mobile phone networks to store and process contents in decentralised clouds in the vicinity of network users which can directly communicate with each other. Information will not necessarily be directed via central nodes, where lawful interception is currently implemented. Therefore, data may not always be available anymore. As network functions and components which used to exist physically become virtual or may be moved abroad, existing measures to ensure confidentiality of interception (protection against access to or even altering target lists by having specifically vetted staff to carry out the measures on the national territory and physical protection measures such as access restrictions) will no longer work.
CH-LI4	LI in hybrid deployment	In real deployments, LI legacy nodes and NFV need to co-exist and be interconnected with implicit trust. This therefore means that the NFV are connected to management and service control plane links which include LI legacy nodes that do not implement the same level of security as the NFV. There are two logical attack models which should be considered for LI: • Virtualised node compromise using a legacy LI node; • Legacy node compromise using the VNFs or host OS, hypervisor or CIS or associated signalling within the NFV domain.

3.3 NFV VULNERABILITIES

Based on and inspired by the ENISA 5G threat landscape[55], the list of potential vulnerabilities related to the 5G NFV challenges are classified into the following categories. In addition to virtualisation vulnerabilities, the potential vulnerabilities due to legacy systems are considered in this analysis.

- service-based vulnerabilities of NFV components;
- improper protection of data and information of NFV components;
- improper hardening of NFV components;
- virtualisation layer vulnerabilities;
- vulnerable mechanisms for authentication and authorisation of NFV components;
- insufficient or improper monitoring mechanisms of NFV;
- vulnerabilities due to legacy OSS/BSS systems;
- improper protection of service based interfaces;
- vulnerabilities of 5G NFs;
- vulnerabilities in operating systems supporting 5G NFs;
- improper hardening of 5G core components;
- vulnerabilities of SDN;
- vulnerabilities of MEC;

[54] Several network and service providers may be able to operate on the same physical infrastructure. For example, one company will provide enhanced mobile broadband, cellular phones for example, another one will provide massive machine type communications and a third one will provide low latency communications. Each service provider will use a customised virtualisation layer of the same physical infrastructure, with different technical specifications. Relevant telecommunication monitoring information may therefore not be available in every network slice.
[55] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

Annex C provides a description of the different 5G NFV vulnerabilities with their associated assets belonging to the above categories that can be exploited to perform attacks impacting the confidentiality, integrity and availability of the 5G NFV system.

3.4 NFV ATTACK SCENARIOS

Attacks are defined by the ways an attacker can compromise system vulnerabilities or weaknesses, impacting the confidentiality, integrity and availability of a NFV system.

There are many variants of attacks on 5G NFV and they can be organised according to the following two factors (the attack taxonomy is provided and detailed in Annex D):

1. **Attack sources belong to three categories:**
    - attacks from within a NFV (internal weakness),
    - attacks from outside a NFV (external threat),
    - attacks occurring between NFV components (migration of an attack).
2. **Impact is organised into three categories:**
    - **Denial of Service**: attacks that cause service outages. Examples include hardware vandalism, radio signal jamming, and traffic flooding.
    - **Access Breach**: attacks that lead to unauthorised system access, manipulation, or a data breach. Examples include malicious changes to system configurations, exploiting software vulnerabilities, communications hijacking and disclosure of sensitive data.
    - **Integrity Compromise**: attacks that impact the integrity of infrastructure through hardware, software, communications or operational tampering. Examples include implanting malicious hardware components in system devices, altering operating system code, modifying data, and circumventing organisational security policies.

Figure 15 shows the three attack sources categories with their associated attacks and Table 15 shows the impact of each attack.

Figure 15: Attack taxonomy

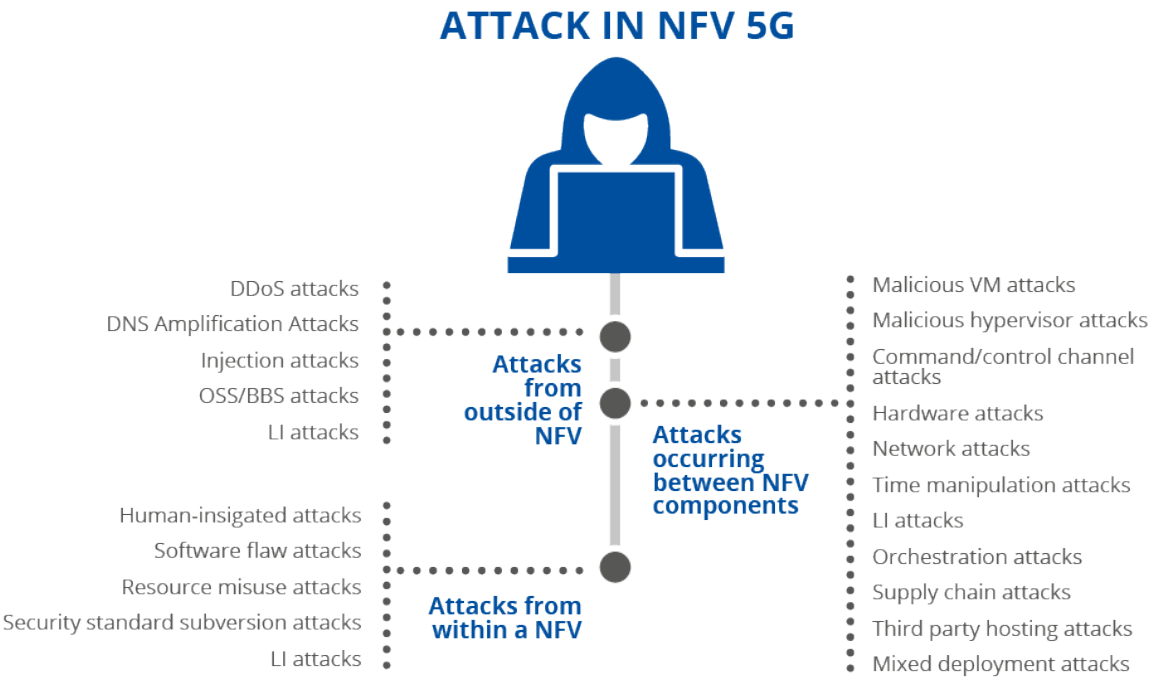


Table 15: Impact of attacks

ID	Categories	Attacks	Impacts
ATT1	Attacks from within an NFV	Human-instigated attacks	Access breach
ATT2		Software flaw attacks	Access breach, denial of service, integrity compromise
ATT3		Resource misuse attacks	Access breach, denial of service, integrity compromise
ATT4		Security standard subversion attacks	Access breach, integrity compromise
ATT5		LI attacks	Access breach, integrity compromise
ATT6	Attacks from outside an NFV	DDoS attacks	Denial of service
ATT7		DNS Amplification attacks	Denial of service
ATT8		Injection attacks	Access breach, denial of service, integrity compromise
ATT9		OSS/BSS attacks	Access breach, denial of service, integrity compromise
ATT10		LI attacks	Access breach, integrity compromise
ATT11	Attacks occurring between NFV components	Malicious VM or container attacks	Access breach, denial of service, integrity compromise
ATT12		Malicious hypervisor or CIS attacks	Access breach, integrity compromise
ATT13		Command/control channel attacks	Access breach
ATT14		Hardware attacks	Access breach, Integrity compromise
ATT15		Network attacks	Access breach, denial of service, integrity compromise
ATT16		Time manipulation attacks	Denial of service, integrity compromise
ATT17		LI attacks	Access breach, integrity compromise
ATT18		Orchestration attacks	Access breach, denial of service, integrity compromise
ATT19		Supply chain attacks	Access breach, denial of service, integrity compromise
ATT20		Third party hosting attacks	Access breach, denial of service, integrity compromise
ATT21		Mixed deployment attacks	Access breach, denial of service, integrity compromise

4. 5G NFV SECURITY BEST PRACTICES

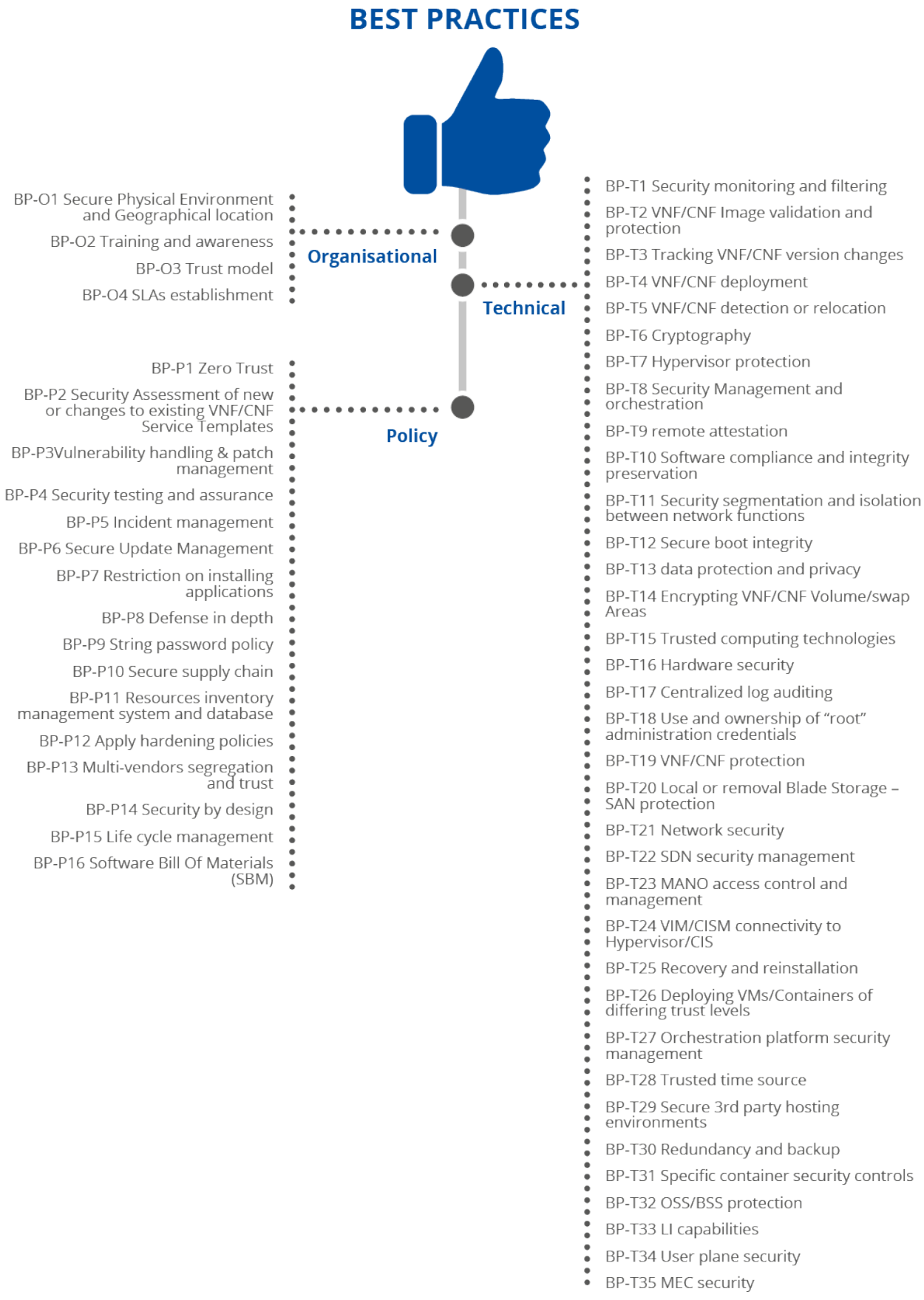
4.1 CATEGORISATION OF SECURITY MEASURES

The development of security measures and best practices is one of the major objectives of this study in order to help mitigate the challenges identified, thus improving 5G NFV security.

A list of security measures and best practices has been established by analysing relevant documents and standards identified during desktop research. This analysis allowed the identification of frequently mentioned topics regarding NFV security and their classifications into different security domains. The resulting list is grouped into three main categories, namely policies, organisational and technical practices (see Figure 16). The full register of best practices with references are provided in Annex E.

The mapping between categories of challenges, vulnerabilities, attacks, affected assets and best practices is provided in section 4.4.

Figure 16: List of best practices



4.1.1 Technical

In this section, we shed light on technical best security practices that should be followed in order to achieve better security protection in a 5G NFV environment against the challenges identified above. Table 16 highlights thirty-five technical measures and best practices. They are detailed in Annex E.

Table 16: Technical best practices

ID	Best Practice title	Best Practice description
BP-T1	Security monitoring and filtering	This covers the use of virtual network security appliances such as anti-virus, virtual firewalls or virtual IDS/IPS to achieve a level of security comparable to traditional networks. Further, machine learning (ML) assisted solutions can be used to detect attack traffic (e.g. DoS attacks) and distinguish it from normal traffic, so that it can be handled appropriately.
BP-T2	VNF image validation and protection	A mechanism should be provided to verify all VNF before they are installed on the orchestration platform or other vendor specific deployment platform.
BP-T3	Tracking VNF version changes	The orchestration and VNF management systems should have the ability to keep track of multiple versions, multiple environments, multiple instances and allow the service provider's team to perform updates or upgrades with clear expectations of service continuity based on metadata information including component dependencies.
BP-T4	VNF deployment	New VNF components must only be deployed into a production network where security policies have been tested and applied, and where appropriate hardening measures have been taken to ensure that unused ports, unrequired services, and insecure protocols have been disabled.
BP-T5	VNF deletion or relocation	The orchestration platform should manage VNF deletion or relocation in a secure way. Security mechanisms such us secure backup, storage, destruction, and isolation of sensitive data must be applied.
BP-T6	Cryptography	Well-known, standardised and secure cryptographic schemes and protocols (e.g. NIST56, ANSSI57, BSI58) shall be used for the cryptographic operations and the key management process. Proprietary schemes and protocols must be avoided.
BP-T7	Hypervisor protection	The hypervisor shall enforce the network security policies regarding the isolation between VNFs, memory access control, protection of sensitive data, etc. The hypervisor enables virtualisation between underlying hardware and VMs. Security of the hypervisor is a must in order to protect the whole virtualisation infrastructure. One of the best security practices is to keep the hypervisor up to date by regularly applying security patches as they are released. Failure to do so would result in exposure to security risks. Another best practice is to disable all services that are not in use. For example, remote access services may not be needed all the time and therefore it would be a good idea to enable these services only when they are required. Administrators are the gatekeepers of the whole infrastructure and their accounts are the keys. It should be mandated that admin accounts should be secured through the application of a strong password policy along with strict adherence to an organisation's security guidelines.
BP-T8	Security management and orchestration	NFV management and orchestration operations must be made secure, especially the lifecycle management of VNF workloads.
BP-T9	Remote attestation	Today's deployed NFV systems face a huge number of threats that have the capability to compromise them partly or fully. In many cases this involves an attacker modifying a system in such a way that malicious software is executed. Execution of code that was not intended to be executed on the system is expected to be detectable. One defensive measure that addresses the execution of malicious software is remote attestation (RA) as described in ETSI GR NFV-SEC 018[59]. The remote attestation technique should be used to remotely verify the trust status of a NFV platform.
BP-T10	Software compliance and integrity preservation	Mechanisms for checking integrity must be used to verify software, firmware, and information integrity within the NFV.

[56] https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines
[57] https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/liste-des-documents-constitutifs-du-rgs-v-2-0/
[58] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html
[59] https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/018/01.01.01_60/gr_NFV-SEC018v010101p.pdf

ID	Best Practice title	Best Practice description
BP-T11	Security segmentation and isolation between network functions	The security zoning concept (or segmentation) should be used to divide 5G networks horizontally and vertically into portions in which different security controls can be applied. Security zoning enables the application-specific customisation of security services. A zone could, for instance, provide its own AAA (Authentication, Authorisation, Accountability) and security monitoring functionalities. Consequently, different segments have different security or trust levels, i.e. can be trusted to address different security risks.
BP-T12	Secure boot integrity	The NFV platform shall support a secure boot from hardware to VNFs to prevent tampering during the system boot and integrity check on the sensitive NFV software files and running code to prevent tampering at runtime, enhancing the protection of system integrity.
BP-T13	Data protection and privacy	To prevent disclosure of user data (e.g. subscriber identifiers), 5G networks should use security mechanisms such as the encryption cryptographic operation. It is important to pay attention to the requirements of lawful interception[60]. Privacy and security, both of individuals' personal data and of critical infrastructure, are important preconditions for GDPR. Encryption is a crucial tool to achieve these goals. Any approach to weaken or grant backdoor access to encryption methods defeats the entire purpose of encryption and undermines users' trust, exposing 5G systems to increased risks. At the same time, it remains vitally important that companies and law enforcement authorities continue to work together, ensuring that authorities have the best methods and access to electronic evidence without weakening or putting strong encryption at risk.
BP-T14	Encrypting VNF volume/swap areas	Virtual volume disks associated with VNFs may contain sensitive data. Therefore, they need to be protected.
BP-T15	Trusted computing technologies	NFV requires trusted computing technologies for ensuring secure root of trust, remote attestation[61], integrity monitoring, and secure storage. Such trusted computing technologies include Intel TXT, SGX, AMD SEV or ARM Trustzone silicon-based security functionality implemented with a TPM that stores measurements of the entire hypervisor stack and boot process.
BP-T16	Hardware security	Dedicated hardware should be used to ensure strong isolation (e.g. physical separation) between tenants. In addition, hardware security devices should be used to ensure a secure boot, integrity check, secure storage and trusted execution environment.
BP-T17	Centralised log auditing	All the NFV, SDN and MANO elements should submit information on security events to a centralised platform, which shall monitor and analyse the logs in real time for possible attempts at intrusion.
BP-T18	Use and ownership of 'root' administration credentials	NFV components should be configured to support multiple administration roles. As a minimum there shall be an admin role (highest privilege) and a separate operational role with minimal privileges to complete normal operational support.
BP-T19	VNF protection	VNF data protection shall be enforced at rest and in transit.
BP-T20	Local or removal blade storage – SAN protection	If local, non-volatile, fixed or removable storage is used to support a VNF then it should not store sensitive data. SAN should be protected by a mutual authentication process, hard zoning, data protection at rest and in transit, etc.
BP-T21	Network security	• All internal interfaces between VNF elements, supporting MANO platforms and IT elements (mediation, provisioning) that are not required to communicate publicly outside the operators network, should use private IP addresses. • Each VM or container supporting VNFs should have a predefined network security profile. • Separate physical interfaces should be implemented for traffic segregation. • All connectivity between internal NFV components and the external world should pass through a firewall (or vFirewall). • Communication should be monitored, and security events should be recorded in audit logs. • Rules governing segmentation and zoning security should be followed with the use of firewalls, IDS/IPS or other controls. • VPNs should be created between VNFs and both internal and external non-VNF environments. • Patch management is important to fix vulnerabilities on network security devices (e.g. firewall, VPN, IDS/IPS) to keep them up-to-date and running smoothly. • The management of all operational traffic and interfaces should be protected by integrity mechanisms and encryption. Unprotected sessions should not be accepted.

[60] https://www.digitaleurope.org/wp/wp-content/uploads/2020/03/DIGITALEUROPE-Position-on-Encryption-Policy-.pdf
[61] https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/018/01.01.01_60/gr_NFV-SEC018v010101p.pdf

ID	Best Practice title	Best Practice description
BP-T22	SDN security management	Communication between SDN elements should support a strong identity framework to uniquely identify all components and users of a SDN system and verify identities with a trusted source. Without a strong identity framework, the ability to build effective authentication, authorisation and accounting implementations will be limited. A strong identity should have the following properties: • ability to distinguish its owner from other entities within a pre-defined scope, • ability to be generated, updated and revoked, • prevention of impersonation, preferably through strong cryptographic mechanisms. Analysis of the SDN architecture identifies numerous means for elements inside the system's trust boundary to compromise the availability of the logically centralised control. Strong authentication based on assured identity and access control mechanisms with various privilege levels should be employed to authorise external parties and authenticate their access to the system, e.g. role-based access control.
BP-T23	MANO access control and management	The common aspects for RESTful NFV MANO APIs have been defined in ETSI GS NFV-SOL 013[62]. NFV MANO APIs, applications and their supporting platforms (OS, Database) should have comprehensive user access controls and privileged access management. NFV-MANO APIs shall only allow themselves to be accessed by authorised users. One solution for authorising access is the use of OAuth2.0 with access token as described in ETSI GS NFV-SEC 022[63].
BP-T24	VIM connectivity to virtualisation layer	The connectivity between the VIM and the virtualisation layer should support a secure access protocol.
BP-T25	Recovery and reinstallation	A fast recovery and reinstallation process shall be in place to ensure high availability of the sensitive NFV components and resources. The recovery process should be clearly documented, reviewed at regular intervals for updates and made available to all the staff concerned.
BP-T26	Deploying VMs/Containers of differing trust levels	The VIM should be configured to ensure that VMs or containers of differing trust levels are not deployed on the same physical host.
BP-T27	Orchestration platform Security Management	The orchestration platform sits over the NFV environment and allows the management and deployment of VNFs across the whole NFV environment. Security controls should be implemented to protect this critical platform such as strong authentication, access control rules, information flow controls, audit logs, etc. The orchestration platform should support security monitoring and patch management processes to provide continuous security updates.
BP-T28	Trusted time source	The system should provide a protected and trusted network time source to the NFV components such as GPS or an atomic clock[64].
BP-T29	Secure 3rd party hosting environments	Sensitive information of VNFs shall be confidentially protected by operators when using a 3rd party environment (e.g. NFVI).
BP-T30	Redundancy and backup	The NFV platform should support redundancy and backup protection to improve reliability and ensure the availability and integrity of 5G NFV data, components, applications, and services.
BP-T31	Specific container security controls	• Appropriate restrictions on container placement and on the use of container caching should be applied. • A security policy that restricts the placement and co-existence of containers belonging to different trust domains should be defined and implemented. • A security policy which restricts which sub-functions within an NF, which has been implemented using containers, may be cached within the general unencrypted container cache or which requires security protection mechanisms for sensitive containers at rest within the cache to be defined and implemented.
BP-T32	OSS/BSS protection	There should be a sharing of responsibility between the traditional OSS and the newly deployed SDN controllers and NFV orchestration. The OSS will manage the relatively static configuration parameters and limit overall resources assigned to sub-networks or services. The SDN controller and NFV orchestration platforms will then dynamically manage these network resources to apply policy-based services in real-time to individual traffic flows.

[62] https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/013/03.05.01_60/gs_NFV-SOL013v030501p.pdf
[63] https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/022/02.08.01_60/gs_NFV-SEC022v020801p.pdf
[64] https://serverfault.com/questions/622094/what-is-an-acceptable-secure-time-source-in-a-datacentre-environment

ID	Best Practice title	Best Practice description
BP-T33	LI capabilities	LI capabilities should be consistent with 3GPP and ETSI specifications [65] [66] [67] [68] [69] on Lawful Interception. They cover all necessary aspects in a 5G context: requirements, architecture and functions, protocol, and procedures.
BP-T34	User plane security	While firewalls at trust boundaries provide some defence against attacks by limiting communication between trusted entities to only permitted IP addresses using only valid protocols on allowed ports, additional security controls are needed on the user plane to effectively mitigate DDoS, botnet attacks, and malware infections. Network-based security functions such as firewalls, volumetric DDoS protection, antibot net, anti-virus, and web filtering can be deployed on the user plane to provide end-to-end protection[70].
BP-T35	MEC security	MEC is designed to support various use cases such as video analytics, location services, Internet of Things (IoT), augmented reality (AR), optimised distribution of local content, data caching, and more. The MEC system should provide a secure environment for running services for the various actors involved such as user, network operator, third-party application provider, application developer, content provider and platform vendor. MEC security relies on specifications provided by recognised bodies to address specific aspects, especially ETSI ISG NFV for infrastructure virtualisation and management, the Trusted Computing Group (TCG) for physical platform security, and IETF specifications for securing access to MEC services. Furthermore, 3GPP TR 33.848 [47] is investigating the security consequences of virtualisation of 3GPP NFs. This 3GPP report is applicable to many MEC use cases where the need for additional security controls is higher than in core network datacentre implemented network functions. It is expected to result in additional ETSI NFV security requirements that can be utilised for MEC. Moreover, security assurance is an important topic which is beginning to be required by regulators for 5G infrastructure components such as MEC. While the traditional common criteria technology (ISO 15408) remains a global reference for security assessment, tailored schemes that address the specific constraints of 5G ecosystems, such as GSMA NESAS, are expected to play an important role in this respect.

4.1.2 Policy

This second category of security measures encompasses the various policies and procedures to be established to ensure an appropriate level of cybersecurity. The following 16 technical policy measures and best practices have been identified (see Table 17 and a detailed description in Annex E).

Table 17: Policy best practices

ID	Best Practice title	Best Practice description
BP-P1	Zero Trust	5G NFV deployments should build on mature cybersecurity standards employed in enterprise and cloud environments. Examples include the NIST Cybersecurity Framework and ISO Information Security Management System series[71], the ETSI GS NFV-SEC 003[72] Security and Trust Guidance and the UK NCSC Zero Trust Architecture Design Principles[73]. Zero Trust represents an overarching access security model that deliberately avoids assuming implicit trust between elements in a network. This is particularly important in 5G as various external stakeholders may need to access infrastructure components or services for management, maintenance, or monitoring purposes[74] [75].

[65] https://www.etsi.org/deliver/etsi_ts/133100_133199/133127/15.00.00_60/ts_133127v150000p.pdf
[66] https://www.etsi.org/deliver/etsi_ts/133100_133199/133126/15.00.00_60/ts_133126v150000p.pdf
[67] https://www.etsi.org/deliver/etsi_ts/133100_133199/133128/15.00.00_60/ts_133128v150000p.pdf
[68] https://www.etsi.org/deliver/etsi_ts/133100_133199/133108/12.08.00_60/ts_133108v120800p.pdf
[69] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2266
[70] https://www.ericsson.com/4a49ce/assets/local/reports-papers/further-insights/doc/02092021-12911-security-considerations-for-cloud-ran-6-edits.pdf
[71] https://csrc.nist.gov/publications/detail/sp/800-207/final
[72] https://www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/003/01.01.01_60/gs_nfv-sec003v010101p.pdf
[73] https://www.ncsc.gov.uk/collection/zero-trust-architecture/introduction-to-zero-trust
[74] https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g
[75] https://www.ericsson.com/4a49ce/assets/local/reports-papers/further-insights/doc/02092021-12911-security-considerations-for-cloud-ran-6-edits.pdf

BP-P2	Security assessment of new or changes to existing VNF service templates	New or modified VNF service templates should be validated through proper risk assessment by a security professional.
BP-P3	Vulnerability handling & patch management	NFV and MANO software components will need to be monitored for vulnerabilities and patched as quickly as possible to address evolving risks and ensure security and functionality.
BP-P4	Security testing and assurance	Regular penetration and vulnerability testing should be performed across the NFVi and MANO production environment to identify any vulnerabilities (e.g. OSs, hypervisor, CIS, VMs or containers) or compromise of the network zoning rules. 5G stakeholders should also leverage internationally recognised product testing, assurance, and certification regimes. Potential solutions to these requirements include, among others, the Network Equipment Security Assurance Scheme (NESAS)[76], jointly defined by 3GPP and GSMA, and the ENISA EUCC[77], EUCS[78] schemes.
BP-P5	Incident management	An incident detecting and handling process should be established to support incident response and restoration activities.
BP-P6	Secure update management	An update management process is required for introducing a new component or a software or hardware change into the 5G system. Continuous integration and testing tools make the patching process efficient and reduce the prolonged risk of exposure. NFV and MANO must support reactive and proactive security monitoring and patch management to provide continuous security updates.
BP-P7	Restriction on installing applications	It should not be possible to install a VNF application into the operational NFV environment without validation and approval by the operator.
BP-P8	Defence-in-depth	Security must be implemented for the hardware, virtualisation, VNF, MANO and application layers. Multilayer, defence-in-depth security with protective mechanisms must be present.
BP-P9	Strong password policy	It should be mandated that all user accounts accessing the NFV/MANO system be secured by the application of a strong password policy. Securing NFV/MANO passwords requires implementing and enforcing a password policy that includes: • strong passwords for every account • the use of a password manager • two-factor authentication (2FA) • role-based access control (RBAC) • privileged access management (PAM) for the most sensitive NFV/MANO components.
BP-P10	Secure supply chain	Large elements of the supply chain are outside the direct control of the operator, and thus operators should seek to impose obligations onto the supply chain to enhance security of the NFV.
BP-P11	Resources inventory management system and database	An inventory management system must account for all the physical elements, open source and NFV software components that the operator owns on premises and in the cloud. In addition, the resource inventory database should be protected by security controls. Inventories should be reviewed and updated at regular intervals.
BP-P12	Apply hardening policies	NFV, MANO and SDN components should be submitted to a continuous or repetitive hardening process to ensure that known vulnerabilities are identified and addressed.
BP-P13	Multi-vendors segregation and trust	Multi-vendor segregation should be applied to ensure each vendor can only manage or impact its own resources. In addition, trust vendors of NFV components should be selected. A security SLA should also be established between the operator and vendors to define the security level that they must meet.
BP-P14	Security-by-design	The security-by-design principle is to be followed in order to inspire trust in end users. This requirement highlights the need to consider security aspects from the very beginning of the development of a 5G system, throughout the supply chain, and over the whole lifecycle of 5G components.

[76] https://www.gsma.com/security/network-equipment-security-assurance-scheme/
[77] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1
[78] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

BP-P15	Lifecycle management	The security posture of a NFV deployment must consider that cloud-based networks are dynamic and that threats are constantly evolving. Lifecycle management (LCM) will become more complex in a NFV environment and will require automated management and orchestration functions[79]. Containers inherently provide software modularity and decomposition, which allow for independent LCM following DevOps principles and continuous integration and continuous delivery (CI/CD). The NIST secure software development framework (SSDF)[80] and DevSecOps project[81] for cloud-native applications integrate security into the DevOps process, reducing vulnerabilities, mitigating the potential impacts of vulnerabilities, and preventing the recurrence of vulnerabilities.
BP-P16	Software bill Of materials (SBOM)	Vendors of 5G NFV software components should include a SBOM with the software package. The generated SBOM should follow the NTIA guidelines and be in a machine-readable format such as SPDX[82], or CycloneDX[83].

4.1.3 Organisational

Organisational best practices are of the utmost importance to ensure 5G NFV security. In what follows, four organisational rules and best practices are introduced in Table 18 and detailed in Annex E.

Table 18: Organisational best practices

ID	Best Practice title	Best Practice description
BP-O1	Secure physical environment and geographical location	Security is not just about encrypting data streams but also about the physical deployment of equipment. NFV devices and equipment location, type of equipment, and type of services running on the equipment are all parts of the complete system and must be protected in a secure physical environment.
BP-O2	Training and awareness	The following activities should be considered: • information sharing between different 5G actors; • adopting a holistic approach to security training and awareness among the employees, including employees at all levels of the organisation; • ensuring that security training is continuous, regular and frequently updated.
BP-O3	Trust model	A trust model of relationships among various 5G stakeholders should be built and be able to answer questions such as: 'for what one does on trust?', 'How much should one trust?' and 'How much anyone can trust?'.
BP-O4	SLAs establishment	SLAs established between 5G stakeholders should include important security and compliance measures. In this respect, SLAs are like an insurance policy for the 5G network services. SLAs set the expectations for the performance of a service provider and for the security level. They also establish penalties for missing targets. In that concept, NFV could not leave unaffected the evolution of SLA models and their flexibility in adapting to more demanding parameters. An SLA management framework should be defined in order to fill the gap between 5G stakeholders.

4.2 SECURITY REQUIREMENTS AND MEASURES OF THE EECC

Article 40 and Article 41 of the EECC define security requirements and measures as technical and organisational measures for managing the risks posed to the security of networks and services. ENISA guidance[84] [85] on security measures under the EECC are guidelines on security measures addressed to competent authorities concerning the technical details of implementing Articles 40 and 41 of the EECC: how to ensure that providers assess risks and take appropriate security measures.

These guidelines list twenty-nine high-level security objectives, which are grouped in eight security domains. For each security objective they list specific detailed security measures which could be taken by providers to reach that particular security objective. Those security measures

[79] https://www.ericsson.com/4a49ce/assets/local/reports-papers/further-insights/doc/02092021-12911-security-considerations-for-cloud-ran-6-edits.pdf
[80] https://csrc.nist.gov/Projects/ssdf
[81] https://csrc.nist.gov/Projects/devsecops
[82] https://spdx.github.io/spdx-spec/
[83] https://cyclonedx.org
[84] https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc
[85] https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc

are technology neutral. They should be applicable to a wide range of different types of technologies including NFV in 5G.

4.3 OTHER RELEVANT SECURITY HARDENING GUIDANCE

For additional security hardening guidance, see among others:

- ENISA - Security aspects of virtualisation focusing on virtualisation security[86].
- NIS cooperation group security measures for OES providing technical and organisational security measures to manage risks posed to the security of NIS (Network and Information Systems)[87]. Moreover, ENISA released a mapping of security measures for OESs to international standards used by operators in particular business sectors, namely energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructures[88].
- CISA's Security Guidance for 5G Cloud Infrastructures:
    - Part I: Prevent and Detect Lateral Movement[89]: detect malicious cyber actor activity in 5G clouds and prevent actors from leveraging the compromise of a single cloud resource to compromise the entire network;
    - Part II: Securely Isolate Network Resources[90]: ensure that there is secure isolation among customer resources with emphasis on securing the container stack that supports the running of virtual network functions;
    - Part III: Data Protection[91]: ensure that network and customer data is secured during all phases of the data lifecycle (at rest, in transit, while being processed, upon destruction);
    - Part IV: Ensure Integrity of Cloud Infrastructure[92]: ensure that 5G cloud resources (e.g. container images, templates, configuration) are not modified without authorisation.
- ETSI ISG NFV specifications:
    - Published specifications:
        - ETSI GR NFV-SEC 005: 'Network Functions Virtualisation (NFV); Trust; Report on Certificate Management';
        - ETSI GR NFV-SEC 018: 'Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture';
        - ETSI GS NFV-SEC 022: 'Network Functions Virtualisation (NFV) Release 2; Security; Access Token Specification for API Access'.
    - Draft Specifications (work in progress):
        - Draft ETSI GR NFV-SEC 016: 'Network Functions Virtualisation (NFV); Location, locstamp and timestamp; Report on location, timestamping VNFs';
        - Draft ETSI GS NFV-SEC 023: 'Network Functions Virtualisation (NFV) Release 4; Security; Container Security Spec';
        - Draft ETSI GS NFV-SEC 024: 'Network Functions Virtualisation (NFV) Release 4; Security; Security Management';
        - Draft ETSI GS NFV-SEC 025: 'Network Functions Virtualisation (NFV) Release 4; Security; Secure E2E VNF & NS management';
        - Draft ETSI GS NFV-SEC 026: 'Network Functions Virtualisation (NFV) Release 4; Security; Isolation and trust domain'
        - Draft ETSI GR NFV-SEC 027: 'Network Functions Virtualisation (NFV) Release 4; Security; Report on security assurance of NFVI'.

[86] https://www.enisa.europa.eu/publications/security-aspects-of-virtualization
[87] https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf
[88] https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services
[89] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_I_508_Compliant.pdf
[90] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_II_Updated_508_Compliant.pdf
[91] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_III_508_Compliant.pdf
[92] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_IV_508_Compliant.pdf

4.4 CHALLENGES, VULNERABILITIES, ATTACKS AND BEST PRACTICES

This section describes the high-level interrelations, at the category level, between the categories of challenges, the categories of vulnerabilities, attacks, affected assets and best practices for addressing those challenges. The detailed matrix showing the link between a challenge and its associated vulnerabilities, attacks, affected assets and best practices is provided in Annex F.

Challenges categories	Vulnerabilities categories	Attacks	Affected Assets	Best practices
Virtualisation/ containerisation	• Service-based vulnerabilities of NFV components • Improper protection of data and information of NFV components • Virtualisation layer vulnerabilities • Vulnerable mechanisms for authentication and authorisation of NFV components • Insufficient or improper monitoring mechanisms of NFV • Improper protection of service based Interfaces • Vulnerabilities in implementation of 5G network security functionalities • Improper protection of data and information of 5G NFs • Improper protection of availability and integrity of 5G NFs • Vulnerable mechanisms for authentication and authorisation of 5G NFs • Improper session protection mechanisms of 5G NFs • Insufficient or improper monitoring mechanisms of 5G NFs • Vulnerabilities in operating systems supporting 5G NFs • Improper hardening of 5G core components • Vulnerabilities in implementation of SDN functionalities • SBA/SBI vulnerabilities of SDN components • Vulnerable mechanisms for authentication and authorisation of SDN components • Improper hardening of SDN components • Insufficient or improper monitoring mechanisms of SDN components • Virtualisation vulnerabilities of relevant SDN components • Physical and environmental vulnerabilities of relevant SDN components • Vulnerabilities in implementation of MEC security functionalities • SBA/SBI vulnerabilities of MEC components • Improper protection of data and information • Virtualisation vulnerabilities of relevant MEC components • Improper hardening of MEC Components • MEC application vulnerabilities • Vulnerabilities of the MEC virtualisation platform • Physical and environmental vulnerabilities of relevant MEC components	• Human-instigated attacks • Software flaw attacks • Resource misuse attacks • Security standard subversion attacks • LI attacks • DDoS attacks • DNS Amplification attacks • Injection attacks • OSS/BSS attacks • Malicious VM or container attacks • Malicious hypervisor or CIS attacks • Command and control channel attacks • Hardware attacks • Network attacks • Time manipulation attacks • Orchestration attacks • Supply chain attacks • Third party hosting attacks	NFVI; NFV MANO; VNF; VNFM; VIM/CISM; Ve-Vnfm-em; Ve-Vnfm-vnf; Os-Ma-nfvo; Control plane UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF; SM Application data traffic MEC Host 3GPP SA6 interfaces; ETSI MEC interfaces; Application data traffic; MEC platform; Customer facing service (CFS) portal; MEC applications; Edge Application Server (EAS) Virtualisation infrastructure	BP-T1 - Security monitoring and filtering BP-T2 – VNF image validation and protection BP-T3 - Tracking VNF version changes BP-T4 - VNF deployment BP-T5 - VNF deletion or relocation BP-T6 - Cryptography BP-T7 - Hypervisor protection BP-T9 - Remote attestation BP-T10 - Software compliance and integrity preservation BP-T11 - Security segmentation and isolation between network functions BP-T12 - Secure boot integrity BP-T13 - Data protection and privacy BP-T14 - Encrypting VNF volume or swap areas BP-T15 - Trusted computing technologies BP-T16 - Hardware security BP-T17 - Centralised log auditing BP-T19 – VNF protection BP-T20 - Local or removal blade storage- SAN protection BP-T21 - Network security BP-T22 - SDN security management BP-T26 - Deploying VMs or containers of differing trust levels BP-T28 - Trusted time source BP-T29 - Secure third party hosting environments BP-T30 - Redundancy and backup BP-T31 - Specific container security controls BP-T34 - User plane security BP-T35 - MEC security

	• Vulnerable mechanisms for authentication and authorisation of MEC components • Insufficient or improper monitoring mechanisms of MEC components		LCM Proxy; MEC orchestrator SDN controller Northbound interface; Southbound interface; Eastbound-Westbound interface SDN application; SDN resources SDN infrastructure layer	BP-P1 - Zero trust BP-P7 - Restriction on installing applications BP-P8 - Defence-in-depth BP-P9 - Strong password policy BP-P12 - Apply hardening policies BP-P13 - Multi-vendors segregation and trust BP-P14 - Security-by-design BP-O1 - Secure physical environment and geographical location BP-O3 - Trust model BP-O4 - SLAs establishment
Orchestration and management	• Service-based vulnerabilities of NFV components • Improper protection of data and information of NFV components • Improper hardening of NFV components • Virtualisation layer vulnerabilities • Vulnerable mechanisms for authentication and authorisation of NFV components • Insufficient or improper monitoring mechanisms of NFV • Vulnerabilities due to legacy OSS/BSS systems • Improper protection of service based interfaces • Vulnerabilities in implementation of 5G network security functionalities • Improper protection of data and information of 5G NFs • Improper protection of availability and integrity of 5G NFs • Vulnerable mechanisms for authentication and authorisation of 5G NFs • Improper session protection mechanisms of 5G NFs • Insufficient or improper monitoring mechanisms of 5G NFs • Vulnerabilities in operating systems supporting 5G NFs • Improper hardening of 5G core components	• Human-instigated attacks • Software flaw attacks • Resource misuse attacks • LI attacks • DNS Amplification attacks • Injection attacks • OSS/BSS attacks • Malicious VM or container attacks • Malicious hypervisor or CIS attacks • Network attacks • Orchestration attacks	NFV MANO; VNF; NFVI; VNFM; VIM/CISM; Ve-Vnfm-em; Ve-Vnfm-vnf UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF OSS/BSS systems	BP-T2 – VNF image validation and protection BP-T4 – VNF deployment BP-T5 – VNF deletion or relocation BP-T6 – Cryptography BP-T8 - Security management and orchestration BP-T10 - Software compliance and integrity preservation BP-T23 - MANO access control and management BP-T27 - Orchestration platform security management BP-P11 - Resource inventory management system and database BP-P14 - Security-by-design
Administration and access control	• Service-based vulnerabilities of NFV components • Improper protection of data and information of NFV components • Virtualisation layer vulnerabilities • Vulnerable mechanisms for authentication and authorisation of NFV components • Improper protection of service based interfaces	• Human-instigated attacks • DNS Amplification attacks • OSS/BSS attacks • Malicious VM or container attacks	NFV MANO, NFVI; VNFM; VNF; VIM/CISM; Ve-Vnfm-em; Ve-Vnfm-vnf UPF/User data;	BP-T1 - Security monitoring and filtering BP-T2 – VNF image validation and protection BP-T7 - Hypervisor protection BP-T8 - Security management and orchestration BP-T9 - Remote attestation

	• Vulnerabilities in implementation of 5G network security functionalities • Improper protection of data and information of 5G NFs • Improper protection of availability and integrity of 5G NFs • Vulnerable mechanisms for authentication and authorisation of 5G NFs • Improper session protection mechanisms of 5G NFs • Insufficient or improper monitoring mechanisms of 5G NFs • Vulnerabilities in operating systems supporting 5G NFs • Improper hardening of 5G core components	• Malicious hypervisor or CIS attacks • Command and control channel attacks • Network attacks	UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	BP-T18 - Use and ownership of 'root' administration credentials BP-T23 - MANO access control and management BP-T24 - VIM connectivity to virtualisation layer BP-T27 - Orchestration platform security management BP-P1 - Zero trust BP-P9 - Strong password policy BP-O2 - Training and awareness
New and legacy technologies	• Service-based vulnerabilities of NFV components • Virtualisation layer vulnerabilities • Vulnerabilities due to legacy OSS/BSS systems	• OSS/BSS attacks • Hardware attacks • Mixed deployment attacks	Control plane; NFVI; OSS/BSS systems	BP-T16 - Hardware security BP-T25 - Recovery and reinstallation BP-T30 - Redundancy and backup BP-T32 - OSS/BSS protection BP-P5 - Incident management BP-P8 - Defence-in-depth BP-P12 - Apply hardening policies BP-P14 - Security-by-design BP-O3 - Trust model BP-O4 - SLAs establishment
Adoption of open source/COTS	• Improper hardening of NFV components • Virtualisation layer vulnerabilities • Improper protection of service based interfaces • Vulnerabilities in implementation of 5G network security functionalities • Improper protection of data and information of 5G NFs • Improper protection of availability and integrity of 5G NFs • Vulnerable mechanisms for authentication and authorisation of 5G NFs • Improper session protection mechanisms of 5G NFs • Insufficient or improper monitoring mechanisms of 5G NFs • Vulnerabilities in operating systems supporting 5G NFs • Improper hardening of 5G core components	• Software flaw attacks • Injection attacks • Hardware attacks • Third party hosting attacks	VNF; NFVI UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	BP-T29 - Secure third party hosting environments BP-P2 - Security assessment of new or changes to existing VNF service templates BP-P3 - Vulnerability handling and patch management BP-P5 - Incident management BP-P6 - Secure update management BP-P12 - Apply hardening policies BP-P15 - Lifecycle management BP-P16 - Software bill of materials (SBOM) BP-O3 - Trust model BP-O4 - SLAs establishment
Supply chain	• Service-based vulnerabilities of NFV components • Improper hardening of NFV components • Virtualisation layer vulnerabilities • Vulnerable mechanisms for authentication and authorisation of NFV components • Improper protection of service-based interfaces • Vulnerabilities in implementation of 5G network security functionalities	Supply chain attacks	Hardware platform Os-Ma-nfvo; NFV-MANO; VNF; NFVI UPF/User data; UPF/Signallin	BP-T25 - Recovery and reinstallation BP-T29 - Secure third party hosting environments BP-P1 - Zero trust BP-P2 - Security assessment of new or changes to existing VNF service templates

	• Improper protection of data and information of 5G NFs • Improper protection of availability and integrity of 5G NFs • Vulnerable mechanisms for authentication and authorisation of 5G NFs • Improper session protection mechanisms of 5G NFs • Insufficient or improper monitoring mechanisms of 5G NFs • Vulnerabilities in operating systems supporting 5G NFs • Improper hardening of 5G core components		g data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	BP-P3 - Vulnerability handling and patch management BP-P4 - Security testing and assurance BP-P5 - Incident management BP-P6 - Secure update management BP-P8 - Defence-in-depth BP-P10 - Secure supply chain BP-P15 - Lifecycle management BP-P16 - Software bill of materials (SBOM) BP-O3 - Trust model BP-O4 - SLAs establishment
Lawful interception (LI)	• Service-based vulnerabilities of NFV components • Improper protection of data and information of NFV components • Improper hardening of NFV components • Virtualisation layer vulnerabilities • Vulnerable mechanisms for authentication and authorisation of NFV components • Vulnerabilities due to legacy OSS/BSS systems • Improper protection of service-based interfaces • Vulnerabilities in implementation of 5G network security functionalities • Improper protection of data and information of 5G NFs • Improper protection of availability and integrity of 5G NFs • Vulnerable mechanisms for authentication and authorisation of 5G NFs • Improper session protection mechanisms of 5G NFs • Insufficient or improper monitoring mechanisms of 5G NFs • Vulnerabilities in operating systems supporting 5G NFs • Improper hardening of 5G core components	LI attacks	VNF; NFV MANO; NFVI; VNFM; Ve-Vnfm-em; Ve-Vnfm-vnf SM Control plane UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF OSS/BSS systems	BP-T6 – Cryptography BP-T15 - Trusted computing technologies BP-T33 - LI capabilities BP-P5 - Incident management BP-P8 - Defence-in-depth BP-P12 - Apply hardening policies BP-P14 – Security-by-design

5. OPEN AND FUTURE SECURITY CHALLENGES

Although many solutions have been proposed to overcome the security challenges in NFV, many potential security challenges remain. Table 19 illustrates some of the research challenges and future directions for NFV security.

Table 19: Open and future security challenges

Challenge	Challenge description	References
Encrypted data processing	The risks of being able to capture encrypted data in an unencrypted form due to processing of that data increases significantly. If that processing is highly sensitive (e.g. AUC (authentication centre) or LI functions) then the risk may not be acceptable.	[47]
Performance degradation	To truly understand performance, we must simulate growth in network usage. If overall loads grow by 50%, how will VNF performance be impacted? And if all the load is centred on one type or pattern of traffic or usage vs multiple types? What is the expected performance degradation when using resource oversubscription? Different types of usage may require different service chains that impact resources in a completely different way.	[48]
Host failure	What to do when something breaks? When a host fails, are the VNFs that are running transitioned appropriately to other hosts? Are the correct rules set up to govern that transition? How long does it take for the VNFs to resume service and is there an interruption of service? It is crucial to validate the answers to these questions in system testing and in production to prevent critical issues.	[48]
Compromised virtualisation layer	Substantial and structural security issues may still remain around isolation of sensitive functions where hypervisors, host OS and CISs are hostile or compromised.	[49]
Runtime attestation	One of the security challenges is to define the standard interface in the ETSI NFV architecture to deploy virtual security functions to react to various threats in real time. Such functionalities should be able to communicate with the orchestration modules and follow the instructions provided. Another challenge is to securely manage and monitor VNFs by maintaining their configuration and information on their state during migration. This can be difficult to do due to the dynamicity and elasticity of VNF operations in cloud environments. Another challenge is to perform trust management between different vendors who build NFV hardware and software. The challenge is to efficiently manage the trust chain among vendors and provide trustiness in the final VNF products. At the moment, attestation technologies only provide boot time attestation. This does not guarantee modification during runtime or prevent tampering with the system's critical components, and such modifications would only be detected when the system is rebooted. Runtime attestation is still an open research area that needs to be explored further. There is also a strong need to develop a comprehensive security architecture to take care of these security challenges in NFVI. To achieve these goals, network operators and vendors need to work together to form a vibrant security eco-system. New standards, testbeds, and proofs of concept would serve as a catalyst for securing NFV infrastructure. The services in this new virtualised environment are evolving rapidly and, in turn, create new opportunities for innovation.	[50], [132]
Distributed denial-of-service attacks	How to utilise the flexibility of VNF to defend against DDoS attacks in the network is a major challenge.	[51]
Trust management in NFV	The emergence of NFV provides opportunities for various vendors to enter the networking infrastructure market by providing NFV compatible hardware and software. It will be common to have multiple vendors involved in a NFV supported network. However, how to manage the trust chain and evaluate the trustworthiness of products is another research challenge. Also, how to adaptively configure VNFs by choosing software to minimise security risk of the network is another research topic.	[51]

Trust between VNFs	It is important to maintain trust between the VNFs for the provision of security validation and integrity. The following are three types of trusts which are important between VNFs: • trust in the correctness of information output between software components; • trust that the software components will operate correctly; • trust in the performance of operations that have an indirect influence on data. Trusting relationships are basic requirements for the software programs to be able to work with each other in NFV environment. The trusting relationships chain needs to be made longer in order to reach the level of complete security.	[52]
Challenges with VNF images validation and VNF onboarding/deploying	There is a risk when validating images, onboarding and deploying VNFs on NFVI. Currently, these processes are not part of the orchestration. Every operator has its unique network configuration of hardware and software vendors plus all the vast numbers of parameter settings. In real time communication there is also a number of real-time dependencies, timers and correct sequences that must be considered. To consider these challenges, a comprehensive certification process, standardised testing framework and the creation of assets to automate the validation, onboarding and deployment of VNFs are required to reduce risks.	[53]

6. CONCLUSION

NFV in 5G is a technology that is continuously evolving through time due to the new technologies, requirements and services that need to be addressed. Security, as an inherent quality that has to be conceived along with the new services, is no exception and must keep up with the pace. Security in the NFV era presents a long-term challenge. As NFV security technology continues to develop, automated and virtualised protection systems with robust security models will enable NFV networks to thrive.

5G deployments uses modern virtualisation techniques for distributed and cloud computing and networking. NFV and SDN are approaches where these modern techniques are brought into consistent frameworks which 5G systems builders can use to be effective and to create vendor products that are interoperable. Those technologies that allow progress to take place are also technologies that can expose new security challenges. Securing 5G must be designed-in and not be an afterthought. Hence, a careful approach to the new aspects of cloud-native services, SDN and NFV can improve their security. Additionally, taking a zero trust approach, combined with the advanced techniques of cyberthreat intelligence, will further enhance 5G's security.

In this report we have highlighted the main security challenges that (i) open up with these technologies and (ii) arise due to the interoperability among them, which enables NFV in 5G. Some of the main challenges highlighted in this report have shown the following.

- **Centralisation of management capabilities** presents a single-point-of-failure weakness.
- **Use of standardised general-purpose server and storage machines**, routinely built with open-source code, represent an increase in threats or attack surfaces.
- The growing **participation of multiple partners or vendors**, processes and subsystems in the creation and delivery of services introduce the risks of data leaks, data residue, and attacks. It can also create very complex **supply chains**. It's difficult to manage so many vendors. All it takes is a security flaw in one of the vendor's environments to launch a supply chain attack whose impact can reach far and wide.
- The more **software components** in a NFV, the more possibilities there are of finding potential software vulnerabilities.
- **5G NFV architecture security should be decentralised** by dividing it into a core network and an edge network. Because the protection targets are widely distributed, there are issues with the visibility of security.

To solve challenges, we have provided a list of technical, organisational and policy best practices in security. The security architecture for NFV must be multi-layered. The aim should be to have security-by-design across all 5G NFV network elements and layers. It is imperative that security is 'designed-in' at all levels to ensure resilience, robustness and address the connected world of the future enabled by 5G.

Security management and orchestration are necessary to coordinate security protection across layers. Hardening and patching NFV security can counteract software vulnerabilities. Isolating resources between different VMs or containers on the same physical machine on the virtualisation layer can prevent data theft and malicious attacks between VMs or containers.

In-house or third-party security audits, or both, should be encouraged as a best practice for empowering mobile networks (not limited to 5G NFV only). Operators need to be alert and always one step ahead of possible security events.

Efforts should be concentrated on developing, automating and refining technologies, policies and processes for service orchestration, on the detection and prevention of intrusions, on solutions to protect against viruses and malware, on dynamic authentication, identity, access and the management of trust relationships, on the encryption of user traffic and its control or management, on the screening, filtering and inspection of traffic, and on the segregation of data and networks.

The level of security automation to automate the provisioning of networks, their security and management in order to continuously maximise network efficiency and functionality should be increased. With virtualised and highly distributed networks, effective 5G NFV end-to-end security requires automated monitoring, mechanisms to prevent threats and protection systems to provide swift responses to known and unknown threats in real-time.

A truly end-to-end approach to NFV security needs to consider the current ETSI and 3GPP standards. 3GPP technical specifications on security architecture and procedures for 5G system and ETSI technical specifications on security for NFV come with a set of security features and improvements. To ensure the expected security benefits are realised, it is important that security requirements defined in the 3GPP and ETSI specifications are fully and correctly implemented and used, including relevant optional requirements.

Creation of a secure NFV architecture in 5G will enable customer privacy and security, build trust and encourage adoption of 5G for critical functions (e.g. critical national infrastructure or functions requiring high reliability such as healthcare).

In addition to the security challenges and best practices explored in this report, we have outlined the roles and responsibilities in terms of security of the main 5G stakeholders and administrators providing and managing the NFV in 5G.

Moreover, we highlighted the main assets to be protected with CIA security properties, the vulnerabilities of various components and network interfaces that can be exploited by the adversary, and the attack scenarios that may impact NFV in 5G. Links between all those elements are provided in the annexes.

At the end of this report, a list of annexes is included to provide the full taxonomies of and the links between the different elements from the core of the report. In addition, the annex provides the standardisation efforts on NFV and SDN from various entities in the telecom industry and other bodies.

LIST OF ABBREVIATIONS

Term	Description
3GPP	Third Generation Partnership Project
AF	Application Function
AMF	Access and Mobility Management Function
API	Application Programming Interface
ARPF	Authentication Credential Repository and Processing Function
AUC	Authentication Centre
AUSF	Authentication Server Function
BBF	Broadband Forum
BBU	Base Band Unit
BSS	Business Support System
CAPEX	Capital Expenditure
CDPI	Control to Data-Path Interface
CIA	Confidentiality, Integrity and Availability
CIR	Container Image Registry
CISM	Container Infrastructure Service Management
CN	Container
CNCF	Cloud Native Computing Foundation
CNF	Cloud-native Network Function
CNFD	Cloud Native Network Function Descriptor
CNFI	Cloud Native Network Function Instance
CNI	Critical National Infrastructure
COTS	Commercial Off The Shelf
CP	Control Plane
CPRI	Common Public Radio Interface
C-RAN	Cloud RAN
CSP	Communication Service Provider
CU	Central Unit
DANOS	Disaggregated Network Operating System
DN	Data Network
DoS	Denial of Service

DPDK	Data Plane Development Kit
DPI	Deep Packet Inspection
DRM	Digital Rights Management
DU	Distributed Unit
ECOMP	Enhanced Control, Orchestration, Management and Policy
eCPRI	Evolved CPRI
EMS	Element Management System
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FCAPS	Fault, Configuration, Accounting, Performance and Security Management
FD.io	Fast Data Project Input/Output
GDPR	General Data Protection Directive
GDT	Global Descriptor Table
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
HLR	Home Location Register
HMEE	Hardware Mediated Execution Environment
HSM	Hardware Security Module
HSS	Home Subscriber Server
IAAS	Infrastructure As A Service
ICT	Information Communication Technology
IDS	Intrusion Detection System
IDT	Interrupt Descriptor Table
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
IPUPS	Inter-PLMN UP Security
KVM	Kernel-based Virtual Machine
LADN	Local Area Data Network
LAN	Local Area Network
LI	Lawful Interception
LEA	Law Enforcement Agency

MANO	Management and Orchestration
M-CORD	Mobile Central Office Re-architected as Datacentre
MCIOP	Managed Container Infrastructure Object Package
MEC	Multi-access Edge Computing
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MNO	Mobile Network Operator
MSB	Micro-services Bus Project
MVNO	Mobile Virtual Network Operator
N3IWF	Non-3GPP Inter-Working Function
NSD	Network Service Descriptor
NFVI	Network Function Virtualisation Infrastructure
NFVO	NFV Orchestrator
NAAS	Network As A Service
NAS	Non- Access Stratum
NEF	Network Exposure Function
NF	Network Function
NFV	Network Functions Virtualisation
NGC	Next Generation Core
NGIC	Next Generation Intelligent Core
NRF	Network Repository Function
NRP	Network Repository Protocol
NS	Network Service
NSA	Non-Standalone
NSSF	Network Slice Selection Function
NWDAF	Network Data Analytics Function
OAM	Operation and Maintenance
OCP	Open Compute Project
OAI	Open Air Interface
OCP	Open Compute Project
ODL	Open Daylight
ONAP	Open Network Automation Project
ONOS	Open Network Operating System

O-RAN	Open Radio Access Network
OS	Operating System
OSD	Open-Source Definition
OSI	Open-Source Initiative
OSS	Operations Support System
PCF	Policy Control Function
PCI	Peripheral Component Interconnect (PCI Bus)
PLMN	Public Land Mobile Network
PNF	Physical Network function
PoP	Point of Presence
QoS	Quality of Service
RAN	Radio Access Network
REC	Radio Equipment Controller
REST	Representational State Transfer
RRH	Remote Radio Head
RRU	Remote Radio Unit
SAN	Storage Area Network
SBA	Service Based Architecture
SBI	Service Based Interface
SCMF	Security Context Management Function
SDHC	Secure Digital High Capacity
SDN	Software Defined Networking
SDO	Standards Development Organisation
SEAF	Security Anchor Function
SEPP	Security Edge Protection Proxy
SIDF	Subscription Identifier De-concealing Function
SIP	Session Initiation Protocol
SLA	Service-level Agreement
SMF	Session Management Function
SMS	Short Message Service
SQL	Structured Query Language
SSD	Solid State Drive
SSL	Secure Sockets Layer

STP	Signalling Transfer Point
TDM	Time Division Multiplexing
TIP	Telecom Infra Project
TOSCA	Topology and Orchestration Specification for Cloud Applications
TPM	Trusted Platform Module
TLS	Transport Layer Security
TSS	Task State Segment
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UI	User Interface
UP	User Plane
UPF	User Plane Function
USB	Universal Serial Bus
UICC	Universal Integrated Circuit Card
VIM	Virtual Infrastructure Manager
VLAN	Virtual LAN
VM	Virtual Machine
VNF	Virtual Network Function
VNFC	Virtual Network Function Component
VNFI	Virtual Network Function Instance
VNFD	Virtual Network Function Descriptor
VNFM	VNF Manager
VNIC	Virtual Network Interface Controller
VPN	Virtual Private Network
VPP	Vector Packet Processing
VXLAN	Virtual Extensible LAN
WAN	Wide Area Network
XaaS	Anything As A service
XSS	Cross Site Scripting
YML	YAML Script, human-readable data serialisation language
ZOOM	Zero-touch Orchestration, Operations and Management

REFERENCES

[1] 5G PPP Architecture Working Group – *View on 5G Architecture*, V3.0, February 2020 https://5g-ppp.eu/wp-content/uploads/2020/02/5G-PPP-5G-Architecture-White-Paper_final.pdf

[2] 3GPP TS 33.501 - *Security architecture and procedures for 5G System* https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

[3] 3GPP 23.501 - *System architecture for the 5G System (5GS)* https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

[4] 3GPP 23.502 - *Procedures for the 5G System (5GS)* https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3145

[5] F. Mademann, *The 5G System Architecture*, in Journal of ICT Standardisation, vol.6, no. 5, pp. 77–86, May 2018

[6] ENISA - *THREAT LANDSCAPE FOR 5G NETWORKS*, December 2020 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

[7] ETSI GS NFV 002 - Network Functions Virtualisation (NFV); *Architectural Framework* https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf

[8] ETSI GS NFV 006 Network Functions Virtualisation (NFV) Release 2; *Management and Orchestration; Architectural Framework Specification*

[9] ETSI GS NFV-IFA 040 - Network Functions Virtualisation (NFV) Release 4; *Management and Orchestration; Requirements for service interfaces and object model for OS container management and orchestration specification*

[10] ETSI GR NFV-IFA 029 - Network Functions Virtualisation (NFV) Release 3; *Architecture; Report on the Enhancements of the NFV architecture towards 'Cloud-native and 'PaaS'*

[11] *Guidelines for 5G End to End Architecture and Security Issues*, December 2019 https://arxiv.org/pdf/1912.10318.pdf

[12] ETSI GS NFV-IFA 010 - Network Functions Virtualisation (NFV) Release 4; *Management and Orchestration; Functional requirements specification* https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/010/04.01.01_60/gs_NFV-IFA010v040101p.pdf

[13] ETSI GS NFV-IFA 011 - Network Functions Virtualisation (NFV) Release 4; *Management and Orchestration; VNF Descriptor and Packaging Specification* https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/011/04.02.01_60/gs_NFV-IFA011v040201p.pdf

[14] A Technical Paper SCTE/ISBE – *Bridging the Gap Between ETSI-NFV and Cloud Native Architecture*, https://www.nctatechnicalpapers.com/Paper/2017/2017-bridging-the-gap-between-etsi-nfv-and-cloud-native-architecture
[15] 5G Americas White Paper – *5G and the Cloud*, https://www.5gamericas.org/wp-content/uploads/2019/12/5G-Americas_5G-and-the-Cloud..pdf
[16] ETSI GR NFV 003 Network Functions Virtualisation (NFV); *Terminology for Main Concepts in NFV*
[17] ETSI GS NFV-IFA 026 - Network Functions Virtualisation (NFV) Release 3; *Management and Orchestration; Architecture enhancement for Security Management Specification*
[18] ETSI GS NFV-SEC 024 - Network Functions Virtualisation (NFV); *Security; Security Management Release 4* (Draft specification - work in progress)
[19] CISCO – *SDN vs NFV: What's the difference?* https://www.cisco.com/c/en/us/solutions/software-defined-networking/sdn-vs-nfv.html
[20] IEEE Communications Magazine – *Network Slicing for 5G with SDN/NFV: Concepts, Architectures and Challenges*, March 2017
[21] ICIT 2015 - *An Overview of Integration of Mobile Infrastructure with SDN/NFV Networks*, May 2015
[22] Elsevier Computer Networks - *5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges*, 2020
[23] Elsevier Computer Networks – *A stakeholder-oriented security analysis in virtualised 5G cellular networks*, January 2021
[24] VMWARE - *Organization Transformation for Network Function Virtualisation Infrastructure As A Service (NFVIaaS)*, November 2015
[25] FFTelecoms – *Référentiel d'objectifs de sécurité en matière de fonctions réseau virtualizées*, 2019, https://www.fftelecoms.org/app/uploads/2021/02/fftelecoms_referentiel_objectifs_securite_virtualization.pdf
[26] 5GIA 5G Infrastructure Association Vision and Societal Challenges Working Group Business Validation, Models, and Ecosystems Sub-Group – *5G ecosystems*, 2021
[27] CISCO – *5G Cybersecurity Guidance*, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-5g-cybersecurity-guidance.pdf
[28] Universitat Politècnica de Catalunya – *Network function virtualisation technologies applied to cellular systems*, January 2020 https://upcommons.upc.edu/bitstream/handle/2117/178276/NFV_Cellular_Systems.pdf?sequence=4&isAllowed=y
[29] IBM - *La anatomía de un hipervisor Linux»*, May 2009 https://web.archive.org/web/20160806114016/http:/www.ibm.com/developerworks/ssa/library/l-hypervisor/index.html
[30] IEEE Access - *Network Functions Virtualisation: The Long Road to Commercial Deployments* A. U. Rehman, R. L. Aguiar and J. P. Barraca, vol. 7, 2019.
[31] VapourApps – *What is Hypervisor and what types of hypervisors are there?* https://vapour-apps.com/what-is-hypervisor/
[32] VMWARE – *vSphere Documentation Center*, https://pubs.vmware.com/vsphere-50/index.jsp
[33] 5G ESSENCE project - *Deliverable D4.1 - Optimisation of virtualisation, orchestration, and resource allocation*, May 2018. https://www.5g-essence- h2020.eu/Portals/0/5G%20ESSENCE_%20Deliverable%204.1_v1.0_Final.pdf?ver=2018-10-04-144621-157
[34] NIST Special Publication 500-322 – *Evaluation of Cloud Computing Services Based on NIST SP 800-145*
[35] NIST Special Publication 800-145 – *The NIST Definition of Cloud Computing*
[36] ENISA - *THREAT LANDSCAPE FOR 5G NETWORKS*, November 2019 https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[37] ETSI GS NFV-SEC 001 - *NFV Security; Problem Statement*. V1.1.1, Oct. 2014.
[38] ETSI GS NFV-SEC 013 - Network Functions Virtualisation (NFV) Release 3; *Security; Security Management and Monitoring specification*
[39] IEEE Communications Surveys Tutorials - *Security in Software Defined Networks: A Survey*, I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, vol. 17, no. 4, 2015
[40] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, *AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-defined Networks*, ACM SIGSAC Conference on Computer ACM, 2013, pp. 413–424
[41] P. Fonseca, R. Bennesby, E. Mota, and A. Passito, *A replication component for resilient OpenFlow-based networking* in 2012 IEEE Network Operations and Management Symposium, April 2012, pp. 933–939
[42] M. Liyanage, A. Gurtov, and M. Ylianttila, *Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*, John Wiley & Sons, 2015
[43] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, *Opportunities and Challenges of Software-Defined Mobile Networks in Network Security*, IEEE Security Privacy, vol. 14, no. 4, pp. 34–44, July 2016
[44] M. Liyanage, M. Ylianttila, and A. Gurtov, *Securing the control channel of software-defined mobile networks*, in Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, June 2014, pp. 1–6
[45] S. Shin and G. Gu, *Attacking software-defined networks: A first feasibility study*, in Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, ACM, 2013, pp. 165–166
[46] M. Liyanage, A. Braeken, A. D. Jurcut, M. Ylianttila, and A. Gurtov, *Secure communication channel architecture for Software Defined Mobile Networks*, Computer Networks, vol. 114, pp. 32 – 50, 2017
[47] 3GPP TR 33.848 – *Study on Security Impacts of Virtualisation (Release 17)* https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3574
[48] IXIA – *Mitigating risk in NFV with continuous simulation and testing* https://www.keysight.com/us/en/assets/7019-0411/technical-overviews/NFV-5-Major-Risks.pdf
[49] Technical Report on *5G Network Architecture and Security*, A collaborative paper DCMS Phase 1 5G Testbeds & Trials Programme, December 2018 https://uk5g.org/media/uploads/resource_files/5G_Architecture_and_Security_technical_report_-_04Dec18.pdf
[50] IEEE Communications Magazine – *NFV: Security Threats and Best Practices*, Vol 55, pp 211-216, May 2017
[51] Wei Yang and Carol Fung Department of Computer Science Virginia Commonwealth University – *A Survey on Security in Network Functions Virtualisation* https://www.people.vcu.edu/~cfung/research/NetSoft2016.pdf
[52] Ahamed Aljuhani and Talal Alharbi, *Virtualised Network Functions Security Attacks and Vulnerabilities*, Computing and Communication Workshop and Conference (CCWC), pp 1-4, January 2017
[53] Ericsson – *Accelerate 5G services with partner VNF certification program*, June 2019 https://www.ericsson.com/en/blog/2019/6/accelerate-5g-services-with-partner-vnf-certification-program
[54] INSPIRE 5Gplus – *D2.1: 5G Security: Current Status and Future Trends*, V1.0, May 2020, https://www.inspire-5gplus.eu/wp-content/uploads/2020/05/i5-d2.1_5g-security-current-status-and-future-trends_v1.0.pdf?x87609&x51934
[55] Alcatel Lucent – *Network functions virtualisation challenges and solutions* https://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2013/9377-network-functions-virtualization-challenges-solutions.pdf

[56] A comprehensive guide to 5G security – *Regulatory Impact on 5G Security and Privacy*, January 2018
[57] China Academy of Information and Communications Technology (CAICT) – *5G Security Report*, February 2020, http://www.caict.ac.cn/english/research/whitepapers/202003/P020200327550639218995.pdf
[58] IEEE Network – *NFV: State of the Art, Challenges and Implementation in Next Generation Mobile Networks (vEPC)*, September 2014
[59] IEEE Conference on Standards for Communications and Networking (CSCN) – *5G Security: Analysis of Threats and Solutions*, September 2017
[60] United States Government Accountability Office – *5G Wireless Capabilities and Challenges for an Evolving Network*, November 2020 https://www.gao.gov/assets/gao-21-26sp.pdf
[61] 5G Americas – *Security considerations for the 5G ERA*, July 2020, https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf
[62] CISA – *Overview of risks introduced by 5G adoption in the United States*, July 2019 https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf
[63] 5G PPP 5G IA – *Edge Computing for 5G Networks*, v1.0, January 2021 https://bscw.5g-ppp.eu/pub/bscw.cgi/d397473/EdgeComputingFor5GNetworks.pdf
[64] ETSI, *An ETSI OSM Community White Paper*, OSM RELEASE THREE, A TECHNICAL OVERVIEW, October 2017
[65] SONATA, *SONATA NFV: Agile service development and orchestration in 5G*
[66] F. Z. Yousaf, M. Bredel, S. Schaller and F. Schneider, *NFV and SDN Key Technology Enablers for 5G Networks*, in IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2468-2478, Nov. 2017.
[67] OPNFV, Open platform for NFV (OPNFV), Open-Source Project, 2017
[68] ONAP, ONAP Documentation, Beijing Release, June 2018, http://onap.readthedocs.io/en/beijing/
[69] IEEE SoutheastCon 2018 – *A Survey of Network Function Virtualisation Security* April 2018, DOI: 10.1109/SECON.2018.8479121
[70] Alcatel.Lucent – *Providing security in NFV challenges and opportunities* https://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/10172-providing-security-nfv.pdf
[71] CLOUD SECURITY ALLIANCE – *The Treacherous 12 – Top Threats to Cloud Computing + Industry Insights*, 2017, https://downloads.cloudsecurityalliance.org/assets /research/top-threats/treacherous-12-top-threats.pdf
[72] ORANGE- Network Functions Virtualisation (NFV) – *Understanding the concepts and technical foundations*, December 2018
[73] ETSI GS NFV-SEC 003 – *Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance*, https://www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/003/01.01.01_60/gs_nfv-sec003v010101p.pdf
[74] NOKIA – *Building Secure Telco clouds*, https://onestore.nokia.com/asset/200289
[75] NGMN Alliance – *5G security recommendations Package #2: Network Slicing*, April 2016, https://www.ngmn.org/wp- content/uploads/Publications/2016/160429_NGMN_5G_Security_Network_Slicing_v1_0.pdf
[76] *A Classification and Characterization of Security Threats in Cloud Computing*, March 2016
[77] Wei Yang and Carol Fung, *A Survey on Security in Network Functions Virtualisation*, NetSoft Conference and Workshops (NetSoft), pp 15-19, 2017
[78] ETSI GS NFV-SEC 002 – *Network Functions Virtualisation (NFV); NFV Security; Cataloguing Security Features in Management Software* https://www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/002/01.01.01_60/gs_nfv-sec002v010101p.pdf

[79] ETSI GS NFV-SEC 009 – *Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration* https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/009/01.02.01_60/gr_NFV-SEC009v010201p.pdf
[80] Tariqul Islam and D. Manivannan, Department of Computer Science, University of Kentucky - *A Classification and Characterization of Security Threats in Cloud Computing*
[81] Security Technical Implementation Guides (STIGs) - Information Assurance Support Environment (IASE)
[82] VMWARE - *Hardening Security Guide*, https://www.vmware.com/security/hardening-guides.html
[83] CSA - *And Again About 5G Network Security*, April 2021 https://cloudsecurityalliance.org/blog/2021/05/04/and-again-about-5g-network-security/
[84] NIST SP 800-190 - *APPLICATION CONTAINER SECURITY GUIDE* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf
[85] T.-S. Chou, *Security Threats on Cloud Computing Vulnerabilities*, IJCSIT, Jun. 2013.
[86] IEEE Conference on Network Softwarization (NetSoft 2016) - *Attacks against Network Functions Virtualisation and Software-Defined Networking: State-of-the-art*, June 2016
[87] Future Generation Computer Systems - *Security challenges with network functions virtualisation*, July 2016
[88] Université de Lorraine - *Software-defined Security for Distributed Clouds*, 2018 https://hal.univ-lorraine.fr/tel-02096145/file/DDOC_T_2018_0307_COMPASTIE.pdf
[89] *NFV builds 5G trustworthiness through security compliance* https://www.ericsson.com/en/blog/2020/11/nfv-security-improves-5g-trustworthiness
[90] Technische Universität Berlin and Kaitiaki Labs - *New Vulnerabilities in 5G Networks* https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf
[91] 3rd USENIX Security Symposium - *On the Practical Exploitability of Dual EC in TLS Implementations*, August 2014, http://dualec.org/DualECTLS.pdf
[92] Matthew Green - *The strange story of 'Extended Random'*, February 2021 https://blog.cryptographyengineering.com/category/rngs/
[93] ITU-R, *Framework and overall objectives of the future development of IMT for 2020 and beyond* Recommendation ITU-R M.2083-0, 2015 https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf
[94] Council of the European Union - *Law enforcement and judicial aspects related to 5G*, 2019, https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf
[95] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie. *A survey on software-defined networking*, IEEE Communications Surveys Tutorials, 17(1):27–51, 2015
[96] D. Kreutz, F. M. V. Ramos, P. E. Verıssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig. *Software-defined networking: A comprehensive survey*, IEEE, 2015
[97] ONF - *Principles and Practices for Securing Software-Defined Networks*, 2015
[98] IEEE Access - *Service Level Agreements for 5G and beyond: Overview, Challenges and Enablers of 5G-Healthcare Systems*, 2020
[99] ONF - *Impact of SDN and NFV on OSS/BSS*, March 2016 https://opennetworking.org/wp-content/uploads/2014/10/sb-OSS-BSS.pdf
[100] Gaurav Bhorkar, Aalto University - *Security Analysis of an Operations Support System*, November 2017
[101] Journal of Computer and Communications - *Coordinated Management of 5G Core Slices by MANO and OSS/BSS*, June 2021
[102] ICC - *Global business recommendations and best practices for lawful intercept requirements*, June 2010
[103] Subsentio - *Is your lawful intercept solution secure?* https://www.subsentio.com/lawful-intercept-solution-secure/
[104] Cisco White paper. *Cisco Ultra 5G Packet Core Solution*, 2018 https://fr.scribd.com/document/430414369/Cisco-5G

[105] 5G Americas - *The Status of Open Source for 5G*, February 2019 https://www.mavenir.com/wp-content/uploads/2020/01/5G-Americas-White-Paper-The-Status-of-Open-Source-for-5G-Feb-2018.pdf

[106] Linux Foundation Networking and Orchestration White Paper - *Harmonization 2.0: How Open Source and Standards Bodies Are Driving Collaboration Across IT*, March 2018, https://www.linuxfoundation.jp/wp-content/uploads/2019/01/LF_StandardsOpenSource_Whitepaper_012418.pdf

[107] ENISA - *5G SUPPLEMENT to the Guideline on Security Measures under the EECC*, July 2021, https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc

[108] 5G ENSURE - *Deliverable D2.5 Trust model*, February 2018

[109] RedHat - *Understanding random number generators, and their limitations, in Linux*, June 2019, https://www.redhat.com/en/blog/understanding-random-number-generators-and-their-limitations-linux

[110] 3GPP TSG-SA3 Meeting #97

[111] D. Kreutz, F. M. Ramos, and P. Verissimo, *Towards Secure and Dependable Software-defined Networks*, in Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, ACM, 2013, pp. 55–60

[112] CISA/NSA whitepaper - *POTENTIAL THREAT VECTORS TO 5G INFRASTRUCTURE*, 2021, https://media.defense.gov/2021/May/10/2002637751/-1/-1/0/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF

[113] Ericsson - *Security Considerations of Cloud RAN*, August 2021 https://www.ericsson.com/4a49ce/assets/local/reports-papers/further-insights/doc/02092021-12911-security-considerations-for-cloud-ran-6-edits.pdf

[114] NIST Special Publication 800-209 - *Security Guidelines for Storage Infrastructure*, October 2020

[115] ETSI GS NFV-IFA 014 - Network Functions Virtualisation (NFV) Release 3; *Management and Orchestration; Network Service Templates Specification*

[116] IETF - ETSI *NFV Management and Orchestration - An Overview* https://datatracker.ietf.org/meeting/88/materials/slides-88-opsawg-6.pdf

[117] GSMA - *Considerations, Best Practices and Requirements for a Virtualised Mobile Network* https://www.gsma.com/futurenetworks/wp-content/uploads/2017/05/Virtualization.pdf

[118] IFIP Annual Conference on Data and Applications Security and Privacy - *Modeling and Mitigating Security Threats in Network Functions Virtualisation (NFV)*, June 2020

[119] AutoVNF - *An Automatic Resource Sharing Schema for VNF Requests* http://isyou.info/jisis/vol7/no3/jisis-2017-vol7-no3-03.pdf

[120] P. Paganini. INFOSEC - *Hardware Attacks, Backdoors, and Electronic Component Qualification*, October 2013

[121] ENISA – *Threat Landscape and Good Practice Guide for Software Defined Networks/5G*, January 2016, https://www.enisa.europa.eu/publications/sdn-threat-landscape

[122] ETSI GS NFV-IFA 010 Network Functions Virtualisation (NFV) Release 3; *Management and Orchestration; Functional requirements specification*

[123] ENISA - *Security aspects of virtualisation*, February 2017 https://www.enisa.europa.eu/publications/security-aspects-of-virtualization

[124] VMWARE white paper- *Intrinsic Security for Telco Clouds at the Dawn of 5G. An Integrated Approach to Helping CSPs Meet Emerging Security Standards*, March 2021

[125] ETSI GS NFV-SEC 012 Network Functions Virtualisation (NFV) Release 3; *Security; System architecture specification for execution of sensitive NFV components*

[126] ETSI White Paper – *MEC security: Status of standards support and future evolutions*, May 2021, https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_WP_46-_MEC_security.pdf

[127] ETSI GR NFV-SEC 011 - *Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture* , https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/011/01.01.01_60/gr_nfv-sec011v010101p.pdf

[128] NTIA - *The Minimum Elements For a Software Bill of Materials (SBOM)*, 2021, https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

[129] GSMA - *Open Networking & the Security of Open Source Software Deployment*, January 2021, https://www.gsma.com/futurenetworks/wp-content/uploads/2021/01/Open-Source-Software-Security_v1.0.pdf

[130] Ericsson - *Open source software security in an ICT context – benefits, risks, and safeguards*, 2021, https://www.ericsson.com/en/blog/2021/1/open-source-security-software

[131] Ericsson - *Zero trust and 5G – Realizing zero trust in networks*, May 2021 https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g

[132] ETSI GR NFV-SEC 018 - Network Functions Virtualisation (NFV); *Security; Report on NFV Remote Attestation Architecture*

[133] ETSI GR NFV-SEC 005- Network Functions Virtualisation (NFV); *Trust; Report on Certificate Management*

[134] ETSI GS NFV-SOL 013 - Network Functions Virtualisation (NFV) Release 3; *Protocols and Data Models; Specification of common aspects for RESTful NFV MANO APIs*

[135] ETSI GS NFV-SEC 022 - Network Functions Virtualisation (NFV) Release 2; *Security; Access Token Specification for API Access*

[136] ETSI GR NFV-SEC 016 - Network Function Virtualisation (NFV); *Location, locstamp and timestamp; Report on location, timestamping of VNFs* (Draft specification - work in progress)

[137] ETSI GS NFV-SOL 018 - Network Functions Virtualisation (NFV) Release 4; *Protocols and Data Models; Profiling specification of protocol and data model solutions for OS Container management and orchestration*

[138] David Soldani, *5G and the Future of Security in ICT*, April 2021 https://www.researchgate.net/publication/350879167_5G_and_the_Future_of_Security_in_ICT

[139] Piret Pernik, Taťána Jančárková, Kadri Kaska, Urmas Ruuto, Costel-Marius Gheorghevici and Henrik Beckvard, Research Report - *Supply Chain and Network Security for Military 5G Networks*, NATO CCDCOE, 2021 https://ccdcoe.org/uploads/2021/10/Report_Supply_Chain_and_Network_Security_for_Military_5G_Networks.pdf

A ANNEX: ROLES AND RESPONSIBILITIES

Roles	Responsibilities	5G Stakeholders
Network Equipment Administrator	He is in charge of: • installation, maintenance or replacement of the network device; • configuration of the network device; • collection and analysis of log events generated by the network device; • deploying firmware patches in compliance with network vendor's guidance on deployment; • monitoring, identifying and notifying network vendors of vulnerabilities discovered; • regularly testing the configuration of the network device.	MNO Network equipment vendors
Virtualisation software infrastructure administrator	He is in charge of: • deployment of patches in compliance with the provider's guidance on the deployment of the virtualisation software infrastructure; • monitoring, identifying and notifying the providers of virtualisation software infrastructure of vulnerabilities discovered; • securely configuring the virtualisation software infrastructure; • regularly testing the configuration of the virtualisation software infrastructure; • analysing log events generated by the virtualisation software infrastructure; • access control management.	MNO MVNO Virtualisation software infrastructure provider Cloud providers
Virtualisation Hardware Infrastructure Administrator	He is in charge of: • deployment of patches in compliance with the provider's guidance on the deployment of the virtualisation hardware infrastructure; • monitoring, identifying and notifying the providers of virtualisation hardware infrastructure of vulnerabilities discovered; • securely configuring the virtualisation hardware infrastructure; • regularly testing the configuration of the virtualisation hardware infrastructure; • analysing log events generated by the virtualisation hardware infrastructure; • access control management.	MNO Virtualisation hardware infrastructure provider Cloud providers
NFV security administrator	He is in charge of: • management of user accounts and credentials; • management of secrets (keys, certificates); • configuration of remote access; • vulnerability handling.	MNO MVNO
NFV system administrator	He is in charge of: • audit of NFV components; • monitoring and analysis of security events and logs; • configuration of NFV components; • monitoring of network traffic; • patch management; • backups.	MNO MVNO

NFV system integrator	He is in charge of: • appropriately integrating NFV HW and SW components; • ensuring that those components function together as expected; • securely configuring (system level) the NFV system; • testing patches after deployment to ensure that they do not break other parts of the NFV system or even expose new vulnerabilities.	MNO MVNO
VNF administrator	He is in charge of: • configuration of VNFs; • management and monitoring of the daily operational tasks (notably provisioning) of VNFs; • access control management; • logs management.	MNO MVNO NF vendors Service providers Vertical markets
VIM administrator	He is in charge of: • configuration of VIM; • management and monitoring of the daily VIM activities and operational tasks; • access control management; • mogs management.	MNO MVNO
VNFM administrator	He is in charge of: • configuration of VNFM; • management and monitoring of the daily VNFM activities and the operational tasks; • access control management; • logs management.	MNO MVNO NF vendors Service providers Vertical markets
Storage administrator	He manages the shared storage between VNFs: resources management, management of access control and secure destruction.	MNO MVNO NF vendors Service providers Vertical markets
Security devices administrator	He is in charge of key management (LI keys, VNF keys, encryption keys, certificates, etc.) within security devices (e.g. HSM, TPM): generation, protection, management of access control, secure destruction, and import/export.	MNO MVNO
Internal validation laboratory	He is responsible for security assessment and verification of the NFV components received from vendor before their deployment.	MNO MVNO

B ANNEX: ASSETS MAPS

Diagrams of the 5G NFV asset mind maps are illustrated in the following figures.

Figure 17: NFV network components assets mind map

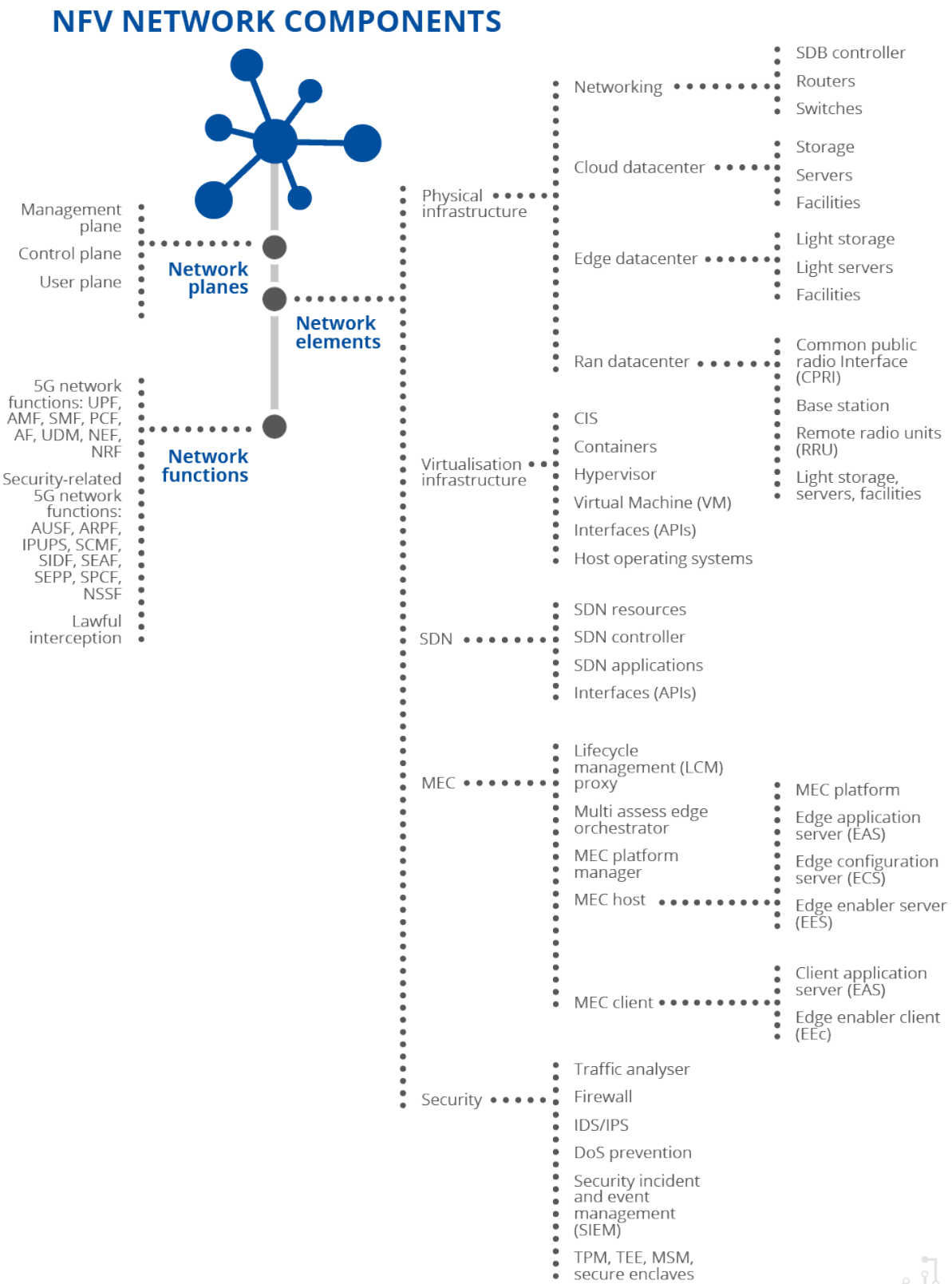


Figure 18: NFV MANO network components assets mind map

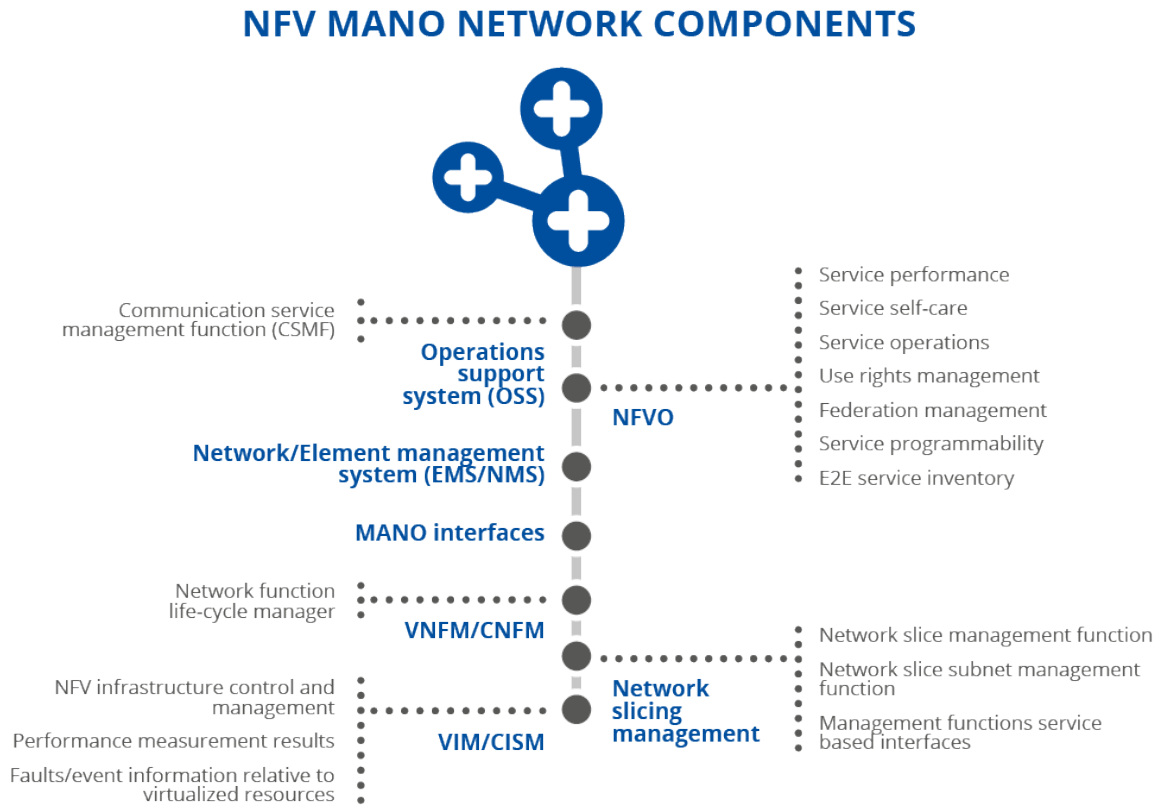


Figure 19: NFV processes and environment assets mind map

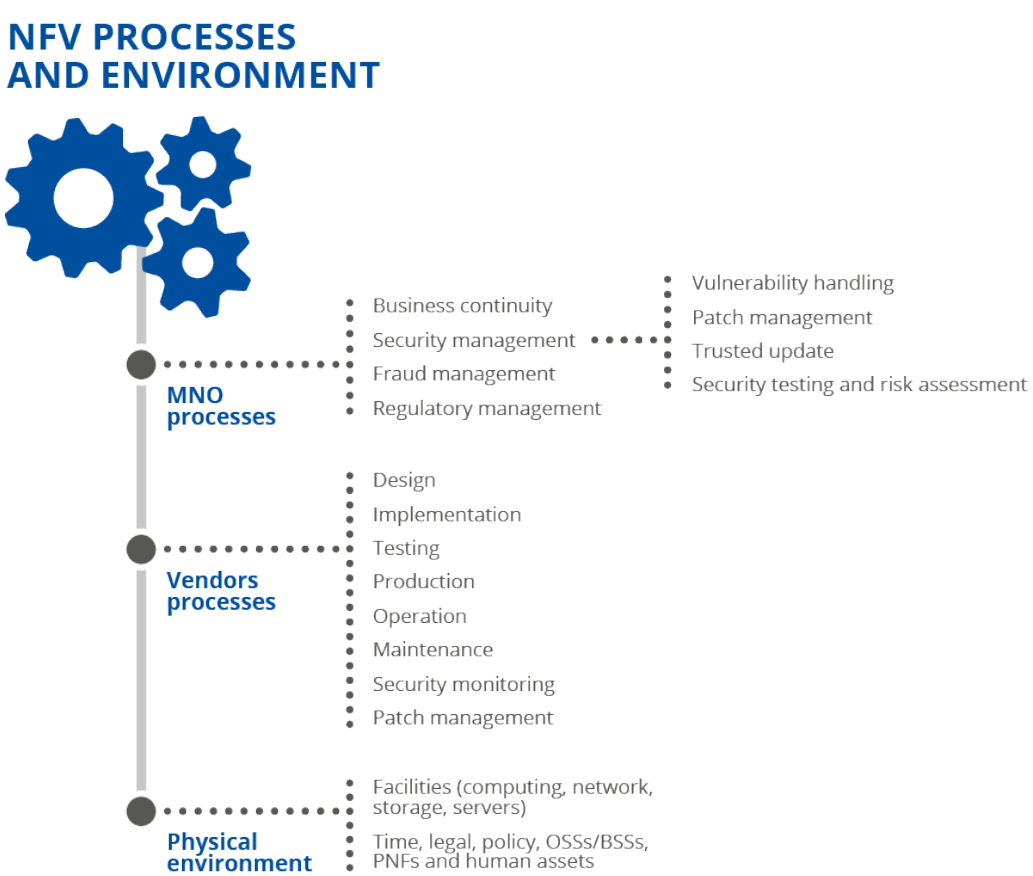
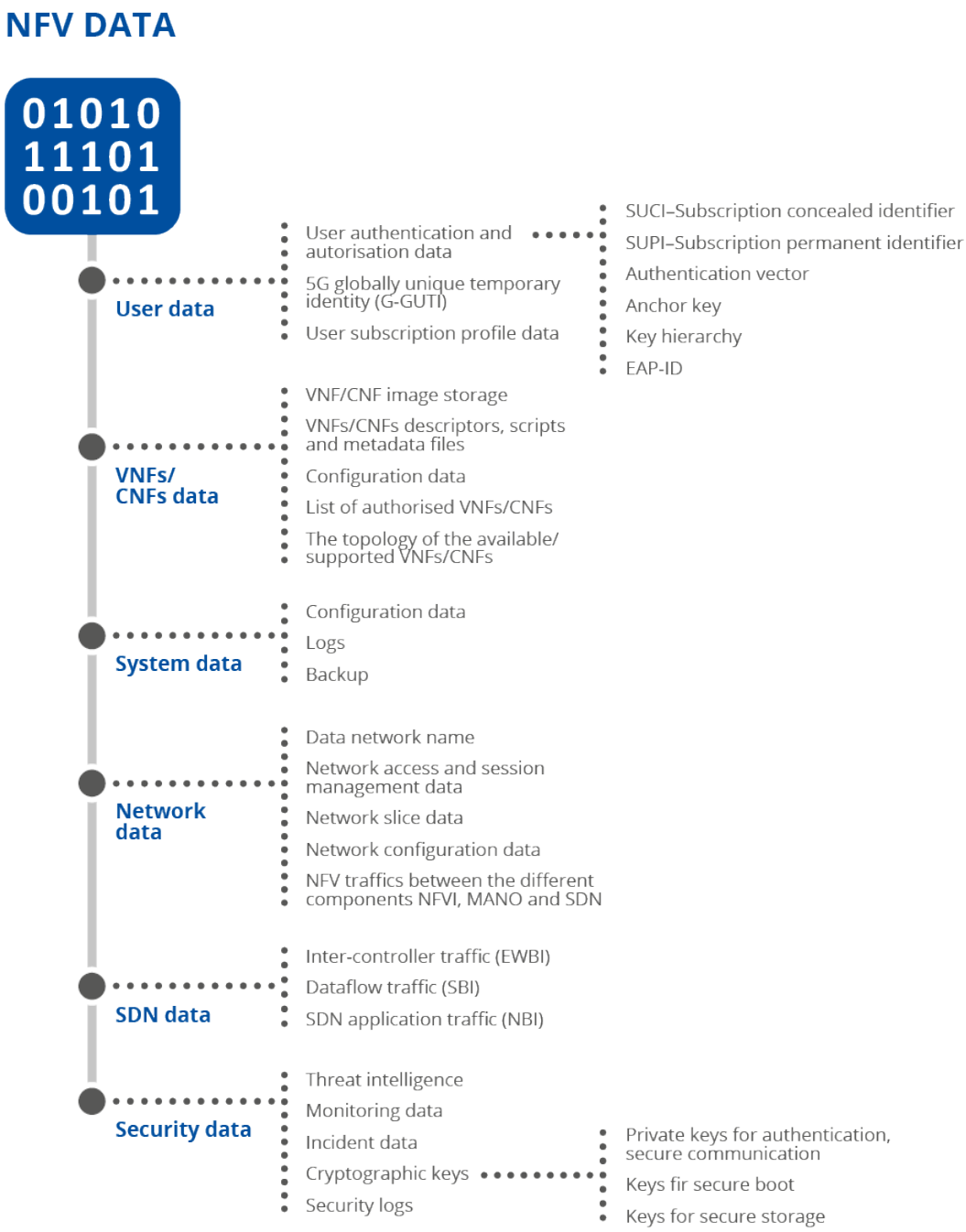


Figure 20: NFV data assets mind map



Assets	Asset description	Confidentiality	Integrity	Availability
	NFV network components			
VNFs	• VNF package e.g. the software and some descriptors; • VNF instance with the guest OS (in case of VM), libs, the virtual links, the VNFC instance included in the VNF instance, the security and configuration parameters.		x	x
Virtualisation/ Containerisation platform	Software on compute nodes such as hypervisors, host operating systems, and CISs.		x	x
NFVI	It holds virtual computing, networking and storage resources. This includes: • physical hardware resources for computing, storage and network connectivity; • virtualisation resources allowing VNFs to run.		x	x
	NFV MANO network components			
NFV MANO	Management and orchestration of VNFs, the NFVI and the virtualisation layer. It includes the virtual infrastructure manager (e.g. OpenStack) and container orchestration engines (e.g. Kubernetes) which support the full lifecycle management of VNFs that carry out the functions of the network. • NFV orchestrator (NFVO): resource management of the NFV infrastructure and lifecycle management of network services (e.g. instantiation, scale-out/in, performance measurement results, event collection and correlation, termination); • VNFM: lifecycle management of VNF instances; • VIM: controlling and managing the NFV infrastructure computing, storage and network resources and collection and forwarding of the results of performance measurement and faults or events information relative to virtualised resources.		x	x
	NFV data			
VNFs data	• VNF image store: the repository of VNF images and VNF descriptors (VNFD), scripts and metadata files; • VNF instance identity, security policies, data associated to the VNF for the license management and enforcement (e.g. service provider ID); • some data related to the service-based architecture are also sensitive data, e.g. the VNF registration information, access policies and access token used to control access to the API of the VNF; • the interdependency between VNFs implementing a network service (VNF Set) and VNF forwarding graph (sequence of data to flow); • list of authorised VNF; • configuration data; • the topology of the available or supported VNFs; • VNF data used for the attestation process, such as the VNF integrity measurement that are used by the attestation server to check the integrity of the VNF software; • time reference, timestamping information and location; • the lawful interception data, the VNF monitoring information (e.g. metrics, measurements, events) and the VNF instance states; • VNF application data: ○ subscriber data managed by UDM and UDR network functions,	x	x	x

	○ policy data managed by PCF and UDR network functions, ○ exposure function data managed by NEF and UDR network functions, ○ application data such as those managed by NEF and UDR network functions, ○ UE context managed by AMF and UDSF network functions.			
NS data	• the network topology, describing constituents of the NS, their communication links, their affinity or anti-affinity rules, the priority information; • monitoring data, such as metrics, measurements, and events • LCM scripts; • SLA that the service provider needs to protect (e.g. bandwidth, latency, availability).	x	x	x
NFV traffic	NFV Traffic (data and command flow) between the various components of NFV, MANO and SDN.	x	x	x
NFV crypto keys	Keys belonging to NFV: • private keys to initiate secure communications between VNF (e.g. IPSec/TLS keys); • encryption/decryption keys of VNF executables and their data; • the cryptographic keys managed by the hypervisor or CIS to encrypt volumes and images; • private/public authentication keys specific to each VM or container: ○ a private key allowing a VM or container to authenticate itself with other VMs or containers, ○ a public key (or a collection of public keys) allowing a VM or container to authenticate data received from another VM or container; • Keys used for a secure boot.	x	x	x
Security logs	Logs - access to compute nodes; Logs - access to physical network equipment; Logs - access to NFV core platform management and configuration interfaces; Logs - real-time operations; Logs – system; Logs - administrative activities; Logs - VNF behaviour; Logs - behaviour of host OS, hypervisors, CIS, VIM, CISM, NFVO and VNFM; Issue, switching logs, etc.; Logs - access to shared storage.	x	x	x
NFV processes and environment				
MNOs processes	Business continuity, fraud management, regulatory management, security management (vulnerability handling, patch management, trusted update, security testing and risk assessment).		x	x
Vendors processes	Management of the different lifecycle phases (design, implementation, testing, production, operation, maintenance, security monitoring, patch management).		x	x
Physical Environment	Facilities (computing, network, storage, servers) for running services, time, legal, policy, OSSs/BSSs, PNFs and human assets.	x	x	x

C ANNEX: VULNERABILITY TAXONOMY

ID	Categories	Vulnerability	Vulnerability description	Associated assets
VUL1	Service-based vulnerabilities of NFV components	Improper message and session integrity checks on internal interfaces	The transmitter of a message should provide a means to allow for determining whether any modification, deletion, insertion or replay has occurred. The receiver should have corresponding verification mechanisms. Lack of such measures or improper messages facilitate the abuse and modification of sessions and messages.	NFV MANO
VUL2		Improper protection of confidentiality of data transferred over internal interfaces to MANO	Lack of appropriate protection of the confidentiality of data transferred over any internal interface of MANO.	NFV MANO; VNF
VUL3		Improper API Access implementation	TLS not implemented for API communication, or implementation shortcomings such as lack of TLS-based authentication: client and authorisation servers are not mutually authenticated or client does not authenticate the resource server.	Os-Ma-nfvo
VUL4		Use of legacy PNF	Vulnerabilities of a PNF could be used as a starting point for an attack against VNFs, potentially taking advantage of any legacy security used by PNFs and not provided by the virtualisation layer.	Control plane
VUL5		Improper verification of identity and location of transmitting party on internal interfaces	If an internal interface allows any actions from data received without successfully identifying and verifying the identity and location of the transmitting party, it enables masquerading of the orchestrator and other forms of privilege escalation that in turn can lead to abuse of VIM or VNFM functions by unauthorised parties.	NFV MANO
VUL6	Improper hardening of NFV components	Inability to provide proof of integrity of the data stores used for VM or container images	Poor monitoring of stored images to determine if any unauthorised modification, deletion or insertion has occurred renders VIM unable to ensure the integrity of VM or container images and of data transfers.	VIM/CISM
VUL7		Lack of protection of user and control planes data	An attacker could read and/or manipulate data in transit if control and user planes data in transit between hosts is not sent over an encrypted, signed and authenticated channel.	Control plane
VUL8		Improper patch management	Once identified, vulnerabilities in software can be fixed through security patches whereas hardware vulnerabilities are much more costly to fix. Security patches may require a reboot and could cause service disruption, particularly if many commodity servers have to be rebooted over a short period. Security patches are not always done in time. Failure to apply necessary patches leave the systems open to the exploitation of known vulnerabilities.	VNF
VUL9		Misconfiguration	Complexity brought by virtualisation increases the probability that errors and misconfigurations will remain undetected. Accidental misconfigurations or failure to follow security standards and practices can cause service problems directly, or leave open unintended vulnerabilities, which will cause service problems if exploited.	VNF

VUL10		No mechanism to enforce geo-restrictions	The MANO system should allow instantiation of MANO components and managed entities, the NFVIs, only at explicit geographic locations. Failure to do so may leave the system vulnerable to legal and licensing risks.	NFV MANO
VUL11		Time manipulation	VNFs must synchronise with trusted time servers. Failure to do so, leaves the system vulnerable to an attack that manipulates the network timing source or VNF clock, thus causing the network to be compromised. It is possible to move clock back and forth in order to confuse the NFVI and VNFs.	VNF
VUL12	Virtualisation layer vulnerabilities	Inadequate access privileges in virtualised environments	Administrative models that enable an admin/root/super user account type to have full access to system resources allow visibility and modification of cryptographic keys, passwords in memory, configuration files, intellectual property and other resources within the NFV. The hypervisor is fully aware of the current state of each guest OS it controls. Hypervisor introspection can enable the ability to view, inject, and/or modify information on operational state associated with the NFV through direct or indirect methods. Access to status information can result in the ability to arbitrarily read and/or write the contents of memory, storage, key storage and other NFV operational aspects.	NFVI
VUL13		Improper key management system	The host system shall provide cryptographically separated secure environments for different applications. In the absence of these conditions, the virtualised environment can be abused to compromise sensitive functions from less protected ones.	SM
VUL14		Lack of a proper mechanism for ensuring a hardware-based root of trust (HBRT)	A hardware-based root of trust (HBRT) should act as an initial root of trust to ensure a safe environment for running sensitive virtualised components.	NFVI
VUL15		Software vulnerabilities in NFV implementation	The risks from software vulnerabilities could be higher with NFV than with traditional bespoke appliances because VNFs are expected to run on commodity software and hardware and because NFV is built on cloud technology with a standard level of security. Virtualisation technology will need to be re-assessed before it can be considered suitable for protecting critical network infrastructure.	VNF
VUL16	Vulnerable mechanisms for authentication and authorisation of NFV components	Improper VNF on-boarding	Improper procedures for signing and managing associated cryptographic keys may enable the manipulation and compromise of the integrity of VNF Packages.	VNFM
VUL17		Improper VNF instantiation	Lack of or improper mechanisms to prevent the instantiation of VNF packages unless their signature is verified may enable the manipulation and compromise of the integrity of VNFs.	Ve-Vnfm-em; Ve-Vnfm-vnf
VUL18		Improper authentication policy	Unauthenticated access to the system functions of NFV management and orchestration: the use of a system function without successful authentication on the basis of the user's identity and at least one authentication attribute (e.g. password, certificate) opens an opportunity for exploitation and limits accountability. This includes M2M communication.	NFV-MANO; VNF; NFVI
VUL19		Insecure or insufficient authentication attributes	Failure to protect accounts by at least one authentication attribute or active predefined authentication attributes: depending on information sensitivity, different levels of strong authentication mechanisms are required. Failure to identify the proper correspondence between levels of protection and the authentication mechanisms implemented creates the possibility unauthorised entities will be allowed to access unallocated resources.	NFV-MANO; VNF; NFVI

VUL20		Insecure password policy	A password policy must address password structure, password change, hidden password display capabilities and consecutive failed login attempts. A weak password structure and/or a password validity period that is too long could lead to a successful brute force attack. Failure to block consecutive failed login attempts may lead to a password being guessed.	NFV-MANO; VNF; NFVI
VUL21		Insecure authentication mechanisms to management or maintenance interfaces	The network product management must support mechanisms for mutual authentication. The mutual authentication mechanism can rely on the protocol used for the interface itself or other means.	NFV-MANO; VNF; NFVI
VUL22		Insecure authorisation and access control mechanisms	The authorisations for accounts and applications must be reduced to the minimum required for the tasks they have to perform.	NFV-MANO; VNF; NFVI
VUL23	Insufficient or improper monitoring mechanisms of NFV	Insufficient or inadequate logging of security events for MANO and NFVI	A lack of security events being logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time an incident occurred do not allow a correct and rapid audit in the event of security incidents occurring	NFV-MANO; NFVI
VUL24		Logs not transferred to centralised storage	Security event logs should be forwarded or uploaded to a central location or external systems. Security event log files shall also be protected in storage and transfer states.	NFV-MANO; NFVI
VUL25		Improper protection of security event log files	Availability and integrity of log files of security events could lead to delays, wrong audit results, delays in the restoration of security and the persistence of threats.	NFV-MANO; NFVI
VUL26	Vulnerabilities due to legacy OSS/BSS systems	Use of weak cryptographic algorithms	The OSS/BSS applications may use weak cryptography in their components. According to ANSSI, BSI, SOG-IS and NIST reports, several encryptions and hashing algorithms are considered insecure. For instance, TDES, MD5, SHA1, RSA (key size smaller than 2048 bits) algorithms are still used for encryption, signature and hashing purposes. These algorithms are considered inadequate for modern security requirements. A weak encryption algorithm is a critical security problem in an OSS/BSS system since the encrypted data transmitted with NFV/MANO includes sensitive information.	OSS/BSS systems
VUL27		Insecure interface between OOS/BSS and NFV/MANO	The security of each interface depends on the type of interface, manufacturer, etc. Newer interfaces such as SOAP and REST over TLS are more secure than older interfaces. Unsecure interfaces may still be in use such as TLSv1, FTP, SNMP and compromised by exploiting vulnerabilities in protocols such as insecure settings, spoofing, and other vulnerabilities.	OSS/BSS systems
VUL28		Insufficient or inadequate logging of sensitive data	OSS/BSS systems log high amounts of data, which includes request logs, provisioning logic execution logs, user audit trails, etc. Apart from helping in finding faults in the application, logging also helps in finding security breaches. Nevertheless, the high amount of data that goes into OSS/BSS logs makes logging an important asset to secure. Logs may be archived in insecure network storage. Attackers can use a combination of attacks to get access to logs.	OSS/BSS systems
VUL29	Improper protection of service-based interfaces	Improper transport layer protection of service-based interfaces (SBI)	Service-based-interfaces of network functions should provide adequate protection for access and for data in transit. Relevant vulnerabilities include: • improper transport layer protection, and improper authentication mechanisms; • vulnerable authorisation mechanisms on service access.	All 5G network functions (NF) utilising SBI

VUL30	Vulnerabilities of 5G NFs	Incorrect implementation of 5G network functions security requirements	Incorrect or incomplete implementation of security requirements, as defined in 3GPP TS 33.501 open confidentiality, integrity and availability risk, for all data passed across networks and for unprotected access to network functions. Relevant vulnerabilities in 5G NFs implementation include: • incorrect implementation of cryptographic material handling; • handling of cryptographic material beyond connection-specific scope; • incorrect implementation of protection policies mismatch handling; • no authentication on application function; • no authorisation on northbound APIs.	UPF; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF
VUL31		Improper protection of data and information of 5G NFs components	Relevant vulnerabilities include: • system functions revealing confidential data; • improper protection of data and information in storage; • lack of or improper cryptographic protection of data in transfer; • no traceability of access to personal data.	UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF
VUL32		Improper protection of availability and integrity of 5G NFs	Relevant vulnerabilities include: • failure to address overload situation; • boot from unauthorised memory devices; • improper handling of unexpected input; • insufficient assurance of software package integrity.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF
VUL33		Vulnerable mechanisms for authentication and authorisation of 5G NFs	Relevant vulnerabilities include: • unauthenticated access to system functions; • improper authentication mechanisms; • predefined or default accounts and/or authentication attributes; • weak or missing password policy; • lack of mutual authentication of entities for management interfaces; • improper authorisation and access control policy.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF
VUL34		Improper / missing functionality for session protection	The system must have a function that allows a signed in user to logout at any time. All processes under the logged in user ID shall be terminated on log out. A permanent exposed session increases the vulnerability of the system as an entry point for an unauthorised person. An OAM user interactive session must be terminated automatically after a specified period of inactivity. It must be possible to configure an inactivity time-out period.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF

VUL35		Lack of or improper security event logging	A lack of security events logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred do not allow for a correct and rapid audit should a security incident occur. Security restoration is delayed.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF
VUL36	Vulnerabilities in operating systems supporting 5G NFs	Vulnerabilities in operating systems supporting 5G NFs	Relevant vulnerabilities include: • improper or missing controls for the protection of security event log files; • improper handling of growing content by file system; • processing of ICMP packets not required for operation; • processing of IP packets with unnecessary options or extensions; • privileged escalation allowed without re-authentication; • recurrent UIDs for UNIX System accounts.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF
VUL37	Improper hardening of 5G core components	Improper hardening of 5G core components	Relevant vulnerabilities include: • unnecessary or insecure services or protocols; • unrestricted reachability of services; • unused software or hardware components; • unsupported components; • remote login of privileged users; • excessive file system authorisation privileges; • lack of protection against IP-source address spoofing; • unneeded kernel network functions; • automatic launch of removable media; • no protection against buffer overflows; • no or improper external file system mount restrictions; • unused file type- or script-mappings; • unrestricted access to files; • presence of default content; • inadequate traffic separation of traffic belonging to different network domains.	Service-based interfaces (SBI); all 5G NFs; control plane
VUL38		Improper mechanisms for preventing flow rules confliction	Lack of functionality in the SDN control layer to support the prevention of conflicts between flow rules in order to avoid mandatory network policies from being bypassed.	SDN controller
VUL39		SBA/SBI vulnerabilities of SDN components	Relevant vulnerabilities include: • insecure APIs, • improper mechanisms to protect the integrity and confidentiality of configuration data.	SDN controller Northbound interface; Southbound interface;

				Eastbound-Westbound Interface
VUL40	Vulnerabilities of SDN	Improper authentication and authorisation	Improper authentication and/or authorisation mechanism for SDN controller or defective implementations of these mechanisms.	SDN controller
VUL41		Improper hardening of SDN components	Relevant vulnerabilities include: • multiple vulnerabilities in operating system; • software vulnerabilities; • improper mechanisms for the management of cryptographic keys; • lack of, or improper, DoS protection mechanisms.	SDN controller
VUL42		Insufficient or improper monitoring mechanisms of SDN components	Relevant vulnerabilities include: • improper log and audit mechanisms; • lack of, or improper, hardware monitoring mechanisms.	SDN controller
VUL43		Virtualisation vulnerabilities of relevant SDN components	Vulnerabilities in the virtualisation layer may lead to risks such as unauthorised access to SDN resources. Cloud solutions used for SDN implementation may lead to vulnerabilities specific to cloud technology. SDN offers programmers a high level of abstraction. When applications are developed, caution is required to protect the network operation against application misbehaviour and bugs.	SDN application; SDN resources
VUL44		Datacentre vulnerabilities	Many SDN systems are deployed within datacentres. The security vulnerabilities of datacentres need to be considered. Data servers are using data centre interconnect (DCI) protocols, which may lack authentication and encryption to secure the packet contents.	SDN infrastructure layer
VUL45	Vulnerabilities of MEC	Vulnerabilities in implementation of MEC security functionalities	Relevant vulnerabilities include: • improper mechanisms for collection, secure storage and transmission of charging-related information; • improper mechanisms for lawful interception at edge level.	Application data traffic; MEC host; multi-edge computing
VUL46		SBA/SBI vulnerabilities of MEC components	Relevant vulnerabilities include: • improper implementation of APIs; • improper traffic path update for mobility support.	3GPP SA6 interfaces ; ETSI MEC interfaces ; application data traffic
VUL47		Improper access control to information	The mobile edge platform must only provide a mobile edge application with the information for which the application is authorised.	MEC platform; MEC application; EAS
VUL48		Vulnerable virtualisation, / container / micro-service environment	Security risks and concerns around virtual systems can be broadly classified into three types: (1) *architectural*: the layer of abstraction between the physical hardware and the virtualised systems running services is a potential target for attack. A VM or container or group of VMs or containers connected to the same network can be the target of attacks from other VMs or containers on the network. (2) The *virtualisation layer* (host OS, hypervisor and CIS software): the most important software in a virtual system is the virtualisation layer. Any security vulnerability in the virtualisation	VIM/CISM

			layer and associated infrastructure and management software or tools puts VNFs at risk. (3) *configuration*: given the ease of cloning and copying images in a virtual environment, a new infrastructure can be deployed very easily. This introduces configuration drift. As a result, controlling and accounting for rapidly deployed environments becomes a critical task.	
VUL49		Lack of / improper DDoS rotection	Due to the distributed nature of edge computing deployments, appropriate DDoS mechanisms may be impractical to deploy. Alternative protection mechanisms need to be implemented in order to deter attacks.	Customer facing service (CFS) portal
VUL50		Vulnerabilities in MEC applications	Vulnerabilities in MEC applications may be used as an entry point for attacks aiming at exploiting the virtualisation environments, unauthorised access to data, elevation of privileges or denial of service.	MEC applications; Edge Application Server (EAS)
VUL51		Improper isolation of resources	Physical and logical resources should not be shared with components which do not have the same criticality. This constraint requires the right level of isolation around the service to prevent regulation pollution to its own components and infrastructures.	Virtualisation infrastructure; MEC host; MEC platform
VUL52		Physical and environmental vulnerabilities of relevant MEC components	Relevant vulnerabilities include: • improper physical and environmental security of edge computing facilities; • improper security monitoring of edge computing facilities; • insecure service environment.	MEC host
VUL53		Vulnerable mechanisms for authentication and authorisation of MEC components	Relevant vulnerabilities include: • improper authentication policy, such as unauthenticated access to system functions, use of generic accounts; • insecure or insufficient authentication attributes, such as failure to protect accounts by at least one authentication attribute or active predefined authentication attributes; • weak or missing password policy; • insecure authentication mechanisms for management or maintenance of interfaces; • insecure authorisation and access control mechanisms.	LCM proxy; MEC orchestrator
VUL54		Insufficient or improper monitoring mechanisms of MEC components	Relevant vulnerabilities include: • insufficient or inadequate logging of security events for MEC app and MEC host; • logs not transferred to centralised storage; • improper protection of security event log files.	MEC platform; MEC host; MEC application; VIM/CISM

D ANNEX: ATTACK TAXONOMY

ID	Categories	Attacks	Attack scenario	Impacts	References
ATT1	Attacks from within an NFV	Human-instigated attacks	This category of attack occurs when the administrator adheres to objectionable operations over the VNFs. An attack on a single VNF installed in NFVI can compromise the entire infrastructure. A malicious administrator manages to obtain confidential information about a user thanks to some badly implemented virtualisation procedures in an NFV context. Since the malicious administrator has root access to the virtualisation layer, by using a search operation he can extract the user ID, passwords and cryptographic keys from the memory dump, which in turn violates user privacy and data confidentiality. To execute this attack, the attacker first creates a backup copy of the VM drive and then uses open-source tools, such as kpartx and vgscan, to extract sensitive data from it. Another attacker scenario is that the hypervisor or CIS administration role can be used to manage the VM or container and vSwitch environment. The administrator could use this environment to monitor or eavesdrop security critical information operating on a VM or container or passing between NFVs components. The administration role may eavesdrop unsecured traffic (e.g. unsecured SIP - session initiation protocol) or create a memory dump of a running VM or container to obtain security critical or personal information, e.g. customer authentication credentials, which would allow them to log into the customer SIP account and fraudulently use their service or have access to compromise customer privacy. Note: the risk posed by the hypervisor or CIS administrator role exists in all deployment scenarios. However, the risk is increased if this role is not under the direct control of the operator. Impacts: As one of the objectionable operations, the administrator can extract and use the memory dump of a user's VM or container to extract a user's ID and password and TLS keys which is a direct breach of the user's privacy.	Access breach	[50]
ATT2	Attacks from within an NFV	Software flaw attacks	Software components with NFV are vulnerable to different types of attacks. The security breaches brought to the NFVI by one software can spread out to other components and therefore make the entire environment vulnerable. Software NFV components may carry flaws in their design, but not specifically related to their code. Misconfigurations are typically exploited to perform such attacks. Another attack can be obtaining a privileged status by using return-oriented-programming. Impacts: A vendor with wrong intentions may provide weak security features in the software which makes the software vulnerable to attack and therefore puts the entire network to risk. This example will qualify for both human-instigated and software vulnerability. It could be possible to bypass firewall restrictions or to take advantage of a buffer overflow to execute arbitrary code.	Access breach Denial of service Integrity compromise	[86], [52], [88]

ATT3	Attacks from within an NFV	Resource misuse attacks	Misuse of shared resources (by user or VNF): resource misuse attacks e.g. RFA and FRC attacks	Access breach Denial of service Integrity compromise	[87]
ATT4	Attacks from within an NFV	Security standard subversion attacks	Vulnerabilities present in security standards can be exploited. Consequently, all the components supporting those standards are affected. Two examples are set out here below: 1. *Vulnerabilities in the 5G or 4G security standards*: new vulnerabilities are revealed affecting both the operator infrastructure and end-devices (including mobiles, NB-IoT, laptop etc). As demonstrated in the paper *New Vulnerabilities in 5G Networks*[93], these vulnerabilities can be exploited in 4G base stations or in commercially available NB-IoT protocols using low-cost hardware and software platforms to mount battery draining, hijacking and bidding down attacks. Those attacks affect the range from gigabit high speed LTE devices to NB-IoT devices. 2. *Vulnerabilities in the NIST Special Publication 800-90A and ISO 18031 standards*[94] [95]: these standards contain algorithms for generating the random numbers used, for example, to generate keys for cryptographic systems. One of the algorithms contained within these documents is a pseudorandom number generator called the dual elliptic curve deterministic random bit generator (Dual EC DRBG) that has long been known to admit a serious potential back door in the event that an attacker generates the standard algorithm parameters. Several cryptographic software vendors have implemented Dual EC in their products. For example, OpenSSL's FIPS module includes Dual EC as an optional random number generator. The backdoor which used Dual_EC_DRBG as a CSPRNG would allow the attacker with knowledge of the trapdoor to decrypt, for example, TLS encryption or VPN traffic, read all traffic, and modify the data as needed.	Access breach Integrity compromise	[90], [91], [92]
ATT5	Attacks from within an NFV	LI attacks	Attack scenario due to the hybrid legacy or virtual LI architecture: *Compromise of legacy node*: In this scenario, an attacker makes use of the VNFs or host OS or hypervisor or CIS or associated signalling within the NFV domain to attack legacy nodes which were otherwise previously secure. This could be as simple as the legacy nodes now sharing the same administration domains as VNFs such that the legacy node operations become more visible to MANO than was possible in the full legacy network. Legacy nodes are unlikely to implement many of the mechanisms an LI VNFCI POI would utilise based on ETSI GS NFV-SEC 012. Therefore, NFV may considerably compromise the security by protecting the obscurity of legacy POIs. Furthermore, it may be relatively simple to monitor overt events in the NFV domain and then look for corresponding SDN/NFV actions taken by legacy POIs in mixed networks. Furthermore, the physical firewalls and other protection mechanisms around the legacy nodes may be virtualised, considerably increasing the attack exposure surface to those nodes. It is also possible to consider a scenario where an attacker initiates an attack from within the legacy domain which is then allowed to route through VNFs (not directly impacting the VNFs), which then returns as a trusted message into the legacy domain which does result in an attack.	Access breach Integrity compromise	[127]

[93] https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf
[94] http://dualec.org/DualECTLS.pdf
[95] https://blog.cryptographyengineering.com/category/rngs/

ATT6	Attacks from outside an NFV	DDoS attacks	They consist in blocking or disrupting the entire network and the operation of NFV components. These attacks do not aim at gaining control over the resource nor at exfiltrating data, but only affect its availability. The major reason behind such attacks are: 1) VNFs getting controlled remotely (by a third party), 2) due to a completely external malicious attack in order to destroy the NFVI such as can be done with a DDOS. A VNF's internal vulnerabilities also make it open to external attacks. Impacts: 1. A denial-of-service attack (DoS) can be attempted on the NFV infrastructure in order to make it run out of resources and therefore also shut down its service to some extent. During the DoS attack, one VNF can be targeted for the attack and be made to generate numerous amount of traffic to be sent to other VNFs running on the same host or on a different host. The danger of DDoS could also affect untargeted services and tenants that are hosted on the same physical host. 2. Such an attack can be performed from the hypervisor or CIS by using the management console (or a service controlling it) to shut down the targeted VM container. 3. Network protocols can be used to flood the hypervisor or CIS and/or its execution environment using DDoS attacks. 4. A more discreet manner to proceed with such a denial of service is to reconfigure the virtual hardware environment to cause VM or container dysfunction (e.g. reducing allocated RAM) to reduce the footprint of the attack. 5. The networking environment may be shared with other tenants of the NFV sharing the same virtualisation layer. The traffic introduced by the other tenants may cause increased risks including DoS on the NFVI.	Denial of service	[50], [77], [85], [86], [87], [52], [88]
ATT7	Attacks from outside an NFV	DNS Amplification attacks	The NFVI supports a virtual DNS and the NFV orchestrator can increase the number of DNS servers depending upon the number of queries. An attacker generates multiple DNS queries using IP spoofing and as a response more virtual DNS are rolled out by the orchestrator. This can lead to a further shutting down of the services of the NFV.	Denial of service	[50]
ATT8	Attacks from outside an NFV	Injection attacks	It is a malware injection attack on the hypervisor or CIS and its VMs or containers. A hypervisor or CIS allows multiple VMs or containers to communicate and integrate with each other, taking care to manage the virtualisation layer of the NFV system. A malware injection aims to affect the virtualisation layer in the infrastructure of NFV via altering its internal code. The degree as to how badly a malware attack affects the system varies, including slowing down the response time for the system. Malware injection attacks implemented on VMs or containers can also cause modification to the permissions of the virtual service. It may lead to having the sensitive data of VNFs visible to other VNFs in unauthorised ways. Also, this attack could affect the NFV host OS and hypervisor or CIS, which may lead to dysfunction in the CPU, VMs or containers and in the memory of the system. An attacker (e.g. supplier that has installed some Trojan in its VNF supply to attack other co-hosted VNF) can break the confidentiality and integrity of a software (code + data) once it is launched.	Access breach Denial of service Integrity compromise	[69], [87]

ATT9	Attacks from outside an NFV	OSS/BSS attacks	An attacker may spoof an OSS/BSS system. A malicious system posing as an OSS/BSS can disrupt the network by sending incorrect configuration requests to the NFV/MANO and SDN systems. If the attacker is able to spoof a system, it can mount a man-in-the-middle (MitM) attack, which might lead to tampering with data or sniffing out important information on the interface with MANO and NFV systems. Alternately, the attacker might just passively listen to the information (sniff) on an interface. In addition, the attacker may perform DoS attacks on the NFV/MANO and SDN systems. An attacker can deny service to the OSS/BSS systems by using several techniques such as resource exhaustion by sending multiple login requests or a high number of provisioning requests. An attacker may be able to sniff the credentials used by the OSS/BSS systems due to a weak authentication or authorisation implementation to authenticate with the NFV or MANO. Data transfer in plaintext is vulnerable to sniffing, which can reveal subscribers' personal information and secret network parameters.	Access breach Denial of service Integrity compromise	[100]
ATT10	Attacks from outside an NFV	LI attacks	Attack scenario due to the hybrid legacy-virtual LI architecture: *Compromise of virtualised node*: In this scenario, an attacker makes use of a legacy LI node (POI or wider node functionality) or associated signalling to that node, in order to attack an otherwise secure VNF containing a vPOI. This could be as simple as capturing unencrypted or poorly secured messages sent to legacy nodes and then using these messages to perform attacks on the VNF. Since the VNF is required to trust the legacy nodes and communicate with them using legacy protocols, the VNFs becomes at risk of bid down, man-in-the-middle or plain text attacks on the messages or interfaces. Furthermore, an attacker, by studying the operation of a legacy node, may be able to identity inference attacks against a VNF of the same type and manufacture (e.g. legacy CSCF vs VNF CSCF). It is also possible to consider a scenario where an attacker initiates an attack from within the NFV domain which is then allowed to route through legacy nodes (not directly impacting the legacy nodes), which then returns as a trusted message into the NFV domain which does result in an attack.	Access breach Integrity compromise	[127]
ATT11	Attacks occurring between NFV components	Malicious VM/Container attacks	*Hypervisor or CIS resource monopolisation attacks*: the hypervisor or CIS resource monopolisation attacks consist of a malicious VM or container taking control of a hypervisor or CIS to gain exclusive access to these resources. This leads to the violation of the isolation of the hypervisor or CIS resource or to the theft of data from other VMs or containers. *VM or container hopping attacks*: a VM or container hopping attack consists of a malicious VM or container that directly targets another VM or container from the virtualisation environment. Such attacks permit the tampering and the elevation of privilege in the virtualisation architecture. *VM or container monitoring attacks*: the attacks consist of a VM or container monitoring another VM or container to collect information about that VM or container without compromising it. They can typically rely on passive monitoring of another VM container. These attacks are mainly conditioned by the exploitation of side channels, and the co-residence of VMs or containers. *VM or Container escape attacks*: the VM or container escape attack aims at compromising the hypervisor or CIS in order to access another VM or container or execute code in the physical host. It is very similar to VM or container hopping, and corresponds to the same threats, but relies on the hypervisor or CIS compromise to break the isolation. Once the attacker gains access to one of the VMs or containers, it uses this VM or container's network connectivity to reach the hypervisor or CIS API and then attacks the hypervisor or CIS to cause great damage. The major supporting factor behind this type of attack is the improper isolation of hypervisor or CIS and VMs or containers. Impacts:	Access breach Denial of service Integrity compromise	[50], [88]

			1. These attacks may affect memory pages owned by other VMs or containers, to proceed to in-memory information leakage or even to build a hidden channel between both VMs or containers. 2. These attacks may contribute to leaks of cryptography keys.		
ATT12	Attacks occurring between NFV components	Malicious hypervisor/CIS attacks	These attacks target the hypervisor or CIS of the virtualisation architecture. The threats related to these attacks affect the hypervisor or CIS itself, by tampering with it, repudiating the traceability of its behaviour, disclosing information about its configuration and the configuration of the VM or container, and elevating the privilege of a VM or container user to that of the hypervisor or CIS administrator. The VM or container introspection attack exploits a malicious hypervisor or CIS to analyse the behaviour of a VM or container and infer its internal state. The inter-VM or container communication introspection attacks may also provide interesting information regarding the communications of the VM or container with other hosted VMs or containers through I/O or networking subsystems that are handled by the hypervisor or CIS. This raises privacy issues related to the interception and introspection of communications. If a type 2 solution or container is deployed then the virtual environment is subject to any vulnerability that might exist in the underlying OS. For example, a missed patch or update could expose the host OS, hypervisor CIS and VMs or containers to attack.	Access breach Integrity compromise	[88], [47]
ATT13	Attacks occurring between NFV components	Command/control channel attacks	The command and control channel is a privileged communication medium between the hypervisor or CIS and a VM or container. This threat targets the hypervisor or CIS, through the repudiation of malicious activities in a VM or container.	Access breach	[88]
ATT14	Attacks occurring between NFV components	Hardware attacks	Hypervisors or CISs and host OSs are running at the top of a hardware layer. They are therefore constrained by the hardware layer, which is composed of devices with their own firmwares. These firmwares may carry their own flaws, providing the necessary material to an attacker to compromise them. The corresponding threats are tampering with hardware, the disclosure of information based on side channels, and the elevation of privileges to get control on the software components running over the hardware. These attacks are emphasised by the hard constraints regarding the upgrade procedure of these firmwares. Such upgrades are typically limited by the degradation of services during the upgrade process, or by a lack of support from manufacturers. The Spectre and Meltdown issues[96] are substantial threats that have severe impacts on security. The vulnerabilities allow processes to read information in memory that should not be accessible to them. User processes can access information from other processes and the kernel, and in a virtualised environment they can also access information on the host and, potentially, other guests.	Access breach Integrity compromise	[88]
ATT15	Attacks occurring between NFV components	Network attacks	Attackers may find a way to compromise the communication between NFV and MANO. Privilege escalation is a common attack on the VIM, and, if successful, it can lead to partial control over the host. Attacks on network functions and/or resources (e.g. spoofing, sniffing and denial of service) can also take place. An attacker can compromise virtual firewalls to restrict firewall functionality while allowing sufficient access to carry out the attack.	Access breach Denial of service Integrity compromise	[86]

[96] https://stack8.com/spectre-and-meltdown-update-cve-2017-5753-cve-2017-5715-cve-2017-5754/

			An amplification attack in NFV could be realised by provisioning a rogue network element that requests new elements to be booted up with the same malicious configuration. A rogue element could also generate and amplify traffic, log data or any other type of data that require other network elements to act upon it. The goal of such an attack is to limit the ability of the network to cope with the current traffic load and to disrupt the network's ability to provide the services intended.		
ATT16	Attacks occurring between NFV components	Time manipulation attacks	This could introduce several threats such as tampering with security logs, expiry of used certificates or UEs getting out of sync with the network. If an attack manipulates the network timing source or VNF clock, the network can be compromised.	Denial of service Integrity compromise	[110]
ATT17	Attacks occurring between NFV components	LI attacks	An example of this attack could be manipulating the lawful intercept functionality, which may provide the attacker with the ability to access this function at will through enabling unauthorised accounts or the redirection of IP traffic. A national memory stack segment (MSS) may be deployed in a foreign datacentre where local LEA (law enforcement agency) legislation allows access to the security critical customer and LI information.	Access breach Integrity compromise	[127]
ATT18	Attacks occurring between NFV components	Orchestration attacks	*Attack scenario 1*: Spoofing of the orchestration platform's service requests may result in an attacker being able to generate service requests to cause DoS by: • provisioning new instances in order to deplete the number of resources available to the NFV or SDN components; • retiring NFV instances or SDN elements that are in use by the operational network; • changing the SDN configuration. This risk could impact a single element or the whole mobile network. *Attack scenario 2*: Spoofing as an SDN controller, VIM or VNFM to send service management requests to the orchestration platform on the resource performance could cause the orchestration platform to initiate changes on the infrastructure. This exploit could be used by an attacker who wants to force the orchestration platform to move a NFV component to another datacentre where the attacker may have physical access or has compromised the virtualisation layer and wants to monitor customer traffic.	Access breach Denial of service Integrity compromise	[86], [6]
ATT19	Attacks occurring between NFV components	Supply chain attacks	Compromised components could affect network performance and compromise the confidentiality, integrity and availability of network assets. Furthermore, compromised devices may provide malicious actors with persistent access to 5G networks and the capability to intercept data that routes through the devices. Compromised devices may infect connected computers, phones and other devices with malware and may have data rerouted, changed or deleted. Untrusted companies that have significant international market share within telecommunication networks may introduce risks even if they do not have a large presence within EU networks. Therefore, even if the EU network were completely secure, data traveling overseas may pass through untrusted telecommunication networks and potentially be vulnerable to interception, manipulation, disruption, or destruction. This may result in anything from an attacker being able to install a malicious configuration and ultimately control the network element or function or, in the case of a damaged deployment, it could lead to limited or total failure of all the network elements that are scheduled to be updated.	Access breach Denial of service Integrity compromise	[62]

			An untrusted host OS and hypervisor or CIS may have embedded vulnerabilities (for example embedded Trojan software or rooted OS), exposing all VMs or containers and associated NFVs to attack. An attacker may exploit these embedded vulnerabilities to allow them to compromise VMs or containers operating within the hypervisor or CIS. As different virtualisation environments may provide different levels of security protection for the application layer, stand-alone testing of a VNF may not ensure that the desired level of assurance of the VNF remains the same when deployed in different virtualised scenarios. Furthermore, VNFs used in different service types (e.g. network slices) or different services (e.g. vertical services) may face requirements for security assurance that are different from the service layer. A VNF successfully tested in isolation may not provide the required level of assurance for a specific slice or service, for a given NFVI.		
ATT20	Attacks occurring between NFV components	Third party hosting attacks	A third-party tenant has direct access to the SAN (storage area network) and any local storage used by NFVs within the datacentre. This privileged access could facilitate access to security critical or customer information, or a DoS attack. When deployed by an operator who uses a third party host environment not under the operator's control, without appropriate protection, the sensitive information of a VNF could be compromised by the third party. An attacker with physical access to the hardware environment may be able to tamper or remove the TPM (trusted platform module), disabling the trusted computing platform function and facilitating other attacks, e.g. allowing an untrusted host OS and hypervisor or CIS to be installed.	Access breach Denial of service Integrity compromise	[61], [6]
ATT21	Attacks occurring between NFV components	Mixed deployment attacks	Vulnerabilities of a PNF could be used as a starting point for an attack against VNFs, potentially taking advantage of legacy security used by PNFs and not understood by VNFs. Vulnerabilities of a VNF could be used as a starting point to forward malicious messages to a PNF which has not been secured against attacks of that nature.	Access breach Denial of service Integrity compromise	[6]

E ANNEX: BEST PRACTICES REGISTER

ID	Measures/Best practices	Description	References
BP-T1	Security monitoring and filtering	Below are three approaches to deploy virtual security functions (e.g. antivirus, firewall, IDS/IPS). **Security function embedded within the VM container:** the advantage of this option is that the network security function is aware of the context of the VM or container. For example, the firewall is aware of any new port used by the network function and thus requires less configuration. The disadvantage is that the operator may not be able to choose or change the vendor of the security function, who is chosen by the provider of the network function. **Security function as a standalone VM/Container**: the network security functions are standalone VMs or containers. This option provides the operator with the flexibility to choose a vendor of security functions to protect particular network interfaces. However, such an architecture is exposed to malicious changes of the network topology and other network layer risks. **Security function in the virtualisation layer**: the network security agents are outside of the VMs or containers within the virtualisation layer. A single security function can protect all the VMs or containers managed by the virtualisation layer instead of having one security function per VM or container. The operator can easily change the vendor of the security function as the security function is independent of the VM or container. This option may, however, require more configuration compared with the first option where the security function is embedded within the VM or container. Network interfaces should be locked down so that they only accept a restricted number of expected protocols.	[1], [61], [47], [25]
BP-T2	VNF Image validation and protection	A VNF Package is composed of several components such as, for example, VNFD, software images, scripts, etc. During the on-boarding of the VNF package, a validation of the package should be performed. The validation should be a procedure that verifies the integrity of the VNF package. A package is certified by performing acceptance testing and full functional testing against the VNF including configuration, management and service assurance. It is easy to tamper with VNF images. It requires only a few seconds to insert some malware into a VNF image file while it is being uploaded to an image database or being transferred from an image database to a compute node. Luckily, VNF images can be cryptographically signed and verified during launch time. This can be achieved by setting up some signing authority and modifying the hypervisor or CIS configuration to verify an image's signature before they are launched. The software package and the artefacts within the package of a VNF shall have their integrity protected by the vendor's signature. The software package and the artefacts within the package of a VNF and the software catalogue holding its image should have their integrity protected after onboarding. The software package and the artefacts within the package of a VNF containing sensitive information must support the protection of confidentiality. Software package and artefacts within the package of a VNF must be bound to a specific network after onboarding, such that unauthorised software cannot be instantiated even if it has a valid vendor certificate.	[1], [13] [50], [47], [25], [133]
BP-T3	Tracking VNF version changes	The orchestration and VNF management systems should have the ability to keep track of multiple versions, multiple environments, multiple instances and allow the service provider team to perform updates or upgrades with clear expectations of service continuity based on metadata information including component dependencies.	[13], [38]

BP-T4	VNF deployment	Minimum baseline security controls and hardening measures should be configured for new VNF deployments. This can be done in many ways such as using pre-hardened golden images, deployment time configuration, etc. Such controls include fully implemented access control rules and ensuring that any unused ports, features, insecure protocols, or services are disabled.	[6], [25]
BP-T5	VNF deletion or relocation	The NFVO may only relocate or retire a VNF after backup and storage of critical data such as encryption keys or subscriber information to ensure this data is not lost during migration or restructuring of the network. This also applies when a request to relocate or retire a VNF comes from the EMS. The NFVO may only relocate or retire a VNF after having validated that the security and affinity policies can be and will be applied upon reintroduction of the element either in the same or a new location. This validation must take into account both operator and regulatory requirements. The NFVO may only relocate or retire a VNF after its operational state is no longer depended upon by other VNFs. In the event of a VNF being attacked or compromised it should be possible to isolate the VNF from the production environment and restore the VNF to a state prior to the attack. It should also be possible to take a snapshot of the affected VNF to allow for security investigation and analysis.	[38], [122]
BP-T6	Cryptography	Secure key management must be implemented to manage all the steps of a key lifecycle: key generation using an appropriate level of entropy from a reliable source, secure key storage, key rotation and revocation, secure key destruction, etc. The use of tamper resistant hardware security modules for secure boot and secure execution of cryptographic algorithms should be considered. Specific security cryptographic mechanisms include bidirectional authentication, transmission encryption and integrity protection. 3GPP TS 33.501[97] offers a detailed explanation of the security architecture and procedures for 5G. ENISA[98] lists several cryptographic best practices to accomplish this, including: • encrypt UE by default; • apply not-NULL ciphering for user and signalling data; • use a secure protocol on the network for both user and control plane data; • use state-of-the-art mechanisms for transport protection and mutual authentication; • implement the required authentication specifications and consider secondary authentication; • ensure keys are properly protected and stored; • ensure use of current security protocols for TLS (TLS 1.2 and above) and appropriate key and certificate management practices; • use tamper-resistant hardware for storing or processing critical data. ETSI GR NFV-SEC 005[99] provides a guide to the use of public key infrastructures (PKI) for the purpose of distributing public key certificates (PKC) as applicable to the ETSI ISG NFV for the support of public key cryptography in authenticating, authorising and encrypting links between objects in NFV. ENISA also recommends establishing PKI infrastructure for secure admin access and protecting your network against external access, especially in a cloud environment.	[25], [133]
BP-T7	Hypervisor/CIS protection	Hypervisor or CIS introspection can be used to scrutinise software running inside VMs or containers to find abnormal activities. It acts as a host-based IDS that has access to the states of all VMs or containers, so that the root kit and boot kit inside VMs or containers cannot hide easily. Using introspection capabilities, the hypervisor's or CIS's functionalities are enhanced, enabling it, among other things, to monitor network traffic, access files in storage, and to execute read memory. Hypervisor or CIS introspection APIs are powerful tools to perform deep VM or container analysis and	[1], [50], [47], [25]

[97] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169
[98] https://www.enisa.europa.eu/publications/security-in-5g-specifications/
[99] https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/005/01.02.01_60/gr_NFV-SEC005v010201p.pdf

		potentially increase VM or container security. However, they can also be used as an exploit that makes it possible to break and bypass the isolation between VMs or containers and the hypervisor or CIS. Example: LibVMI is the library for hypervisor introspection for various platforms, implemented in C language with Python bindings. It gives the hypervisor the means to perform deep inspection of VMs (e.g. memory checking, vCPU register inspection, and recording trapping events). The hypervisor or CIS must enforce network security policies. This includes, but is not limited to, ensuring that; • VMs or containers are isolated from each other, • VMs or containers are prevented from accessing each other's memory spaces, • keys used to encrypt memory are also under hypervisor or CIS control, • hypervisors or CISs are not allowed to write directly to memory, • hypervisors or CISs are not allowed to bypass normal memory access controls and security within the VM or container, • hypervisors or CISs are not allowed to change data within a VNF at run-time. Note: a Type 1 hypervisor is considered significantly more secure than a Type 2 'hosted' solution (where the hypervisor is installed on top of the host OS directly controlling the hardware and network adapters) as there are less attack services (OS and hypervisor).	
BP-T8	Security Management and Orchestration	One best practice consists of designing a NFV orchestrator incorporating the security and trust requirements of the NFVI. The orchestration and management of security functions requires integration by enabling interaction among the security orchestrator, the VNFM, and the element management systems (EMS). This type of protection can be achieved by setting scaling boundaries in the VNFD or network service descriptor (NSD), for example, and having the NFVO enforce these restrictions to protect from attacks such as a DNS amplification attack. Operators must ensure that they use an out-of-band (OOB) management network that is not accessible from the internet so management interfaces are secured from remote access. If an operator allows for remote access into the OOB for employees and/or OEM support, the operator must ensure that they use a multi-factor authentication (MFA), at a minimum, for any type of VPN access. An MFA VPN combined with zero-trust greatly improves secure remote access to protect the 5GC Network. Secure management and administration of the NFVI and NFV-MANO is critical for the security of a virtualised network. The following describe the basic principles for such secure management. a) Administration of the NFVI is only available over mutually authenticated, encrypted and integrity protected channels or APIs. b) All channels or APIs are separated from each other and use separate credentials. c) The number of privileged accounts for the NFVI is constrained to a minimal manageable number to meet the CSP's needs. d) NFV-MANO and NFVI administrators do not have any privileged rights to other services within the CSP. e) NFV-MANO and NFVI administrators are only provided with the privileges and accesses required to carry out their role. f) NFV-MANO and NFVI administrators do not have access to workloads running within the virtualised environment. g) NFV-MANO and NFVI administration access is limited to best practice configuration methods (e.g. authorised API calls). h) Internal components within VNFs are not able to directly connect to entities or management functions outside of the network trust domain, except via interfaces that are explicitly part of the VNF security design. i) NFV-MANO and NFVI administration is automated wherever possible. j) Manual administration of the NFVI is by exception and raises a security alert. k) Functions that manage the administration and security of the NFVI (e.g. MANO) are physically separate and do not run on the same NFVI as the NFs they manage.	[1], [50], [57], [61], [18]

		l) Functions that support the administration and security of the NFVI are treated as security critical functions.	
BP-T9	Remote attestation	The remote attestation (RA) technique can be used to remotely verify the trust status of an NFV platform. ETSI suggests leveraging hardware security module (HSM), trusted platform module (TPM) and virtual TPM/HSM (vTPM/vHSM) to provide trusted protection for VNFs. These modules are used to shelter integrity measurements (i.e. hash values), cryptographic keys and certificates that are required to empower remote attestation of VNF components. Indeed, remote attestation guarantees the integrity of VNF instances at load time. Practical implementations of the remote attestation service include the open cloud integrity tool (openCIT), an open-source software hosted on GitHub. It shall be possible to attest a VNF through the full attestation chain from the hardware layer through the virtualisation layer to the VNF layer. Attestation of a platform's integrity should be linked to the application layer and possible for other functions to query. If platform attestation fails, the VNF should not be allowed to run. Attestation of the VNF should be performed prior to deployment or network integration and during operations. In ETSI GR NFV-SEC 018, several use case scenarios are described that aim to establish specific trust between NFV stakeholders: (1) measurement of VM during launch, (2) protected VM launch on a trusted NFVI, (3) measurement of VM during launch and while in use, (4) remote attestation of secret storage, (5) secure VM migration between two trusted NFVIs. Other Examples of attestation solutions are Hytrust and OpenAttestation. In the OpenAttestation example, the launch of a VM only occurs when the Openstack Controller gets the confirmation that the compute node is trustworthy from a so-called attestation server (AS) which performs the appraisal of the trusted compute pool that Openstack Controller wants to use for the VM.	[1], [50], [47], [132]
BP-T10	Software compliance and integrity preservation	(6) A software checksum (hash or signature) should be created by the vendor during NFV and a supporting NFVI (e.g. host OS, hypervisor or CIS, SDN Controllers) software compilation that can be validated with a corresponding checksum created during any testing and validation process operated by the operator or a third party. (7) TEE is an important enabler for that goal. Tamper-proofing techniques enable the preservation of software integrity by causing an altered software to fail. (8) The concept of trusted execution and the associated technologies (e.g. Intel SGX enclave) that make certain that even a malicious host OS or operator cannot tamper or inspect any managed payload memory space.	[1], [63]
BP-T11	Security segmentation and isolation between network functions	To prevent a VM or container from impacting other VMs, containers or hosts, it is a best practice to separate VM or container traffic and management traffic. This will prevent attacks by VMs or containers tearing into the management infrastructure. It is also a good idea to separate the VLAN traffic into groups and disable all other VLANs that are not in use. Likewise, VMs or containers of similar functionalities can be grouped into specific zones and their traffic should be isolated. Each zone can be protected using access control policies and a dedicated firewall based on security level it needs. One example of such zones is a demilitarised zone (DMZ). Due to differing security requirements, a separate virtual environment using separate clusters should be setup for VNFs and MANO. Physical and/or logical separation shall be applied to keep sensitive control plane sub-components within a VNF (e.g. key material or billing data) away from lower security sub-functions or other general user plane traffic handling sub-functions. Best practices include:	[1], [50], [75], [78], [79], [47], [25], [17]

		(1) Linux kernel security: in virtualised platforms, the kernel of the host systems is a highly important component that provides isolation between the applications. The SELinux module, developed by the National Security Agency (NSA), is implemented in the kernel and provides robust isolation between the tenants when virtualisation technology is used over the host. Secure virtualisation (sVirt) is a new form of SELinux, developed to integrate mandatory access control security with Linux based hypervisors. sVirt provides isolation between VM processes and data files. Beyond these tools, other kernel hardening tools can be useful to secure the Linux kernel. A notable example is hidepd, which can be used to prevent unauthorised users from seeing the process information of other users. Another example is GRSecurity, which provides protection against attacks on corrupted memory. (2) Best practices are to avoid co-hosting, on the same hardware, VNFs that have very different levels of sensitivity or very different levels of vulnerability to influence by an attacker. (3) The trust domains of network functions should be identified. Each trust domain should be managed separately. Security policies for each trust domain should be managed independently. (4) Delegated administrator roles must be used, with roles which could give a user or administrator the ability to inspect the memory of functions only in exceptional circumstances. (5) Confidentiality protection should be provided to protect information traveling between memory locations in a single or multiple logical memory block.	
BP-T12	Secure boot integrity	Using trusted platform module (TPM) as a hardware root of trust, the measurement of system sensitive components such as platform firmware, BIOS, bootloader, OS kernel, and other system components can be securely stored and verified. The platform measurement can only be taken when the system is reset or rebooted; there is no way to write the new platform measurement in TPM during the system run-time. The validation of the platform measurements can be performed by TPM's launch control policy (LCP) or through the remote attestation server.	[50], [79], [25]
BP-T13	Data protection and privacy	For the RAN operator, theft of sensitive or private data may result in churn, fines and loss of business due to compromised business reputation or regulatory violation. The operator is responsible for ensuring that data in transit, at rest and in use are protected according to the requirements of the regulatory agency and use case using the following best industry practices: **Data at rest** Sensitive information of a VNF shall be protected during its lifecycle process to avoid leakage of the information to other VNFs reusing the storage resource. Data should be backed up, while sensitive data, such as security logs, should be encrypted before storage in the persistent volume. Access control and monitoring data access and usage are other essential functions for protecting data. A privacy impact assessment (PIA) for personally identifiable information (PII) should be performed to identify and mitigate privacy risks to data assets. When VNF moves from one host to another or when VNF is terminated, the system should ensure that resources, privacy sensitive data, and/or keys are fully cleared. Security policy which restricts where certain types of data can reside should be defined and implemented by CSPs. **Data in transit** Data must be encrypted, and its integrity protected, when it flows between the different parts of the VNFs and, externally, between NFV nodes to defend against internal and external attacks. 3GPP 33.501 stipulates mutual authentication with X.509 certificates. In addition, the following security protocols among others should be used: • air interface: 5G provides encryption and integrity protection of control signalling and encryption and optional integrity of user data; • control plane: DTLS 1.2; • management plane: Mutual TLS using version 1.2 and above.	[47], [25], [113]

		Data-in-use Depending on the existing protection of the cloud infrastructure, additional protection of data in use could be needed. For instance, the use of trusted execution environments (TEE) has the potential to increase the security of crypto and key-management operations and protect data in use.	
BP-T14	Encrypting VNF volume/swap areas	The best practice to secure the VNF volumes is by encrypting them and storing the cryptographic keys at safe locations. TPM or HSM modules can be used to securely store these keys. In addition, the hypervisor or CIS should be configured to securely wipe out the virtual volume disks in the event a VNF is crashed or intentionally destroyed to prevent it from unauthorised access. VM or container swapping is a memory management technique used to move memory segments from the main memory to disk, which is used as a secondary memory in order to increase system performance in case the system runs out of memory. These transferred memory segments can contain sensitive information such as passwords and certificates. They can be stored on the disk and remain persistent even after system reboot. This enables an attack scenario whereby a VM or container swap is copied and investigated to retrieve any useful information. One way to avoid this kind of attack is to encrypt VM or container swap areas. Linux based tools such as dm-crypt can be used for this purpose.	[50], [25], [133]
BP-T15	Trusted computing technologies	To provide a trusted hardware platform, the hardware (blade servers) should support Intel TXT, SGX, AMD SEV or ARM Trustzone silicon-based security functionality implemented with a TPM that stores measurements of the entire hypervisor or CIS stack and boot process. This measure should be applied to: • blade clusters supporting VNF that support security critical functions; for example, lawful interception, customer access credential (HSS), security key management (AuC) or that have external traffic interfaces directly accessed by third parties or customers (Internet, GRX); • all other MANO and VNF blade clusters to improve base platform security and reduce the complexity of affinity rules and hardware cluster of differing security trust levels. A mechanism should be in place to identify any attempt to physically remove the TPM from a system board. If physical tampering has been identified the blade server should be considered compromised and no longer be used to support VNFs. For example, on HP blades any attempt to remove an installed TPM from the system board breaks or disfigures the TPM security rivet.	[25]
BP-T16	Hardware security	If hardware is provided by a third party cloud provider, then a dedicated cluster supporting only the operator's VNFs should be provided to ensure physical, not logical, segregation from other tenants. It is also recommended that separate dedicated hardware is used to provide independent NFV management (MANO) and service clusters (NFV). In addition, separated clusters should be used to provide MANO and NFVI. The use of HW secure enclave technologies, such as AMD SEV and Intel TDX provide stronger tenant isolation from the cloud provider. The general commercial off-the-shelf (COTS) hardware may have varying levels of security functionality, such as hardware rooted secure storage, unique hardware identities, secure boot with software integrity check, and trusted execution environment (TEE), built-in depending on the manufacturer. TEE refers to a technique of storing or running code in a protected memory area where no other applications or the host have access. An example is secure enclaves that can be used as a hardware root-of-trust for secure storage of secrets and running sensitive code. A HSM or TPM can be used to provide hardware rooted protection of keys.	[113]
BP-T17	Centralised log auditing	All the NFV, SDN and MANO elements should submit security events (e.g. authentication, authorisation and accounting, login attempts, administration functions and configurations) to a centralised platform, which shall monitor and analyse in real time the messages for possible attempts at intrusion. It is also recommended that all the elements make use of the same trust time synchronising source (e.g. NTP server) to support accurate correlation of events across the network. It is also recommended that all audit logs are transferred to a log management platform outside the NFV to maintain their integrity and remove the risk of tampering.	[79], [80], [25]

BP-T18	Use and ownership of 'root' administration credentials	It is recommended that: • each hypervisor or CIS has a single 'root' admin account that is used for local administration and to connect the host to VIM; • to avoid sharing this common 'root' account, across the whole NFVI, at least one local named user account be created and assigned full admin privileges, and this account should be the primary account for operating the hypervisor or CIS; • strong access controls, account privileges and security logging are enabled; • the hypervisor or CIS is configured to support multiple administration roles, and as a minimum there must be an admin role (highest privilege) and a separate operational role with minimal privileges to complete normal operational support; • delegated administrator roles be used, with the global administrator role only being used in exceptional cases, e.g. to add permissions for other high-level administrators; • all administration login attempts and critical operations must be logged and audited.	[79], [6], [47], [25]
BP-T19	VNF protection	**Protection of VNFs** It should be possible to deploy a VNF to a host that provides specific security resources (e.g. HMEE, secure compute, secure memory) in order to bind a VNF to a specific host or group of hosts. Binding should be verified by secure hardware backed attestation of the health and security of the host. Controls should be verified and enforced at boot time and each time a function is migrated. The system should manage (e.g. assign or log bindings) key storage and confidential data in a manner that provides protection against data compromise. Sensitive data should only be decrypted or handled in an unencrypted format in VNFs on trusted and well-known hosts. It must be possible to control whether untrusted or less trusted VNFs are allowed to run on the same host as VNFs in a higher trust domain. It must be possible to further restrict VNFs on a single host depending on whether they handle decrypted sensitive data. The system should prevent and detect unauthorised or unintended data manipulation and leakage (e.g. modification of VNF images, instantiating parallel VM(s) or container(s) on the same physical CPU). **Securing internal VNF communication** Where a NFV is composed on multiple VNFs the vendor should demonstrate how it protects the internal communication of its NFV, as it transits between VMs or containers. **Protection of stored data** NFV vendors should ensure that any security critical (including LI), customer privacy or confidentiality related information is stored securely on any shared or local storage (e.g. SAN, SSD). Vendors should be able to clearly state the security mechanisms used to protect this data using industry standard best practice (e.g. encryption). **Protection of LI data and functionality** NFV vendors should demonstrate how they are protecting LI functionality to ensure that it cannot be compromised or weakened by running their VNF in the NFV environment. It is recommended that vendors are asked to clearly state how they are compliant in protecting sensitive LI data and interfaces and to specify whether there are any specific deployment requirements to allow their VNF to operate in a multi-vendor virtualised environment and ensure that the integrity of their security mechanisms is maintained.	[6], [47], [25], [123], [17]

BP-T20	Local or removable blade storage – SAN protection	**Local storage protection** If local blade storage is supported, then it should not store sensitive information such that its theft or removal would enable an attacker to gain a copy of the stored data. **Mutual authentication between VMs or containers and SAN** Mutual authentication should be implemented between each VM or container and its associated SAN storage using CHAP (e.g. DH-CHAP, FCPAP). **SAN data protection in transit** The operator should consider protecting sensitive data in transit between NFV and SAN using encapsulated security payload (ESP), as specified by the fibre channel protocol (FC-SP) or equivalent. **SAN physical blade interface** It is recommended that a separate physical interface module is used on each blade or rack mounted server for connectivity to the SAN. It is not recommended for any SAN connectivity to share common IP interface with other operational traffic. **SAN storage protection** The SAN storage shall protect against tampering and any ability to create unauthorised local copies of any of the stored data. In the event of tampering or unauthorised copying, an alarm and log event should be generated recording what data has been copied and which user initiated the action. Note: it is expected that the SAN security (including backup management) will be addressed through existing IT security controls for the operation, access, backup and availability of the SAN.	[6], [47], [25], [114]
BP-T21	Network security	**Topology hiding** All internal interfaces between VNF elements, supporting MANO platforms and IT elements (mediation, provisioning) that are not required to publicly communicate outside the operators network, should use private IP addresses. It is recommended that all external interfaces are NAT through a firewalling function to provide additional protection of the identity of the elements within the VNFI. **VNF network security profile** Each VNF supporting VNFC functions should have a predefined network security profile describing its requirements for vNICs, ports, port group, VLANs and the requirement for internal VXLAN connections. The security profile shall also define the vNIC firewall rules related to protocols (port numbers) that need to be supported on each VLAN or VXLAN connection. It is expected that vendors will provide a security profile for their applications, which will have to be aligned with the operators' zoning guidelines. Note: there should never be a requirement for all ports to be open, particularly on external standard based interfaces (e.g. GTP). **Deploy NFVs with separate dedicated interfaces** Ideally, separate physical interfaces should be implemented to maintain different traffic segregation in line with security zoning and X.805 principles. However, if this is not supported by a vendor then a separate logical interface and VLAN must be used to maintain security zoning. **Production and O&M traffic separation** O&M interfaces should not share the same physical NIC, vNIC, distributed port group (DPG) or port group with other production traffic types (e.g. BSS, User Plane or Signalling).	[6], [47], [25]

		Connectivity from management to production cluster Any connectivity between the operation and management (MANO) cluster and the production cluster should pass through a firewall. If a virtual firewall is implemented, it should be implemented within the management cluster. Note: it is expected that MANO systems would not share the same hypervisor or CIS environment as production NFV elements. **Network resource pools** To prevent a VM or container causing a DoS by monopolising system and network resources, it is recommended that network resource pools should be configured. **Internal virtual switching control** The internal hypervisor or CIS controlled virtual IP network (vSwitch/VDS) should be controlled to ensure a policy of positive enabling and must not support default connectivity or 'any to any' functionality. **Virtual network monitoring** In some deployments, internal network monitoring functions can be installed on the virtualisation layer. If these are installed, the functions must be restricted to the administrator only and should not provide a mechanism for compromising the security of the hypervisor or CIS or other VMs or containers. Additionally, any operation of this type of monitoring functionality should generate an alarm to the VIM and be recorded in the audit logs. **VLAN and VXLAN zoning** A comprehensive set of common VLAN and VXLANs must be created across each NFVi to ensure traffic separation and security zoning requirements. Note: VLAN and VXLAN zoning should ensure that clear vendor separation is maintained. Only VLAN and VXLANs necessary to support VNFs hosted on a cluster should be configured on the 'leaf' and 'spine' switching layers. The VLAN IP infrastructure should follow existing segmentation and zoning rules with the use of firewalls or other security controls to provide protection between zones. Existing hardware firewall appliances can continue to be used to provide boundary protection when connecting to untrusted or semi-trusted networks (e.g. internet or GRX). However, it is recognised that virtualised security appliances may be used in the future. **Use of VPNs** Where possible, VPNs should be created between VNFs and both internal and external non-VNF environments, e.g. interconnectivity between P-GW and Mediation for EDR transfer or HLR/HSS provisioning interfaces with the BSS Provisioning platform. **Dedicated network infrastructure** If a third party XaaS provider is being used then it is recommended that dedicated local 'leaf' switching infrastructure supporting only the operator VNFs is provided to ensure segregation from other tenants. Additionally, it is also recommended that dedicated spine switches be provided also but this may not always be practical. **Protect all OAM traffic** Link security can be provided through the use of native traffic encryption such as HTTPS, SFTP, SMNP v3 or using TLS or IPsec tunnelling protocols. Note: it is recommended this control should be applied in addition to any security protection provided if, for example, OAM traffic is carried over an IPsec tunnel.	

BP-T22	SDN security management	The following controls apply if using a message bus technology for communication between SDN elements. However, it is expected this technology will be widely used in 5G architectures. • A strong mechanism to authenticate the integrity of messages must be deployed between the 'publisher' and 'producer' over the message bus. No messages should be accepted or processed by the message broker or 'consumer' systems from unknown, 'fake' or unauthenticated users. It is recommended to that communications be secured using TLS (TLS 1.2 and above) security or certificates where supported (e.g. Kafka),. • The message bus should be monitored for any unauthenticated messages or 'fake' or default usernames and a security alarm raised for investigation. • If an SDN is deployed to support the NFVi then it is recommended that security functionality is deployed that identifies potential attacks on any SDN elements. Any security functionality should provide automated alarms and the ability to change the network or element configuration to mitigate the attack. For example: o DoS attacks on SDN elements (specifically, NEs and SDN Controllers); o Access control failures or attempts to use functions or services where the user does not have the correct privileges. • A high availability architecture should be implemented for key SDN components (e.g. SDN Controllers) to ensure operational service is maintained. The design should include primary and secondary IP links with, where possible, diverse routing to allow for single point of network failure. • It is recommended, in order to maintain operational integrity, that any changes to network, service and virtual environments are restricted to the orchestrator. Therefore, the SDN Controller and the VNFM and VIM should have additional controls applied to them to restrict such access for normal operation. Restricting the SDN Controller and the VNFM and VIM will prevent the application of rules and changes that may break policy and rules during deployment of service templates. • For operational emergencies a high-level administration account should be created. However such an account must not be available to support engineers or used during normal operations. The credentials should be stored safely and be maintained by operations management. Ideally, these should be stored in a safe physical location such as a safe with monitored and recorded access. • The orchestration layer and SDN must be architected so that SDN networks and NFV environments are not operationally dependent on the orchestration or MANO layer to maintain operating services under circumstances that may render the orchestration platform unavailable.	[6], [97], [121]
BP-T23	MANO access control and management	The MANO components should support a high-level of role granularity to ensure appropriate levels of privilege can be assigned to all users to protect key processes and the integrity of data. Ideally, all OAM access should be controlled through a centralised single sign-on or PAM solution with all access (success and failure) recorded in the audit log mechanism. Multi-factor authentication should be used to log into administrator accounts. All administration and management should only be permitted from known, attested devices and multi-factor authentication should be enforced. In ETSI GS NFV-SEC 022, ETSI defines an access token mechanism for the authorisation of access for NFV-MANO APIs and the associated procedure for the verification of the access token. One solution defined to handle these authorisations for API request and notification is the use of OAuth 2.0 protocol as defined by IETF RFC 6749[100]. The confidentiality and data integrity of all messages must be ensured, e.g. by using a transport-layer mechanism, such as TLS (TLS 1.2 and above), on each interface. The authorisation server database used to authenticate the user	[6], [47], [123], [134], [135]

[100] https://datatracker.ietf.org/doc/html/rfc6749

		and store associated user credentials, access tokens and refresh tokens must be stored in a tamper resistant location (e.g. HSM). See ETSI GS NFV-SOL 013 and ETSI GS NFV-SEC 022 for technical details.	
BP-T24	VIM connectivity to virtualisation layer	The connectivity between the VIM and the virtualisation layer should support a secure access protocol (e.g. IPSec, TLS) to protect against the eavesdropping of password information. It is also recommended that the secure access should support mutual authentication before allowing any O&M connectivity. Additionally, it is advised that any vendor defaults (e.g. self-signed certificates) be removed and replaced with operator generated certificates. Each operator should develop a certificate policy in accordance with their regional and national requirements as described in ETSI GR NFV-SEC 005.	[6], [25], [133]
BP-T25	Recovery and reinstallation	Recovery mechanisms in NFV must ensure the following: • The NFVI must be restored completely, with all configurations and settings adjusted correctly. This includes controller nodes pointing to the right set of components, settings reloaded with correct parameters, and full inter-operability restored. Of particular importance is restoring the interoperation between NFV, SDN, and MANO systems, in an automated way, without the need for human intervention to reconfigure these systems to become functional again. • VNFs must be fully restored. This includes reloading virtual machines, containers and network services and setting the last state in place correctly. • In the event of a suspected compromised of a hypervisor or CIS, or a VM or container it should be possible to overwrite a hypervisor or CIS installation or individual VM or container with minimal need for platform re-configuration. • Any reload mechanism should be securely controlled and managed remotely by the VIM, or locally using secure access through the LMT, and also include verification of hardware integrity (e.g. boot disc, UEFI). • When instantiating a new VM or container instance it is recommended that a different guest operating system 'root' administration credentials or security keys (IPSec, TLS) should be used for each instance.	[49], [38], [122]
BP-T26	Deploying VMs/containers of differing trust levels	The VIM should be configured to ensure that VMs or containers of differing trust levels are not deployed on the same physical host or blade and that VMs or containers requiring a 'hardware root of trust' cannot be installed on a physical host or blade that does not fully support trusted boot (e.g. Intel-TXT) and TPM. For example, a VNF that requires a 'trusted computing' environment to support LI functions should only be installed on a cluster than can support this level of security.	[6], [25], [123]
BP-T27	NFVO security management	A mutual authentication mechanism should exist between the NFVO, VIM and EMS platforms to provide a level of trust and to ensure only the authorised NFVO can make requests to the VIM and EMS platforms and vice versa. The NFVO should provide internal workflow rules to prevent accidental changes to the NFVi and NFV services that could have an impact on service delivery. A mechanism should exist to provide configuration roll-back in the event of any unauthorised or accidental service changes. The NFVO should create and maintain a comprehensive audit log of all service changes including the identity of the user making each change. The NFVO should implement robust transaction management for any NFV management for supporting NFVi changes to ensure that the opportunity for configuration integrity errors across the orchestration controlled elements and service inventory is eliminated. Best practice for provisioning platform controls for configuration roll-back and failure alarming must be implemented.	[6], [38], [122], [123]

BP-T28	Trusted time source	The VNFs should synchronise with trusted time servers such as a GPS or an atomic clock. In 5G networks, high precision time synchronisation within microseconds will be required. 5G will not only provide personal mobile service, but also massive machine type communications (MTC) and services where latency and reliability are critical. These critical services require trusted and protected time sources. ETSI GR NFV-SEC 016 (Draft specification - work in progress) is a study on how the location of sensitive VNFs (e.g. LI functions, VNFs handling data with restrictions on the location where data protection is handled and network security functions) can be attested. The study considers using trusted locstamp and timestamp information derived from global navigation satellite systems (GNSS), such as Galileo. The study also considers other binding solutions for physical location. The report outlines several solutions for timestamp-time synchronisation and distribution (e.g. White Rabbit Network, IEEE® 1588-2019, based on trusted GNSS/ LEOs), for timestamp datacentre time protocol (DTP) and for locstamp (e.g. based on binding a trusted hardware's ID with the location of a vertical hierarchy, indoor positioning such as RFID tagging and trusted GNSS positioning).	[47], [136]
BP-T29	Secure 3rd party hosting environments	Third party hosting environments that support VNFs should meet 3GPP virtualisation security requirements to enable operators to meet legal or regulatory requirements. The system should be able to monitor the attestation of third party hosting environments.	[47]
BP-T30	Redundancy and backup	**Recovery** The system should be deployed in such a way as to provide isolation and redundancy to increase the resiliency and defence against a single point of failure. MANO functions should include internal health checks to detect potential intrusion and take protective action. There are a variety of ways operators should consider redundancy. Below are three ways the operator should be thinking about redundancy when it comes to its recovery plan. • *Network redundancy*: network redundancy is the process of adding additional instances of network devices and lines of communication to help ensure network availability and decrease the risk of failure along the critical data path. Having redundancy by providing additional pathways through your network via redundant routers or switches would ensure minimal downtime and complete continuity of NFV services. • *Power redundancy*: backup power supply (a generator, for instance) that specifically keeps critical NFV hardware running in colocation facilities. • *Geographic redundancy*: geographic redundancy is important for how sensitive data is backed up. Having a redundant backup in an entirely different location will allow quicker recovery with little downtime. • The recovery plan should already identify a fail-over location for the NFV system in the event that the current location is inoperable. **Backup** Backups is the process of creating and storing copies of NFV data to protect against data loss. A backup involves duplicating important data like VNF code and data, configurations, cryptographic materials, network configurations, audit logs or anything that the NFV system needs to stay operational. Regardless of the backup solution chosen, offsite backups are a must across all industries. Operators are required to store backups in a secure location, preferably an off-site facility, such as an alternate or backup site. Having both backups and redundancy contributes to the NFV system running smoothly. Backups make sure that if something is lost, corrupted or stolen then a copy of the sensitive NFV data is available. Redundancy makes sure that if something fails, the NFV system is able to work regardless of the problem.	[47]
BP-T31	Specific container security controls	Appropriate restrictions on container placement and on the use of container caching should include: • user handling containers relative to network management containers within a VNF; • separation of containers belonging to different NFs on different physical servers;	[47]

		• special handling of containers implementing interfaces between different trust domains (intra-VNF and inter-VNF). The virtualisation layer must provide capabilities to limit the impact on co-hosted containers caused by a rogue container escaping its isolation. One of the commonly practiced security controls is to enforce strict resource limits on container usage, which helps in preventing resource starvation due to an attack by a rogue container. The virtualisation layer must enforce the principle of 'least privilege' which ensures that no containers run with a privilege higher than what is actually required. The VNF images shall not be packaged with embedded secrets such as passwords or credentials, or any other critical configuration data. NIST SP 800-190[101] and ANSSI[102], Container security[103], Redhat[104] and others provide detailed best practices for the security of containers.	
BP-T32	OSS/BSS protection	The contrasting attributes of the legacy and virtualised infrastructures should be considered from an overall management perspective. This will be particularly important during the migration phase while both types of infrastructure are running in parallel. The OSS/BSS would, therefore, need to be adapted for near-real time operation and be able to support a hybrid network across SDN/NFV and non-SDN, non-NFV domains. OSS systems should be consistent with the ETSI NFV architectural framework [7] and support the Os-Ma interface between the traditional OSS/BSS and the NFV management and orchestration (MANO) framework. OSS/BSS systems should delegate fine-grained management of the NFV Infrastructure and the specific VNFs to the VIM and the VNFM, which in turn are orchestrated by the NFV orchestrator (NFVO). Thus, the OSS/BSS will be responsible for the high level configuration of the infrastructure and network functions, but the NFV MANO framework will manage the dynamic aspects of infrastructure and services[105]. The integration with the SDN controller and applications will follow a similar approach. The OSS will manage the configuration of the SDN data plane, configure and set policies for the SDN controller and control SLAs for SDN applications, but the dynamic control of the SDN forwarding plane will be managed by the SDN controller and the SDN control to data-path interface (CDPI)[106] [107]. Operators moving to deploy virtualised network architectures based on SDN and NFV are likely to evolve the OSS/BSS systems in stages. Existing operators have a significant installed base and it is unrealistic to replace all existing infrastructure. The new capability will be deployed first where it brings the most value or where the legacy network requires upgrades anyway[108].	[99], [100], [101]
BP-T33	LI capabilities	General recommendations involve: • Dialogue between governments and 5G stakeholders to define clear, modular and transparent LI; • Efficient LI implementation through regulatory consistency, adoption of existing international technical standards (e.g. 3GPP, ETSI), and centralised, multi-country LI solutions; • LI law and regulation that is clear, transparent and judiciously implemented. The following provides a brief checklist of security measures that 5G stakeholders should consider. • *Passwords and authentication*: LI operations should be managed by the principle of least privilege (POLP), which limits each user to the minimum access privileges needed to perform his or her job. Access controls for the users should use two-factor authentication. • *Encryption*: all LI data should be transmitted, both within the network and on the external delivery interface, with strong encryption.	[102], [103], [127]

[101] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf
[102] https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-au-deploiement-de-conteneurs-docker/
[103] https://cdn2.hubspot.net/hubfs/1665891/Assets/Container%20Security%20by%20Liz%20Rice%20-%20OReilly%20Apr%202020.pdf
[104] https://www.redhat.com/cms/managed-files/cl-container-security-openshift-cloud-devops-tech-detail-f7530kc-201705-en.pdf
[105] https://opennetworking.org/wp-content/uploads/2014/10/sb-OSS-BSS.pdf
[106] https://opennetworking.org/wp-content/uploads/2014/10/sb-OSS-BSS.pdf
[107] https://opennetworking.org/wp-content/uploads/2014/10/sb-OSS-BSS.pdf
[108] https://opennetworking.org/wp-content/uploads/2014/10/sb-OSS-BSS.pdf

		• *Host hardening*: the LI solution device(s) should be equipped with a robust host intrusion detection system to guard against unauthorised users. • *Network hardening*: the network should contain properly-configured firewalls and use routing methods to keep the LI functionality and data segregated from all other network activity. • *Network monitoring*: a network monitoring system, including a network intrusion prevention system and a network intrusion detection system, enables you to see which users enter and exit the network and when. The system also monitors uptime and downtime on different devices and provides visibility into broadband utilisation and link status. • *Dedicated solution*: the LI solution should be dedicated to LI purposes only. Trying to leverage the LI device for commercial uses such as traffic monitoring may expose the equipment to unauthorised use or operational risks. • *Potential breach reporting*: any compromise or potential compromise of an LI must be reported to law enforcement. • *Testing*: once the LI solution is installed, it must be tested. The communication features to be tested will vary depending on the type of network (e.g. broadband, wireless, VoIP) and the communication features offered on the given network. • *Periodic testing*: communication networks evolve over time. A network change may disable or impair the workings of the LI solution. For this reason the network operator should schedule periodic testing of the solution. • *Software maintenance*: like most forms of software, an LI solution requires maintenance. Any LI licensing agreement should arrange for patches, updates and upgrades as needed. Specifically, all security patches and updates for all LI platforms must be installed and kept current. • *Penetration testing*: in a penetration test, an external entity searches for cyber vulnerabilities in the LI solution and tries to 'hack' into it. • *Security policy*: the LI security policy should be included in the operator's written network security policy, which should implement industry standards such as ISO 27001, NIST SP 800 series, etc.	
BP-T34	User plane security	Additional security controls are needed on the user plane as follows: • to protect NFV components from attacks sourced from the public internet and cloud; • to protect the network from attacks sourced from internally attached NFV components; • to protect the NFVI from attacks sourced from internally attached components and the internet. Inline detection and mitigation functions in the network can be used at the internet edge to prevent volumetric DDoS attacks from the internet, including TCP SYN floods, UDP floods, and DNS floods, which can attack the availability of the network or service. Threat detection or prevention and response using IDS/IPS should also be used to effectively defend against or prevent malware and ransomware infections on NFVI and network functions.	[113]
BP-T35	MEC security	To address the issue of inadequate isolation, MEC can include network segmentation, resource separation, data segregation, software and network attestation, etc. The hardening of MEC needs to ensure that all the default configurations (including OS software, firmware, and applications) are appropriately set and, further, that these settings can be verified against a reference. Countermeasures such as the filtering of packets heading for the target site under attack, restriction of the communication port used for DoS/DDoS attacks, and the reduction or suspension of the operations of target telecommunications facilities need to be considered. A regular security testing programme or certification of MEC components is required as part of a secure value chain. Control measures to ensure the security of physically isolated areas of MEC components include earthquake-proofing, automatic fire control equipment, monitoring by a remote office to detect facility failures, physically secure perimeters, supporting automatic alert function, etc. The physical	[126]

		security may not be fully guaranteed in a MEC environment and critical MEC components (e.g. security end points and crypto functions) need to be implemented in HMEEs (hardware mediated execution environments) e.g. Intel SGX or ARM TrustZone. SBI (service-based interface) of MEC components should provide adequate protection for access and data in transit. The confidentiality and data integrity of all messages should be ensured by using TLS on each interface. Appropriate security controls are required for protecting sensitive data during storage, processing and transfer by MEC applications. The MEC platform should authenticate all MEC application instances and only provide them with the information for which the application is authorised. OAuth 2.0 based on X.509 client certificates are used for authorisation of access to RESTful MEC service APIs as defined by ETSI ISG MEC. In the case of service-producing applications defined by third parties, other mechanisms such as standalone use of JWT (JSON web token) can be used to secure related APIs. In addition, since MEC is based on virtualised infrastructure, it needs to include real-time security management based on NFV specifications (see ETSI GS NFV-SEC 013 [38]). Especially when deploying MEC in NFV environments, MEC should be considered as part of a whole system real-time security monitoring and management strategy. Appropriate mechanisms for the collection and processing of security events should be in place, where the log functions should upload log files securely to a central location or to an external system. Secure transport protocols should be used. Access to the security event log should be controlled to allow only privileged users to have access to the log files. Critical event logs must be enhanced with mechanisms to enable independent third parties to audit them, preserving their arrow of time and their links to the identities of the elements involved. As part of regulatory issues, the European regulation (NIS-Directive) expects isolation of physical and logical components of critical services from services with low criticality. The MEC system needs to support regulatory requirements for lawful interception and retained data based on ETSI and 3GPP standards (e.g. in ETSI TS 101 331[109], ETSI TS 102 656[110] and 3GPP TS 33.126[111]).	
BP-P1	Zero trust	Treat 5G infrastructure as an untrusted environment and explicitly authenticate and authorise interactions between all assets in all areas - both inside and outside the network - prior to allowing access. Secure and limit interactions to the minimum necessary, and continuously monitor asset security posture, adjusting access rights accordingly. Zero trust represents an overarching access security model that deliberately avoids assuming implicit trust between elements in a network. This is particularly important in 5G as various external stakeholders may need to access infrastructure components or services for management, maintenance or monitoring purposes. For example, enterprise users may need to select access to 5G slice management services. Third party vendors may need access to select components for configuration or troubleshooting. Properly implemented, zero trust can provide appropriate stakeholder access while securing 5G services against misuse. Strong digital identities with digital signing from a certificate authority (CA) establishes a root of trust for VNFs while mutual authentication using transport layer security (TLS) or datagram TLS (DTLS) with public-key infrastructure and X.509 (PKIX) and strong cipher suites ensures trust between network functions, between the network and NFV, and between application clients and server. (D)TLS with X.509 digital certificates provide automation and security to ensure that only trusted devices are permitted access to a trusted network and application. 5G also provides strong mutual authentication using 5G-AKA, EAP-AKA and EAP-TLS. A zero trust architecture includes automated security configuration for control policies over user access with visibility, monitoring and logging for alerting and auditing. Multifactor authentication (MFA), an important component of zero trust, should be used to ensure secure human access to management interfaces and applications in the 5G NFV. NFV components should be assumed to be untrusted and be able to establish trust through the process of certificate based mutual authentication. Any of the NFV entities or components should have a certificate and an associated and protected private key to execute cryptographic security functions with other terminating entities as described in ETSI GR NFV-SEC.	[61], [27], [113], [131], [133]
BP-P2	Security assessment of new or changes to existing VNF service templates	New or modified VNF service templates should be validated through proper risk assessment by a security professional. This process ensures that the template complies with applicable legal and regulatory requirements. It also ensures that the template adheres to specific security policies on interface security, security affinity/anti-affinity rules, NFV network zoning and application security.	[6], [47], [25], [123]

[109] https://www.etsi.org/deliver/etsi_ts/101300_101399/101331/01.07.01_60/ts_101331v010701p.pdf
[110] https://www.etsi.org/deliver/etsi_ts/102600_102699/102656/01.03.01_60/ts_102656v010301p.pdf
[111] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3181

BP-P3	Vulnerability handling & patch management	NFV/MANO software components will need to be monitored for vulnerabilities and patched as quickly as possible to address evolving risks and ensure security and functionality. According to the report of the Cyberspace Solarium Commission, patch development and distribution—the process whereby a software developer creates a fix for a vulnerability and distributes it to users—is key to eliminating the risk that a given vulnerability can pose. The report recommends, among other things, that developers and manufacturers of software and hardware components establish a publicly accessible process for reporting vulnerabilities, retain records documenting when a vulnerability was made known or discovered by the company, and maintain a vulnerability disclosure and patching policy for their products. In addition, the report recommends that the US government study the potential effectiveness of directing NIST to develop guidance or expectations about how quickly patches should be implemented once released.	[60], [25], [123]
BP-P4	Security testing assurance	Regular penetration and vulnerability testing should be performed across the NFVI and MANO production environment to identify any known vulnerabilities or compromise of the network zoning rules. It is recommended that testing should be carried out if new infrastructure or IP based interconnect elements have been deployed or as a minimum on an annual basis. Security assurance testing of a VNF needs to be performed using a standardised NFVI environment used to test all VNFs. When testing the security assurance of a VNF, the scope of testing should be clarified, including defining the pre-conditions of the virtualised test environment or platform and defining assumptions made in the process. Where possible, recreate these assumptions in the product deployment, e.g. close ports which do not need to be open. Both positive and common vulnerability testing (e.g. negative testing) should be carried out against VNFs and the underlying virtualisation and hardware layers. This is required to mitigate the increased attack surface which was partly addressed by physical security assurance protections in physical networks. VNFs should be checked regularly to see if they are using out-of-date or insecure versions of a library and these libraries should be updated if and when possible. This is required to mitigate the increased attack surface which was partly addressed by physical security assurance protections in physical networks. It is recommended to use certified components (e.g. hypervisors, OSs, TEE, TPM, etc.) according to a recognised scheme such as Common Criteria. Potential solutions to the above requirements include, among others, the NESAS 3GPP(SCAS)/GSMA and ENISA EU certifications schemes (Currently, three cybersecurity certification schemes are under development by ENISA. One scheme, covering ICT products and called EUCC, is almost ready. It is based on an existing international scheme called Common Criteria. There is a second scheme covering cloud services (this is the EUCS scheme) and a third one on 5G networks (EU5G)).	[6], [47], [25], [139]
BP-P5	Incident management	Implement defensive security controls and continuous monitoring backed by machine learning capabilities and establish incident response operations to detect and mitigate threats. Key capabilities include the following. - *Vulnerability management*: adopt internationally-accepted standards and best practices on the coordinated disclosure of vulnerabilities and handling to effectively identify, mitigate, and remediate security vulnerabilities (e.g. software patching) in a timely manner. - *Denial-of-service defence systems*: monitor network traffic to detect and mitigate network flooding attacks. - *Intrusion detection and prevention systems*: monitor network traffic to detect and mitigate unauthorised access or attempts to exploit system vulnerabilities. - *Malicious traffic filtering systems*: monitor network traffic to block malicious or unwanted traffic such as spam or attempts to interact with malicious domains and websites. - *Anti-malware systems*: monitor network traffic and endpoint and server devices to detect and block malware files or malware execution. - *Security operations centre*: establish a centralised security monitoring, incident response, and threat intelligence organisation responsible for rapidly detecting and mitigating security breaches. Adopt integrated cybersecurity capabilities and automation tools that simplify and streamline security operations.	[27]

BP-P6	Secure update management	The process must consider the ability to update the cryptographic algorithms and to adapt to upcoming 5G security challenges. Updates must be applied in a timely manner to protect against hardware or software bugs and security flaws, including those which are newly found.	[50], [47]
BP-P7	Restrictions on installing applications	It should not be possible to install a VNF application into the operational NFV environment without validation and approval by the operator. Note: this can be a manual control process but it is expected that additional technical security controls will be adopted that allow only signed code to be installed in the NFV infrastructure.	[1], [50], [6], [47], [25]
BP-P8	Defence-in-depth	Operators need to use all the layers of security (defence-in-depth) to protect the NFV platforms including firewalls, access control lists, IP tables, rate limiting, closing all unnecessary ports, disabling all unnecessary services (for example, TLS and remote access service may not be needed all the time, so therefore it would be a good idea to enable these services only when needed), using strong confidential integrity algorithms, and so forth.	[50], [61]
BP-P9	Strong password policy	A strong complex password should be configured for each hypervisor or CIS 'root' account and secured in a safe location with physical and procedural controls on its access and use. It is recommended that the 'root' account is only used in exceptional operational circumstances by the hypervisor or CIS administrator and that separate user accounts are configured with less privilege for day-to-day operational management. Note: in the virtual environment hypervisor or CIS 'root' password has a greater significance as it controls multiple VMs or containers and provides access to security sensitive information.	[50], [6], [123]
BP-P10	Secure supply chain	Trustworthy equipment (all supply chain), resilient system and verification must all be based on standards. Devising the required standards must be a collaborative effort between private (industry, SME, and research) and public (policy makers, regulators) parties, as no single vendor, operator or government can do it alone. Operators should implement effective supply-chain and procurement controls to ensure the services they operate and provide comply with legal requirements and manage supply-chain threats. Processes should be in place to identify, prioritise and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process. Zero trust principles should be implemented to identify supply chain weaknesses across product creation, manufacturing, testing, and delivery — without the need for disruptions that ultimately can halt operations. Cybersecurity audits and certifications should be conducted by an independent and accredited body against a defined set of criteria, standards, and the issuing of a certificate indicating conformance. Globally, there are two international arrangements relevant to assuring 5G product security. The Network Equipment Security Assurance Scheme (NESAS), developed jointly by GSMA and 3GPP, covers security assessments of 5G vendor development and product lifecycle processes and security evaluations of network products. Secondly, 5G products can also be certified under the Common Criteria scheme. Through collaboration, a shared responsibility model, zero trust principles, and security assurance, supply chains will strengthen as security improves.	[60], [138], [139]
BP-P11	Resources inventory management system and database	**Hardware inventory** It is expected a hardware (blade) for hypervisor or CIS and bare metal installation for inventory shall exist to support operational management. However, in addition, to providing the ability to complete security investigations and meet possible local regulatory or legal requirements, it is recommended that the inventory stores: 1. the location of each blade server (e.g. country, datacentre, rack, shelf); 2. mapping VNF to hypervisor or CIS and blade server showing the current and historic records; 3. information as to whether any native installations are sharing the same blade server chassis, associated resources and network infrastructure. **Software inventory**	[6], [123]

		A mechanism should exist to identify all VNFCs running in each VM or container within each hypervisor or CIS. It should also be possible to identify which hardware, datacentre, location and country is being used and the assigned IP addresses and types of communication flows, routing tables and effective security policies and filtering rules are in place. In addition, automatic validation should be completed against the VIM and EMS platforms to ensure only authorised VNFC applications are running and installed. **Open source inventory** Organisations must set up accurate inventories of open-source software dependencies used by their various applications, or a process to receive and manage notifications concerning discovered vulnerabilities or available patches from the community supporting the open-source. Data integrity should be maintained between the NFVi and SDN controller layers and the resource inventory through a robust mechanism implemented during deployment. Such mechanism must have the capability to check the SDN and NFV configuration against the one stored on the resource inventory. It must also have the capability to validate the security policies to ensure they are still being applied correctly, e.g. verifying firewall rules on the orchestration interface or check location of any VNF. A detection or audit mechanism must be implemented to identify where a workflow has been initiated requesting changes to the NFV or SDN environment but where no acknowledgement has been received on its success or failure. Upon detection of such changes an alarm must be raised so the operational team can investigate the incident.	

BP-P12	Apply hardening policies	For instance, the hypervisor or CIS should be hardened to allow only the minimum services and processes necessary to operate VMs or containers, and all other services should be removed by default. As a minimum, the following configuration changes must be made among others:
		• remove all unused features;
		• when a VM or container is deleted the virtual disk should be zeroed to prevent an attacker reconstructing the contents of the VM or container disk;
		• disable the ability to connect external devices to VMs or containers (e.g. CD, serial and parallel ports);
		• make sure a VM does not have the ability to run with the full OS privilege level and can only operate at guest level; this can be controlled using Intel VT-x and AMD-V extensions;
		• make sure each VM or container has a predefined set of restricted resources to ensure one VM or container cannot impact the resources and performance of another in the same hypervisor or CIS;
		• disable the ability of a VM to initiate 'disk shrinking';
		• enable persistent disk mode;
		• restrict the visibility of one VM or container to detect another VM or container existing on the same host;
		• use zoning and LUN masking to segregate SAN activity with each VM having unique authentication credentials;
		• remove direct access to the O&M functionality of the hypervisor or CIS for management only through a secure connection from the VIM; however, this may not always be operationally feasible, so the hypervisor or CIS installation should limit access to the hypervisor or CIS 'root' operating system to either:
		  ○ a dedicated O&M interface supporting a secure protocol (e.g. TLS) with only an IP address,
		  ○ ACL restriction on which domain can connect successfully;
		• only allow 'root' access from the local terminal (LMP);
		• where a hardware manufacturer provided monitoring tools that are implemented on the hypervisor or CIS or they utilise embedded support for industry standard protocols such as Common Information Model (CIM), these functions must be installed and operated on the hypervisor or CIS with limited privileges.
			[37], [79], [81], [82], [125]

BP-P13	Multi-vendor segregation and trust	**Segregation** Multi-vendor segregation is necessary to ensure each vendor can only manage or impact the resources related to their own VM or container across the NFVI architecture. Ideally, different vendors should not share the same VM or container. Note: this can be achieved by following VMware guidelines[112] for implementing secure multi-tenancy. **Trust** Select VNF vendors that make their vulnerabilities public so their customers can take appropriate actions and mitigations as quickly as possible. There is no security in obscurity.	[124]
BP-P14	Security by design	The security-by-design concept should be used to address the protection of NFV resources and components at design time through the integration of security mechanisms. This should concern the hardware layer, the virtualisation layer, MANO and VNFs. Use secure software development lifecycle (SDLC) principles to avoid vulnerabilities and thus contribute to developing NFV software applications and services in a secure manner. Promote the use of DevSecOps[113] methodology. The DevSecOps process aims at merging the security discipline within DevOps, thus considering security in every stage of the development process. By having security and development teams working together early in the development lifecycle, security naturally finds itself in the product by design.	[49], [88]
BP-P15	Lifecycle management	Secure software development principles for VNFs incorporate the following industry best practices: • validating the removal of unused software modules and execution paths; • validating the disabling of unused protocols and the closure of unused ports;Run VM or container image and software package scanning to find known vulnerabilities and fix them before release; • using container-specific host OSs to reduce risk by limiting the attack surface, as recommended in ENISA 5G threat landscape[114], the ENISA security aspects of virtualisation[115], NIST SP 800-190[116], NIST guidance[117], and others; • enforcing Centre for Internet Security (CIS) benchmarks[118] for K8S, docker, and Linux to establish a hardened baseline; • ensuring that the software supplier practices proper due diligence when using commercial third-party and open-source software in their projects[119]; • validating application performance on the hardened infrastructure.	[6], [113]
BP-P16	Software bill of materials (SBOM)	A SBOM is a formal record containing the details and supply chain relationships of various open source and commercial software components, libraries and modules used in building software. Complex systems such as the 5G NFV might include hundreds or even thousands of software components that software development and cybersecurity teams must track through all stages of the lifecycle.	[128], [129]

[112] https://telco.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/microsites/telco/vmware-telco-security-whitepapers.pdf
[113] https://www.redhat.com/en/partners/devsecops
[114] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks
[115] https://www.enisa.europa.eu/publications/security-aspects-of-virtualization
[116] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf
[117] https://csrc.nist.gov/glossary/term/Virtualization
[118] https://www.cisecurity.org/cis-benchmarks/
[119] https://www.ericsson.com/en/blog/2021/1/open-source-security-software

		An SBOM provides those who produce, purchase and operate software with information that enhances their understanding of the supply chain, which enables multiple benefits, most notably the potential to track known and newly emerged vulnerabilities and risks. The minimum elements an SBOM NTIA describes are organised into these three categories: • data fields, • automation support, • practices and processes.	
BP-O1	Secure physical environment and geographical location	A datacentre site supporting NFVi and MANO elements should be operated and controlled by the operator and, ideally, not be outsourced using a third party IaaS supplier. While not recommended, if the operator chooses to use a third party operated datacentre then additional security controls are necessary to ensure the third party complies with the operator's physical and outsourcing security controls. The geographical location of any hardware supporting the NFV must comply with each operators local regulatory and legal requirements for operating a telecoms network or handling sensitive data for customers or LI. Anti-affinity rules should be applied to protect against possible infringement. Privacy sensitive information of a VNF must be protected from being leaked out of its legal jurisdiction. The system should manage the physical location of the VNFs and sub-components and SDN routing to provide attestation that the VNFCs provide a commensurate level of security to match the requirements of the service or to meet legal or regulatory requirements.	[6], [47], [25], [123]
BP-O2	Training and awareness	*Information sharing between different 5G actors*: all 5G stakeholders, including operators, suppliers, etc. should work together to enhance the security of 5G. 5G stakeholders should participate in international security events and working groups formed to enable discussion, cooperation and intelligence sharing to improve security awareness. Adopt a comprehensive approach to security training and awareness among the employees, including employees on all levels. Security training should cover 5G relevant threats and be tailored to the employees' roles and responsibilities. Ensure that security trainings are continuous, regular and frequently updated. Training programmes should be updated after new important threats are disclosed and should be adjusted according to the lessons learned from ongoing incident handling and recovery activities.	[107]
BP-O3	Trust model	Foster security-related information sharing between different 5G stakeholders while protecting intellectual property. Suppliers and service providers should provide evidence about the implementation of their cybersecurity management system to operators. For transparency purposes, OEMs should consider providing similar evidence to their suppliers and service providers as well. Define the relevant cybersecurity aspects of the partnerships along the supply chain and develop security requirements and procurement guidelines between 5G stakeholders. To prevent security risks and threats that may stem from outsourced services or components or systems provided by third party suppliers, operators should define procurement guidelines as well as security requirements to be applied to the suppliers to their third parties. A security SLA may also be established between the operator and its supplier to define the security level that the supplier should meet.	[108]
BP-O4	SLAs establishment	SLAs between 5G stakeholders should consider the security aspects to identify mitigation strategies and how to implement actions in response to those responsible for the security assessment of the 5G NFV. The SLAs for security management and maintenance can include plans to mitigate known threats and respond to future threats. Addressing security in the SLA promotes transparency, facilitates communication between the stakeholders involved, including their internal entities (e.g. teams for security management and monitoring) and establishes consensus practices to solidify the overall 5G system security.	[98]

F ANNEX: MAPPING OF CHALLENGES, VULNERABILITIES, ATTACK SCENARIOS, AFFECTED ASSETS AND BEST PRACTICES

ID	Challenges	Vulnerabilities	Attacks	Affected Assets	Best practices
Virtualisation/Containerisation					
CH-V1	Challenges within the runtime software	VUL5 Improper verification of identity and location of transmitting party on internal interfaces VUL8 Improper patch management VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper or missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT2 Software flaw attacks ATT6 DDoS attacks ATT11 Malicious VM/Container attacks ATT15 Network attacks	NFV MANO; VNFs; VNFs data; NS data User data Signalling data UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	BP-T2 – VNF image validation and protection BP-T3 - Tracking VNF version changes BP-T4 – VNF deployment BP-T5 – VNF deletion or relocation BP-T9 - Remote attestation BP-T11 - Security segmentation and isolation between network functions
CH-V2	Flexibility and openness of service environment	VUL10 No mechanism to enforce geo-restrictions VUL12 Inadequate access privileges in virtualised environments VUL16 Improper VNF on-boarding VUL17 Improper VNF instantiation	ATT6 DDoS attacks ATT8 Injection attacks	NFV MANO; NFVI; VNFM; Ve-Vnfm-em; Ve-Vnfm-vnf VNFs data; NS data Network data Security data	BP-T1 - Security monitoring and filtering BP-T3 - Tracking VNF version changes BP-T9 - Remote attestation BP-T10 - Software compliance and integrity preservation BP-T11 - Security segmentation and isolation between network functions

					BP-P8 - Defence-in-depth
CH-V3	Challenges within the hypervisor/CIS	VUL15 Software vulnerabilities in NFV implementation VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper or missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT12 Malicious hypervisor or CIS attacks	VNF; UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data System data Security data	BP-T7 - Hypervisor/CIS protection BP-T9 - Remote attestation BP-T11 - Security segmentation and isolation between network functions BP-T12 - Secure boot integrity BP-T15 - Trusted computing technologies BP-T16 - Hardware security BP-P12 - Apply hardening policies BP-P14 - Security by design
CH-V4	Time manipulation	VUL11 Time manipulation VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT16 Time manipulation attacks	VNF; UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	BP-T15 - Trusted computing technologies BP-T16 - Hardware security BP-T28 - Trusted time source
CH-V5	Entropy generation	VUL13 Improper key management system	ATT4 Security standard subversion attacks ATT11 Malicious VM/ Container attacks	SM System data Security data	BP-T6 - Cryptography BP-T15 - Trusted computing technologies BP-T16 - Hardware security
CH-V6	Encrypted data processing	VUL2 Improper confidentiality protection of data transferred over internal interfaces to MANO VUL3 Improper API access implementation VUL29 Improper transport layer protection of service-based interfaces (SBI)	ATT4 Security standard subversion attacks ATT11 Malicious VM/Container attacks	NFV MANO; VNF; Os-Ma-nfvo UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	BP-T6 – Cryptography BP-T13 - Data protection and privacy BP-T15 - Trusted computing technologies

		VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components		System data Security data	BP-T16 - Hardware security BP-T34 - User plane security BP-P1 - Zero Trust
CH-V7	Challenges within IP layer vs application layer	VUL9 Misconfiguration VUL12 Inadequate access privileges in virtualised environments VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT4 Security standard subversion attacks ATT11 Malicious VM/Container attacks	VNF; NFVI UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data System data Security data	BP-T1 - Security monitoring and filtering BP-T13 - Data protection and privacy BP-P8 - Defence-in-depth
CH-V8	Default deployment or configuration	VUL9 Misconfiguration VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper or missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT11 Malicious VM/Container attacks	VNF; UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data	BP-T7 - hypervisor or CIS protection BP-P8 - Defence-in-depth

CH-V9	Network traffic exposure	VUL1 Improper message and session integrity checks on internal interfaces VUL2 Improper protection of confidentiality of data transferred over internal interfaces to MANO VUL3 Improper implementation of API access VUL7 Lack of protection of user and control planes data VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT7 DNS Amplification attacks ATT15 Network attacks	NFV MANO; VNF; Os-Ma-nfvo ; Control plane UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data System data Security data	BP-T1 - Security monitoring and filtering BP-T21 - Network security BP-T34 - User plane security
CH-V10	Security logs troubleshooting failure	VUL23 Insufficient / inadequate logging of security events for MANO and NFVI VUL24 Logs not transferred to centralised storage VUL25 Improper protection of security event log files	ATT6 DDoS attacks ATT16 Time manipulation attacks	NFV-MANO; NFVI System data	BP-T17 - Centralised log auditing
CH-V11	Container acceleration capabilities	VUL10 No mechanism to enforce geo-restrictions	ATT2 Software flaw attacks ATT3 Resource misuse attacks ATT8 Injection attacks ATT11 Malicious VM/Container attacks ATT12 Malicious hypervisor/CIS attacks	NFV MANO User data VNFs data NS data	BP-T31 - Specific container security controls BP-P12 - Apply hardening policies BP-P14 – Security-by-design
CH-V12	Container isolation failure	VUL10 No mechanism to enforce geo-restrictions	ATT2 Software flaw attacks ATT3 Resource misuse attacks ATT8 Injection attacks	NFV MANO VNFs data NS data Network data	BP-T11 - Security segmentation and isolation between network functions BP-T12 - Secure boot integrity BP-T31 - Specific container security controls

			ATT11 Malicious VM/Container attacks ATT12 Malicious hypervisor/CIS attacks		
CH-V13	Sensitive ata in NF container images	VUL10 No mechanism to enforce geo-restrictions	ATT2 Software flaw attacks ATT3 Resource misuse attacks ATT8 Injection attacks ATT11 Malicious VM/Container attacks ATT12 Malicious hypervisor/CIS attacks	NFV MANO Security data	BP-T31 - Specific container security controls BP-P12 - Apply hardening policies
CH-V14	Core network functions in the MEC	VUL45 Vulnerabilities in implementation of MEC security functionalities VUL46 SBA/SBI vulnerabilities of MEC components VUL47 Improper access control to information VUL48 Vulnerable virtualisation / container / micro-service environment VUL49 Lack of / improper DDoS protection VUL50 Vulnerabilities in MEC applications VUL51 Improper isolation of resources VUL52 Physical and environmental vulnerabilities of relevant MEC components VUL53 Vulnerable mechanisms for authentication and authorisation of MEC components VUL54 Insufficient or improper monitoring mechanisms of MEC components	ATT11 Malicious VM/Container attacks ATT12 Malicious hypervisor/CIS attacks ATT18 Orchestration attacks ATT19 Supply chain attacks ATT20 Third party hosting attacks	Application data traffic MEC host 3GPP SA6 interfaces; ETSI MEC interfaces; Application data traffic MEC platform VIM/CISM Customer facing service (CFS) portal MEC applications; Edge application server (EAS) Virtualisation infrastructure LCM proxy; MEC orchestrator	BP-T35 - MEC security BP-P7 - Restriction on installing applications BP-P8 - Defence-in-depth BP-P12 - Apply hardening policies
CH-V15	Wide geographical distribution of MEC infrastructures	VUL45 Vulnerabilities in implementation of MEC security functionalities VUL46 SBA/SBI vulnerabilities of MEC components VUL47 Improper access control to information VUL48 Vulnerable virtualisation / container / micro-service environment VUL49 Lack of / improper DDoS protection VUL50 Vulnerabilities in MEC applications	ATT11 Malicious VM/Container attacks ATT12 Malicious hypervisor/CIS attacks ATT18 Orchestration attacks	Application data traffic MEC host 3GPP SA6 interfaces; ETSI MEC interfaces ; Application data traffic MEC platform VIM/CISM	BP-T1 - Security monitoring and filtering BP-T35 - MEC security BP-P8 - Defence-in-depth BP-O1 - Secure physical environment and geographical location

		VUL51 Improper isolation of resources VUL52 Physical and environmental vulnerabilities of relevant MEC components VUL53 Vulnerable mechanisms for authentication and authorisation of MEC components VUL54 Insufficient or improper monitoring mechanisms of MEC components	ATT19 Supply chain attacks ATT20 Third party hosting attacks	Customer facing service (CFS) portal MEC applications; Edge application server (EAS) Virtualisation infrastructure LCM proxy; MEC orchestrator	
CH-V16	Insecure API/improper authentication of MEC components	VUL45 Vulnerabilities in implementation of MEC security functionalities VUL46 SBA/SBI vulnerabilities of MEC components VUL47 Improper access control to information VUL48 Vulnerable virtualisation / container / micro-service environment VUL49 Lack of / improper DDoS protection VUL50 Vulnerabilities in MEC applications VUL51 Improper isolation of resources VUL52 Physical and environmental vulnerabilities of relevant MEC components VUL53 Vulnerable mechanisms for authentication and authorisation of MEC components VUL54 Insufficient or improper monitoring mechanisms of MEC components	ATT11 Malicious VM/Container attacks ATT12 Malicious hypervisor/CIS attacks ATT18 Orchestration attacks ATT19 Supply chain attacks ATT20 Third party hosting attacks	Application data traffic MEC host 3GPP SA6 interfaces ; ETSI MEC interfaces ; application data traffic MEC platform VIM/CISM Customer facing service (CFS) portal MEC applications; Edge application server (EAS) Virtualisation infrastructure LCM proxy; MEC orchestrator	BP-T35 – MEC security BP-P1 – Zero Trust BP-P9 – Strong password policy BP-P14 – Security-by-design
CH-V17	Insufficient/improper Monitoring Mechanisms of MEC components	VUL45 Vulnerabilities in implementation of MEC security functionalities VUL46 SBA/SBI vulnerabilities of MEC components VUL47 Improper access control to information VUL48 Vulnerable virtualisation / container / micro-service environment VUL49 Lack of / improper DDoS protection VUL50 Vulnerabilities in MEC applications VUL51 Improper isolation of resources VUL52 Physical and environmental vulnerabilities of relevant MEC components VUL53 Vulnerable mechanisms for authentication and authorisation of MEC components VUL54 Insufficient or improper monitoring mechanisms of MEC components	ATT11 Malicious VM/Container attacks ATT12 Malicious hypervisor/CIS attacks ATT18 Orchestration attacks ATT19 Supply chain attacks ATT20 Third party hosting attacks	Application data traffic MEC host 3GPP SA6 interfaces ; ETSI MEC interfaces ; Application data traffic MEC platform VIM/CISM Customer facing service (CFS) portal MEC applications; Edge Application Server (EAS) Virtualisation infrastructure	BP-T35 - MEC security BP-P14 - Security-by-design

				LCM proxy; MEC orchestrator	
CH-V18	Centralisation of the SDN control platforms	VUL38 Improper mechanisms for preventing flow rules confliction VUL39 SBA/SBI vulnerabilities of SDN components VUL40 Improper authentication and authorisation VUL41 Improper hardening of SDN components VUL42 Insufficient or improper monitoring mechanisms of SDN components VUL43 Virtualisation vulnerabilities of relevant SDN components VUL44 Data centre vulnerabilities	ATT5 LI attacks ATT9 OSS/BSS attacks ATT18 Orchestration attacks	SDN controller Northbound interface; Southbound interface; Eastbound-Westbound interface SDN application; SDN resources SDN infrastructure layer SDN data	BP-T22 - SDN security management BP-P8 - Defence-in-depth BP-P12 - Apply hardening policies BP-P14 - Security-by-design
CH-V19	Malicious SDN applications	VUL38 Improper mechanisms for preventing flow rules confliction VUL39 SBA/SBI vulnerabilities of SDN components VUL40 Improper authentication and authorisation VUL41 Improper hardening of SDN components VUL42 Insufficient or improper monitoring mechanisms of SDN components VUL43 Virtualisation vulnerabilities of relevant SDN components VUL44 Data centre vulnerabilities	ATT5 LI attacks ATT9 OSS/BSS attacks ATT18 Orchestration attacks	SDN controller Northbound interface; Southbound interface; Eastbound-Westbound interface SDN application; SDN resources SDN Infrastructure layer SDN data	BP-T22 - SDN security management BP-P7 - Restriction on installing applications BP-P14 - Security-by-design
CH-V20	Common SDN interfaces	VUL38 Improper mechanisms for preventing flow rules confliction VUL39 SBA/SBI vulnerabilities of SDN components VUL40 Improper authentication and authorisation VUL41 Improper hardening of SDN components VUL42 Insufficient or improper monitoring mechanisms of SDN components VUL43 Virtualisation vulnerabilities of relevant SDN components VUL44 Data centre vulnerabilities	ATT5 LI attacks ATT9 OSS/BSS attacks ATT18 Orchestration attacks	SDN controller Northbound interface; Southbound interface; Eastbound-Westbound interface SDN application; SDN resources SDN infrastructure layer SDN data	BP-T22 - SDN security management
CH-V21	Isolation failure between VNFs	VUL3 Improper API access implementation VUL8 Improper patch management VUL12 Inadequate access privileges in virtualised environments VUL18 Improper authentication policy VUL19 Insecure / insufficient authentication attributes VUL20 Insecure password policy	ATT11 Malicious VM/Container attacks	Os-Ma-nfvo; NFV-MANO; VNF; NFVI UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data	BP-T2 – VNF image validation and protection BP-T3 - Tracking VNF version changes BP-T4 – VNF deployment BP-T5 – VNF deletion or relocation

		VUL21 Insecure authentication mechanisms to management / maintenance interfaces VUL22 Insecure authorisation and access control mechanisms VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components		NS data Network data	BP-T7 - hypervisor/CIS protection BP-T10 - Software compliance and integrity preservation BP-T11 - Security segmentation and isolation between network functions BP-T14 - Encrypting VNF Volume/swap Areas BP-T19 – VNF protection
CH-V22	Memory introspection	VUL9 Misconfiguration VUL12 Inadequate access privileges in virtualised environments VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of Data and Information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT1 Human-instigated attacks ATT8 Injection attacks ATT11 Malicious VM/Container attacks ATT12 Malicious hypervisor/CIS attacks	VNF; NFVI UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data System data Security data	BP-T2 – VNF image validation and protection BP-T4 – VNF deployment BP-T5 – VNF deletion or relocation BP-T7 - hypervisor/CIS protection BP-T11 - Security segmentation and isolation between network functions
CH-V23	Trusted domains segmentation	VUL1 Improper message and session integrity checks on internal interfaces VUL2 Improper confidentiality protection of data transferred over internal interfaces to MANO VUL13 Improper key management system VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs	ATT3 Resource misuse attacks ATT8 Injection attacks ATT11 Malicious VM/Container attacks ATT12 Malicious Hypervisor/CIS attacks ATT15 Network attacks	NFV MANO; VNF; SM UPF/User Ddata; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data	BP-T7 - hypervisor/CIS protection BP-T9 - Remote attestation BP-T11 - Security segmentation and isolation between network functions BP-T15 - Trusted computing technologies BP-T16 - Hardware security

		VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components			BP-T26 - Deploying VMs/Containers of differing trust levels
CH-V24	Access to storage resources	VUL6 Inability to provide proof of integrity of the data stores used for VM/Container images	ATT3 Resource misuse attacks ATT8 Injection attacks ATT14 Hardware attacks	VIM/CISM VNFs data Security data	BP-T6 – Cryptography BP-T11 - Security segmentation and isolation between network functions BP-T20 - Local or removable Blade Storage- SAN protection BP-T30 - Redundancy and backup BP-P8 - Defence-in-depth BP-P12 - Apply hardening policies
CH-V25	Sharing of private keys between VNFs and confidentiality of sensitive data	VUL1 Improper message and session integrity checks on internal interfaces VUL2 Improper confidentiality protection of data transferred over internal interfaces to MANO VUL3 Improper API Access implementation VUL13 Improper key management system VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of Data and Information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in Operating Systems supporting 5G NFs VUL37 Improper hardening of 5G Core components	ATT3 Resource misuse attacks ATT11 Malicious VM/Container attacks	NFV MANO; VNF; Os-Ma-nfvo ; SM UPF/User Data; UPF/Signalling Data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF Security data	BP-T2 – VNF Image validation and protection BP-T3 - Tracking VNF version changes BP-T4 – VNF deployment BP-T5 – VNF deletion or relocation BP-T7 - Hypervisor/CIS protection BP-T10 - Software compliance and integrity preservation BP-T14 - Encrypting VNF Volume/swap Areas BP-T15 - Trusted computing technologies BP-T16 - Hardware security BP-T19 – VNF protection BP-P1 - Zero Trust
CH-V26	Availability of network functions	VUL1 Improper message and session integrity checks on internal interfaces	ATT8 Injection attacks	NFV MANO; VNF; VIM/CISM; Os-Ma-nfvo ; Control plane	BP-T2 – VNF Image validation and protection

		VUL2 Improper confidentiality protection of data transferred over internal interfaces to MANO VUL3 Improper API Access implementation VUL4 Use of legacy PNF VUL5 Improper verification of identity and location of transmitting party on internal interfaces VUL6 Inability to provide proof of integrity of the data stores used for VM/Container images VUL7 Lack of protection of user and control planes data VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of Data and Information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in Operating Systems supporting 5G NFs VUL37 Improper hardening of 5G Core components		UPF/User Data; UPF/Signalling Data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data System data	BP-T3 - Tracking VNF version changes BP-T4 – VNF deployment BP-T5 – VNF deletion or relocation BP-T7 - Hypervisor/CIS protection BP-T12 - Secure boot integrity BP-T30 - Redundancy and backup
CH-V27	Software catalogue image exposure	VUL6 Inability to provide proof of integrity of the data stores used for VM/Container images VUL7 Lack of protection of user and control planes data	ATT8 Injection attacks ATT11 Malicious VM/Container attacks ATT12 Malicious hypervisor/CIS attacks	Control plane Network data User data VNFs data NS data	BP-T9 - Remote attestation BP-P7 - Restriction on installing applications BP-P8 - Defene-in-depth
CH-V28	Multi-vendors integration	VUL5 Improper verification of identity and location of transmitting party on internal interfaces VUL6 Inability to provide proof of integrity of the data stores used for VM/Container images	ATT2 Software flaw attacks ATT8 Injection attacks	NFV MANO; VIM/CISM VNFs data NS data	BP-T29 - Secure 3rd party hosting environments BP-P7 - Restriction on installing applications BP-P13 - Multi-vendors segregation and trust BP-O3 - Trust model BP-O4 - SLAs establishment
CH-V29	Multi-tenants co-residency	VUL18 Improper authentication policy VUL22 Insecure authorization and access control mechanisms	ATT20 Third party hosting attacks	NFV-MANO; VNF; NFVI	BP-T9 - Remote attestation

		VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of Data and Information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in Operating Systems supporting 5G NFs VUL37 Improper hardening of 5G Core components		UPF/User Data; UPF/Signalling Data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data System data Security data	BP-T29 - Secure 3rd party hosting environments BP-P7 - Restriction on installing applications
CH-V30	Elastic nature of NFVI-migration of VNFs	VUL9 Misconfiguration VUL12 Inadequate access privileges in virtualised environments VUL13 Improper key management system VUL14 Lack of a proper mechanism for ensuring a Hardware-Based Root of Trust (HBRT) VUL15 Software Vulnerabilities in NFV implementation VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of Data and Information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in Operating Systems supporting 5G NFs VUL37 Improper hardening of 5G Core components	ATT11 Malicious VM/Container attacks ATT12 Malicious Hypervisor/CIS attacks ATT13 Command/control channel attacks ATT14 Hardware attacks	NFVI; VNF; SM UPF/User Data; UPF/Signalling Data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data	BP-T2 – VNF Image validation and protection BP-T3 - Tracking VNF version changes BP-T4 – VNF deployment BP-T5 – VNF deletion or relocation BP-T7 - Hypervisor/CIS protection BP-T14 - Encrypting VNF Volume/swap Areas BP-T19 – VNF protection BP-P8 - Defense in depth
CH-V31	Geographical Location	VUL10 No mechanism to enforce geo-restrictions	ATT11 Malicious VM/Container attacks ATT12 Malicious Hypervisor/CIS attacks ATT13 Command/control channel attacks	NFV MANO User data VNFs data NS data Network data	BP-T30 - Redundancy and backup BP-P7 - Restriction on installing applications BP-P8 - Defence-in-depth BP-O1 - Secure physical environment and geographical location

			ATT14 Hardware attacks ATT15 Network attacks		
CH-V32	Data lifecycle and location	VUL14 Lack of a proper mechanism for ensuring a hardware-based root of trust (HBRT) VUL16 Improper VNF on-boarding VUL17 Improper VNF instantiation VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT11 Malicious VM/Container attacks ATT12 Malicious Hypervisor/CIS attacks ATT13 Command/control channel attacks ATT14 Hardware attacks ATT15 Network attacks	VNF; NFVI; VNFM; Ve-Vnfm-em; Ve-Vnfm-vnf UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data	BP-T13 - Data protection and privacy BP-T30 - Redundancy and backup BP-P1 - Zero trust BP-P8 - Defence-in-depth
CH-V33	VNF host spanning	VUL16 Improper VNF on-boarding VUL17 Improper VNF instantiation VUL18 Improper authentication policy VUL19 Insecure / insufficient authentication attributes VUL20 Insecure password policy VUL21 Insecure authentication mechanisms to management / maintenance interfaces VUL22 Insecure authorisation and access control mechanisms VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging	ATT11 Malicious VM/Container attacks ATT13 Command/control channel attacks ATT15 Network attacks	NFV-MANO; VNF; NFVI; VNFM; Ve-Vnfm-em; Ve-Vnfm-vnf UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data System data Security data	BP-T2 – VNF image validation and protection BP-T3 - Tracking VNF version changes BP-T4 – VNF deployment BP-T5 – VNF deletion or relocation BP-T14 - Encrypting VNF volume/swap areas BP-T19 – VNF protection

		VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components			
CH-V34	Dynamic nature of network functions	VUL9 Misconfiguration VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT15 Network attacks	VNF UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data	BP-T3 - Tracking VNF version changes BP-T7 - Hypervisor/CIS protection BP-T9 - Remote attestation
Orchestration and management					
CH-OM1	MANO single point of failures	VUL2 Improper confidentiality protection of data transferred over internal interfaces to MANO VUL8 Improper patch management VUL14 Lack of a proper mechanism for ensuring a hardware-based root of trust (HBRT) VUL23 Insufficient / inadequate logging of security events for MANO and NFVI VUL26 Use of weak cryptographic algorithms VUL27 Insecure interface between OOS/BSS and NFV/MANO VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT2 Software flaw attacks ATT7 DNS Amplification attacks ATT8 Injection attacks	NFV MANO; VNF; NFVI UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF OSS/BSS systems VNFs data NS data Network data	BP-T4 – VNF deployment BP-T5 – VNF deletion or relocation BP-T8 - Security management and orchestration BP-T10 - Software compliance and integrity preservation BP-T23 - MANO access control and management

CH-OM2	Orchestration compromise and policy violations	VUL5 Improper verification of identity and location of transmitting party on internal interfaces VUL9 Misconfiguration VUL12 Inadequate access privileges in virtualised environments VUL15 Software vulnerabilities in NFV implementation VUL16 Improper VNF on-boarding VUL17 Improper VNF instantiation VUL18 Improper authentication policy VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT5-ATT10-ATT17 LI attacks ATT7 DNS Amplification attacks ATT8 Injection attacks ATT9 OSS/BSS Attacks ATT11 Malicious VM/Container attacks ATT15 Network attacks	NFV MANO; VNF; NFVI; VNFM; Ve-Vnfm-em; Ve-Vnfm-vnf UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data	BP-T2 – VNF image validation and protection BP-T8 - Security management and orchestration BP-T10 - Software compliance and integrity preservation BP-T23 - MANO access control and management BP-T27 - Orchestration platform security management BP-P14 - Security-by-design
CH-OM3	Resource integrity caused by manual changes or failure to update resource inventory	VUL6 Inability to provide proof of integrity of the data stores used for VM/Container images VUL16 Improper VNF on-boarding VUL17 Improper VNF instantiation	ATT1 Human-instigated attacks ATT3 Resource misuse attacks ATT8 Injection attacks ATT9 OSS/BSS Attacks ATT11 Malicious VM/Container attacks ATT12 Malicious hypervisor/CIS attacks	VIM/CISM; VNFM; Ve-Vnfm-em; Ve-Vnfm-vnf VNFs data NS data	BP-T6 – Cryptography BP-T10 - Software compliance and integrity preservation BP-P11 - Resource Iinventory management system and database BP-T23 - MANO access control and management
CH-OM4	Vulnerabilities within orchestration protocols	VUL5 Improper verification of identity and location of transmitting party on internal interfaces VUL18 Improper authentication policy VUL29 Improper transport layer protection of service-based interfaces (SBI)	ATT18 Orchestration attacks	NFV-MANO; VNF; NFVI UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	BP-T8 - Security management and orchestration BP-T23 - MANO access control and management

		VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components		User data VNFs data NS data Network data	BP-T27 - Orchestration platform security management
Administration and access control					
CH-AC1	Malicious insiders	VUL16 Improper VNF on-boarding VUL17 Improper VNF instantiation VUL18 Improper authentication policy VUL19 Insecure / insufficient authentication attributes VUL20 Insecure password policy VUL21 Insecure authentication mechanisms to management / maintenance interfaces VUL22 Insecure authorisation and access control mechanisms	ATT1 Human-instigated attacks	NFV MANO, NFVI; VNFM; Ve-Vnfm-em; Ve-Vnfm-vnf User data VNFs data NS data Network data	BP-T2 – VNF image validation and protection BP-T23 - MANO access control and management BP-P9 - Strong password policy BP-P1 - Zero Trust
CH-AC2	Single administrator domain	VUL12 Inadequate access privileges in virtualised environments	ATT1 Human-instigated attacks	NFVI User data VNFs data NS data Network data	BP-T7 - Hypervisor/CIS protection BP-T8 - Security management and orchestration BP-T18 - Use and ownership of 'root' administration credentials BP-P9 - Strong password policy
CH-AC3	Lack of staff with the skillsets needed to operate virtualised networks	VUL18 Improper authentication policy VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs	ATT1 Human-instigated attacks	NFV-MANO; VNF; NFVI UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data	BP-O2 - Training and awareness

		VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components		NS data Network data Security data System data	
CH-AC4	Insecure management configuration, and monitoring interfaces	VUL1 Improper message and session integrity checks on internal interfaces VUL2 Improper confidentiality protection of data transferred over internal interfaces to MANO VUL16 Improper VNF on-boarding VUL17 Improper VNF instantiation VUL18 Improper authentication policy VUL19 Insecure / insufficient authentication attributes VUL20 Insecure password policy VUL21 Insecure authentication mechanisms to management / maintenance interfaces VUL22 Insecure authorisation and access control mechanisms VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT11 Malicious VM/Container attacks ATT12 Malicious hypervisor/CIS attacks ATT13 Command/control channel attacks	NFV MANO; VNF; VNFM; Ve-Vnfm-em; Ve-Vnfm-vnf; NFVI UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data Security data System data	BP-T1 - Security monitoring and filtering BP-T23 - MANO access control and management
CH-AC5	Compromise of orchestration access control	VUL16 Improper VNF on-boarding VUL17 Improper VNF instantiation VUL18 Improper authentication policy VUL19 Insecure / insufficient authentication attributes VUL20 Insecure password policy VUL21 Insecure authentication mechanisms to management / maintenance interfaces VUL22 Insecure authorisation and access control mechanisms	ATT1 Human-instigated attacks ATT7 DNS Amplification attacks ATT9 OSS/BSS Attacks ATT15 Network attacks	VNFM; Ve-Vnfm-em; Ve-Vnfm-vnf; NFV-MANO; VNF; NFVI UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data	BP-T8 - Security management and orchestration BP-T9 - Remote attestation BP-T23 - MANO access control and management BP-T27 - Orchestration platform security management BP-P9 - Strong password policy

		VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components		NS data Network data	
CH-AC6	Weak or insecure authentication/access control/authorisation to VIM	VUL5 Improper verification of identity and location of transmitting party on internal interfaces VUL6 Inability to provide proof of integrity of the data stores used for VM/Container images VUL18 Improper authentication policy VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT1 Human-instigated attacks ATT7 DNS Amplification attacks ATT15 Network attacks	VIM/CISM; NFV-MANO; VNF; NFVI UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data	BP-T8 - Security management and orchestration BP-T23 - MANO access control and management BP-T24 - VIM connectivity to virtualisation layer BP-P1 - Zero Trust BP-P9 - Strong password policy
New and legacy technologies					
CH-LG1	Mixed virtual and legacy PNF deployments	VUL4 Use of legacy PNF	ATT21 Mixed deployment attacks	Control plane Network data	BP-T25 - Recovery and reinstallation BP-P8 - Defence-in-depth BP-P12 - Apply hardening policies BP-P14 - Security-by-design BP-O3 - Trust model BP-O4 - SLAs establishment

CH-LG2	Vulnerabilities of physical hosts	VUL12 Inadequate access privileges in virtualised environments VUL14 Lack of a proper mechanism for ensuring a hardware-based root of trust (HBRT)	ATT14 Hardware attacks ATT21 Mixed deployment attacks	NFVI User data VNFs data NS data Network data Security data System data	BP-T16 - Hardware security BP-T30 - Redundancy and backup BP-P8 - Defence-in-depth BP-P12 - Apply hardening policies
CH-LG3	Transformation of legacy OSS/BSS	VUL26 Use of weak cryptographic algorithms VUL27 Insecure interface between OOS/BSS and NFV/MANO VUL28 Insufficient / inadequate logging of sensitive data	ATT9 OSS/BSS attacks	OSS/BSS systems	BP-T32 - OSS/BSS protection BP-P5 - Incident management BP-P8 - Defence-in-depth BP-P14 - Security-by-design
CH-LG4	Integration with existing legacy OSS/BSS	VUL26 Use of weak cryptographic algorithms VUL27 Insecure interface between OOS/BSS and NFV/MANO VUL28 Insufficient / inadequate logging of Sensitive Data	ATT9 OSS/BSS attacks	OSS/BSS systems	BP-T32 - OSS/BSS protection BP-P5 - Incident management BP-P8 - Defence-in-depth BP-P12 - Apply hardening policies BP-P14 - Security-by-design BP-O3 - Trust model BP-O4 - SLAs establishment
Adoption of open source/COTS					
CH-OC1	Adoption of open-source software	VUL8 Improper patch management VUL15 Software vulnerabilities in NFV implementation VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs	ATT2 Software flaw attacks ATT8 Injection attacks	VNF; UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data	BP-P2 - Security assessment of new or changes to existing VNF service templates BP-P3 - Vulnerability handling & patch management BP-P5 - Incident management BP-P6 - Secure update management BP-P12 - Apply hardening policies BP-P15 - Lifecycle management

		VUL37 Improper hardening of 5G core components			BP-P16 - Software bill Of materials (SBOM)
CH-OC2	Adoption of COTS hardware	VUL12 Inadequate access privileges in virtualised environments	ATT14 Hardware attacks ATT20 Third party hosting attacks	NFVI User data VNFs data NS data Network data	BP-T29 - Secure 3rd party hosting environments BP-P3 - Vulnerability handling & patch management BP-P5 - Incident management BP-P6 - Secure update management BP-P12 - Apply hardening policies BP-O3 - Trust model BP-O4 - SLAs establishment
Supply chain					
CH-SC1	Separation of test and production environments	VUL9 Misconfiguration VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT19 Supply chain attacks	Hardware platform, NFVI, VNF, MANO UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF VNFs data NS data Security data	BP-P5 - Incident management BP-P8 - Defence-in-depth BP-P10 - Secure supply chain
CH-SC2	Untrusted partners	VUL3 Improper API access implementation VUL8 Improper patch management VUL12 Inadequate access privileges in virtualised environments VUL18 Improper authentication policy VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs	ATT19 Supply chain attacks	Os-Ma-nfvo; NFV-MANO; VNF; NFVI UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF VNFs data NS data Security data	BP-T25 - Recovery and reinstallation BP-T29 - Secure 3rd party hosting environments BP-P3 - Vulnerability handling & patch management BP-P5 - Incident management BP-P6 - Secure update management

		VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components			BP-P8 - Defence-in-depth BP-P10 - Secure supply chain BP-P15 - Lifecycle management BP-P16 - Software bill of materials (SBOM) BP-O3 - Trust model BP-O4 - SLAs establishment
CH-SC3	Infected/untested/unauthorised untested patches or upgrades	VUL8 Improper patch management VUL15 Software vulnerabilities in NFV implementation VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT19 Supply chain attacks	NFVI, MANO, VNF UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data Security data System data	BP-T25 - Recovery and reinstallation BP-P1 - Zero Trust BP-P3 - Vulnerability handling & patch management BP-P5 - Incident management BP-P6 - Secure update management BP-P10 - Secure supply chain BP-P15 - Lifecycle management BP-P16 - Software bill of materials (SBOM)
CH-SC4	Test isolation and assurance	VUL15 Software vulnerabilities in NFV implementation VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT19 Supply chain attacks	VNF; UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data Security data System data	BP-P2 - Security assessment of new or changes to existing VNF service templates BP-P3 - Vulnerability handling & patch management BP-P4 - Security testing and assurance BP-P5 - Incident management BP-P10 - Secure supply chain
CH-SC5	Use of counterfeit components	VUL15 Software vulnerabilities in NFV implementation VUL29 Improper transport layer protection of service-based interfaces (SBI)	ATT19 Supply chain attacks	VNF; UPF/User data; UPF/Signalling data; gNB;	BP-P2 - Security assessment of new or changes to existing VNF service templates

		VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components		AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data Security data System data	BP-P3 - Vulnerability handling & patch management BP-P5 - Incident management BP-P6 - Secure update management BP-P10 - Secure supply chain BP-P15 - Lifecycle management BP-P16 - Software bill of materials (SBOM) BP-O3 - Trust model BP-O4 - SLAs establishment
CH-SC6	Use of Inherited Components	VUL15 Software vulnerabilities in NFV implementation VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and Information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT19 Supply chain attacks	VNF; UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF User data VNFs data NS data Network data Security data System data	BP-P2 - Security assessment of new or changes to existing VNF service templates BP-P3 - Vulnerability handling & patch management BP-P5 - Incident management BP-P6 - Secure update management BP-P10 - Secure supply chain BP-P15 - Lifecycle management BP-P16 - Software bill of materials (SBOM) BP-O3 - Trust model BP-O4 - SLAs establishment
Lawful interception (LI)					
CH-LI1	Encryption of Communications	VUL2 Improper confidentiality protection of data transferred over internal interfaces to MANO VUL7 Lack of protection of user and control planes data VUL26 Use of weak cryptographic algorithms VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components	ATT5-ATT10-ATT17 LI attacks	NFV MANO; VNF; Control plane UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF OSS/BSS systems	BP-T6 – Cryptography BP-T15 - Trusted computing technologies BP-T33 - LI capabilities BP-P5 - Incident management

		VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components			
CH-LI2	Cooperation of Numerous Network Providers	VUL8 Improper patch management VUL9 Misconfiguration VUL10 No mechanism to enforce geo-restrictions VUL11 Time manipulation VUL12 Inadequate access privileges in virtualised environments VUL13 Improper key management system VUL14 Lack of a proper mechanism for ensuring a hardware-based root of trust (HBRT) VUL15 Software vulnerabilities in NFV implementation VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT5-ATT10-ATT17 LI attacks	VNF; NFV MANO; NFVI; SM UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	BP-T33 - LI capabilities BP-P5 - Incident management BP-P8 - Defence-in-depth BP-P14 - Security-by-design
CH-LI3	Availability of Data at the LI Central Nodes	VUL10 No mechanism to enforce geo-restrictions VUL12 Inadequate access privileges in virtualised environments VUL16 Improper VNF on-boarding VUL17 Improper VNF instantiation VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components	ATT5-ATT10-ATT17 LI attacks	NFV MANO; NFVI; VNFM; Ve-Vnfm-em; Ve-Vnfm-vnf UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	BP-T33 - LI capabilities BP-P5 - Incident management BP-P8 - Defence-in-depth

		VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components			
CH-LI4	LI in Hybrid Deployment	VUL10 No mechanism to enforce geo-restrictions VUL12 Inadequate access privileges in virtualised environments VUL16 Improper VNF on-boarding VUL17 Improper VNF instantiation VUL29 Improper transport layer protection of service-based interfaces (SBI) VUL30 Incorrect implementation of 5G network functions security requirements VUL31 Improper protection of data and information of 5G NFs components VUL32 Improper protection of availability and integrity of 5G NFs VUL33 Vulnerable mechanisms for authentication and authorisation of 5G NFs VUL34 Improper / missing functionality for session protection VUL35 Lack of or improper security event logging VUL36 Vulnerabilities in operating systems supporting 5G NFs VUL37 Improper hardening of 5G core components	ATT5-ATT10-ATT17 LI attacks	NFV MANO; NFVI; VNFM; Ve-Vnfm-em; Ve-Vnfm-vnf UPF/User data; UPF/Signalling data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	BP-T33 - LI capabilities BP-P5 - Incident management BP-P8 - Defence-in-depth BP-P12 - Apply hardening policies BP-P14 - Security-by-design

G ANNEX: REFERENCES FOR CHALLENGES

ID	Challenge	References
	Virtualisation and containerisation	
CH-V1	Challenges within the runtime software	[1], [23], [60], [54], [56], [49], [84], [47], [17]
CH-V2	Flexibility and openness of service environment	[1], [50], [23], [73], [74]
CH-V3	Challenges within the hypervisor/CIS	[6], [25]
CH-V4	Time manipulation	[47], [136]
CH-V5	Entropy generation	[109]
CH-V6	Encrypted data processing	[47]
CH-V7	Challenges within IP layer vs application layer	[47]
CH-V8	Default deployment or configuration	[84], [6], [25]
CH-V9	Network traffic exposure	[48], [60], [61], [84], [25]
CH-V10	Security logs troubleshooting failure	[50]
CH-V11	Container acceleration capabilities	[47]
CH-V12	Container isolation failure	[47]
CH-V13	Sensitive data in NF container images	[47]
CH-V14	Core network functions in the MEC	[112]
CH-V15	Wide geographical distribution of MEC infrastructures	[126]
CH-V16	Insecure API/improper authentication of MEC components	[126]
CH-V17	Insufficient/improper monitoring mechanisms of MEC components	[126]

CH-V18	Centralisation of the SDN control platforms	[59], [39], [40], [41]
CH-V19	Malicious SDN applications	[59], [111], [112]
CH-V20	Common SDN interfaces	[59], [42], [43], [44], [45], [46]
CH-V21	Isolation failure between VNFs	[50], [23], [55] , [56], [58], [63], [71], [74], [75], [76], [84], [47], [25]
CH-V22	Memory introspection	[47]
CH-V23	Trusted domains segmentation	[47], [25], [17]
CH-V24	Access to storage resources	[25], [114]
CH-V25	Sharing of private keys between VNFs and confidentiality of sensitive data	[37], [47]
CH-V26	Availability of network functions	[47]
CH-V27	Software catalogue image exposure	[47]
CH-V28	Multi-vendors integration	[55], [56], [25]
CH-V29	Multi-tenants co-residency	[47], [25], [118], [119]
CH-V30	Elastic nature of NFVI-migration of VNFs	[50], [55], [56], [74], [83], [84], [6], [47], [25]
CH-V31	Geographical location	[50], [47], [25]
CH-V32	Data lifecycle and location	[47]
CH-V33	VNF host spanning	[47]
CH-V34	Dynamic nature of network functions	[50], [77]
Orchestration and management		
CH-OM1	MANO single point of failures	[6], [47]
CH-OM2	Orchestration compromise and policies violations	[6], [13], [47], [84], [115], [116]
CH-OM3	Resource integrity caused by manual changes or failure to update resource inventory	[84], [6], [47]
CH-OM4	Vulnerabilities within orchestration protocols	[6], [13], [47], [84], [115], [116], [134], [135]
Administration and access control		

CH-AC1	Malicious insiders	[50], [23], [79], [84], [47]
CH-AC2	Single administrator domain	[47], [17]
CH-AC3	Lack of staff with the skillsets needed to operate virtualised networks	[60], [6]
CH-AC4	Insecure management, configuration and monitoring interfaces	[23], [55], [56], [84], [47]
CH-AC5	Compromise of orchestration access control	[57], [61], [84], [6]
CH-AC6	Weak or insecure authentication/access control/authorisation to VIM	[57], [61], [84], [6]
New and legacy technologies		
CH-LG1	Mixed virtual and legacy PNF deployments	[47]
CH-LG2	Vulnerabilities of physical hosts	[47]
CH-LG3	Transformation of legacy OSS/BSS	[99], [100], [101]
CH-LG4	Integration with existing legacy OSS/BSS	[99], [100], [101]
Adoption of open source and COTS		
CH-OC1	Adoption of open-source software	[57], [61], [130]
CH-OC2	Adoption of COTS hardware	[120], [121]
Supply chain		
CH-SC1	Separation of test and production environments	[117]
CH-SC2	Untrusted partners	[60], [62]
CH-SC3	Infected/untested/unauthorised untested patches or upgrades	[84], [6], [117]
CH-SC4	Test isolation and assurance	[47]
CH-SC5	Use of counterfeit components	[112]
CH-SC6	Use of inherited components	[112]
Lawful interception (LI)		
CH-LI1	Encryption of communications	[94]

CH-LI2	Cooperation of numerous network providers	[94]
CH-LI3	Availability of data at the LI central nodes	[94]
CH-LI4	LI in hybrid deployment	[127]

H ANNEX: NFV MANO PLATFORMS

This annex details the main MANO platforms for both VMs and/or containers.

H.1 OSM

Open-Source MANO (OSM) is an ETSI-hosted open-source community delivering a production-quality MANO stack for NFV, capable of consuming openly published information models, available to everyone, suitable for all VNFs, operationally significant and VIM-independent. OSM is aligned to NFV ISG information models while providing first-hand feedback based on its implementation experience[120] [121].

OSM Release EIGHT brings several improvements over previous releases. It allows the flexibility of cloud-native applications to be combined within the same network service with the predictability of traditional virtual and physical network functions (VNFs and PNFs) and all the required advanced networking required to build complex E2E telecom services. OSM Release EIGHT is at the forefront of Edge and 5G operations technology, deploying and operating containerised network functions on Kubernetes with a complete lifecycle management, and automated integration.

In addition, OSM extends the SDN framework to support the next generation of SDN solutions providing higher level primitives and increasing the number of available options for supporting I/O-intensive applications. Furthermore, the plugin models for intra- and inter-datacentre SDN have been consolidated, and the management, addition and maintenance of SDN plugins significantly simplified.

OSM Release EIGHT also brings major enhancements designed to improve the overall user experience and interoperability choices. This includes an improved workflow for VNF configuration which allows much faster and complex operations, and the support of additional types of infrastructures, such as Azure and VMware's vCD 10, complementing the previously available choices (OpenStack-based VIMs, VMware VIO, VMware vCD, AWS, Fog05 and OpenVIM). It improves the orchestration of diverse virtualisation environments, including PNFs, a number of different VIMs for VNFs, and Kubernetes for Cloud native NFs.

H.2 ONAP

Open Network Automation Platform (ONAP) is an open-source project hosted by the Linux Foundation[122], officially launched in 2017, enabling telco networks to become increasingly more autonomous. ONAP is capable of providing a real-time, policy-driven service orchestration and automation, enabling telco operators and application developers to instantiate and configure network functions. ONAP, through different releases, supports features such as a) multi-site and multi-vendor automation capabilities, b) service and resources deployment, thus providing c) cloud network elements and services instantiation in a dynamic, real-time and closed-loop manner for several major telco activities, (e.g. design, deployment and operation of services at design-time and run-time.

[120] https://osm.etsi.org/docs/user-guide/02-osm-architecture-and-functions.html
[121] https://www.etsi.org/technologies/open-source-mano
[122] Open Network Automation Platform, https://docs.onap.org/en/elalto/index.html#

Various edge cloud architectures have already emerged from different communities and potentially can be plugged into the ONAP architecture for service orchestration. The ONAP community analyses the orchestration requirements of services over various edge clouds and how these requirements impact ONAP components in terms of data collection, processing, policy management, resource management, control loop models and security, as well as application and network function deployment and control. We invite the reader to read more detail in this link[123].

H.3 OPNFV

It was launched by the Linux Foundation in September 2014 [67]. OPNFV focuses on NFVI and includes an SDN controller and switch. OPNFV is a platform for implementing NFV and can provide feedback on the necessary information to the ONAP platform. The four goals of OPNFV are as follows:

- after testing, to use continuous integration or continuous delivery (CI/CD) to develop an open-source platform that can build NFV system functions;
- to invite operators of telecommunication services to join the programme and verify that OPNFV meets user expectations;
- to join other open-source projects that will use OPNFV to ensure consistency, performance and interoperability.
- To build an ecosystem of NFV solutions based on open source.

H.4 SONATA

The SONATA project[124] is a component of an EU-funded project, Horizon 2020, and part of the 5G-PPP initiative. The SONATA [65] service platform is implemented as a modular microservice, which is very flexible and helps the operator to modify a customised function. Software Defined Networking (SDN) and Network Function Virtualisation (NFV) are emerging as major transformational technologies towards 'software networks', a new paradigm that is furthering the evolution of the telecom sector with new network capabilities and business opportunities. SONATA addresses the significant challenges associated with both the development and deployment of the complex services envisioned for 5G networks and empowered by these technologies. Core objectives include:

- *reduced time-to-market of networked services*: SONATA streamlines development with abstract programming models, SDK and a DevOps model that integrates operators, manufacturers and third-party developers;
- *optimised resources and reduced costs of service deployment and operation*: SONATA orchestrates complex services for connectivity, computing and storage resources, and automatically re-configures running services.
- *accelerated industry adoption of software networks*: SONATA supports the full service lifecycle, i.e. development, testing, orchestration, deployment, management and operations, and will define a roadmap for the uptake of results towards stakeholders' larger transition to SDN/NFV.

H.5 OPENSTACK TACKER

OpenStack Tacker[125] is under the big tent of OpenStack projects and aims at building an open orchestrator with a general purpose VNF Manager to deploy and operate virtual network functions on an NFV platform. It is based on the ETSI MANO architectural framework and provides a full functional stack to orchestrate VNFs end-to-end. Today, Tacker offers features like a VNF catalogue, a basic VNF lifecycle management, VNF configuration management

[123] https://wiki.onap.org/display/DW/Edge+Automation+through+ONAP+Arch.+Task+Force+-+Distributed+Management+%28ONAP+etc.%29+components
[124] http://sonatanfv.org/content/objectives
[125] OpenStack Tacker," https://wiki.openstack.org/wiki/Tacker

framework, and a VNF health monitoring framework. The VNF catalogue makes use of the topology and orchestration specification for cloud applications (TOSCA) language for the definition of VNF meta-data and OpenStack Glance to store and manage the VNF images. Tacker VNF lifecycle management takes care of the instantiation and termination of virtual machines, self-healing and auto-scaling, and VNF image updates. It also takes care of interfaces to vendor specific element management systems. Like the VNF catalogue, the basic VNF lifecycle management relies on existing OpenStack services and uses OpenStack Heat to start and stop virtual machines that contain the VNF. Thus, the TOSCA templates are automatically translated to OpenStack Heat templates.

H.6 OPENBATON

OpenBaton[126] is an open source project by Fraunhofer FOKUS that enables implementation of the ETSI management and orchestration specification. Its main components are a network function virtualisation orchestrator, a generic virtual network function manager that manages VNF lifecycles based on the VNF description, and an SDK comprising a set of libraries that could be used for building a specific VNF Manager.

The NFV orchestrator, which is the main component of OpenBaton, is written in Java using the spring.io framework. To interconnect the NFV orchestrator to different VNF managers, OpenBaton relies on the Java messaging system. The NFV orchestrator is currently using OpenStack as an integrated virtual infrastructure manager, supporting dynamic registration of NFV points of presence and deploys in parallel multiple slices consisting of one or multiple VNFs. Through this functionality the orchestrator provides a multi-tenant environment distributed on top of multiple cloud instances.

H.7 KUBERNETES

Over the last few years Kubernetes[127] (noted as K8s) has become a de facto standard for container orchestration. As container transformation unfolds in the telecom industry, VM based VNFs give way to cloud native NFs.

Kubernetes is a container orchestration system for automating application deployment, scaling, and management. In the parlance of ETSI's NFV architecture, it performs the role of the container infrastructure service management (CISM) function (which performs equivalent 'virtualised resource management' as VIMs do but for the container deployment case as described in ETSI GR NFV-IFA 029 and ETSI GS NFV-IFA 040).

ETSI GS NFV-SOL 018[128] (Draft specification - work in progress) provides a mapping of the NFV object model for OS container management and orchestration to managed objects of Kubernetes® and Helm™ as specified by the CNCF® along with a specification of a mapping between a common set of input parameters (e.g. derived from VNFD/NSD and/or NFV-MANO RESTful APIs) and output parameters associated with the management and orchestration of the managed objects.

It profiles the reference Kubernetes® API as an NFV protocol and data model solution for OS container management and orchestration. It profiles the reference Helm™ documentation as an NFV protocol and data model solution for the management of OS container workloads based on an MCIOP (managed container infrastructure object package). It profiles the reference OCI™ Distribution Specification API (which is based on the Docker™ registry API) as an NFV protocol

[126] "OpenBaton" https://openbaton.github.io/
[127] https://kubernetes.io
[128] https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=62022&curItemNr=77&totalNrItems=80&optDisplay=100000&titleType=all&qSORT=HIGHVERSION&qETSI_ALL=&SearchPage=TRUE&qTB_ID=789%3BNFV&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qSTART_CURRENT_STATUS_CODE=0%3BM40&qEND_CURRENT_STATUS_CODE=9+AB%3BN24&qSTOP_FLG=N&qKEYWORD_BOOLEAN=OR&qCLUSTER_BOOLEAN=OR&qFREQUENCIES_BOOLEAN=OR&qSTOPPING_OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=FALSE&qREPORT_TYPE=SUMMARY

and data model solution for OS container image management.

The latest published versions of the Kubernetes® API, Helm™ documentation and OCI™ distribution specification API are profiled against the requirements of the functions and the management service interfaces of the container infrastructure service management (CISM) and container image registry (CIR) functions as specified in ETSI GS NFV-IFA 040 and ETSI GS NFV-IFA 010.

ETSI GS NFV-SOL 018 includes guidelines and rules on how the profiled and referenced solutions can be adopted in a way that facilitates their integration with the NFV-MANO framework solutions.

In the Kubernetes ecosystem, there is a project called KubeVirt that provides a way to take an existing VM and run it inside a container. With KubeVirt, it possible to deploy and manage applications that comprise any arbitrary mix of native container workloads and VM workloads using Kubernetes. The underlying infrastructure can be OpenStack, VMware, bare metal or any of the main public clouds including Azure, AWS or Google.

I ANNEX: NFV STANDARDISATION, OPEN-SOURCE AND ACADEMIA/INDUSTRY INITIATIVES

I.1 STANDARDISATION

Table 20 provides the standardisation efforts on NFV and SDN from different telecom industry and bodies. It covers the following standards [22].

Table 20: NFV standardisation

Standardisation Body	Focus
3GPP SA3	Threat analysis, requirements on security, security architecture and protocol specifications
ETSI ISG NFV	Security monitoring and administration for NFV Security assessment for NFV platform Etc.
GSMA	5G trust model, NESAS, NFV threat model, etc.
IETF	Network virtualisation overlay, dynamic service chaining, network service header
OPNFV	NFV Open Platform/eCOMP/OPNFV Community TestLabs
ONAP	Linux Foundation
OSM	Open-Source MANO (management and orchestration)
IEEE	Standard for software defined networking and network function virtualisation (SDN/NFV) security
NGMN	5G security requirements (DoS protection, network slicing, MEC)

I.2 OPEN-SOURCE PROJECTS IN 5G

There are numerous open-source projects across multiple domains of infrastructure, management, control, access and core. Determining the applicability of open source to an appropriate domain can be overwhelming. Table 21 provides a snapshot of some projects to be considered when determining the applicability of open source across different layers of the 5G network [22], [7], [105], [106].

Table 21: Open source projects in 5G

Project	Area	Focus	Description	Link
Open compute project (OCP)	Infrastructure	Hardware	The mission of OCP is 'to apply the benefits of open source to hardware and rapidly increase the pace of innovation in, near and around the datacentre and beyond.' OCP's Telecom Working Group has developed the CG-OpenRack-19 specification. This specification offers operators of telecom datacentres the benefits of open platform standards combined with the carrier-grade and environmental enhancements required for edge computing, which will be one of the most important building blocks for successful 5G deployments.	http://www.opencompute.org/about/ocp-adoption http://www.eenewseurope.com/news/open-compute-projects-first-carrier-grade-specs
Disaggregated network operating system (DANOS)	Infrastructure	Operating system	DANOS is an open and flexible alternative to traditional networking operating systems. It will support a network operating system framework that leverages existing open-source resources and complementary platforms such as switches and white box routers.	https://www.danosproject.org
Linux	Infrastructure	Operating system	Linux enables white box to be used in carrier grade networks.	https://www.linuxfoundation.org/projects/linu x/
Berkley software distribution (BSD)	Infrastructure	Operating system	BSD is an operating system (also includes the kernel) which has been derived from the Unix operating system.	http://www.bsd.org
P4	Infrastructure	Hardware	P4 is an open-source initiative designed primarily to provide a declarative language for interacting with networking forwarding planes. P4 programs specify how a switch processes the packets. P4 controls silicon processor chips in network forwarding devices such as switches, routers and network interface cards.	https://p4.org
VPP	Infrastructure	Network	The VPP platform is an extensible framework that provides out-of-the-box production quality switch or router functionality. It is the open-source version of Cisco's Vector Packet Processing (VPP) technology, a high performance, packet-processing stack that can run on commodity CPUs.	https://fd.io
O-RAN	Access Control	Radio	The O-RAN alliance uses two themes: 'openness and intelligence' for next generation wireless networks and beyond. 'Building a more cost-effective, agile RAN requires openness. Open interfaces are essential to enable smaller vendors and operators to quickly introduce their own services' and 'intelligence networks will become increasingly complex with the advent of 5G, densification and richer and more demanding	https://www.o-ran.org/

			applications. To tame this complexity, we cannot use traditional human intensive means of deploying, optimising and operating a network. Instead, networks must be self-driving, they should be able to leverage new learning-based technologies to automate operational network functions and reduce OPEX'.	
Openair5G	Access control	Radio	Openair5G is an open software that gathers a community of developers from around the world, who work together to build wireless cellular radio access network (RAN) and core network (CN) technologies.	https://gitlab.eurecom.fr/oai/openairinterface 5g/wikis/home https://openairinterface.org
Telecom infra project (TIP)	Access control	Radio	TIP focuses on decoupling the RAN control plane from the user plane, building a modular RAN software stack that uses commodity hardware and publishing open north- and south-bound interfaces.	https://telecominfraproject.com
Openair CN	Core network	Wireless core network	Openair CN is for implementing 4G LTE EPC and 5G NGC.	https://gitlab.eurecom.fr/oai/openairinterface 5g/wikis/home
M-CORD	Core network	SDN controller	M-CORD is an open-source reference solution for operators deploying 5G. It is built on the CORD infrastructure platform, which brings datacentre economics and cloud agility to operator networks. M-CORD transforms the mobile network by disaggregating and virtualising cellular network functions, as well as operator-specific services. M-CORD lays the foundation for 5G networks and services through support for disaggregated and virtualised EPC, end-to-end slicing from RAN to EPC, mobile edge computing and a programmable radio access network.	https://www.opennetworking.org/m- cord/
OpenDayLight (ODL)	Management & control	SDN controller	ODL is set to provide dynamic services in the era of 5G by optimising softwarised and virtualised networks in order to meet the continuously evolving service demands of the end-users.	https://www.opendaylight.org
ONOS	Management & control	SDN controller	ONOS can enable the network slicing concept through VNF composition in the central office where tenants can easily create network services using northbound abstractions.	https://onosproject.org
OpenMANO	Management & control	MANO	OpenMANO provides a practical implementation of the NFV MANO reference architecture.	https://github.com/nfvlabs/openmano
OSM	Management & control	MANO	OSM is MANO with SDN control, multi-site and multi-VIM capability.	https://osm.etsi.org
OPNFV	Management & control	MANO	OPNFV facilitates the development of multi-vendor NFV solutions across various open-source ecosystems.	https://www.opnfv.org
ECOMP	Management & control	MANO	ECOMP or enhanced control, orchestration, management and policy, provides the necessary automation platform that enables aggressive	https://about.att.com/innovationblog/linux_foundation

			virtualisation goals across enterprise, infrastructure, mobility and consumer use cases to be achieved	
T-NOVA	Management & control	MANO	T-NOVA is an open-source MANO stack for NFV.	http://www.t-nova.eu/open-source/
Open Baton	Management & control	MANO	Open Baton is a an extensible and customisable NFV MANO-compliant framework.	https://openbaton.github.io
Cloudify	Management & control	MANO	Cloudify is an open-source orchestration platform and a widely deployed, production-grade implementation of the TOSCA[129] standard.	https://cloudify.co
ZOOM	Management & control	MANO, OSS/BSS	Zoom is aimed at modernising OSS/BSS models and introducing faster responses to service problems and opportunities.	https://www.tmforum.org
CloudNFV	Management & control	MANO	CloudNFV is an open platform for implementing network functions virtualisation (NFV) based on cloud computing and software defined networking (SDN) technologies in a multi-vendor environment.	https://www.cloudnfv.com
HP OpenNFV	Management & control	MANO	The OpenNFV programme is an open approach that allows HP and external partners, such as network equipment providers and independent software vendors, to take advantage of the open and standards-based NFV reference architecture, HP OpenNFV Labs, and the HP OpenNFV partner ecosystem of applications and services.	https://www.hp.com/ae-en/cloud/nfv-overview.html
Intel ONP	Management & control	MANO	Intel's open network platform (Intel ONP) for servers is designed to make it easier to test and deploy SDN and NFV solutions.	https://www.intel.com/content/www/us/en/communications/open-network-platform-server-datasheet.html
OPEN-O	Management & control	MANO	The Open Orchestrator Project (OPEN-O) is an open source project backed by the Linux Foundation that enables telecommunications and cable operators to effectively deliver end-to-end services across network functions virtualisation (NFV) infrastructure, as well as software defined network (SDN) and legacy network services.	https://www.openhub.net/p/open-o
ExperiaSphere	Management & control	MANO	ExperiaSphere is an open-source universal MANO architecture.	http://www.experiasphere.com
ONAP	Management & control	MANO	The Open Network Automation Platform (ONAP) project automates 5G using software defined networking (SDN) and network functions virtualisation (NFV) technologies.	https://www.onap.org
SONATA	Management & control	MANO	The SONATA NFV platform is a flexible and integrated platform that allows the creation of a versatile and modular ecosystem that serves to service developers and testers, telecom operators or vertical industries, managing the full lifecycle of network services. The SONATA NFV platform encompasses everything from development to network services	https://www.sonata-nfv.eu/content/agile-development-testing-and-orchestration-services-5g-virtualized-networks

[129] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca

			testing and their deployment and orchestration in a 5G infrastructure.	
Kubernetes	Management & control	CISM	Kubernetes is a container orchestration system for automating application deployment, scaling and management. In the parlance of ETSI's NFV architecture, it performs the role of the container infrastructure service management (CISM) function (which performs equivalent 'virtualised resource management' as VIMs do, but for the container deployment case as described in ETSI GR NFV-IFA 029 and ETSI GS NFV-IFA 040).	https://kubernetes.io
OpenStack	Management & control	VIM	OpenStack is a cloud operating system that controls large pools of compute, storage and networking resources throughout a datacentre, all managed and provisioned through APIs with common authentication mechanisms.	https://www.openstack.org
Docker	Management & control	NFVI	Docker is a set of platforms as a service product that use OS-level virtualisation to deliver software in packages called containers.	https://www.docker.com
KVM	Management & control	NFVI	KVM (for kernel-based virtual machine) is a full virtualisation solution for Linux on x86 hardware containing virtualisation extensions (Intel VT or AMD-V).	https://www.linux-kvm.org/page/Main_Page
XEN	Management & control	NFVI	Xen is a type-1 hypervisor, providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently.	https://xenproject.org
CITRIX	Management & control	NFVI	Citrix hypervisor provides a highly reliable and secure open-source virtualisation platform for cloud, server and desktop virtualisation infrastructures.	https://www.citrix.com
PNDA (network analytics platform)	Management & control	Network analytics platform	PNDA is a scalable, open-source big data analytics platform for networks and services.	http://pnda.io
OpenSwitch	Management & control	Whitebox NOS, virtual switch	OpenSwitch is a Linux Foundation project with the mission to deliver a turnkey switching software solution based on the OPX open-source network operating system (NOS).	https://www.openswitch.net
JuJu	Management & control	VNFM	The Juju VNF manager enables the Open Baton NFVO to interoperate with Juju as a generic VNFM.	https://github.com/openbaton/juju-vnfm
FD.io	Management & control	Data plane acceleration	FD.io (Fast data – input/output), the universal data plane, is a collection of several projects and libraries to amplify the transformation that began with the data plane development kit (DPDK) to support flexible, programmable and composable services on a generic hardware platform.	https://fd.io
DPDK (fast packet processing)	Management & control	Data plane acceleration	DPDK is a set of libraries used to accelerate packet processing on multiple-core CPUs. DPDK facilitates the quicker expansion of high-speed data packet networking applications.	https://www.dpdk.org

I.3 STANDARDS VS OPEN-SOURCE PROJECTS

In 5G Americas - *The Status of Open Source for 5G* [105] it is stated that there are quite a few similarities between the standards and open-source paradigms. Both have the objectives of increasing interoperability, reducing costs and facilitating the establishment of a healthy business ecosystem. The difference has to do with the method to achieve those goals.

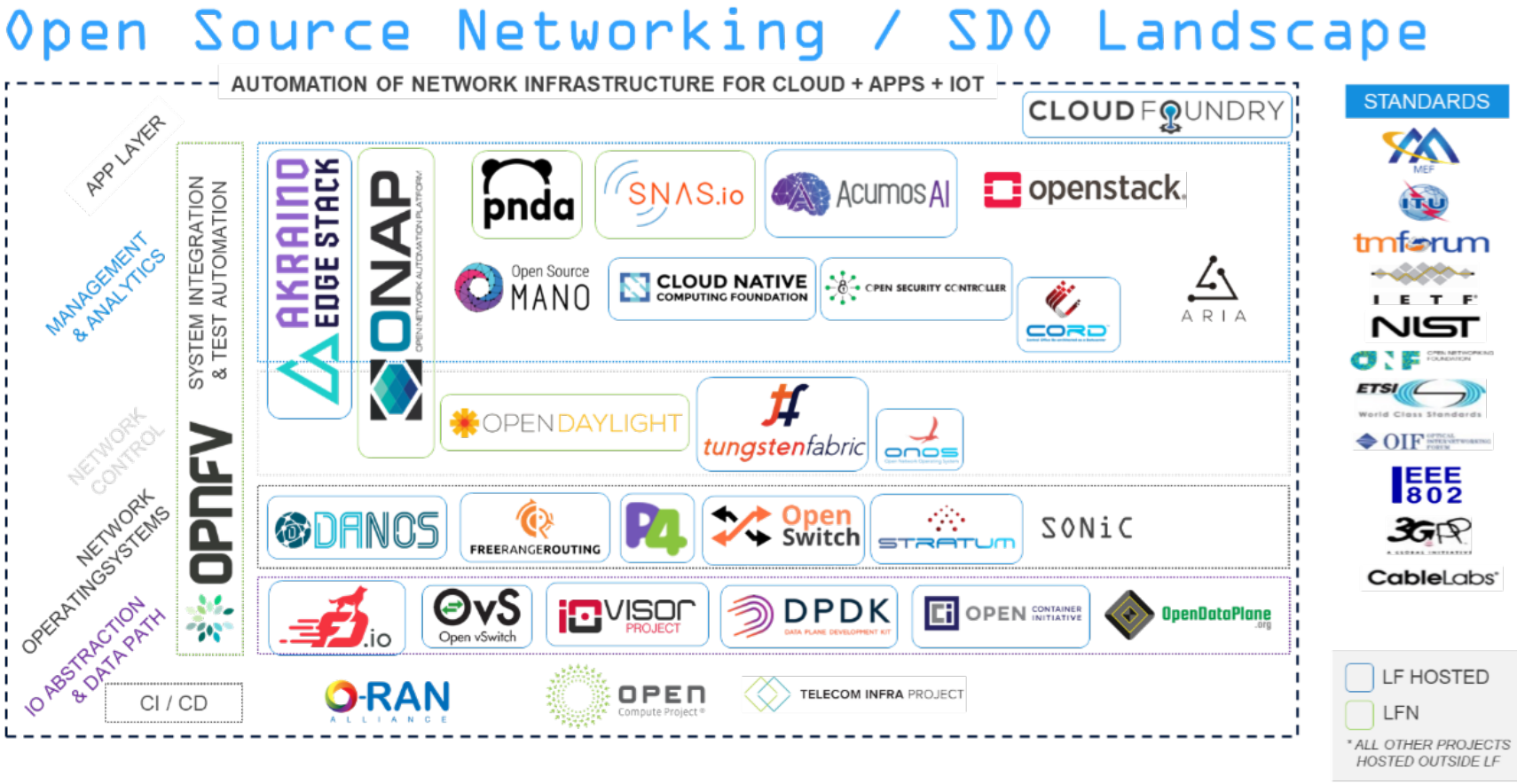
Historically, standards have been developed using consensus-based collaboration in a process that required written documentation of the specific standard (for example, a specification, protocol, an application protocol interface (API)). This is no different than open-source projects, with the exception that for open source, contributions are in the form of running code.

Usually, the collaboration process in standards is a very transparent one based on less transparent or even proprietary implementations. Open-source projects can bring implementation transparency during the harmonisation or standardisation process, as well as after the finalisation of a standard as a way to establish implementations as reference.

Therefore, open-source projects should be considered complementary to the development of standards, as a way to accelerate and improve the process of creating interoperable solutions. Figure 21 shows where standards and open-source initiatives work together to benefit vendors, service providers and end users. Combined with automation tools, continuous testing and integration, as well as broad adoption of DevOps within large organisations, this combination can be a powerful catalyst for innovation and rapid development[130].

Figure 21: Open source projects and standard organisations[131]

[130] https://www.researchgate.net/publication/275037585/download
[131] https://www.linuxfoundation.jp/wp-content/uploads/2019/01/LF_StandardsOpenSource_Whitepaper_012418.pdf



I.4 ACADEMIA & INDUSTRY PROJECTS

Table 22 gives a summary of academia and industry 5G projects focusing on SDN/NFV [22].

Table 22: Academia and industry 5G projects focusing on SDN/NFV

Project	Area	Link

5G-NORMA	Multi-service and context-aware adaptation of network functions to support a variety of services and corresponding QoE/QoS requirements.	https://5g-ppp.eu/5g-norma/
5G-MEDIA	A flexible network architecture that provides dynamic and flexible UHD (4K/8K) content distribution over 5G CDNs.	http://www.5gmedia.eu
5G-MoNArch	Employs network slicing to support the orchestration of both access and core network functions, and analytics to support a variety of use cases in vertical industries such as automotive, healthcare, and media.	https://5g-monarch.eu
SESAME	Develops programmable 5G network infrastructure that supports multi-tenancy, decreasing network management OPEX whilst increasing the QoS and QoE and security.	https://5g-ppp.eu/sesame/
MATILDA	Provides orchestration of 5G-ready applications and network services over sliced programmable platforms.	https://www.matilda-5g.eu
5G-Transformer	Develops an SDN/NFV-based 5G network architecture that meets the requirements of specific vertical industries (e.g. eHealth, automotive, industry 4.0 and media).	http://5g-transformer.eu
5G-Crosshaul	Designs 5G transport architectural solutions that support multi-domain orchestration among multiple network operators or service providers (e.g. multiple tenants).	https://5g-ppp.eu/xhaul/
5G-XHaul	Develops a scalable SDN control plane and mobility aware demand prediction models for optical or wireless 5G networks.	https://5g-ppp.eu/5g-xhaul/
CogNET	Dynamically adapts to network resources of VNFs whilst minimising performance degradations to fulfil SLA or ELAs requirements.	https://5g-ppp.eu/cognet/
CHARISMA	Develops a software-defined converged fixed 5G mobile network architecture that offers both multi-technology and multi-operator features.	https://5g-ppp.eu/charisma/
SaT5G	Provides integrated management and orchestration of network slices in 5G SDN/NFV based satellite networks.	https://www.sat5g-project.eu
SLICENET	Develops a cognitive network control, management and orchestration framework that supports infrastructure sharing across multiple operator domains in SDN/NFV-enabled 5G networks.	https://slicenet.eu
SONATA	Enables integrated management and control to be part of the dynamic design of the softwarised 5G network architecture.	https://5g-ppp.eu/sonata/
COHERENT	Delivers efficient radio resource modelling and management in programmable radio access networks.	https://5g-ppp.eu/coherent/
5G Exchange	Enables cross-domain orchestration of services over multiple administrations or over multi-domain single administrations.	https://www.the5gexchange.com
VIRTUWIND	As a part of a 5G PPP programme, VirtuWind develops and demonstrates SDN and NFV ecosystems, based on an open, modular and secure framework showcasing a prototype for intra-domain and interdomain scenarios in real wind parks as a representative use case of industrial networks, and validates the economic viability of the solution demonstrated.	https://5g-ppp.eu/virtuwind/
5GEX	The goal of the 5G Exchange (5GEx) project is to enable cross-domain orchestration of services over multiple administrations or over multi-domain single administrations.	https://5g-ppp.eu/5gex/
5GCITY	5GCity focuses on how common smart city infrastructure (i.e. small cells and processing power at the very edge of networks) can bring benefit to both players based on resource sharing and end-to-end virtualisation, pushing the cloud model to the extreme edge.	https://www.5gcity.eu

5G!Pagoda	5G!Pagoda represents the next evolution step in softwarised networks as supported by NFV and SDN and aimed at the 5G network evolution.	https://cordis.europa.eu/project/id/723172

TP-06-22-045-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-557-9
doi: 10.2824/166009