HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

# BACHELORARBEIT

Herr
**Eric Sabitzer**

## Management und Orchestrierung von virtualisierten Netzwerkfunktionen im 5G Mobilfunknetz – Überblick, Sicherheitsbetrachtung und SCAS-Testentwurf

Mittweida, 2022

Fakultät Angewandte Computer- und Biowissenschaften

# BACHELORARBEIT

# Management und Orchestrierung von virtualisierten Netzwerkfunktionen im 5G Mobilfunknetz – Überblick, Sicherheitsbetrachtung und SCAS-Testentwurf

Autor:
**Herr**
**Eric Sabitzer**

Studiengang:
**Angewandte Informatik /**
**Vertiefung IT-Sicherheit**

Seminargruppe:
**IF19wi2-B**

Erstprüfer:
**Herr Prof. Dr.-Ing. Volker Delport**

Zweitprüfer:
**Herr Ben Lorenz, M. Sc.**

Einreichung:
**Mittweida, 17.10.2022**

Verteidigung/Bewertung:
**Mittweida, 2022**

Faculty Applied Computer Sciences &
Biosciences

# BACHELORTHESIS

# Management and Orchestration of Virtualized Network Functions in the 5G Cellular Network – Overview, Security Considerations and SCAS Test Case Draft

author:
**Mr.**
**Eric Sabitzer**

course of studies:
**Applied Computer Science /**
**field of study „IT security“**

seminar group:
**IF19wi2-B**

first examiner:
**Mr. Prof. Dr.-Ing. Volker Delport**

second examiner:
**Mr. Ben Lorenz, M. Sc.**

submission:
**Mittweida, 17.10.2022**

## Bibliografische Beschreibung:

Sabitzer, Eric:
Management und Orchestrierung von virtualisierten Netzwerkfunktionen im 5G Mobilfunknetz – Überblick, Sicherheitsbetrachtung und SCAS-Testentwurf. - 2022. - VII, 62 Seiten.
Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2022.

## Referat:

In dieser Bachelorarbeit wird ein Überblick über die Management- und Orchestrierungskomponente eines 5G Mobilfunknetzes sowie dafür relevante, zugrundeliegende Konzepte gegeben. Die Sicherheitsrelevanz des MANO-Systems wird anhand der Ergebnisse einer Risikoanalyse eingeordnet. Die daraus abgeleiteten Sicherheitsvoraussetzungen werden mit bereits bestehenden Zertifizierungs-Tests verglichen und somit herausgearbeitet, für welche Sicherheitsaspekte zukünftig ein MANO-spezifischer Zertifizierungstest erstellt werden muss. Um die Arbeit abzuschließen, wird ein beispielhafter Test-Entwurf vorgestellt, mit welchem sich eine der noch offenen Sicherheitsvoraussetzungen überprüfen lassen könnte.

# Inhalt

# Abbildungsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| **3GPP** | 3rd Generation Partnership Project |
| **5G** | Fünfte Generation der Mobilfunknetzwerke |
| **AMF** | Access and Mobility Management Function |
| **API** | Application Programming Interface |
| **AWS** | Amazon Web Services |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik |
| **BSS** | Business Support Systems |
| **CaaS** | Crypto as a Service |
| **CD** | Continuous Delivery |
| **CDN** | Content Delivery Network |
| **CI** | Continuous Integration |
| **COTS** | commercial off-the-shelf |
| **CP** | Control Plane |
| **CPD** | Connection Point Descriptor |
| **DDoS** | Distributed Denial-of-Service |
| **DP** | Data Plane |
| **EM** | Element Manager |
| **EMS** | Element Management System |
| **ENISA** | European Union Agency for Cybersecurity |
| **ETSI** | European Telecommunications Standards Institute |
| **FCAPS** | Fault-, Configuration-, Accounting-, Performance- and Securitymanagement |
| **GCP** | Google Cloud Platform |
| **GR** | Group Report |
| **GS** | Group Specification |
| **GSMA** | Group Speciale Mobile Association |
| **IDS** | Intrusion Detection System |
| **IETF** | Internet Engineering Task Force |
| **IMS** | IP Multimedia Subsystem |
| **IoT** | Internet of Things |
| **IP** | Internet Protocol |
| **IPS** | Intrusion Prevention System |
| **ISF** | Infrastructure Security Function |

| | |
|---|---|
| **ISO** | International Organization for Standardization |
| **ITU** | International Telecommunication Union |
| **MAC** | Message Authentication Code |
| **MANO** | Management and Orchestration |
| **MDCAP** | Multi Data Center Automation Platform |
| **MNO** | Mobile Network Operator |
| **NESAS** | Network Equipment Security Assurance Scheme |
| **NF** | Network Function |
| **NFFG** | Network Function Forwarding Graph |
| **NFV** | Network Function Virtualisation |
| **NFV AUD-DB** | NFV Audit Database |
| **NFVI** | Network Function Virtualisation Infrastructure |
| **Nf-Vi** | Referenzpunkt zwischen Virtualized Infrastructure Manager und NFV Infrastructure |
| **NFVIaaS** | Network Function Virtualisation Infrastructure as a Service |
| **NFVI-PoP** | Network Function Virtualisation Infrastructure – Point-of-Presence |
| **NFVO** | Network Function Virtualisation Orchestrator |
| **NFVSecM-DB** | NFV Security Monitoring Database |
| **NS** | Network Service |
| **Or-Vi** | Referenzpunkt zwischen NFV Orchestrator und Virtualized Infrastructure Manager |
| **Or-Vnfm** | Referenzpunkt zwischen NFV Orchestrator und VNF Manager |
| **OS** | Operating System |
| **OSM** | Open Source MANO |
| **Os-Ma-Nfvo** | Referenzpunkt zwischen OSS/BSS und NFV Orchestrator |
| **OSS** | Operations Support Systems |
| **PNF** | Physical Network Function |
| **PoP** | Point-of-Presence |
| **PSF** | Physical Security Function |
| **RAN** | Radio Access Network |
| **RFC** | Request for Comments |
| **RGW** | Residential Gateway |
| **SC** | Security Controller |
| **SCAS** | Security Assurance Specification |
| **SDN** | Software Defined Networking |
| **SecaaS** | Security as a Service |
| **SEM** | Security Element Manager |

**SF** Security Function

**SM** Security Manager

**SSA** Security Service Agent

**SSP** Security Service Provider

**STP** Set-top Box

**TCO** Total Cost of Ownership

**TLS** Transport Layer Security

**TS** Technical Specification

**TS 33.117** Technical Specification „Catalogue of general security assurance requirements“

**vCDN** Virtual Content Delivery Network

**VDU** Virtual Deployment Unit

**Ve-Vnfm-em** Referenzpunkt zwischen Element Manager und VNF Manager

**Ve-Vnfm-vnf** Referenzpunkt zwischen Virtual Network Function und VNF Manager

**vFW** Virtual Firewall

**VIM** Virtualized Infrastructure Manager

**Vi-Vnfm** Referenzpunkt zwischen VNF Manager und Virtualized Infrastructure Manager

**VLD** Virtual Link Descriptor

**VM** Virtual Machine

**VNF** Virtual Network Function

**VNFaaS** Virtual Network Function as a Service

**VNFC** Virtual Network Function Component

**VNFD** Virtual Network Function Descriptor

**VNFFG** Virtual Network Function Forwarding Graph

**VNFFGD** Virtual Network Function Forwarding Graph Descriptor

**VNFM** Virtual Network Function Manager

**VNPaaS** Virtual Network Platform as a Service

**vNSF** Virtual Network Security Function

**vRGW** Virtual Residential Gateway

**vSEC-GW** Virtual Security Gateway

**VSF** VNF-Layer Security Function

**VSF-VNF-CAT** SSA/VSF Catalogue Database

**vSTB** Virtual Set-top Box

**YAML** Yet Another Markup Language

# 0 Einleitung

Der Ausbau der fünften Generation der Mobilfunknetze ist in Deutschland seit 2019 im vollen Gange. Im Oktober 2021 wurde laut Bundesnetzagentur bereits 53% der Fläche Deutschlands von mindestens einem Mobilfunkanbieter mit 5G abgedeckt – Tendenz steigend. [1] Die neue Generation bringt viele Neuerungen und Vorteile mit sich, um den steigenden Anforderungen von Industrie und Privatpersonen gerecht zu werden. Downloadraten von bis zu 20 Gbit/s, Latenzen von unter einer Millisekunde und einer Kapazität von bis zu einer Million Geräte pro $km^2$ ermöglichen bisher ungeahnte Möglichkeiten in der Anwendung von Mobilfunk. [2]

5G und insbesondere sein cloudbasierter Aufbau bringen dabei jedoch einige hohe, sicherheitstechnische Risiken mit sich, welche aufgrund der schnellen Verbreitung und Verwendung von 5G adressiert werden müssen. Unter anderem besitzt die Management- und Orchestrierungskomponente (MANO) des 5G Netzes eine sehr hohe Kritikalität, da sie den Lebenszyklus sämtlicher Netzwerkfunktionen im Mobilfunknetz verwaltet und einen Überblick über alle Hard- und Softwareressourcen besitzt. Ein erfolgreicher Angriff auf die MANO-Komponente könnte verheerende Folgen nach sich ziehen.

Um Sicherheitslücken in Netzwerkprodukten zu vermeiden, müssen in Deutschland sämtliche kritischen Funktionen und Komponenten in Telekommunikationsnetzen vor Inbetriebnahme vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert werden. Aufgrund der Sicherheitsrelevanz der MANO-Komponente zählt diese zu den kritischen Komponenten und ist demnach zertifizierungspflichtig. [3] Bisher wurden für das Zertifizierungsschema „Network Equipment Security Assurance Scheme“ jedoch noch keine anwendbaren Tests veröffentlicht, mit welchen sich MANO-Komponenten zertifizieren lassen.

Ziel dieser Arbeit ist es, dieses Thema aufzuarbeiten.

Dafür werden im theoretischen Teil dieser Arbeit zunächst zwei relevante, neue Konzepte im 5G Netz vorgestellt: Software Defined Networking (SDN) sowie Network Function Virtualization (NFV). Da NFV eine Management- und Orchestrierungskomponente benötigt, wird anschließend die MANO-Komponente von virtuellen Netzwerkfunktionen und Sicherheitsmanagementfunktionen im NFV-System eingeordnet sowie Aufbau und Funktionsweise des MANO-Systems erläutert.

Im folgenden Teil der Arbeit wird die Sicherheit des MANO-Systems thematisiert. Eine Zusammenfassung des aktuellen Entwicklungsstands von MANO-spezifischen Tests sowie sicherheitsrelevanten Spezifikationen verschafft einen Überblick über aktuell gültige,

offizielle Sicherheitsrichtlinien. Auf Basis einer Risikoanalyse werden Bedrohungen sowie Sicherheitsvoraussetzungen für die MANO-Komponente erläutert.

Im letzten Teil der Arbeit werden Erkenntnisse der Risikoanalyse mit Zertifizierungstests verglichen, welche bereits im Einsatz sind und auf alle Netzwerkprodukte zutreffen sollen. Dabei wird herausgearbeitet, welche Sicherheitsaspekte der MANO-Komponente bereits durch diese Tests abgedeckt sind und welche Sicherheitsaspekte noch in MANO-spezifischen Tests überprüft werden müssen. Abschließend wird ein noch offener Sicherheitsaspekt näher betrachtet und ein Testentwurf vorgestellt, mit welchem sich die festgestellte Sicherheitsvoraussetzung überprüfen lassen könnte.

Im Ausblick der Arbeit werden relevante Spezifikationen betrachtet, welche sich momentan noch im Entwurfsstatus befinden und bei Veröffentlichung relevant für die Sicherheit von MANO sein werden.

# 1 Einführung in 5G: Grundlagen & neue Konzepte

Die fünfte Generation der Mobilfunknetze bringt in Aufbau und Funktionsweise viele technische Neuerungen im Vergleich zu bisherigen Mobilfunkgenerationen mit sich, um die gesetzten Leistungsziele der International Telecommunication Union (ITU) für 5G Mobilfunknetze (Latenzen < 1ms, 1.000.000 Geräte / km², 20 Gbit/s Peak-Downloadrate, …) zu erreichen. [2]

Die für diese Arbeit relevanten Konzepte und Neuerungen im 5G Mobilfunknetz werden in diesem Kapitel vorgestellt.

## 1.1 Software Defined Networking (SDN)

Ein traditioneller Netzwerk-Switch besitzt eine Kontrollschicht (Control Plane, CP) und eine Datenschicht (Data Plane, DP). Die Kontrollschicht legt fest, nach welchen Regeln Pakete gefiltert oder weitergeleitet werden sollen. Die Datenschicht leitet die eingehenden Pakete entsprechend weiter.

Nachteil dieses traditionellen Ansatzes, wie er in bisherigen Mobilfunkgenerationen verwendet wurde, ist, dass Konfigurationsänderungen im Netzwerk aufwändig und langsam sind. Dies liegt daran, dass jeder Switch meist einzeln mittels eines proprietären Interfaces rekonfiguriert werden muss. Im Gegensatz dazu wird bei 5G durch einen softwaredefinierten Netzwerkbetrieb die Kontrollschicht von der Datenschicht entkoppelt. [4, S. 4]

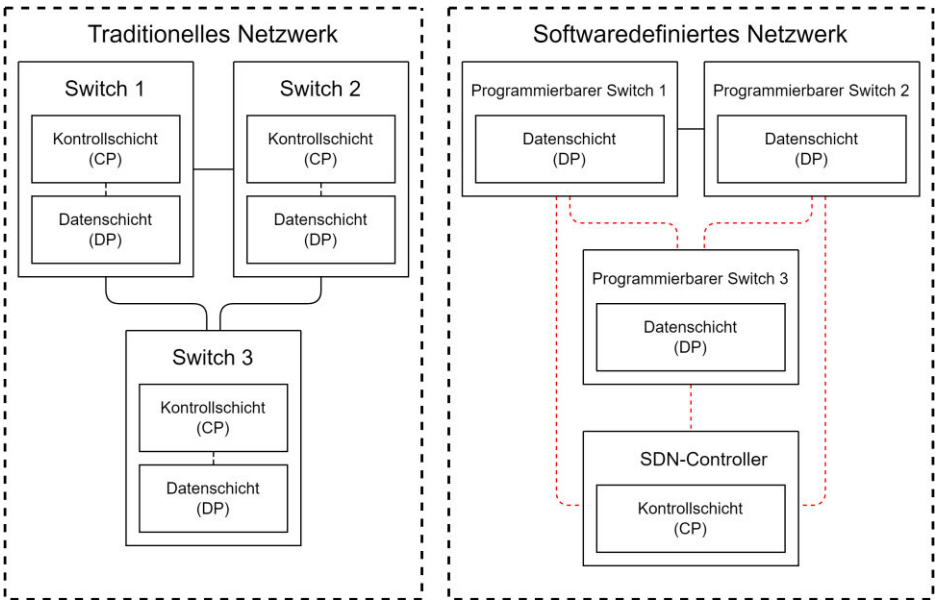


**Abbildung 1: SDN verglichen mit traditionellen Netzwerken, Eigene Abbildung, nach [5, S. 3].**

Die Kontroll-Logik wird nun auf einem zentralisierten commercial off-the-shelf (COTS) – Server ausgeführt. Dieser wird als SDN-Controller bezeichnet. Der SDN-Controller verwaltet den Datenfluss aller Netzwerkpakete. Dafür legt dieser Regeln fest, nach welchen die Pakete gefiltert oder weitergeleitet werden. [4, S. 4]

Mittels einer standardisierten API überträgt er die Kontroll-Informationen an die Switches, welche die Pakete entsprechend weiterleiten.

Vorteil ist hierbei, dass sich aufgrund der Programmierbarkeit des Netzwerks Konfigurationsänderungen sehr schnell umsetzen lassen. Dies ermöglicht ein flexibles Anpassen der Netzwerkkonfiguration, sollte dies beispielsweise aufgrund von geändertem Nutzerverhalten oder Lastanforderungen nötig sein. Zudem können Netzwerkservices schneller zum Netzwerk hinzugefügt werden.

Dies ist insbesondere für 5G von Bedeutung, da Netzwerkfunktionen größtenteils virtualisiert existieren und häufig zum Netz hinzugefügt oder entfernt werden. Da die Netzwerklogik von der darunterliegenden Hardware entkoppelt werden kann, sind zudem Änderungen an der physischen Infrastruktur der Netze einfacher und mit weniger Auswirkung auf aktive Applikationen umzusetzen. [6, S. 113]

Die Entkopplung von Kontroll- und Datenebene führt zudem zu einer Kostenreduktion für Mobilfunknetzbetreiber: sowohl hinsichtlich der Initialkosten, aufgrund von einfacherer COTS-Hardware, als auch hinsichtlich der Betriebskosten, aufgrund der einfacheren (Re)konfiguration. [7, S. 4,13]

## 1.2 Network Function Virtualisation (NFV)

In bisherigen Mobilfunkgenerationen wurden Netzwerkfunktionen (NF) des Kernnetzes weitestgehend als physische Netzwerkfunktionen (PNF) auf proprietärer Hardware bereitgestellt. Das bedeutet, dass Hersteller von NFs diese auf speziell dafür ausgewählter Hardware ausliefern, was den gleichzeitigen Einsatz von Produkten mehrerer Hersteller erschwert. Zudem muss beim Hinzufügen einer PNF diese in der Regel vor Ort installiert werden, da sie auf proprietärer Hardware ausgeliefert wird. [8] Dies erschwert Konfigurationsänderungen und die Skalierung des Netzes, besonders mit Hard- und Software von verschiedenen Herstellern.

In der fünften Mobilfunkgeneration werden deshalb NFs vorrangig auf virtuellen Maschinen (VM) bereitgestellt, welche cloudbasiert und auf beliebiger COTS-Hardware eingesetzt werden können. Eine solche NF wird als virtualisierte Netzwerkfunktion (VNF) bezeichnet.

Vorteil der Virtualisierung ist das vereinfachte Lifecycle-Management von Netzwerkfunktionen. Simpleres Instanziieren, Skalieren und Terminieren von NFs sowie schneller durchführbare Konfigurationsänderungen erhöhen die Flexibilität des Netzwerks. Diese Vorgänge sind zudem automatisierbar.

Des Weiteren reduziert die Verwendung von COTS-Hardware die Anzahl von verschiedenen Hardware-Modellen, welche in der Netzwerkinfrastruktur verwendet werden. Dies simplifiziert die physische Wartung und erhöht die Austauschbarkeit der Hardware. [9] Zudem wird die Effizienz der Ressourcennutzung erhöht und der benötigte Stromverbrauch gesenkt. Der reduzierte Stromverbrauch resultiert daher, dass bei Nicht-Gebrauch der Ressourcen diese kleiner skaliert werden und die Last gleichmäßig auf mehrere Server und Datencenter aufgeteilt werden kann. Im Gegensatz dazu können klassische PNFs nicht dynamisch hinzugefügt oder entfernt werden, wodurch diese auch bei geringer Auslastung weiterhin vergleichsweise viel Strom verbrauchen. Dies ist vor allem für Basisstationen in weniger bewohnten Gebieten von Bedeutung. [9]

Beispielsweise konnte in einer dreimonatigen Studie von Nokia und Telefónica festgestellt werden, dass der RAN-Teil (Radio Access Network) eines 5G Netzwerks bis zu 90% energieeffizienter pro Traffic Unit als in einem 4G Netzwerk sein kann. [10]

In den folgenden Unterkapiteln werden die Architektur, Use Cases und Ziele von NFV sowie das Konzept von VNF Packages vorgestellt.

### 1.2.1 Die NFV-Architektur

Vereinfacht lässt sich die Architektur von Network Function Virtualisation (NFV) mit drei Blöcken beschreiben (Siehe Abbildung 2):

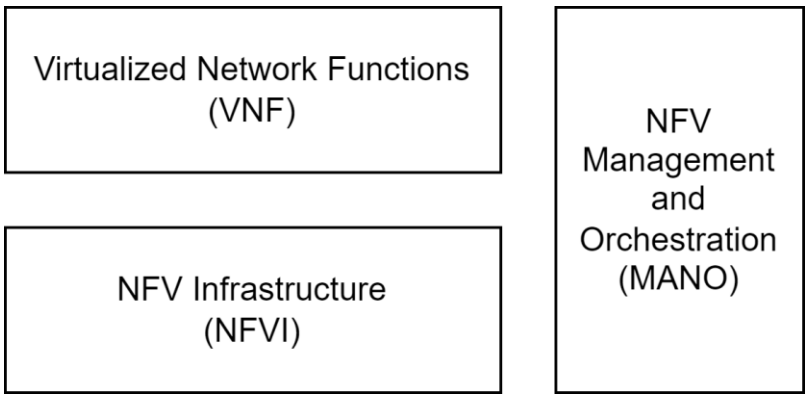


**Abbildung 2: NFV-Architektur, Eigene Abbildung, nach [11, S. 10], vereinfacht.**

Virtualisierte Netzwerkfunktionen (VNF) werden auf einer geteilten NFV-Infrastruktur (NFVI), welche eine Virtualisierungsmöglichkeit bereitstellt, ausgeführt.

Um den Leistungsbedarf zu analysieren, Netzwerkressourcen an VNFs zu verteilen und den Lebenszyklus der VNFs zu verwalten (Instanziieren, Skalieren, Terminieren, etc.), wird im Vergleich zu bisherigen Mobilfunkgenerationen eine weitere Netzwerkkomponente benötigt: NFV-MANO, welche in Kapitel 2 erläutert wird.

Die NFVI besteht aus physischen Rechenkernen, physischem Speicher und einem physischen Netzwerk. Dies umfasst die COTS-Serverhardware und sonstige Netzwerkkomponenten wie Router und Switches.

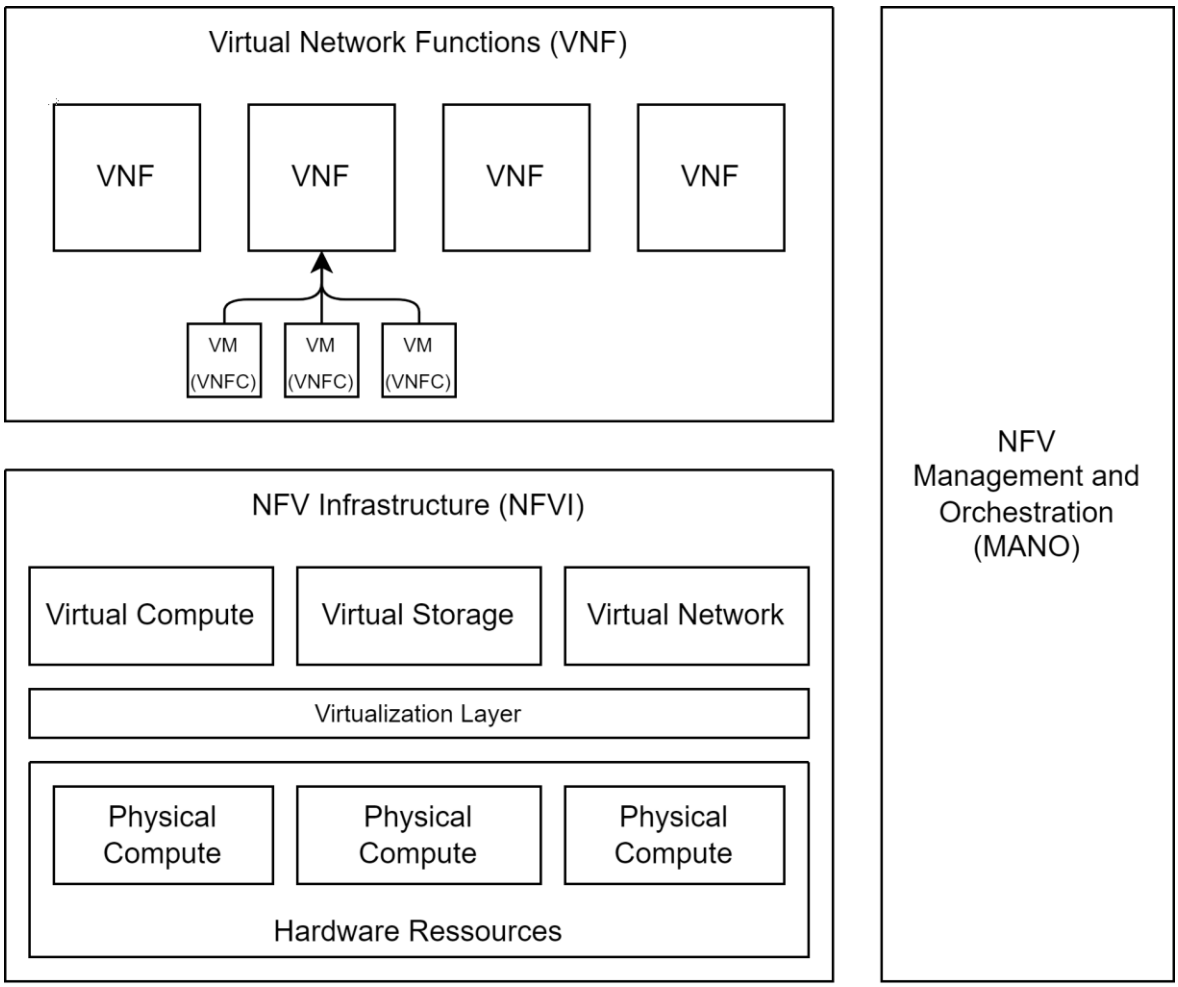


**Abbildung 3: NFV-Architektur, Eigene Abbildung, nach [11, S. 10], modifiziert.**

Eine Virtualisierungsschicht abstrahiert die Hardware, sodass simulierte, virtuelle Hardware als Ausführungsumgebung verwendet werden kann. Virtuelle Rechenkerne, virtueller Speicher und virtuelle Netzwerke bilden eine Infrastruktur, auf welcher virtuelle Maschinen ausgeführt werden. [11, S. 12]

Auf der NFV-Infrastruktur können virtuelle Netzwerkfunktionen ausgeführt werden. Eine VNF besteht meist aus mehreren VNF-Komponenten (VNFCs). Eine VNFC entspricht in der Regel genau einer virtuellen Maschine. [12, S. 12] Die VNFCs sind mittels eines virtuellen Netzwerks verbunden und arbeiten zusammen, um nach außen hin wie ein System zu wirken.

Aufgrund dieses Aufbaus ist ein Skalieren einer VNF einfach möglich. Es sind zwei Skalierungsmodi möglich. Beim horizontalen Skalieren können VNFCs hinzugefügt werden, um Leistung und Kapazität der VNF zu erhöhen. Dies wird als „scale out“ bezeichnet. Nach dem gleichen Prinzip können VNFCs entfernt werden, um die Leistung der VNF zu reduzieren und Ressourcen zu schonen. Dies wird als „scale in“ bezeichnet. [12, S. 21]

Im Gegensatz dazu werden beim vertikalen Skalieren bereits instanziierte Ressourcen rekonfiguriert, um Kapazität und Leistung von VNFs oder VNFCs durch Zuweisung von z. B. Speicher oder CPUs zu erhöhen oder zu senken. Dies wird als „scale up / scale down“ bezeichnet. Im aktuellen NFV-Standard wird automatisiertes, vertikales Skalieren noch nicht unterstützt, weswegen momentan ausschließlich horizontales Skalieren verwendet wird. [12, S. 21]

### 1.2.2 Ziele von NFV

Das Europäische Institut für Telekommunikationsnormen (ETSI) hat im Dokument „ETSI GS NFV 002“ [11] sechs High-Level Ziele für Network Function Virtualisation definiert. [11, S. 8]

1. Das erste Ziel des Virtualisierens von Netzwerkfunktionen ist die Kostenreduzierung im Vergleich zu bisherigen Hardware-Implementationen. Dafür wird COTS-Hardware als NFVI eingesetzt. Das gemeinsame Verwenden von Hardware zwischen mehreren VNFs und die verringerte Anzahl verschiedener Hardwarearchitekturen unterstützen dieses Hauptziel.
2. Ein weiteres Ziel stellt erhöhte Flexibilität im Lebenszyklus einer Netzwerkfunktion dar. VNFs können flexibel Ressourcen zugewiesen und entzogen werden. Dies erhöht die Skalierbarkeit der Netzwerkfunktion und entkoppelt die Funktionalität der NF von ihrem Standort. Die VNF kann in NFVI-Points-of-Presence (NFVI-PoP) ausgeführt werden. Ein NFVI-PoP ist ein physischer Ort, an welchem die benötigte COTS-Hardware installiert ist, zum Beispiel ein Datencenter eines Mobilfunknetzbetreibers, eines Cloudanbieters oder ein Serverraum eines Campusnetzbetreibers.
3. Agile Entwicklungsprozesse können unterstützt und die Frequenz von Release-Zyklen erhöht werden, da durch den servicebasierten Entwicklungsansatz Updates einfacher getestet und eingespielt werden können.
4. Durch Automation und zentrale Managementsysteme soll die Effizienz von Unternehmen und deren Produkten erhöht werden.
5. Da ungenutzte Hardware automatisiert abgeschaltet und die Rechenlast effektiv verteilt werden kann, kann zudem die Energienutzung reduziert werden.
6. Abschließend sollen standardisierte und offene Interfaces zwischen VNFs, NFVI und MANO gleichzeitig Wettbewerb und Flexibilität des Netzes erhöhen, da Elemente verschiedener Anbieter gleichzeitig verwendet werden können. So können die Zusammenarbeit von Netzwerkprodukten mehrerer Hersteller und ein einfacher Umstieg von VNFs eines Herstellers hin zu einem anderen ermöglicht werden. Dies verhindert zudem, dass Abhängigkeiten von einem Hersteller entstehen können.

### 1.2.3 Use Cases von NFV

Im Dokument „ETSI GR NFV 001“ [13] definiert ETSI 18 Use Cases von NFV. Diese bauen auf den vorgestellten Hauptzielen auf und konkretisieren diese anhand von Beispielen. Sie werden in diesem Kapitel zusammengefasst.

#### *1.2.3.1 Network Functions Virtualisation Infrastructure as a Service (NFVIaaS)*

Nur wenige Service Provider besitzen die Kapazitäten, um physische Infrastruktur global zu betreiben und instand zu halten, obwohl ihr Geschäftsmodell von globaler Nutzung profitieren kann. Werden beispielsweise Multimediaanwendungen, welche global verfügbar sein sollen, in mehreren Datencentern global verteilt bereitgestellt, resultiert dies für den Endnutzer in reduzierten Latenzen. Um nicht weltweit Serverräume besitzen und betreuen zu müssen, kann NFVIaaS genutzt werden.

Durch die Möglichkeit, VNFs in einer NFVI eines anderen Service Providers laufen zu lassen, kann ein Service Provider angemietete Hardware nutzen und seine Dienste effizient anbieten. Rechenleistung, Speicherplatz und das physische Netzwerk können als Service genutzt und angeboten werden. [13, S. 15]

#### *1.2.3.2 Virtual Network Function as a Service (VNFaaS)*

Besitzt ein Kunde nicht die Kapazitäten, um eine VNF selbst zu entwickeln und / oder zu unterhalten, kann die Funktion von einem Service Provider entwickelt, verwaltet und auf fremder Infrastruktur ausgeführt werden.

Der Kunde hat hierbei weder Konfigurationszugriff auf VNF noch NFVI. Beide werden vom Service Provider betriebsbereit bereitgestellt, konfiguriert und verwaltet. Der Kunde kann die Instanziierung einer VNF veranlassen. Für die Übermittlung dieses Befehls wird der Os-Ma-Nfvo - Referenzpunkt in der MANO-Architektur (wird in Kapitel 2.1.4.1 erläutert) verwendet. Nach Instanziierung kann die VNF als Service vom Kunden genutzt werden. [13, S. 22]

#### *1.2.3.3 Virtual Network Platform as a Service (VNPaaS)*

Nicht nur das Bereitstellen und Entwickeln einer einzigen Funktion (VNFaaS) oder einer NFVI (NFVIaaS), sondern auch eines kompletten, virtuellen Netzwerks ist in Form von VNPaaS möglich. Hier wird ein komplettes virtuelles Netzwerk einem Kunden bereitgestellt.

Kunden können bei Bedarf eigene Netzwerkdienste im bereitgestellten virtuellen Netzwerk in Betrieb nehmen, konfigurieren und verwalten. Dies geschieht im Rahmen der Nutzungsbedingungen des Operators, welcher das virtuelle Netzwerk bereitstellt. Dem Kunden stehen Verwaltungsmöglichkeiten zu, jedoch muss die Serverhardware nicht mehr physisch bei ihm stehen. [13, S. 29]

#### *1.2.3.4 VNF Forwarding Graphs (VNFFG)*

Ein Network Function Forwarding Graph (NFFG) definiert die Sequenz von Netzwerkfunktionen, welche Pakete nacheinander passieren. Ein VNFFG stellt die logische Verbindung von VNFs dar. Diese Verbindungen werden benötigt, um komplexe Netzwerkservices (NS) bereitstellen zu können.

Die Virtualisierung des NFFGs führt zu erhöhter Effizienz durch gleichmäßigere Ressourcenauslastung, erhöhter Flexibilität durch einfachere, softwarebasierte Netzwerkänderungen und einer Verringerung der Komplexität von Installationen, was ein schnelleres Setup erlaubt. [13, S. 32]

#### *1.2.3.5 NS Offered by Multiple Administrative Domains*

Mehrere Netzwerkservices (NS) können über einen Higher-Level-NS zu einem Ende-zu-Ende Service zusammengefasst und an verschiedenen physischen Standorten Kunden bereitgestellt werden.

Einerseits kann dieser Service dabei in mehreren eigenen Datencentern des Netzwerkbetreibers ausgeführt werden. Anderseits ist es möglich, sollte die benötigte Kapazität für die Anfrage die tatsächliche Ressourcenkapazität des Providers übersteigen, dass ein weiterer Provider hinzugezogen werden kann, der seine Ressourcen zur Verfügung stellt. Dessen NFV Orchestrator (NFVO) operiert dem NFVO des primären Netzwerkanbieters untergeordnet.

Die NFVOs der einzelnen Standorte/Domains werden dabei mithilfe eines übergeordneten Umbrella NFVOs gesteuert. Eine Veranschaulichung dessen wird in Kapitel 2.1.5 „Einsatz mehrerer Orchestratoren“ näher erläutert. [13, S. 38]

#### *1.2.3.6 VNF Composition Across Multiple Administrative Domains*

Gleichermaßen, wie es wie in 1.2.3.5 für Netzwerkservices beschrieben ist, besteht die Möglichkeit, eine VNF über mehrere administrative Domains hinweg anzubieten. Dazu werden die in 1.2.3.4 beschriebenen Forwarding Graphs genutzt, welche die VNF Komponenten über mehrere administrative Domains hinweg zu einer funktionsfähigen Netzwerkfunktion vernetzen. Die zweite Domain kann dabei ebenso einem weiteren Provider gehören. [13, S. 40]

#### *1.2.3.7 Network Slicing*

Beim Netzwerk-Slicing werden mehrere logische Netzwerke auf einer geteilten physischen Infrastruktur ausgeführt. Endgeräte verbinden sich mit der gleichen Provider-Infrastruktur, jedoch nutzen diese dafür verschiedene VNF oder PNF-Instanzen. Netzwerk Slicing wird als eine der Hauptneuerungen im 5G Netz erachtet. Slicing wird erst durch die Verwendung von SDN und NFV ermöglicht.

Mit Slicing können Netzwerkkonfigurationen für verschiedene Anwendungszwecke erstellt und auf der gleichen Hardware-Infrastruktur eingesetzt werden. Beispielsweise hat ein public safety-Slice für Polizeikommunikation andere Netzwerkvoraussetzungen (keinesfalls Verbindungsabbrüche, Latenzen < 1ms, sichere Kommunikation nötig, Downloadraten zweitrangig) als ein Multimedia-Slice für Videostreaming (maximale Datenübertra-

gungsrate, Latenzen <1ms nicht notwendig, kurze Verbindungsabbrüche dank Buffer verkraftbar). Ein Nutzergerät kann gleichzeitig auf bis zu 8 Slices zugreifen. [14, S. 197]

Die Virtualisierung von Netzwerkfunktionen erlaubt hierbei, dass Ressourcen geteilt, automatisch Slices zugewiesen, automatisch skaliert und ausgerollt werden können, jedoch weiterhin ihre eigenen Management-Möglichkeiten behalten. [13, S. 43]

#### *1.2.3.8 Virtualisation of Mobile Core Network and IMS*

Durch die Verwendung und Bündelung von COTS-Hardware in NFVI-Points-of-Presence (NFVI-PoP, z. B. ein physisches Datencenter eines Mobilfunkanbieters), reduzieren sich die Gesamtkosten (Total Cost of Ownership, TCO) für die Mobilfunkanbieter (Mobile Network Operator, MNO).

Daraus ergeben sich folgende Vorteile: [13, S. 48]

1. Durch die flexible und automatische Ressourcenzuweisung von NFV wird die Effizienz des Kernnetzes erhöht.
2. Die Möglichkeit der dynamischen, automatischen Rekonfiguration des Netzwerks führt zu besserer Erreichbarkeit und Resilienz des Kernnetzes.
3. Die Kapazität jeder Netzwerkfunktion lässt sich dynamisch an die Netzwerkauslastung anpassen. Somit wird die Skalierbarkeit des Kernnetzes erhöht.
4. Durch dynamische Rekonfiguration der Netzwerktopologie können neue Netzwerkservices einfach integriert werden.

#### *1.2.3.9 Virtualisation of Mobile Base Station*

Die Anzahl der gleichzeitig aktiven Endgeräte wird in 5G im Vergleich zu bisherigen Netzwerkgenerationen stark zunehmen. In Mobilfunknetzen nehmen Radio Access Network (RAN) – Basisstationen den größten Teil der Gesamtkosten und des Stromverbrauchs ein. In 5G werden virtualisierbare Bestandteile der RAN-Knoten als VNF auf COTS-Hardware bereitgestellt. Dies verringert die physische Größe der Basisstation und den Energieverbrauch und vereinfacht die Lastverteilung auf Hardwareressourcen.

Wenn sich viele Geräte mit einer Basisstation verbinden und damit mehr Netzwerkkapazität notwendig ist, kann durch die Instanziierung neuer VMs die Basisstation skaliert werden.

Wird die Basisstation jedoch weniger stark ausgelastet, kann sie im Gegenzug durch Entfernen von VMs Energie sparen oder die Hardwareressourcen anderweitig einsetzen. [13, S. 52]

#### *1.2.3.10 Virtualisation of the Home Environment*

In privaten Heimnetzwerken sind mehrere Hardwarekomponenten eingebunden, welche sich virtualisieren lassen. Diese umfassen sowohl das Residental Gateway (RGW), z. B.

ein WLAN-Router, als auch netzwerkbasierte Set-top Boxen (STB), z. B. ein Amazon Fire TV oder Apple TV. [15]

Eine Virtualisierung würde für Verbraucher die Hardwarekosten für RGW und (mehrere) STBs reduzieren. Für Hersteller dieser Komponenten werden die Unterhaltskosten verringert sowie die Ferndiagnose bei Fehlern erleichtert. Außerdem ist bei der Einführung neuer Dienste weniger auf Hardwareeinschränkungen durch veraltete Verbrauchergeräte zu achten.

Beide Komponenten lassen sich virtualisiert (als vRGW und vSTB) über die NFV Cloud des Providers anbieten. Beim Endnutzer würde nur ein COTS Layer 2 Netzwerkgerät als Bridge verbleiben. [13, S. 55]

#### *1.2.3.11 Virtual Content Delivery Network (vCDN) – Fulfilment*

Die Bereitstellung von Medien, besonders von Video, stellt für Netzwerkanbieter aufgrund steigender Auflösungen und Bildraten, Virtual Reality und Echtzeit-Videokonferenzen eine der größten Herausforderungen dar.

Eine Virtualisierung und Integration der Content Delivery Networks (CDN) in Betreibernetzwerke würde die Distanz zwischen Endnutzer und Rechen- und Speichernetzwerkknoten verringern. Dies würde zu verringerter Netzwerkauslastung führen.

Zudem musste in bisherigen Netzwerkgenerationen die Kapazität des CDN anhand der benötigten Maximalleistung (Abende an Wochenenden) dimensioniert werden. Virtualisiert könnte außerhalb der Hauptnutzungszeiten die Kapazität des Netzwerks automatisch reduziert werden, um Strom zu sparen.

Bei unvorhergesehenen Spitzenauslastungen (z. B. Berichterstattung bei Katastrophen) könnte die Kapazität des CDN automatisch durch Hinzufügen neuer VMs hochskaliert werden. [13, S. 62]

#### *1.2.3.12 Fixed Access Network Functions Virtualisation*

Netzwerkzugangsknoten stellen oft die Hauptkostenquelle eines Netzwerks dar. Für hohe Bandbreiten müssen diese oft in großer Zahl an Straßen und auf oder in Gebäuden untergebracht werden.

Um Kosten zu reduzieren, können komplexe Berechnungen zentralisiert im Datencenter des Netzwerkbetreibers durchgeführt werden. In Folge dessen kann simpleres und kostengünstigeres Equipment als Zugangsknoten verbaut werden. Zudem wird der Energieverbrauch des Zugangsknotens reduziert. [13, S. 66]

#### *1.2.3.13 Virtualisation of Internet of Things (IoT)*

IoT wurde von der Next Generation Mobile Network Alliance als eine der Hauptmotivationen für 5G festgestellt. IoT Anwendungsfälle umfassen beispielsweise Smart City, Echtzeitsteuerung entfernter Maschinen und Smart Home Anwendungen.

Da IoT eine große Anzahl verschiedener Services und Applikationen verschiedener Komplexität und Anforderungen umfasst, ist für eine effektive Realisierung und Skalierung ein Virtualisieren der IoT-Services mittels NFV unumgänglich. Services können so effizient in Operations Support Systems und Business Support Systems (OSS/BSS, wird in Kapitel 2.1.3.1 erläutert) eingebunden und flexibel verwaltet werden. [13, S. 73]

#### *1.2.3.14 Crypto as a Service (CaaS)*

Sicherheitsrelevante Netzwerkfunktionen wie Firewalls, Intrusion Prevention- und Detection Systeme (IPS / IDS) und Load Balancer werden von NFV virtualisiert, stoßen dabei jedoch auf Probleme mit Schlüsselmanagement, Leistung und Skalierbarkeit.

Die Bereitstellung von kryptographisch wichtigen Funktionen als virtualisierte Netzwerkfunktion, welche als Service von Firewalls, IPS / IDS, etc. genutzt werden kann, löst diese Probleme durch zentralisiertes Schlüsselmanagement, schnelle Schlüsselberechnungen und einfache Handhabung von verschlüsselten Daten. [13, S. 77]

#### *1.2.3.15 Security as a Service (SecaaS)*

Es wird angenommen, dass Anzahl und Komplexität von Angriffen in der Zukunft weiter zunehmen werden. Dies zwingt Unternehmen konstant dazu, ihre Cybersicherheit zu aktualisieren, was mit hohen Kosten und Aufwand einhergeht.

Eine Möglichkeit, um weniger eigene Personalressourcen für konstante Sicherheitsupdates bereitstellen zu müssen, ist die Bereitstellung von Netzwerksicherheit als virtual Network Security Function (vNSF). Unternehmen könnten sich Sicherheits-Services als VNF von darauf spezialisierten Anbietern bereitstellen lassen. Somit müssten sich diese nicht mehr selbst um konstantes Aktualisieren der Sicherheit kümmern, was potentiell Kosten einspart und Sicherheitslücken reduziert. [13, S. 81]

#### *1.2.3.16 Rapid Service Deployment*

Schnelles Ausrollen von Netzwerkservices ist eines der Kernziele von NFV. Dieser Anwendungsfall ist somit grundlegend und wird in vielen anderen Situationen angewandt.

Werden Services als VNF auf einer NFVI verteilt, wird die dafür benötigte Zeit im Vergleich zu einer herkömmlichen, physischen Installation stark reduziert. Zudem kann der Vorgang automatisch ausgelöst werden. [13, S. 85]

#### *1.2.3.17 Devops/CI/CD*

Durch den Einsatz von VNFs statt PNFs können Entwicklungsprozesse in Kombination mit dem Einsatz agiler Entwicklungsmethoden im Vergleich zu traditionellen Methoden stark beschleunigt werden und ermöglichen so schnellere Release-Zyklen. [13, S. 87]

#### *1.2.3.18 A/B testing*

Aufgrund der stark verkürzten Release-Zyklen ist es möglich, die Performance verschiedener Versionen und potentieller Upgrades gegeneinander zu testen und festzustellen, welche Version der Software besser ist. Die leistungsfähigste neuer Softwareversionen oder VNFs kommt somit schneller in den produktiven Einsatz. [13, S. 88]

### 1.2.4 VNF Packages & VNF Deskriptoren (VNFD)

Das Konfigurieren der VNF nach Informationen des VNF Deskriptors, sodass Operationen des Lifecycle Managements verfügbar sind und die VNF lauffähig ist, wird auch als Onboarding bezeichnet. Damit das Onboarding und das Lifecycle Management von VNFs auf eine standardisierte Art automatisiert werden kann und VNFs mit allen standardisiert entwickelten MANO-Implementationen kompatibel sind, müssen diese auch auf eine standardisierte Art von Herstellern ausgeliefert werden.

Dies geschieht in sogenannten VNF Packages. Dabei handelt es sich um TOSCA YAML Cloud Service Archive, welche im ZIP-Dateiformat gepackt sind. Für den Einsatz in 5G werden diese mit zusätzlichen Funktionen für Integritäts- und Authentizitätschecks ergänzt. [16, S. 15-17]

Ein VNF Package wird immer vollständig von einem Hersteller ausgeliefert, ist schreibgeschützt und digital signiert.

Ein VNF Package besteht aus mindestens drei Teilen (siehe Abbildung 4).

1. Die Manifest-Datei des Packages wird für Integritäts- und Authentizitätsprüfung genutzt.
2. Software Image(s) sind der auszuführende Teil bei der Verwendung der VNF.
3. Das VNF Package beinhaltet in Form des VNF Descriptors (VNFD) Metadaten sowie weitere Informationen für das Onboarding und Management der VNF.

Der Deskriptor enthält genügend Informationen über Attribute und Voraussetzungen, damit die VNF vollständig instanziiert und verwaltet werden kann. [17, S. 10] In der Virtual Deployment Unit (VDU) des Deskriptors sind allgemeine Daten über die Netzwerkfunktion angegeben. Dies umfasst die Metadaten der VNF, die benötigte Rechenleistung, den erforderlichen Speicherplatz und interne Netzwerkverbindungen. In der Software Image Description sind Informationen wie eine Liste von unterstützten Lebenszyklus-Operationen und das Verhalten bei diesen (z. B. Verhalten bei Skalierung) enthalten.

Des Weiteren sind im VNF Package mehrere Deployment Flavours definiert. Ein Flavour ist eine Konfigurationsvariante beziehungsweise ein Konfigurationsprofil der VNF, abhängig von der Netzwerkinfrastruktur, auf welcher die virtuelle Netzwerkfunktion laufen soll. So kann beispielsweise ein anderes Instanziierungs- oder Skalierungsverhalten der VNF bei einem kleinen Campusnetz im Vergleich zu einem deutschlandweiten Mobilfunknetz ausgelöst werden. [16, S. 4]

Zuletzt können dem Package weitere Dateien wie Skripts oder sonstige, herstellerspezifische Dateien angefügt werden.

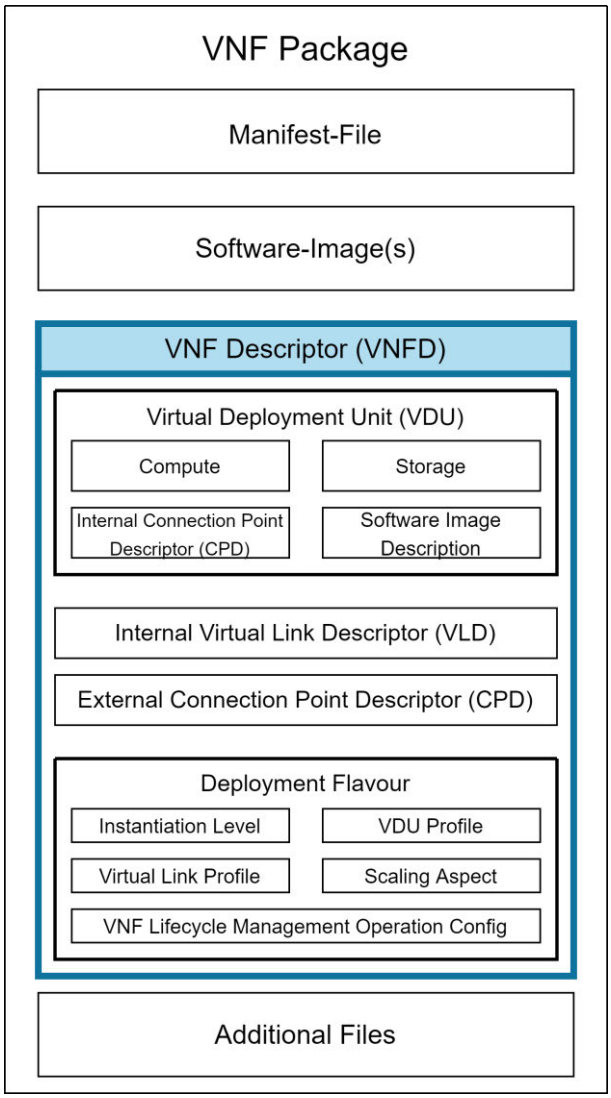


**Abbildung 4: VNF-Package Aufbau, Eigene Abbildung, nach [16, S. 4 & S. 16].**

Nach einer Betrachtung von Aufbau und Use Cases von NFV wird deutlich, wie wichtig ein dynamisches Management und die Orchestrierung von virtuellen Netzwerkfunktionen für NFV ist. Im folgenden Kapitel wird daher die MANO-Komponente des NFV-Systems näher vorgestellt.

# 2 Management & Orchestration (NFV-MANO)

Wie aus dem vorangegangenen Kapitel deutlich wird, ist für Network Function Virtualization (NFV) eine klar definierte Management- und Orchestrierungskomponente, welche virtuellen Netzwerkfunktionen (VNF) die nötigen NFV Infrastructure (NFVI) -Ressourcen zuweist und den Lebenszyklus von VNFs verwaltet, unumgänglich.

Aus diesem Grund veröffentlichte ETSI Spezifikationen, welche Aufbau und Funktionsweise von NFV-MANO in der Dokumentenreihe „NFV-MAN“ definieren und beschreiben.

## 2.1 Architektur und Funktionsweise von NFV-MANO

Die NFV-MANO-Architektur besteht aus drei Hauptkomponenten:

- NFV Orchestrator (NFVO),
- VNF Manager (VNFM) und
- Virtualized Infrastructure Manager (VIM).

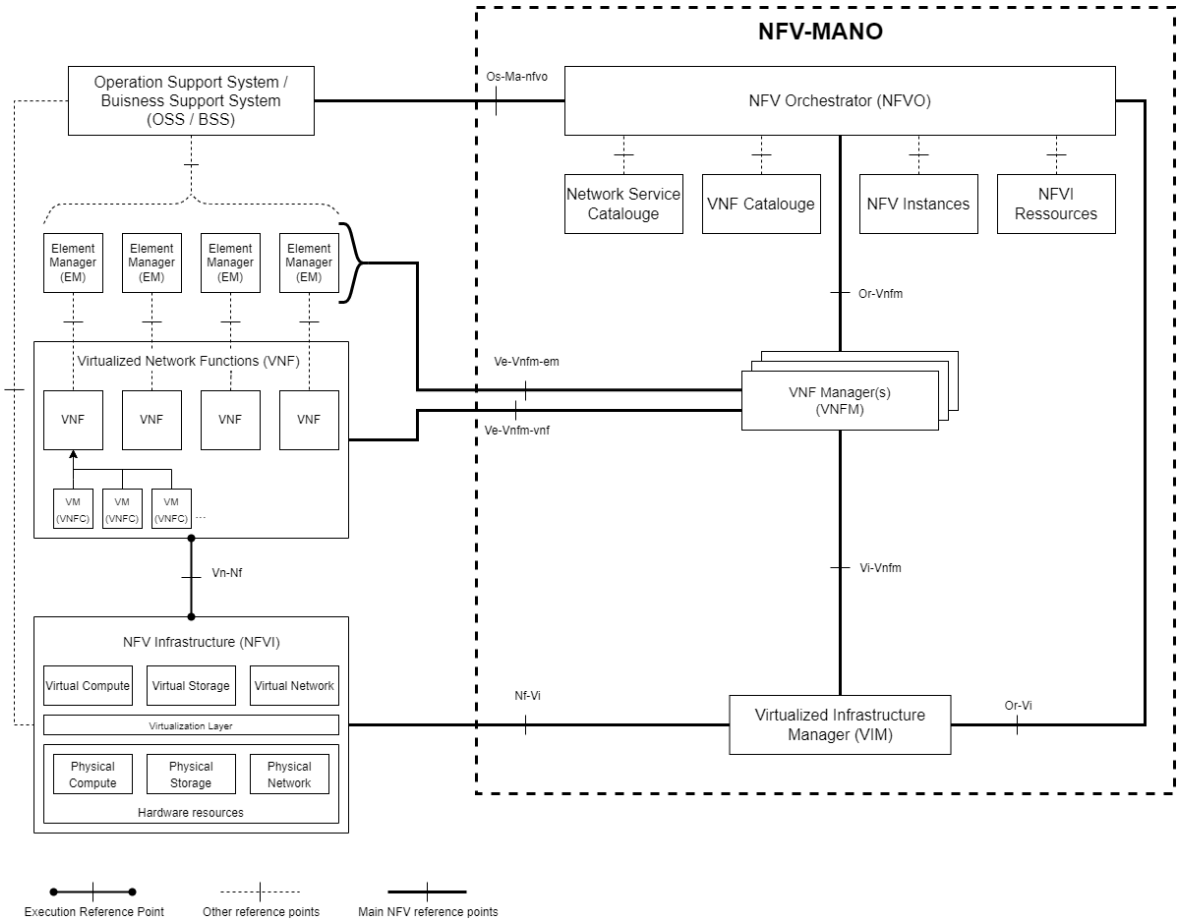


**Abbildung 5: ETSI NFV-MANO Architektur, Eigene Abbildung, nach [11, S. 10] und [18, S. 24]**

Die einzelnen Komponenten der Abbildung werden in den folgenden Unterkapiteln näher erläutert.

Der NFVO besitzt Verbindungen zu vier Datenbanken, mit deren Hilfe er einen Überblick über verfügbare Ressourcen, Services, etc. besitzt. Andere Komponenten können Dienste des Orchestrators nutzen, welche mit Informationen der Datenbanken in Verbindung stehen, müssen jedoch dafür eine entsprechende Serviceanfrage an den NFVO stellen. Der NFVO gewährt oder verweigert diese. [18, S. 25]

Verbunden sind die internen MANO-Komponenten (NFVO, VNFM, VIM) untereinander als auch extern zu NFV-MANO-fremden Komponenten mittels Referenzpunkten. Ein Referenzpunkt ist eine Kommunikationsverbindung zwischen zwei funktionalen Blöcken, über welche Funktionen angeboten und konsumiert werden. Eine präzise Definition der Referenzpunkte ist wichtig, damit austauschbare, funktionale Blöcke verschiedener Hersteller miteinander kommunizieren können.

### 2.1.1 Interne Komponenten

In diesem Kapitel werden die Funktionen der MANO-internen Komponenten vorgestellt.

#### *2.1.1.1 NFV Orchestrator (NFVO)*

Der NFV Orchestrator besitzt einen vollständigen Überblick aller verfügbaren Netzwerkservices (NS) und Ressourcen. Er hat zwei Hauptaufgaben: Die Orchestrierung von NS und die Orchestrierung von Ressourcen (über mehrere VIMs hinweg).

Die Orchestrierung von NS umfasst mehrere Unteraufgaben: [18, S. 24-25]

Erstens ist der NFVO ist für das Lifecycle-Management der NS verantwortlich. Dies beinhaltet einerseits die Instanziierung und das Aktualisieren von Netzwerkservices. Dabei werden mehrere VNFs zu einem funktionalen Service zusammengefasst und die Verbindung zwischen diesen zu einem oder mehreren VNF Forwarding Graphs (VNFFG) gebündelt.

Zudem können Netzwerkservices und Netzwerkfunktionen von ihm skaliert werden, wofür der Orchestrator Services von VIM und VNF Manager nutzt. Außerdem liegt das Aktualisieren und die Performanceüberwachung von Netzwerkservices im Aufgabenbereich des NFV Orchestrators.

Da nur der NFVO eine komplette Übersicht über Ressourcen und VNFs besitzt, müssen die VNFMs für die Instanziierung / Skalierung von VNFs eine Anfrage an den NFVO stellen. Der NFVO prüft und autorisiert die geplante Ressourcennutzung.

Außerdem verwaltet der NFV Orchestrator NS Deployment Templates und VNF Packages.

Abschließend kann der NFVO VNF Manager instanziieren.

Seine zweite Hauptaufgabe, die Orchestrierung von Ressourcen, wird für Services benötigt, die sich über die NFVI mehrerer VIMs erstecken. Manche Netzwerkservices umfassen Ressourcen in mehreren Datencentern eines Netzes (NFVI-PoP). Da keine andere Einheit im MANO-Framework einen solch großen Überblick über die Ressourcen besitzt, werden diese Aufgaben vom NFVO orchestriert. Dafür verwendet er die „NFVI-Resources“ - Datenbank (Kapitel 2.1.1.4.4). Außerdem erhebt der NFVO Daten über die Nutzung der Ressourcen durch VNFs und nutzt diese Daten für Lastverteilung. [18, S. 25]

#### *2.1.1.2 VNF Manager (VNFM)*

Während der NFVO verantwortlich für das Lifecycle Management von kompletten Netzwerkservices ist, verwaltet ein VNF Manager den Lebenszyklus von einzelnen virtualisierten Netzwerkfunktionen.

Die Aufgaben des VNF Managers umfassen die Instanziierung, Updates und Upgrades, Konfigurationsänderungen, Skalierung, Fehlerbehebung und Terminierung der zugewiesenen VNF. Um zu wissen, wie diese Funktionen korrekt ausgeführt werden, greift der VNFM auf Informationen aus dem VNF Deskriptor (VNFD, siehe Kapitel 1.2.4) des VNF Packages zurück.

Die meisten dieser Funktionen sind generisch und lassen sich für mehrere VNFs anwenden. Diese müssen nicht näher spezifiziert werden. Sind jedoch im VNF Package spezielle Anweisungen für das Lifecycle Management definiert, so werden diese verwendet. [18, S. 26]

#### *2.1.1.3 Virtualized Infrastructure Manager (VIM)*

Der Virtualized Infrastructure Manager verwaltet die NFVI Ressourcen, welche ihm zugeteilt wurden. Er kann entweder nur einen Teil eines NFVI-PoPs, einen kompletten PoP oder mehrere PoPs verwalten. Die Implementation vom VIM wird im ETSI NFV-MANO Framework nicht betrachtet. Als VIM werden häufig beispielsweise OpenStack oder VMware verwendet.

Interfaces / Services des VIMs, welche von anderen Komponenten anfragbar sind, sind jedoch Bestandteil des ETSI NFV-MANO Frameworks. Zu diesen Services gehört: [18, S. 27]

1. das Management und die Verbindung von physischen und virtuellen Ressourcen
2. das Optimieren der Auslastung der physischen Ressourcen
3. das Erstellen und Verwalten von Subnetzen und virtuellen Verbindungen zwischen VNFs
4. das Verwalten von Software-Images
5. das Verwalten eines Ressourcenkatalogs, welche noch verfügbar sind.

#### *2.1.1.4 Repositories / Datenbanken*

Repositories sind Datenbanken, welche von den drei internen Komponenten für ihre Dienste genutzt werden können. Die Repositories sind nur über einen Referenzpunkt mit dem NFVO verbunden, sodass die Kommunikation von anderen Komponenten mit den Repositories nur nach genehmigter Anfrage an den NFVO erfolgen kann.

Relevante Datenbanken sind: [18, S. 28]

1. Das NS Catalogue – Repository. Dies ist eine Liste sämtlicher zur Instanziierung verfügbaren Netzwerkservices und wird zur Erstellung von Deployment Templates genutzt. Darin gespeicherte Informationen umfassen:
    - Network Service Descriptor (NSD)
    - Virtual Link Descriptor (VLD)
    - VNF Forwarding Graph Descriptor (VNFFGD).
2. Das VNF Catalogue – Repository. Dies ist eine Liste sämtlicher zur Instanziierung verfügbaren VNF Packages. NFVO und VNFM können in dieser nach VNF Deskriptoren suchen.
3. Das NFV Instances - Repository. Dies ist eine Liste, in welcher sämtliche momentan instanziierten VNFs und NS aufgeführt sind. Die Einträge werden von NFVO (NS-Einträge) und VNFM (VNF-Einträge) stetig aktualisiert.
4. Das NFVI Resources - Repository. Dies ist eine Liste, in welcher sämtliche verfügbaren, reservierten und zugewiesenen Ressourcen gespeichert sind. Sie wird von dem / den VIM(s) stetig aktualisiert.

### 2.1.2 Interne Referenzpunkte

In diesem Kapitel werden die Funktionen der MANO-internen Referenzpunkte vorgestellt. Sie verbinden funktionale Blöcke innerhalb des NFV-MANO Systems.

#### *2.1.2.1 Or-Vi*

Dieser Referenzpunkt ist für die Kommunikation zwischen NFV Orchestrator und Virtualized Infrastructure Manager zuständig. Über diesen kann der NFVO die Infrastruktur-Ressourcen reservieren, freigeben, updaten und zuweisen. Des Weiteren können Software Images aus dem entsprechenden Package hinzugefügt, geupdatet oder entfernt werden. Zuletzt werden Informationen bezüglich Konfigurationen und Ressourcenauslastung an den Orchestrator mitgeteilt. [18, S. 35] [19, S. 23]

#### *2.1.2.2 Vi-Vnfm*

Der Vi-Vnfm Referenzpunkt ist für den Austausch zwischen VNF Manager und Virtualized Infrastructure Manager zuständig. Über diesen kann der VNFM Informationen über die momentane Ressourcenauslastung anfragen sowie Ressourcen anfordern (nach vorheriger Autorisierung durch den Orchestrator) und freigeben. [18, S. 35] [20, S. 18]

#### *2.1.2.3 Or-Vnfm*

Dieser Referenzpunkt beschreibt die Kommunikation zwischen NFV Orchestrator und VNF Manager. Über diesen werden von VNFM Anfragen zur Ressourcenzuweisung- und freigabe an den Orchestrator gestellt, von diesem bearbeitet und beantwortet. Zudem kann der NFVO über diesen Referenzpunkt virtuelle Netzwerkfunktionen instanziieren, updaten, skalieren und terminieren lassen. Treten Ereignisse oder andere Informationen der VNF auf, welche für den gesamten Netzwerkservice relevant sind, so werden diese auch über diesen Referenzpunkt an den Orchestrator übermittelt. [18, S. 35] [21, S. 21]

### 2.1.3 Externe Komponenten

In diesem Kapitel werden die Funktionen der MANO-externen Komponenten vorgestellt. Die Implementation dieser ist nicht Bestandteil von ETSI NFV-MANO. Da sie jedoch mit den MANO-Komponenten interagieren, sind sie in der Übersicht der ETSI-Architektur enthalten.

#### *2.1.3.1 Operations Support System / Business Support System (OSS/BSS)*

Im traditionellen Kontext werden sämtliche Systeme, welche einen Service Provider in seinem Tagesgeschäft unterstützen, als Operations Support Systems (OSS) zusammengefasst. [22, S. 267] Im heutigen Managementkontext ist dies präziser definiert und in OSS und BSS unterteilt. Um Verwechselungen mit dem OSS-Oberbegriff zu vermeiden, wird das OSS hierbei auch als „service OSS“ bezeichnet. [22, S. 274] OSS/BSS umfasst alle Systeme, Funktionen und Applikationen, welche ein Provider verwendet, um sein Geschäft zu betreiben.

Als Business Support System (BSS) werden dabei alle Funktionen zusammengefasst, welche kundenbezogen eingesetzt werden. Dazu zählen beispielsweise Abrechnungsfunktionen für Zahlungsverwaltungen, Rabatte und Rechnungen, das Customer-Relationship-Management mit vertragsrelevanten Funktionen sowie Marketingfunktionen. [22, S. 273]

Als service OSS werden alle Funktionen zusammengefasst, die Netzwerkservice-orientiert eingesetzt werden. Dies umfasst Funktionen, welche das Netzwerk überwachen, kontrollieren, analysieren und verwalten. Hierbei zählte in bisherigen Mobilfunkgenerationen unter anderem das Management von Netzwerkfunktionen. Dafür stand die OSS-Komponente mit jeder Netzwerkfunktion direkt in Verbindung. Da dieser Ansatz für die dynamischen Änderungen in 5G durch NFV jedoch zu unflexibel ist und die Implementierung der Interfaces zwischen VNF und OSS proprietär sein würde, wurde in 5G diese Aufgabe durch das MANO-Framework und seine offenen Interfaces übernommen. [22, S. 274]

Im NFV-MANO Framework ist die Definition von OSS/BSS weitgreifender gewählt: Hier werden unter den funktionellen Block „OSS/BSS“ sämtliche Funktionen gefasst, welche

nicht in anderen Blöcken im Framework enthalten sind, jedoch mit diesen interagieren. Dadurch wird ermöglicht, dass zusätzliche Funktionen durch OSS/BSS hinzugefügt und bereitgestellt werden können, welche in einer spezifischen NFV-MANO Implementation nicht enthalten sind. [18, S. 29]

#### *2.1.3.2 Element Manager (EM)*

Der Element Manager ist eine externe Komponente, welche nicht NFV-MANO-spezifisch ist. Sie wird auch als Element Management System (EMS) bezeichnet. Die Aufgabe des EM im MANO-Framework ist das FCAPS Management einer VNF. [18, S. 28]

FCAPS ist das Fault-, Configuration-, Accounting-, Performance- und Securitymanagement einer virtuellen Netzwerkfunktion und wurde von der International Organization for Standardization (ISO) im Dokument „ITU-T M.3400“ definiert. [23] Es wird auch als OSI/ISO Network Management Model bezeichnet.

#### *2.1.3.3 Network Functions Virtualisation Infrastructure (NFVI)*

Die NFVI umfasst im NFV-MANO Framework sämtliche (physische und virtuelle) Hardware des Netzwerks. [18, S. 28]

### 2.1.4 Externe Referenzpunkte

In diesem Kapitel werden die Funktionen der MANO-externen Referenzpunkte vorgestellt. Im Gegensatz zu den externen Komponenten sind die externen Referenzpunkte noch Bestandteil von ETSI NFV-MANO.

#### *2.1.4.1 Os-Ma-nfvo*

Dieser Referenzpunkt ist für den Informationsaustausch zwischen OSS/BSS und NFV Orchestrator zuständig. Über ihn kann die Instanziierung, das Updaten, das Skalieren und das Terminieren von Netzwerkfunktionen angefragt werden.

Zudem müssen Anfragen der beiden Support-Systeme, welche den Lebenszyklus einer VNF betreffen, über dieses Interface an den Orchestrator gesendet werden. Dieser überprüft die Anfrage und leitet den Befehl dann über den internen Or-Vnfm Referenzpunkt an den entsprechenden Manager weiter.

Abschließend können Ergebnisse von Performance- und Kapazitätsmessungen vom NFVO an OSS/BSS übermittelt werden. [18, S. 33] [24, S. 17-18]

#### *2.1.4.2 Ve-Vnfm-em*

Dieser Referenzpunkt ist für die Kommunikation zwischen Element Manager und VNF Manager zuständig. Über ihn können VNFs auf Anfrage des EMs instanziiert, geupdatet, skaliert und terminiert werden. Zudem können Informationen über Konfigurationen und Events der VNF beidseitig ausgetauscht werden. [25, S. 85]

Der Ve-Vnfm-em Referenzpunkt muss nicht zwingend verwendet werden. Wenn der Element Manager nicht über die Virtualisierung der Netzwerkfunktion informiert wurde, betrachtet er die NF als physische Netzwerkfunktion und übernimmt selbst diese Aufgaben, da der VNF Manager nur für virtuelle NFs zuständig ist. [18, S. 34]

#### *2.1.4.3 Ve-Vnfm-vnf*

Dieser Referenzpunkt ist für den Austausch zwischen VNF und VNF Manager zuständig. Über diesen instanziiert, updatet, skaliert und terminiert der Manager die virtuelle Netzwerkfunktion. Zudem werden Informationen über Konfigurationen und Events beidseitig ausgetauscht. Abschließend kann der VNFM über den Ve-Vnfm-vnf Referenzpunkt testen, ob die Netzwerkfunktion weiterhin aktiv ist und korrekt funktioniert. [18, S. 34] [25, S. 27]

#### *2.1.4.4 Nf-Vi*

Der Nf-Vi Referenzpunkt ist für Kommunikation zwischen Virtualized Infrastructure Manager und NFV Infrastructure zuständig. Über diesen werden virtuellen Maschinen Ressourcen zugewiesen, Ressourcenzuweisungen zur Auslastungsoptimierung geändert und VMs beendet. Des Weiteren werden Verbindungen zwischen VMs erstellt, konfiguriert und entfernt. [18, S. 34]

### 2.1.5 Einsatz mehrerer Orchestratoren

Abhängig von der Größe und Komplexität eines Netzwerks kann zu organisatorischen Zwecken das Netzwerk in mehrere administrative Domains unterteilt werden. Dies wird beispielhaft für den NFV Use Case VNPaaS benötigt, welcher in Kapitel 1.2.3.3 vorgestellt wurde. Jede Domain wird dann von einem eigenen MANO-Stack verwaltet. Um das gesamte Netzwerk zu verwalten und zu orchestrieren ist hierbei ein übergeordneter Orchestrator notwendig. Dieser wird als „Umbrella NFVO“ bezeichnet. [26, S. 20] Aufgabe des Umbrella NFVOs ist die Verwaltung von Netzwerkservices, welche domainübergreifend eingesetzt werden.

Der Umbrella NFVO ist nicht für das Lifecyle Management von Funktionen in den administrativen Domains zuständig und hat auch keinen Überblick über die Ressourcen in den Domains. [26, S. 20]

Zur Veranschaulichung ist der Aufbau beim Einsatz mehrerer Orchestratoren in Abbildung 6 dargestellt.

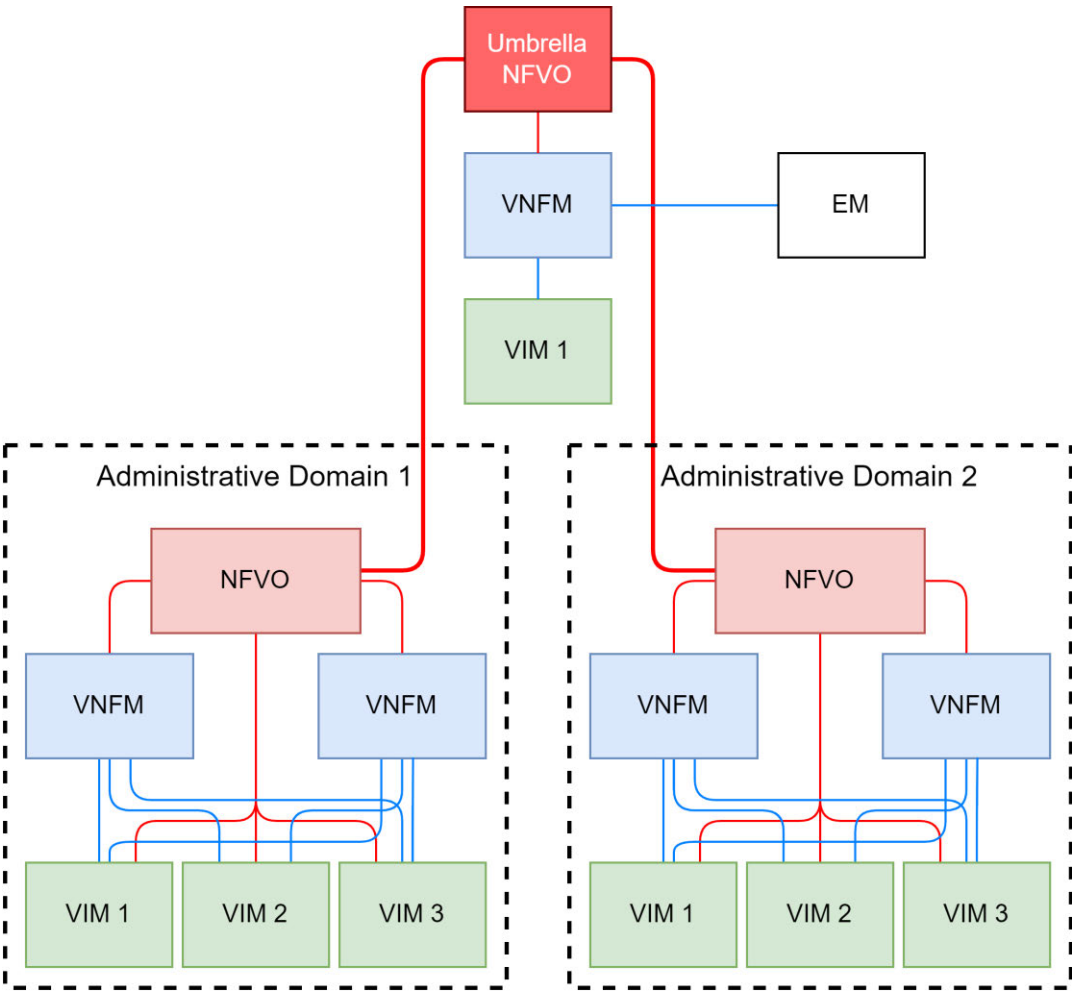


**Abbildung 6: Umbrella NFVO beim Einsatz mehrerer administrativer Domains, Eigene Abbildung, nach [26, S. 20].**

## 2.2 ETSI-Referenzimplementation des NFV-MANO Frameworks

Um die Konzepte des theoretisch beschriebenen Frameworks in einen praktischen Kontext zu setzen, wurde von ETSI eine offizielle MANO-Referenzimplementation entwickelt.

ETSI OSM [27] ist eine Open Source Implementation des ETSI NFV-MANO Stacks, welche in Produktion in kommerziellem Umfeld eingesetzt werden kann. Zudem kann bei der Entwicklung eines MANO-Produkts ETSI OSM als Referenz herangezogen werden.

OSM wurde unter Apache 2.0 Lizenz veröffentlicht. Bei neuen oder geänderten ETSI-Spezifikationen wird ETSI OSM entsprechend den Vorgaben angepasst. Hierbei handelt es sich um ein Community-Projekt, welches als Referenz-Implementation von MANO angesehen werden kann. [27]

OSM stellt NFV Orchestrator und VNF Manager bereit. Der Virtual Infrastructure Manager ist nicht enthalten, da dessen Implementation nicht im Bereich von ETSI NFV-MANO liegt. Für die meisten, verbreiteten VIMs sind jedoch Konfigurationsanweisungen auf der OSM-Website vorhanden.

VIMs, für die Konfigurationen von ETSI bereitgestellt werden, sind OpenStack, Microsoft Azure, Google Cloud Platform (GCP), Amazon Web Services (AWS), VMware vCloud Director und OpenVIM. [28]

Für Testzwecke kann OSM auch ohne serverbasierte VIM betrieben werden, indem eine VIM Sandbox wie DevStack oder MicroStack eingesetzt wird. Dies sind OpenStack Testumgebungen, welche den Funktionsumfang von OpenStack in einer lokalen Installation, beispielsweise auf einem Laptop, bereitstellen. Dies ist nicht geeignet zum Einsatz in einer Produktionsumgebung, kann jedoch für die Durchführung von MANO-Tests verwendet werden. [29]

Neben ETSI OSM sind Distributionen von OSM erhältlich. Die wohl verbreitetste OSM-Distribution stammt von Canonical, der Firma hinter Ubuntu, OpenStack und Kubernetes. Canonical veröffentlichte mit „Canonical Charmed OSM“ ihre eigene, auf ETSI OSM basierte MANO-Distribution. Sie ermöglicht durch Integration von Juju charms eine einfachere Implementation und Skalierbarkeit im Enterprise-Einsatz sowie einfachere Integration mit anderen Juju Applikationen. [30]

# 3 Sicherheitsmanagement von NFV

Aufgrund der schnellen, dynamischen Änderungen von Ende-zu-Ende Netzwerkservices in einem 5G Mobilfunknetzwerk müssen die Sicherheitsrichtlinien des Netzwerks gleichermaßen dynamisch konfiguriert werden. Die OSS-Komponente, welche in bisherigen Mobilfunkgenerationen für Sicherheitsmanagement zuständig war, kann diese Aufgabe in der NFV-Architektur nicht erfüllen, da über den Os-Ma-Nfvo Referenzpunkt lediglich Performance-Management sowie Fehlermanagement unterstützt wird. [31, S. 11]

Des Weiteren werden in NFV-MANO Netzwerkfunktionen ausgerollt, ohne dabei Sicherheitsmanagement zu beachten. Da somit weder OSS noch NFV-MANO für Sicherheitsmanagement zuständig sein können, muss diese Aufgabe von einer neuen Komponente übernommen werden. [31, S. 11]

Um diese Aufgabe zu erfüllen, wird in einem NFV-basierten Netzwerk das Netz von einer Security Management Platform überwacht und verwaltet. Sie besitzt einen Überblick über sämtliche Komponenten eines Netzwerks (inklusive Applikationen, NFVI-Software und Hardware). [32, S. 6]

Die Security Management Platform eines Netzwerks besteht aus einem oder mehreren Security Managern (SM). Der NFV-SM ist für die Sicherheit bei Instanziierung, Modifizierung und Terminierung von VNFs zuständig. Dafür ist er über Referenzpunkte mit dem MANO-System verbunden. Sämtliche Informationen zu Events, die den Lebenszyklus von VNFs betreffen, werden über diese Referenzpunkte in Echtzeit an den Security Manager gesendet. [32, S. 7]

Dessen Aufgabe ist die Auswertung der erhaltenen Informationen des MANO-Systems über den Lebenszyklus aller VNFs und die dementsprechende Durchsetzung von Sicherheitsregeln. So können beispielsweise bei sicherheitsrelevanten Events auf Anweisung vom NFV-SM die betroffenen VNF-Instanzen terminiert oder in Quarantäne verschoben sowie Wiederherstellungsmaßnahmen eingeleitet werden.

MANO-Implementationen müssen den Einsatz von SMs unterstützen, um zu vermeiden, dass beispielsweise das MANO-System einen Neustart einer VNF-Instanz durchführt, welche der NFV-SM terminiert hat. MANO-Komponenten müssen den Befehlen des Security Managers Folge leisten. [32, S. 7]

Das Sicherheitsmanagementsystem ist kein fester Bestandteil des MANO-Frameworks. In diesem Kapitel der Arbeit wird dieses trotzdem vorgestellt, da:

1. es über mehrere Referenzpunkte mit dem MANO-System verbunden ist, über welche sicherheitsrelevante MANO-Informationen ausgetauscht werden,
2. das Sicherheitsmanagementsystem für die Sicherheit von VNFs eine wichtige Rolle spielt,
3. das Sicherheitsmanagement-Framework für die Erstellung des offiziellen „SCAS for MANO“ - Dokuments (siehe Kapitel 4) referenziert wird.

Aufgrund des Umfangs und der Komplexität des Systems kann in dieser Arbeit nicht auf alle Aspekte eingegangen werden. Für weiterführende Informationen wird auf folgende Dokumente verwiesen:

- ETSI GS NFV-SEC 013 – „Security Management and Monitoring Specification“ [31]
- ETSI GS NFV-IFA 026 – „Architecture enhancement for Security Management Specification“ [32]
- ETSI DGS/NFV-SEC024 – Work Item „Security Management Specification“ [33]

## 3.1 Arten der Sicherheitsfunktionen

Für das Security Management von NFV lassen sich Sicherheitsfunktionen (SF) in drei Kategorien einteilen.

1. Eine VNF-Layer Security Function (VSF) bezeichnet eine virtuelle Sicherheitsfunktion, beispielsweise eine virtuelle Firewall (vFW), ein Intrusion Detection System (IDS) oder ein virtuelles Security Gateway (vSEC-GW). Diese Sicherheitsfunktionen werden als VNF auf der NFVI bereitgestellt und dienen dem Schutz anderer VNFs. Die Instanziierung sowie das Lifecycle Management von VSFs erfolgt durch den VNF Manager und die Konfiguration durch einen zugewiesenen EM. [31, S. 11-14]
2. Eine NFV Infrastructure Security Function (ISF) ist eine virtuelle Sicherheitsfunktion, die von der NFVI bereitgestellt wird und auf dieser Ebene arbeitet. Sie wird mithilfe des VIMs verwaltet. Beispiele hierfür wären Hardware-Sicherheitsmodule, Crypto Accelerators oder Trusted Platform Module. [31, S. 11-14]
3. Neben den virtuellen sind weiterhin auch traditionelle SF, wie z. B. physische Firewalls nötig, um die Netzwerkschichten unter VSF und ISF zu schützen. Diese werden als Physical Security Function (PSF) bezeichnet und schützen die NFV-Infrastruktur. Da sie Teil des traditionellen Netzwerks sind, sind sie nicht in ETSI NFV behandelt. [31, S. 11-14]

Aufgrund der Kritikalität der Sicherheitsfunktionen dürfen ausschließlich Administratoren zur Verwaltung von VSF, ISF und PSF berechtigt sein. [31, S. 11]

## 3.2 Probleme des bisherigen Modells

Da im 5G Mobilfunknetz der Lebenszyklus der eingesetzten VNFs automatisiert verwaltet wird, muss auch das Sicherheitsmanagement automatisiert erfolgen.

Wäre dies nicht der Fall, müssten vom Administrator alle VSFs manuell instanziiert und konfiguriert sowie alle ISFs und PSFs manuell konfiguriert werden.

Gleichermaßen müsste eine VSF bei jeder Migration einer VNF ebenso migriert oder re-konfiguriert werden. Die Migration einer VSF darf im Gegensatz zu einer VNF aus Sicherheitsgründen nicht durch NFV-MANO automatisiert stattfinden, sondern müsste manuell vom Administrator erfolgen.

Das gleiche Problem würde beim Skalieren des Netzwerkservices auftreten. Auch hier kann das Skalieren der VNF automatisiert erfolgen, das Instanziieren und Terminieren einer VSF darf aus Sicherheitsgründen aber nicht NFV-MANO - automatisiert erfolgen. [31, S. 12]

Da solch häufige Administrator-Interaktionen fehleranfällig, langsam und nicht gut skalierbar sind, wird im 5G Mobilfunknetz ein neuer Ansatz für Sicherheitsmanagement benötigt.

## 3.3 Regelbasiertes Sicherheitsmanagement

Um nicht jede VSF einzeln betreuen zu müssen, ist der Einsatz einer zentralen, verwaltenden Komponente für virtuelle Sicherheitsfunktionen notwendig – vergleichbar mit dem MANO-System für VNFs.

Diese Aufgabe übernimmt der NFV Security Controller (NFV-SC). Der Administrator kann Regeln für das Lifecycle Management von VSFs sowie Konfigurationen sämtlicher SFs, die für einen Netzwerkservice zuständig sind, festlegen. Der NFV-SC setzt diese Regeln um. [31, S. 12-13]

Wie in Abbildung 7 ersichtlich, ist Administratorinteraktion nur bei der Regelerstellung des Sicherheitsmanagements notwendig. Der Administrator legt im Security Controller Regeln fest, nach welchen die Verwaltung und Konfiguration von Sicherheitsfunktionen erfolgen soll.

Bei Änderungen des Netzes durch eine Aktion des MANO-Systems werden die Sicherheitsfunktionen durch den Security Controller automatisch entsprechend angepasst und (re)konfiguriert.

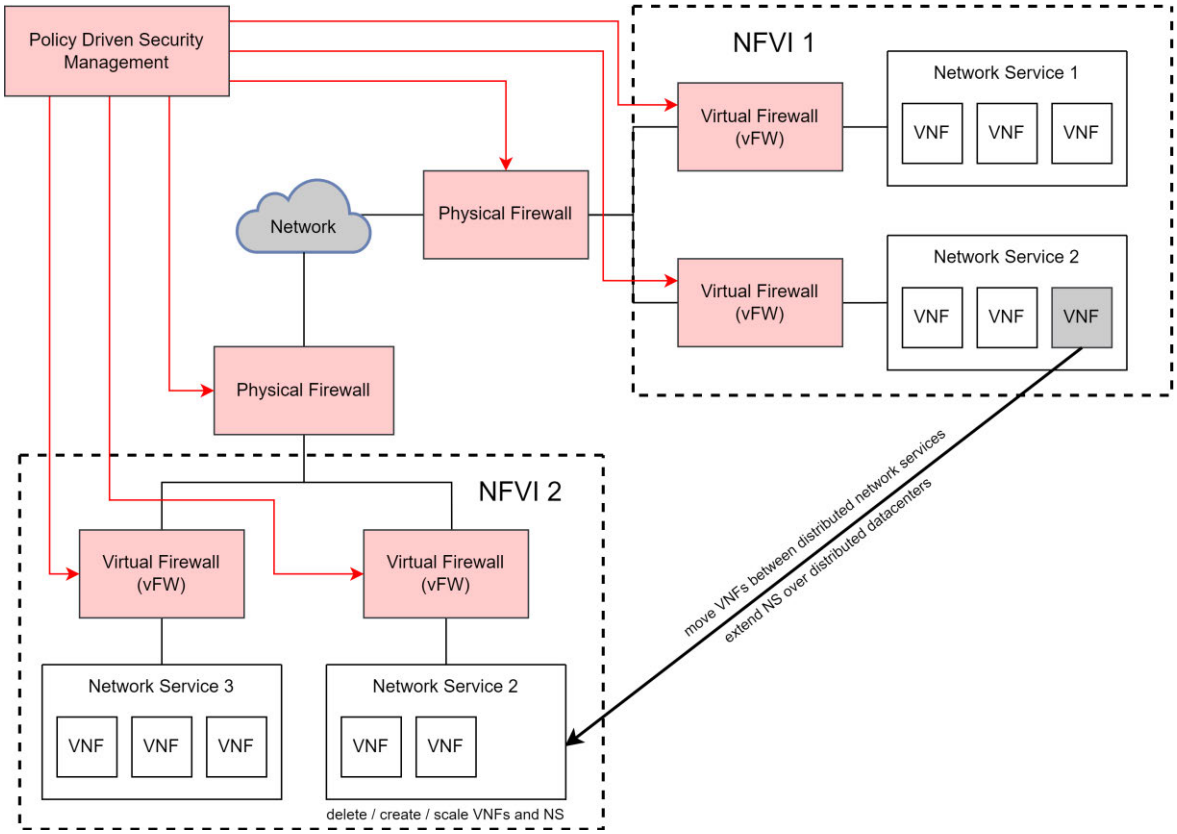


**Abbildung 7: Schematische Übersicht des regelbasierten Sicherheitsmanagements, Eigene Abbildung, nach [31, S. 17].**

## 3.4 Architektur des Security Managers

Die durch das Sicherheitsmanagement in die NFV-Architektur hinzugefügten Bestandteile (siehe Abbildung 8) lassen sich in mehrere Kategorien (SSA, SSP, SC, Analysesystem, Datenbanken sowie Referenzpunkte) einordnen:

1. Security Service Agents (SSA). Diese Komponenten erhalten sicherheitsrelevante Befehle und führen diese aus. Sie können als eine eigenständige VSF existieren oder in eine VNF integriert sein. [31, S. 39]
2. Security Service Provider (SSP). Diese sind zuständig für die Orchestrierung und Durchsetzung von Regeln, welche sie vom Security Controller erhalten und stehen im Austausch mit SSAs. Sie können optional Daten analysieren, die sie von den SSAs erhalten – auf Anweisung des Security Monitoring Analytics Systems. [31, S. 39]
3. Security Controller (SC). Dieser ist für eine systemweite Orchestrierung, Erstellung und Verwaltung von Sicherheitsrichtlinien zuständig. Außerdem verwaltet er den Lebenszyklus von SSAs, damit diese bei Änderungen im NFV-Framework automatisch entsprechend angepasst werden und überwacht diese, um Fehler zu erkennen und zu beseitigen. Wie auch der NFVO im MANO-Framework besitzt der SC eine Verbindung zu mehreren Datenbanken. [31, S. 39]

4. Referenzpunkte. Diese sind mit dem Security Controller verbunden und für den Daten- und Befehlsaustausch zuständig.
5. Security Monitoring Analytics Systems. Dieses System analysiert mittels Machine Learning Daten des NFV-Frameworks, um Auffälligkeiten festzustellen, die auf einen Angriff hinweisen könnten. Werden Auffälligkeiten beobachtet, werden diese dem Security Controller mitgeteilt, welcher Gegenmaßahmen einleitet. [31, S. 40]
6. NFV Security Monitoring Database (NFVSecM-DB). Diese Datenbank enthält sicherheitsbezogene Daten, die für die Sicherheitsüberwachung benötigt werden. Dazu zählen unter anderem festgelegte Sicherheitsregeln, Konfigurationen von sicherheitsbezogenen Komponenten sowie Authentifizierungsdaten von Komponenten, die für die Sicherheitsüberwachung relevant sind. Aufgrund der hohen Sicherheitsrelevanz ist die NFVSecM-DB verschlüsselt und nur vom SC nutzbar. [31, S. 40]
7. SSA/VSF Catalogue Database (VSF-VNF-CAT). Sie ist das Security-Äquivalent des NS- und VNF Catalogue des MANO-Systems. In dieser Datenbank sind VNF Packages der VSFs gespeichert und werden zur Orchestrierung derer verwendet. [31, S. 40]
8. NFV Audit Database (NFV AUD-DB). In dieser Datenbank, werden Daten gespeichert, die für eine Sicherheitsüberprüfung benötigt werden. [31, S. 40]

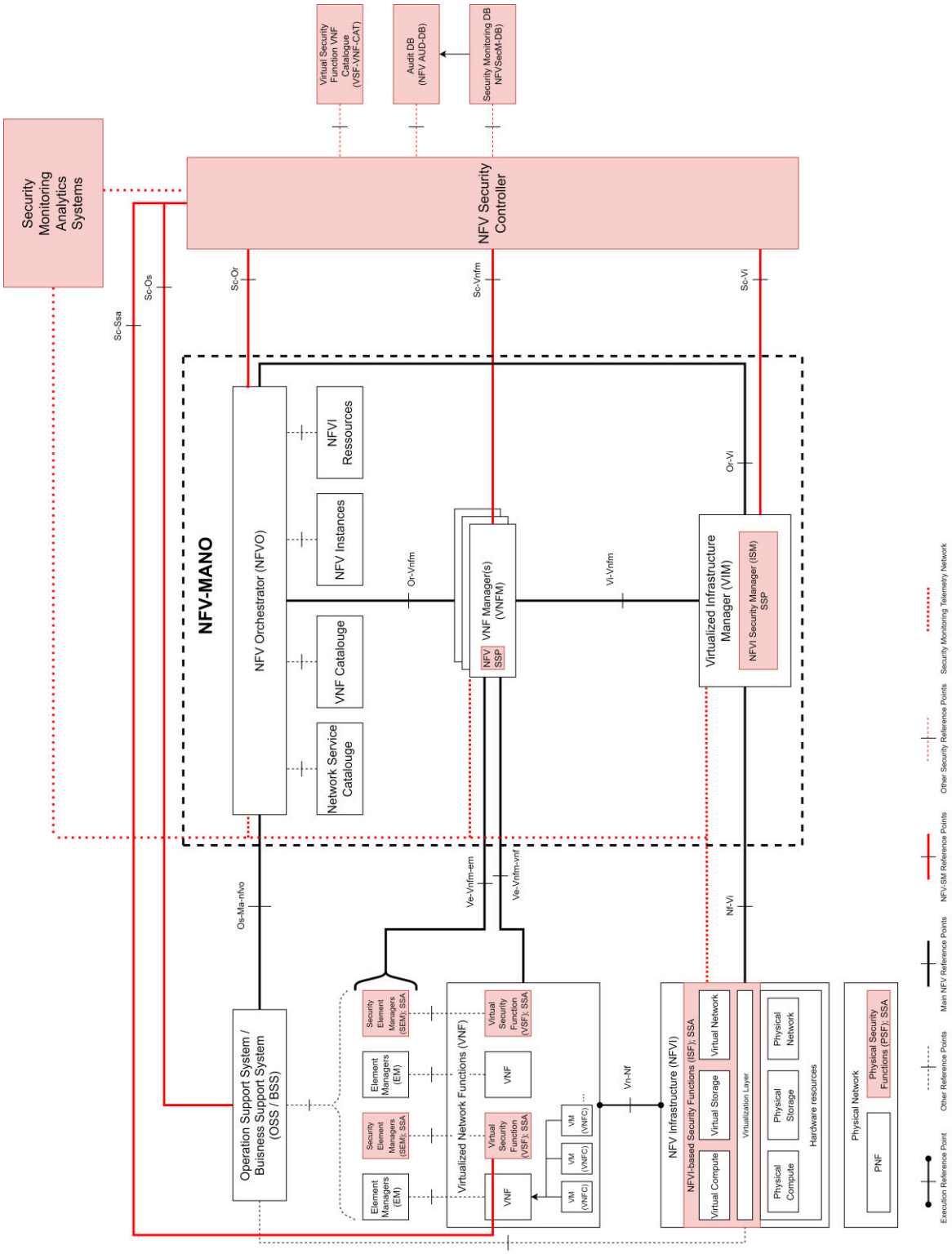


**Abbildung 8: Sicherheitsmanagement-Architektur im NFV-MANO Kontext, Eigene Abbildung, nach [11, S. 10], [18, S. 24] und [31, S. 39].**

# 4 Sicherheitszertifizierung nach NESAS-SCAS

Zur Sicherheitszertifizierung von Mobilfunknetzwerken kann das Network Equipment Security Assurance Scheme (NESAS) verwendet werden. Es wurde von der Group Speciale Mobile Association (GSMA) und dem 3rd Generation Partnership Project (3GPP) speziell für die Anwendung im Mobilfunkbereich entwickelt. Detaillierte Informationen zu Aufbau und Vorgehen sind in [34] und [35] beschrieben.

Sicherheitstests, die für die Zertifizierung durchzuführen sind, sind in Security Assurance Specifications (SCAS) festgehalten.

Im Dokument TS 33.117 „Catalogue of general security assurance requirements“ [36] sind Tests beschrieben, welche auf sämtliche Netzwerkprodukte zutreffen. Diese müssen bei der Zertifizierung von allen Netzwerkprodukten durchgeführt werden.

In zusätzlichen SCAS-Dokumenten sind darüber hinaus Tests definiert, die speziell auf eine bestimme Gruppe von Netzwerkprodukten zutreffen.

Für die Zertifizierung eines Netzwerkproduktes müssen sowohl die generellen Tests, als auch die produktspezifischen Tests durchgeführt werden. Bei der Zertifizierung einer 5G Access and Mobility Management (AMF)-Funktion müssen beispielsweise die Tests aus TS 33.117 sowie TS 33.512 [37] durchgeführt werden.

## 4.1 Offizielles SCAS-Dokument zu MANO

Die MANO-Komponente ist eine der wenigen Komponenten eines 5G Netzes, für welche zu Beginn dieser Arbeit noch kein eigenes Dokument angekündigt oder veröffentlicht wurde. Eine Ankündigung, dass ein offizielles MANO SCAS-Dokument entworfen wird, erfolgte erst im Verlauf der Bearbeitungszeit dieser Arbeit.

### 4.1.1 Zeitplan und Einbeziehung des MANO-spezifischen SCAS-Dokuments in dieser Arbeit

Zu Beginn der Bearbeitungszeit dieser Arbeit (01.07.2022) war noch kein SCAS-Dokument zur MANO-Komponente veröffentlicht oder angekündigt. Am 05.07.2022 wurde ein Work Item des Dokuments „SCAS for MANO“ unter der Dokumentennummer „DGS/NFV-SEC028“ erstellt und somit ein MANO-spezifisches SCAS-Dokument angekündigt. [38]

Im Zeitplan dieses Work Items wurde als Bearbeitungsbeginn der 12.09.2022 festgehalten. Am gleichen Tag sollte bereits ein erster Entwurf veröffentlicht werden.

Der erste Stable Draft soll ab dem 15.04.2023, der Final Draft ab dem 15.05.2023 verfügbar sein. Das finale Dokument soll am 09.09.2023 publiziert werden.

Die Bearbeitung des Work Items unterliegt einer Verzögerung. Zum Abgabetermin dieser Arbeit (17.10.2022) wurde noch nicht mit der Erstellung des Dokuments begonnen. [39]

### 4.1.2 Referenzierte Dokumente

Obwohl das Dokument noch nicht publiziert wurde, sind in der Beschreibung des Work Items bereits drei Dokumente benannt, welche als Grundlage der Erstellung der Tests dienen sollen.

Das erste Dokument ist „GS NFV-SEC 014 - Security Specification for MANO Components and Reference points“ [40]. Dies ist eine veröffentlichte, von ETSI durchgeführte Risikoanalyse des MANO-Systems und wird in Kapitel 5.2 näher vorgestellt.

Die beiden anderen referenzierten Dokumente sind „GS NFV-SEC 024 – NFV Security Management Specification“ [33] und „GS NFV-SEC 025 – NFV Secure End-to-End VNF and NS Management Specification“ [41].

Bei diesen Dokumenten handelt es sich momentan noch um Work Items in der Early Draft – Phase. Beide Dokumente sind von ETSI als „work in progress“ eingestuft und dürfen laut Hinweis auf dem Deckblatt der Entwürfe der Work Items ausdrücklich nicht zitiert oder referenziert werden. Inhaltlich dürfen die Entwürfe demnach in dieser Arbeit nicht betrachtet werden, weswegen im Folgenden ausschließlich die Informationen aus NFV-SEC 014 zur Sicherheitsbetrachtung herangezogen werden können.

## 4.2 Umsetzbarkeit der Zertifizierung von MANO-Produkten nach NESAS-SCAS

Die ETSI NFV-MANO Architektur genießt zwar sehr große Popularität – ein Zertifizieren von MANO-Produkten nach dem NESAS-SCAS Schema besitzt jedoch theoretisch zwei Probleme:

Erstens können MANO-Implementationen von der ETSI-Architektur abweichen.

Beispielsweise definierte die CORD-Plattform der Open Networking Foundation mit dem Service Orchestrator „XOS“ [42] abweichend von der ETSI-Architektur ihre eigene Architektur mit eigener Kommunikationslogik zwischen den einzelnen Komponenten. Die meisten der XOS-Komponenten lassen sich zwar den ETSI-Blöcken NFVO, VIM und VNFM zuordnen - die ETSI-Architektur wurde jedoch in der Entwicklung explizit als not-in-scope angesehen. [43]

SCAS-Tests, welche spezifisch auf MANO-Produkte anhand der ETSI-Architektur formuliert wurden, müssen demnach nicht allgemeingültig für alle MANO-Produkte anwendbar

sein. Gleichermaßen sind Tests nicht universell für alle Architekturen passend formulierbar. Der Grad der Abweichung eines Produkts kann demnach von vollständiger ETSI-Konformität bis hin zur möglichen Unanwendbarkeit von Tests reichen.

Zweitens umfassen umfangreiche, kommerzielle NFV-MANO-Produkte in der Regel noch weitere Komponenten als nur die definierten, internen ETSI NFV-MANO – Komponenten.

Beispielsweise ist „Edge Cloud“ [44] von Rakuten Symphony ein verbreitetes, kommerzielles NFV-Produkt, einschließlich MANO-Funktionalität. Für Management- und Orchestrierungsaufgaben greift dieses Produkt auf die „Robin Multi Data Center Automation Platform (MDCAP)“ zurück. [45] Deren Architektur orientiert sich an den Vorgaben von ETSI NFV-MANO. [46] Um dies zu verdeutlichen, wurden in Abbildung 9 die ETSI NFV-MANO – Komponenten in der Robin MDCAP-Architektur nachträglich rot umrandet hervorgehoben sowie notiert, welchen Referenzpunkten und funktionalen Blöcken die Komponenten entsprechen. Eine detaillierte Erklärung der Robin MDCAP Architektur würde den Rahmen dieser Arbeit überschreiten und kann unter [47] nachgelesen werden.

Ein Durchführen von ETSI NFV-MANO – spezifischen SCAS-Tests wäre demnach für diese markierten Komponenten und Referenzpunkte möglich.

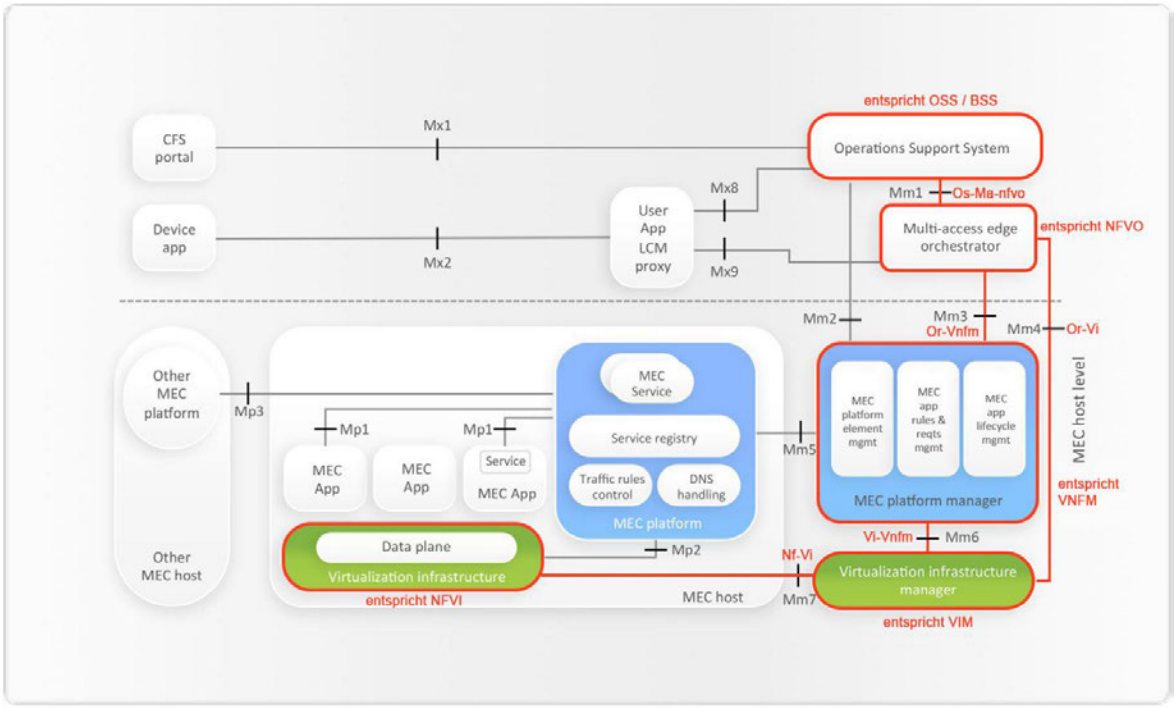


**Abbildung 9: Robin MDCAP Architektur, [47, S. 6], modifiziert.**

Problem bei der Zertifizierung nach NESAS ist jedoch, dass der Funktionsumfang der OSS-Komponente im ETSI NFV-MANO – Framework nicht betrachtet wird. Laut ETSI-Definition, welche in Kapitel 2.1.3.1 beschrieben wurde, umfasst der OSS/BSS-Block sämtliche Funktionen, welche nicht in anderen Blöcken enthalten sind, jedoch mit diesen kommunizieren.

Der spezifische Funktionsumfang der OSS-Komponente kann sich demnach von Produkt zu Produkt drastisch unterscheiden, weswegen für diesen funktionellen Block formulierte SCAS-Tests nicht zwingend bei allen Produkten anwendbar sein müssen. Zudem kann nicht sichergestellt werden, dass neu entwickelte OSS-Funktionen auch durch einen Test im SCAS-Dokument abgedeckt sind. So könnten beispielsweise Tests nicht durchführbar sein, da diese Funktion in der OSS-Komponente des zu zertifizierenden Produkts überhaupt nicht existiert. Gleichermaßen könnten zusätzliche OSS-Funktionen, welche bei der Erstellung des SCAS-Dokuments nicht berücksichtigt wurden, auch nicht getestet werden.

Dabei spielt die OSS-Komponente im Realbetrieb eine wichtige Rolle, da das Netzwerk größtenteils über Management-Plattformen der Operations Support Systems gesteuert wird. Von diesen aus werden im laufenden Betrieb über den Os-Ma-nfvo Referenzpunkt Netzwerkservices instanziiert, skaliert und terminiert. Außerdem werden Analysedaten des NFV-MANO Stacks vom NFV Orchestrator an OSS übertragen.

Aufgrund des ungewissen Funktionsumfangs und der häufig übergeordneten Rolle der OSS-Komponente lassen sich umfangreiche MANO-Produkte inklusive OSS nicht immer vollständig mittels NESAS-SCAS zertifizieren. In diesem Fall wäre eine Einzelfallbetrachtung, zum Beispiel mittels des Common Criteria - Zertifizierungsverfahrens, angebracht.

Teile des Produkts, welche dem ETSI NFV-MANO – Standard entsprechen, ließen sich jedoch mittels NESAS-SCAS zertifizieren.

Ob und wie im offiziellen SCAS-Dokument potentiell abweichende MANO-Architekturen und OSS-Funktionen berücksichtigt werden, bleibt abzuwarten.

# 5 Sicherheitsrelevanz des MANO-Systems

Für die Erstellung eines MANO-spezifischen SCAS-Dokuments (siehe Kapitel 4.1) ist eine umfassende Sicherheitsbetrachtung nötig.

In diesem Kapitel werden Sicherheitsrisiken und daraus abgeleitete Sicherheitsvoraussetzungen im MANO-System vorgestellt. Anschließend werden die Sicherheitsvoraussetzungen mit dem Testkatalog aus dem SCAS-Dokument *TS 33.117 – General Requirements* [36] abgeglichen, um zu überprüfen, welche Voraussetzungen noch in einem MANO-spezifischen SCAS-Dokument behandelt werden müssen.

## 5.1 Sicherheitsrelevanz der MANO-Komponenten

Das MANO-System eines 5G Netzes besitzt eine hohe Sicherheitsrelevanz, da es die Ressourcen und den Lebenszyklus sämtlicher Netzwerkfunktionen des Mobilfunknetzes verwaltet. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) bezeichnet deshalb im Bericht “NFV Security in 5G – Challenges and Best Practices” das MANO-System als “single point of failure”. Eine Kompromittierung von MANO würde effektiv sämtliche VNFs des Netzwerks kompromittieren. [48, S. 45]

Die kritischste Komponente im MANO-System ist dabei der NFV Orchestrator, da die Ausführung von Befehlen im MANO-System immer in Absprache mit dem NFVO erfolgt. Im MANO-System besitzt der NFVO die privilegierteste Position. Der vollständige Systemüberblick und die Befehlsgewalt über VNFM und VIM stellen ein hohes Sicherheitsrisiko dar, sollte ein Angreifer Zugriff auf den NFVO erhalten.

Eine Liste der Funktionen, auf die ein Angreifer bei Kontrolle über den NFVO Zugriff hätte, entspricht dem Funktionsumfang der internen, vom Orchestrator ausgehenden Referenzpunkte. Diese Funktionen sind in den Spezifikationen der Or-Vi (GS NFV-IFA 005) [19] und Or-Vnfm (GS NFV-IFA 007) [21] – Referenzpunkte ersichtlich. Ein grundlegender Überblick über die Funktionen ist in Kapitel 2.1.2 enthalten. Eine Ausführung der Funktionen würde den Rahmen dieser Arbeit überschreiten.

## 5.2 Bedrohungsanalyse

Um potentielle Angreifer und Risiken zu identifizieren, führte ETSI eine Bedrohungsanalyse des MANO-Systems durch. Das Ergebnis der Bedrohungsanalyse wurde im Dokument „GS NFV-SEC 014 - Security Specification for MANO Components and Reference points“ beschrieben. [40]

### 5.2.1 Rahmenbedingungen der Analyse

Bei der Bedrohungsanalyse wurden nur die MANO-internen Komponenten (NFVO, VNFM und VIM) sowie die dazugehörigen internen Referenzpunkte (Or-Vnfm, Or-Vi und Vi-Vnfm) betrachtet.

Die externen Komponenten (OSS/BSS, EM, VNF und NFVI) sowie die dazugehörigen externen Referenzpunkte (Os-Ma-nfvo, Ve-Vnfm-em, Ve-Vnfm-vnf und Nf-Vi) wurden bei der Erstellung der Bedrohungsanalyse explizit ausgeschlossen und „for further study“ deklariert. [40, S. 6]

Da die externen Referenzpunkte die einzigen Zugriffsmöglichkeiten von außen auf das MANO-System sind und diese in der ETSI-Bedrohungsanalyse nicht betrachtet werden, kann MANO in der Bedrohungsanalyse der internen Komponenten und Referenzpunkte als ein abgeschlossenes System betrachtet werden. Da kein Zugriff von außen erfolgen kann, müssen sämtliche betrachteten Angriffe auf das MANO-System Insider-Angriffe sein. Dies bedeutet, dass der Angreifer Zugriff auf das Netzwerk sowie Zugangsrechte für das MANO-System besitzt. Zum Schutz vor Insider-Angriffen müssen zusätzlich zu den hier beschriebenen, technischen Maßnahmen weitere Maßnahmen im Bezug auf Humanressourcen getroffen werden. Diese sollen den entsprechenden Richtlinen der ISO/IEC 27000 [49] – Dokumentenreihe entsprechen. [40, S. 8]

Eine weiterführende Bedrohungsanalyse der externen Komponenten und Referenzpunkte wurde bisher noch nicht veröffentlicht.

### 5.2.2 Kardinalitäten

Für eine Bedrohungsanalyse ist es wichtig zu wissen, welche Kardinalitäten zwischen den Komponenten vorhanden sind. Dies liegt daran, dass eine 1:1 Verbindung einfacher zu sichern ist als eine 1:n oder n:m – Verbindung. In der MANO-Architektur sind verschiedene Kardinalitäten möglich, weswegen diese für eine Bedrohungsanalyse im Voraus festgelegt werden müssen. [40, S. 7]

Für die in *NFV-SEC 014* beschriebene Bedrohungsanalyse hat ETSI eine 1:n – Beziehung zwischen NFVO und VNFM, eine 1:n - Beziehung zwischen NFVO und VIM, eine 1:n - Beziehung zwischen VNFM und VIM sowie eine 1:n - Beziehung zwischen VNFM und VNF gewählt, da dies einer in der Praxis gängigen Konfiguration entspricht.

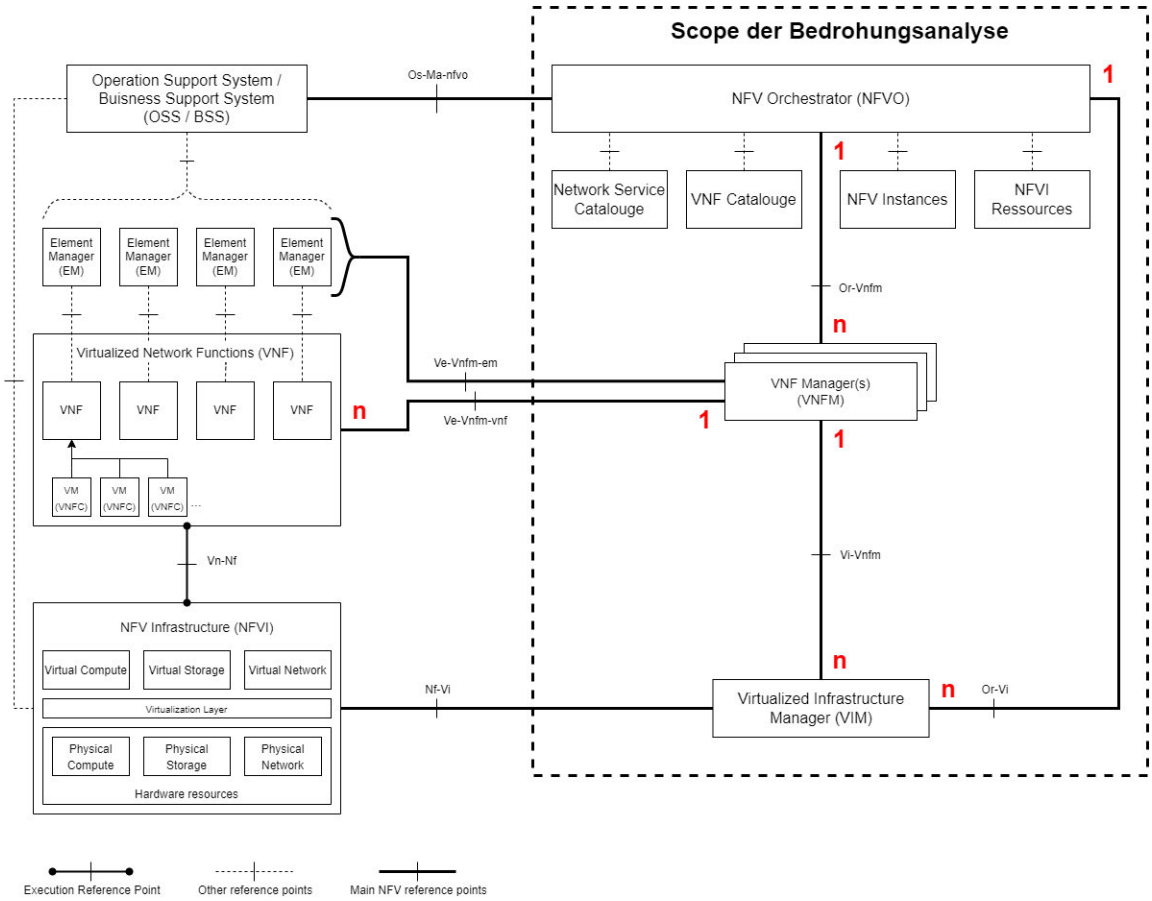


**Abbildung 10: Kardinalitäten der MANO-Architektur und Scope der Bedrohungsanalyse, Eigene Abbildung, nach [11, S. 10], [18, S. 24] und [40, S. 7].**

### 5.2.3 Festgestellte Bedrohungen

Als Ergebnis der Bedrohungsanalyse wurden zwei MANO-spezifische, potentielle Gefahrenquellen und zwei MANO-spezifische Bedrohungen festgestellt. [40, S. 9] Diese werden im folgenden beschrieben.

Die erste, potentielle Gefahrenquelle wird als „active probe on interface“ beschrieben. Bei einem Active Probing – Angriff werden Netzwerkpakete in ein Netzwerk gesendet und die Antwort des Netzwerks auf die Anfrage analysiert. [50, S. 267]

Als zweite, potentielle Gefahrenquelle werden Nutzer oder Administratoren, welche Zugriffsrechte auf funktionelle Blöcke und Referenzpunkte des MANO-Frameworks besitzen, angeführt.

Gefahren, welche von diesen beiden Gefahrenquellen ausgehen können, sind als „Masquerade of NFVO to VIM“ und „Masquerade of NFVO to VNFM“ beschrieben. Bei diesen Angriffen kann sich ein Angreifer unter falscher Identität mit legitimen Zugangsdaten Zugriff zum NFVO verschaffen, z. B. um unbemerkt bereitgestellte Funktionen von VNFM und VIM zu nutzen. [51, S. 255]

Weitere Bedrohungen, z. B. durch Implementierungsfehler, Malware oder Angriffe auf dem Transport Level, wie DDoS Angriffe, wurden nicht betrachtet, da diese nicht MANO-spezifisch sind. [40, S. 9]

### 5.2.4 Abgeleitete Sicherheitsvoraussetzungen

Aus diesen potentiellen Gefahrenquellen und Bedrohungen wurden Sicherheitsvoraussetzungen für das MANO-Framework formuliert. [40, S. 9-11]

Eine der wichtigsten Sicherheitsvoraussetzungen für MANO ist, dass der Empfänger von Daten oder Befehlen die Ausführung dieser ablehnt, bis der Sender verifiziert worden ist. Dies könnte die meisten Fälle von Masquerade Attacks und Priviledge Escalation verhindern.

Zur Verifizierung des Senders muss eine Zugangskontrolle mit Multi-Faktor-Authentifizierung eingesetzt werden. Als einer der Faktoren soll dabei der geografische Standort des Nutzers überprüft werden. Durch eine solche Überprüfung können Anmeldungen mit legitimen Zugangsdaten, jedoch von einem ungewöhnlichen Standort, erkannt und verhindert werden. Außerdem darf das Instanziieren von neuen MANO-Komponenten und NFVIs nur an vorher definierten Datencenter-Standorten möglich sein, um das Einschleusen von fremden Ressourcen zu vermeiden. Diese beiden Sicherheitsbeschränkungen sind umsetzbar, da nur ein sehr beschränkter Personenkreis Zugriff auf das MANO-System haben sollte und die Standorte der verwendeten Datencenter bekannt sind.

Eine weitere, wichtige Sicherheitsmaßnahme ist die Integritätsprüfung von Nachrichten. Der Sender einer Nachricht muss einen Weg bereitstellen, die Integrität einer Nachricht zu überprüfen, z. B. mittels eines Message Authentication Codes (MAC). Der Empfänger einer Nachricht kann beim Empfang anhand dieses Codes ermitteln, ob die Nachricht modifiziert, Teile der Nachricht gelöscht, Teile der Nachricht hinzugefügt oder die Nachricht im Rahmen eines Replay-Attacks mehrfach gesendet wurde.

Dem Virtual Infrastructure Manager kommt gleichermaßen eine eigene Sicherheitsvorgabe zu: Die Images der VMs müssen vom VIM überwacht werden, um zu erkennen, ob ein nicht-autorisiertes Modifizieren, Entfernen oder Hinzufügen stattgefunden hat.

Abschließend muss sichergestellt werden, dass die Kommunikation über die drei internen Referenzpunkte mit einem gängigen, als sicher erachteten Verschlüsselungsverfahren verschlüsselt abläuft.

Werden diese Sicherheitsvoraussetzungen vom MANO-System erfüllt, sollten die Risiken der internen MANO-Komponenten und Referenzpunkte bestmöglich reduziert werden.

## 5.3 Gap-Analyse von MANO-Bedrohungsanalyse und SCAS – General Requirements (3GPP TS 33.117)

Beim Zertifizieren einer Netzwerkkomponente mittels des NESAS-Verfahrens werden die Tests aus Dokument TS 33.117 immer durchgeführt. Deshalb müssen Risiken, welche durch diese Tests bereits abgedeckt werden, nicht erneut im MANO-spezifischen Dokument getestet werden.

Um festzustellen, ob und welche Tests bereits abgedeckt werden und welche Sicherheitsvoraussetzungen noch im MANO-spezifischen Dokument getestet werden müssen, wurden beim Erstellen dieser Arbeit manuell die abgeleiteten Sicherheitsvoraussetzungen aus der Bedrohungsanalyse aus GS NFV-SEC 014 [40] mit den generellen Tests aus TS 33.117 [36] verglichen.

In den folgenden Unterkapiteln werden die Ergebnisse des Vergleichs vorgestellt. Dabei werden jeweils zu den einzelnen Sicherheitsvoraussetzungen aus NFV-SEC 014 die Tests aus TS 33.117 vorgestellt, welche für die Voraussetzung relevant sein können. Abschließend wird festgehalten, ob die Sicherheitsvoraussetzung durch diese Tests bereits erfüllt wird oder noch Lücken (Gap) vorhanden sind, welche in einem MANO-spezifischen SCAS-Dokument geprüft werden müssten.

Betrachtet werden die zum Zeitpunkt der Erstellung dieser Arbeit aktuellsten Dokumentenversionen NFV-SEC 014 V3.1.1 und TS 33.117 V17.0.0.

### 5.3.1 Sicherheitsvoraussetzung 1

„The receiving party shall not allow any actions from received data before successfully identifying and verifying the identity of the transmitting party.“ [40, S. 10]

Dies bedeutet, dass der Empfänger einer Nachricht mit darin enthaltener Aktion, wie beispielsweise ein Remote Procedure Call (RPC), diesen nicht ausführen darf, bis die Identität des Senders identifiziert und verifiziert wurde. Dies geht mit authentifiziertem Netzwerkverkehr einher.

In TS 33.117 existieren in Kapitel 4.2.3.4 „Authentication and Authorization“ drei Tests, welche auf die Voraussetzung zutreffen könnten.

Der erste, dafür relevante Testfall ist in 4.2.3.4.1.1 „System functions shall not be used without successful authentication and authorization“ festgehalten. [36, S. 26]

Unter dem Begriff „system function“ wird in diesem Testfall folgendes verstanden:

- Netzwerkservices wie SSH oder SFTP
- Lokaler Konsolenzugriff
- Lokale Verwendung von Betriebssystemen und Applikationen

Einzige Ausnahme sind Funktionen, die öffentlich sein sollen, z. B. ein Webserver.

In diesem Testfall wird demnach sichergestellt, dass der Zugriff auf ein System und die Verwendung dessen erst nach erfolgter Authentifizierung erfolgen darf. Es wird jedoch nicht auf eingehenden Netzwerkverkehr und eingehende Befehle wie RPCs eingegangen. Aus diesem Grund reicht dieser Testfall nicht aus, um die Sicherheitsvoraussetzung zu erfüllen.

Der zweite, relevante Testfall ist in 4.2.3.4.1.2 „Accounts shall allow unambiguous identification of the user“ festgehalten. [36, S. 27]

In diesem Testfall wird verifiziert, dass ein Nutzeraccount eindeutig einem Nutzer zugeordnet werden kann. Gruppenaccounts und geteilte Accounts zwischen mehreren Nutzern dürfen nicht erlaubt sein. Mit diesem Test wird demnach eindeutige Identifizierbarkeit eines Nutzers zu einem Account sichergestellt. Dies erfüllt jedoch nicht die MANO-Sicherheitsvoraussetzung, da die Authentifizierung bei eingehendem Netzwerkverkehr kein Teil des Tests ist.

Der letzte, relevante Testfall ist in 4.2.3.4.4.1 „Network Product Management and Maintenance interfaces“ festgehalten. [36, S. 39]

In diesem wird getestet, ob „mutual authentication“, also gegenseitiges Authentifizieren, bei Konfigurations- und Wartungsinterfaces des Netzwerkprodukts aktiviert ist. Dies soll verhindern, dass das Netzwerkprodukt von einem Angreifer rekonfiguriert werden kann. Nicht authentifizierte Sender von entsprechenden Management-Nachrichten sollen abgelehnt werden.

Dieser Testfall deckt die MANO-Sicherheitsvoraussetzung nicht vollständig ab, da bei diesem Testfall nur Konfigurations- und Wartungsinterfaces betrachtet werden. In der MANO-Sicherheitsvoraussetzung muss dies hingegen auf sämtlichen, eingehenden Datenverkehr mit enthaltenen Aktionen zutreffen.

Die drei Tests reichen demnach nicht aus, um die Sicherheitsanforderung zu erfüllen. Es ist eine Lücke vorhanden.

Diese lässt sich jedoch einfach schließen, indem der Testfall 4.2.3.4.4.1 im „SCAS for MANO“ – Dokument erweitert wird, sodass nicht mehr nur Konfigurations- und Wartungsinterfaces, sondern alle Interfaces des MANO-Systems (welche aus den Referenzpunkten hervorgehen) überprüft werden müssen.

### 5.3.2 Sicherheitsvoraussetzung 2

„The transmitter of a message shall provide means that will allow for the determination of any of modification, deletion, insertion, or replay has occurred.“ [40, S. 10]

Diese Sicherheitsvoraussetzung bedeutet, dass eine Maßnahme zum Integritätsschutz einer Nachricht, zum Beispiel mittels eines MAC, aktiviert ist.

In 33.117 gibt es mehrere Testfälle, welche das Vorhandensein von Integritätsschutz überprüfen. Jedoch lässt sich von diesen keiner explizit auf den Datenverkehr im MANO-System beziehen.

In Test 4.2.2.2.3.1 „Authorization token verification failure handling within one Public Land Mobile Network“ [36, S. 12] wird die Integrität eines Access Tokens geprüft, wenn ein Nutzergerät einen Netzwerkservice anfordert. Demnach wird sichergestellt, dass ein anfragender Nutzer zugangsberechtigt zum Netzwerkservice ist und keinen abgelaufenen, gefälschten oder sonstig invaliden Access Token verwendet. Ob Integritätsschutz bei einer gesendeten Nachricht über ein internes MANO-Interface aktiviert ist, lässt sich mit diesem Test jedoch nicht überprüfen.

In Test 4.2.3.3.5 „Network product Software integrity validation“ [36, S. 24] wird überprüft, ob die Integrität von zu installierenden/upgradenden Softwarepackages gewährleistet wird. Dieser Test lässt sich aber dementsprechend auch nicht auf die MANO-Sicherheitsvoraussetzung anwenden.

Weitere integritätsbezogene Tests werden in TS 33.117 nicht durchgeführt, es ist eine Lücke vorhanden. Demnach muss diese Sicherheitsvoraussetzung noch im „SCAS for MANO“ – Dokument behandelt werden.

### 5.3.3 Sicherheitsvoraussetzung 3

„The receiver of a message shall be able to determine if any of modification, deletion, insertion, or replay has occurred.“ [40, S. 10]

Während der Sender durch Voraussetzung 2 eine Möglichkeit zur Integritätsprüfung bereitstellen muss, wird in Voraussetzung 3 vorgeschrieben, dass der Empfänger der Nachricht deren Integrität entsprechend prüfen muss.

Da alle integritätsbezogenen Testfälle aus TS 33.117 bereits in Kapitel 5.3.2 beschrieben wurden und diese auch hier nicht zutreffend sind, ist eine Lücke vorhanden und auch diese Sicherheitsvoraussetzung muss noch im „SCAS for MANO“ – Dokument behandelt werden.

### 5.3.4 Sicherheitsvoraussetzung 4

„The VIM shall monitor stored images to determine if any unauthorized modification, deletion or insertion has occurred.“ [40, S. 10]

Dieser Testfall besagt, dass der VIM die Integrität der gespeicherten VM Images sicherstellen und überwachen muss. In Teilen wird diese Sicherheitsvoraussetzung durch drei Testfälle aus TS 33.117 abgedeckt.

Ein bereits erwähnter Testfall ist in 4.2.3.3.5 „Network product Software integrity validation“ [36, S. 24] festgehalten. Dieser Test verfolgt vier Schutzziele.

1. Jede Komponente, welche zertifiziert werden soll, muss eine Möglichkeit für einen Integritätscheck ihrer Software Packages / Images bereitstellen. Außerdem muss das Netzwerkprodukt eine Liste mit digitalen Signaturen oder Zertifikaten von autorisierten Softwarequellen (z. B. der Hersteller der Komponente) führen.
2. Beim Installieren und Upgraden der Softwarekomponente soll die Integrität des Software Packages überprüft werden. Zudem muss die Quelle des Updates / der Software in der Liste der autorisierten Softwarequellen enthalten sein.
3. Die Installation, die Ausführung oder das Upgrade muss abgelehnt werden, wenn die Integritäts- oder Herstellerprüfung fehlschlägt.
4. Mittels Access Control muss sichergestellt werden, dass nur autorisierte Nutzer Installationen und Updates einleiten sowie die Liste der Signaturen und Zertifikate modifizieren dürfen.

Der zweite, zutreffende Testfall ist in 4.2.3.2.1 – „Protecting data and information – general“ [36, S. 17] beschrieben.

Dieser Testfall ist ein genereller Sicherheitshinweis, dass Sicherheitsmaßnahmen zum Schutz sensitiver, gespeicherter Daten implementiert sein müssen. Abhängig von der Relevanz der Daten können zusätzliche Schutzmaßnahmen, über den Rahmen von TS 33.117 hinaus, getroffen werden. Dieser Sicherheitshinweis trifft auf die gespeicherten Software Images zu. Aufgrund der generellen Natur dieses Hinweises, der hohen Sicherheitsrelevanz der Images und da keine expliziten Testschritte für diesen Hinweis beschrieben sind, reicht dieser Testfall jedoch alleine nicht aus, um die Sicherheitsvoraussetzung 4 von NFV-SEC 014 zu erfüllen.

Der dritte, zutreffende Testfall ist in 4.2.3.2.3 – „Protecting data and information in storage“ [36, S. 18] festgehalten.

Dieser Testfall klingt zunächst sehr passend, da ein Teil seiner Beschreibung „[…] Files of a system that are needed for the functionality shall be protected against manipulation. […] [For] [s]tored files on the network product: Examples for protection against manipulation are the use of checksum or cryptographic methods“ lautet.

Jedoch wird bei der Durchführung der Testschritte nur geprüft, ob bei verschiedenen Passworteingaben (nach Änderung des Passworts), wenn von einem Nutzer auf den verknüpften Nutzeraccount-Speicher zugegriffen wird, realistische Werte für einen Ein-Wege-Hash ausgegeben werden.

Ob, wie in der MANO-Sicherheitsvoraussetzung gefordert, der Virtual Infrastructure Manager aber die Integrität der VM Images überwacht, lässt sich mit den Tests aus TS 33.117 nicht genau feststellen. Die durch den VIM gespeicherten Software Images sind nicht explizit als zu überwachendes Ziel und der VIM nicht explizit als überwachende Einheit definiert. Es ist eine Lücke vorhanden. Demnach muss diese Sicherheitsanforderung noch in einem MANO-spezifischen SCAS-Dokument getestet werden.

### 5.3.5 Sicherheitsvoraussetzung 5

„Data transferred over any internal interface of MANO shall be protected to prevent disclosure of data to unauthorized entities.“ [40, S. 10]

Diese Sicherheitsvoraussetzung besagt, dass die Vertraulichkeit des Datenverkehrs gewährleistet sein muss. Dies wird gebräuchlicher Weise mit einer Verschlüsselung des Datenverkehrs erzielt.

In TS 33.117 wird diese Voraussetzung durch Testfall 4.2.2.2.2 – „Protection at the transport layer“ [36, S. 11] abgedeckt.

In diesem Test ist festgelegt, dass alle Netzwerkfunktionen TLS unterstützen sollen. Dafür soll das TLS-Profil nach den Anweisungen aus Dokument TS 33.310 „Network Domain Security; Authentication Framework“ [52], Anhang E konfiguriert werden.

Aktiviertes TLS ist die korrekte Methode, um diese Sicherheitsvoraussetzung zu erfüllen. Jedoch muss ein weiterer Test durchgeführt werden, denn die Verschlüsselung kann deaktiviert sein, trotz aktiviertem und nach den Vorgaben konfigurierten TLS.

Der in 33.117 referenzierte Anhang E aus TS 33.310 verweist wiederum auf Dokument TS 33.210 „IP Layer Security“ [53], in welchem die TLS-Profile beschrieben sind. Im Profil für TLS 1.2 ist dabei festgelegt, dass die Liste der erlaubten Verschlüsselungen aus RFC 5246 der Internet Engineering Task Force (IETF) übernommen werden soll. [53, S. 18] In RFC 5246 ist jedoch die Möglichkeit der „Null Cipher“ enthalten. In diesem Verschlüsselungsmodus wird der Paketinhalt nicht verschlüsselt. [54, S. 21]

Aus diesem Grund ist Testfall 4.2.2.2.2 aus TS 33.117 alleine nicht ausreichend, um die MANO-Sicherheitsvoraussetzung zu erfüllen, da der Test bestanden werden kann (TLS ist aktiv), jedoch bei entsprechender TLS-Konfiguration die Daten weiterhin im Klartext übertragen werden.

Aus diesem Grund ist im MANO-spezifischen SCAS-Dokument ein weiterer Test für diese Sicherheitsvoraussetzung nötig. In diesem muss verifiziert werden, dass TLS-Verschlüsselung aktiv ist und gleichzeitig der Verschlüsselungsmodus von Paketen, die über interne MANO-Interfaces übertragen werden, nicht NULL ist.

### 5.3.6 Sicherheitsvoraussetzung 6

„Security events or alarms shall be recorded in an audit log sufficient to identify the impacted element, the time and location of the event, and the outcome of the event. The severity of the event shall be noted and for severe events the impacted element shall be isolated and where practical excluded from any further activity.“ [40, S. 10]

Diese Sicherheitsvoraussetzung wird durch den Testfall 4.2.3.6.1 - „Security event logging“ [36, S. 45] behandelt, muss jedoch in einem MANO-spezifischen Dokument noch ergänzt werden.

Es wird vorgeschrieben, dass Security Events zusammen mit Zeitstempel und einer einzigartigen Referenz, um das betroffene Element zu identifizieren, gespeichert werden müssen. Des Weiteren können für jedes Event zusätzliche Informationen im Log festgehalten werden.

Diese umfassen:

- Nutzername
- Ausgeführte Aktion
- Ergebnis des Events
- Länge der Session
- Überschrittene oder erreichte Werte

Eine Diskrepanz des geforderten Logging-Inhalts von NFV-SEC 014 und dem Test aus TS 33.117 besteht darin, dass die Sicherheitsvoraussetzung aus NFV-SEC 014 das Ergebnis des Events als notwendig zu loggen definiert. Im Test aus TS 33.117 ist diese Information mit „and/or“ enthalten und muss somit nicht zwingend aufgezeichnet werden.

In einem MANO-spezifischen SCAS-Dokument müsste somit eine Präzisierung des Test 4.2.3.6.1 aus TS 33.117 vorgenommen werden, sodass das Ergebnis des Events nicht mehr optional, sondern immer aufgezeichnet werden muss. Zudem muss im MANO-spezifischen Test die Schwere des Ergebnisses geloggt werden, was im Test aus TS 33.117 nicht erfolgen muss.

Dafür wurden von ETSI in Dokument GS NFV-SOL 009 sechs Stufen der Schwere eines Sicherheitsvorfalls (CRITICAL, MAJOR, MINOR, WARNING, INDETERMINATE, CLEARED) definiert. [55, S. 147]

Der zweite Teil der Sicherheitsvoraussetzung, bezüglich der Schwere des Sicherheitsvorfalls, benötigt für eine konkrete Testformulierung jedoch noch eine Präzisierung, da momentan nicht klar definiert ist, ab welcher der sechs Stufen ein Vorfall als „severe“ eingestuft wird und demnach isoliert werden muss.

Diese Einstufung sowie die Isolierung von Komponenten mit schweren Sicherheitsvorfällen muss nach entsprechender Klarstellung auch in einem MANO-spezifischen Test überprüft werden.

### 5.3.7 Sicherheitsvoraussetzung 7

„The MANO system shall allow instantiation of MANO components and managed entities, the NFVIs, only at explicit geographic locations.“ [40, S. 10]

Diese Aussage wird im Laufe des Dokuments konkretisiert und soll auf zweierlei Arten die Sicherheit von MANO verbessern.

Erstens soll der geografische Standort bei der Anmeldung als ein Faktor der Multi-Faktor-Authentifizierung genutzt werden, sofern das Konto der Anmeldung Zugriffsrechte auf das MANO-System besitzt.

Zweitens muss bei der Erzeugung von NFVIs sowie MANO-Komponenten der Standort des Datencenters verifiziert werden, da die Standorte der eingesetzten Datencenter bekannt sind.

Relevante Tests zur Authentifizierung von Nutzern in TS 33.117 sind in Testgruppe 4.2.3.4 – „Authentication and authorization“ [36, S. 26] enthalten, der Standort des Nutzers wird dabei jedoch in keinem Test erwähnt. Außerdem wird auf den Standort eines Datencenters in keinem Test Bezug genommen.

Aus diesem Grund ist diese Sicherheitsvoraussetzung in einem MANO-spezifischen SCAS-Dokument zu überprüfen.

### 5.3.8 Sicherheitsvoraussetzung 8

„Relying parties shall not allow any actions from received data before successfully identifying and verifying the location of the relied upon party.“ [40, S:10]

Diese Sicherheitsvoraussetzung ist als eine Erweiterung zu Voraussetzung 1 (siehe Kapitel 5.3.1) zu sehen. Miteinander kommunizierende Komponenten des MANO-Systems müssen sich laut Voraussetzung 1 gegenseitig authentifizieren und eingehende Aktionen ablehnen, bis der Sender verifiziert ist.

Laut Voraussetzung 8 soll dabei nun auch der Ort des Kommunikationspartners verifiziert werden. Dafür relevante Tests aus TS 33.117 wurden bereits in Kapitel 5.3.1 vorgestellt. Da in diesen Tests auf den Standort für die Verifikation kein Bezug genommen wird und dieser auch in weiteren Tests nicht enthalten ist, muss Sicherheitsvoraussetzung 8 in einem MANO-spezifischen SCAS-Dokument noch getestet werden.

# 6 Entwurf eines SCAS-Tests für MANO

Wie aus dem Vergleich der Bedrohungsanalyse ersichtlich wird, ist von acht MANO-spezifischen Sicherheitsvoraussetzungen keine einzige in Gänze durch das TS 33.117 „General Requirements“ – SCAS-Dokument abgedeckt. Für alle acht Sicherheitsvoraussetzungen müssen im MANO for SCAS-Dokument noch Tests formuliert werden.

Exemplarisch wird in diesem Kapitel ein Testentwurf vorgestellt, mit welchem sich die noch zu testende Sicherheitsvoraussetzung 4 überprüfen lässt.

*Voraussetzung 4: „The VIM shall monitor stored images to determine if any unauthorized modification, deletion or insertion has occurred.“* [40, S. 10]

Da alle SCAS-Tests nur in englischer Sprache veröffentlicht werden, wurde der Testentwurf ebenfalls auf Englisch formuliert. Formatierung und Aufbau orientieren sich ebenso an bestehenden Tests.

## 6.1 Testentwurf

*Requirement Name:* MANO VIM image integrity monitoring

*Requirement Reference:* GS NFV-SEC 014 [40], clause 5.2.c.1.1.4

*Requirement Description:*

The Virtualised Infrastructure Manager must monitor the stored software images to ensure their integrity. The integrity of the image must be ensured before running it. This allows to determine whether images have been modified, deleted or inserted without authorisation, as stated in [40, clause 5.2.c.1.1.4 and clause 6].

*Threat References*: GS NFV-SEC 014 [40], clause 5.2.a.4

*Test Case:*

**Test Name**:

TC _INT_IMAGE_MONITORING_VIM_MANO

**Purpose**:

Verify that stored software images are integrity protected.

**Pre-Conditions**:

The tester has access to the documentation of the VIM.

Test environment with a configured VIM.

Access to the stored software images and logfiles.

**Execution Steps**:

**Test Case A:**

1. Check that the documentation from the vendor describes that the VIM monitors the integrity of stored images.
2. Start an unmodified VNF.
3. Check the log of the VIM to see if a change in the software image has been detected.

**Test Case B:**

1. Edit, insert or delete a VNF.
2. Try to start the affected VNF.
3. Check the log of the VIM to see if a change in the software image has been detected.

**Expected Results**:

**Test Case A:**

No modification, deletion or insertion was detected. The integrity of the software image is confirmed by a debug output. The VNF starts up normally.

**Test Case B:**

The modification, deletion or insertion was detected and the integrity violation was recorded in the log. The VNF does not start.

**Expected format of evidence**:

Screenshot of the documentation or a comparable statement from the manufacturer as to whether and how the integrity of the images is checked.

Screenshot of the log of the VIM.

## 6.2 Beispielhafte Evaluierung von OpenStack (MicroStack)

OpenStack wurde als Beispiel-VIM für diese Arbeit ausgewählt, da es im Gegensatz zu den meisten anderen VIMs kostenfrei verfügbar und weit verbreitet ist. OpenStack ist jedoch auf Serverbetrieb ausgelegt, was mit hohen Systemvoraussetzungen einhergeht.

Aus diesem Grund wurde für die Recherche in dieser Arbeit MicroStack statt OpenStack verwendet. MicroStack ist eine ebenso von Canonical entwickelte Distribution von OpenStack, welche lokal und in einer virtuellen Maschine installiert werden kann. Es ist eine Mikro-Cloud-Plattform, die auf den Betrieb auf einem Knoten ausgelegt ist. MicroStack stellt die gleichen Grundfunktionalitäten und Services wie OpenStack zur Verfügung, die Installation wird jedoch durch die Auslieferung als Snap-Paket stark vereinfacht und die Komplexität und der Optionsumfang von OpenStack reduziert. [56]

Zur Durchführung des Tests wurde MicroStack nach Herstelleranleitung in einer virtuellen Maschine mit Linux Ubuntu 22.04.1 LTS installiert und konfiguriert. Der VM wurden zwei Prozessorkerne mit 3.90 GHz, 8 GB Arbeitsspeicher sowie 100 GB Festplattenspeicher zugewiesen.

Im Aufbau von OpenStack sind zwei Module für den Testfall relevant:

- „Glance“ ist der Image Service von OpenStack. Dieser Service speichert und verwaltet Software Images der virtuellen Maschinen. [57]
- „Nova“ nutzt die von Glance bereitgestellten Images, um Instanzen der virtuellen Maschinen zu erzeugen. [58]

In der Dokumentation von OpenStack ist eine der Sicherheitsvoraussetzung entsprechende Methode beschrieben, durch welche die gespeicherten Images signiert und bei Bedarf die Signaturen der Images verifiziert werden können.

Die digitale Signierung der Images wird dabei von Glance mittels asymmetrischer Verschlüsselung durchgeführt. Voraussetzung dafür ist, dass das Schlüsselverwaltungstool „Barbican“ installiert ist und in Barbican ein Zertifikat, welches mit dem privaten Schlüssel signiert wurde, hinterlegt ist. [59]

Jedes Image kann nun signiert werden. Bevor ein signiertes Image in Glance geladen wird, wird die Signatur mittels des Zertifikats aus Barbican verifiziert. Schlägt die Verifizierung fehl, wird der Upload unterbunden und das Image wird gelöscht. [60] Somit wird die Integrität von gespeicherten, signierten Images gewährleistet. Parallel dazu besitzt Nova eine Funktion, mit welcher es die Signatur von Glance verifiziert, bevor es eine Instanz erzeugt, neu startet oder wiederherstellt. [61]

Mit diesen aktivierten Optionen wäre die MANO-Sicherheitsvoraussetzung erfüllt, da in Glance gespeicherte Images signiert sind und die Signatur vor Instanziierungen, Neustarts, etc. jedes Mal von Nova verifiziert wird. Die Integrität verwendeter Software Images wird somit gewährleistet.

Jedoch ist dabei eine wichtige Einschränkung vorhanden: Die soeben beschriebene Signierung und Verifizierung von Software Images ist in OpenStack standardmäßig deaktiviert.

Der benötigte Key Manager Barbican ist bei der Installation von OpenStack noch nicht enthalten, sondern muss nachträglich installiert und konfiguriert werden. [59] Außerdem müssen die entsprechenden Optionen in den Konfigurationsdateien erst aktiviert werden, der Standardwert der Variable beträgt „False“ (siehe Abbildung 11).

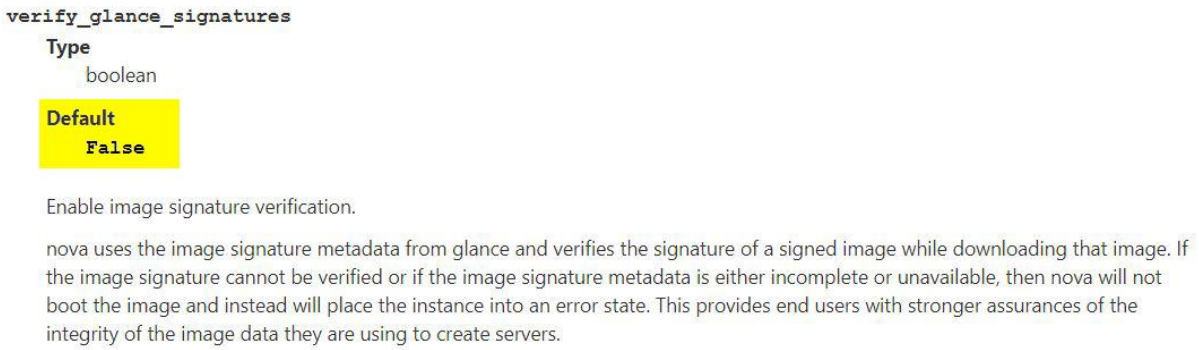


**Abbildung 11: OpenStack Nova-Dokumentation [62], Eigener Screenshot, eingefärbt.**

In der vorgeschlagenen Standardkonfiguration von OpenStack ist es demnach möglich, ohne Signatur des Images eine Instanz dessen zu erzeugen (siehe Abbildung 12).

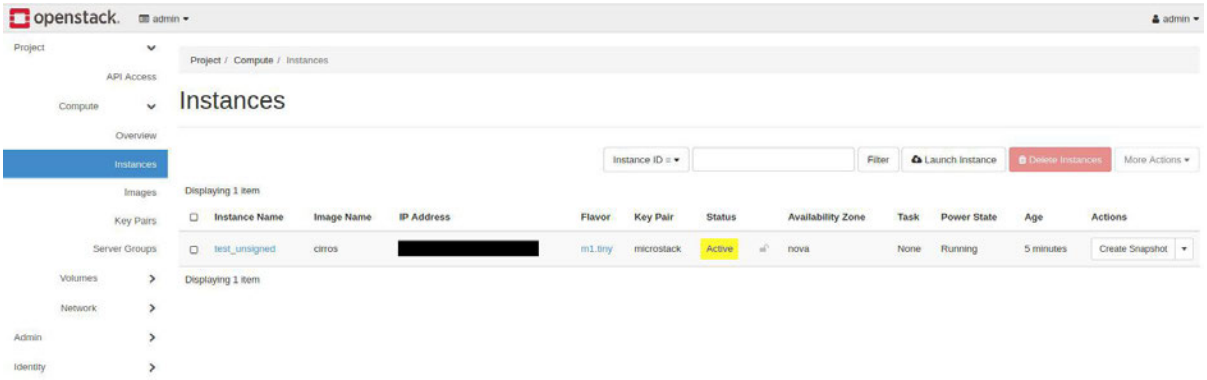


**Abbildung 12: Eine VM-Instanz kann ohne aktivierte Signatur gestartet werden, Eigener Screenshot aus MicroStack / OpenStack.**

OpenStack veröffentlichte zudem einen Security Guide, in welchem Empfehlungen für Maßnahmen zum Integritätsschutz vorgestellt werden. [63] Die Anwendung der Empfehlungen ist jedoch keine Pflicht.

Zusammenfassend lässt sich festhalten: Sofern eine zu zertifizierende MANO-Komponente OpenStack als VIM verwendet, besteht diese nur dann den Testfall, wenn die Signierungsfunktion immer aktiviert sein muss. Wird OpenStack in Standard-Konfiguration verwendet, ist der Testfall nicht erfüllt, da die Image-Signatur standardmäßig deaktiviert ist.

Für den Modifizierungs-Testschritt (Test Case B) ist der Speicherort der Software Images und der Logfiles relevant. Der Speicherort der Images kann variieren, der Pfad ist jedoch in Datei */etc/glance/glance.conf* im Attribut *filesystem_store_datadir* festgehalten. Standardmäßig wird der Pfad */var/lib/glance/images/* verwendet. Die Logdateien vom Glance-Image-Service sind unter */var/log/glance/* verfügbar.

Diese weitere Beispiel-Durchführung des Testentwurfs wird allerdings als „for further study“ erklärt, da der Installations- und Konfigurationsprozess von Barbican, der dafür benötigten Datenbank, des Keystone-Accountmanagers sowie des Glance-Managers den zeitlichen Rahmen der Bachelorarbeit überschreiten würde. Um die weiteren Testschritte durchführen zu können, wäre die vollständige Einrichtung der Signatur-Funktion erforderlich.

Neben der Vervollständigung der beispielhaften Durchführung, haben sich im Verlauf der Anfertigung dieser Arbeit weitere Aspekte aufgetan, die eine vollumfängliche und abschließende Erarbeitung der Sicherheitsbetrachtung der MANO-Komponente verhindert haben – wie in Kapitel 4.1 bereits erwähnt. Diese sind im nächsten Kapitel genauer dargelegt.

# 7 Future Work / Ausblick

Ein vollständiger Abschluss des Themas ist zum Zeitpunkt der Fertigstellung der Arbeit noch nicht möglich, da sich Work Items „DGS/NFV-SEC 024 – NFV Security Management“ und „DGS/NFV-SEC 025 – Secure End-to-End VNF and NS Management Specification“ noch im Entwurfsstadium befinden und inhaltlich nicht zitiert werden dürfen – lediglich, dass es sich um ein „work in progress“-Item handelt.

Im Zeitplan der Work Items sind jedoch Verzögerungen aufgetreten. Beide hätten vor Ende der Bearbeitungszeit dieser Arbeit bereits publiziert werden sollen, müssen jedoch noch mehrere Schritte bis zur Veröffentlichung durchlaufen:

- Dokument NFV-SEC 024 hätte am 14.08.2022 veröffentlicht werden sollen, befindet sich jedoch noch im „Early Draft“-Status. Der aktuellste Entwurf (v0.0.6) wurde am 27.04.2021 veröffentlicht.
- Dokument NFV-SEC 025 hätte am 09.09.2022 veröffentlicht werden sollen, befindet sich aber ebenso noch im „Early Draft“-Status. Der aktuellste Entwurf (v0.0.13) wurde am 25.08.2022 veröffentlicht.

Für die Sicherheitsbetrachtung und Erstellung von SCAS-Tests sind die veröffentlichten Fassungen der beiden Dokumente von zentraler Bedeutung, weswegen diese als die drei Referenzdokumente für die Erstellung des offiziellen „SCAS for MANO“ – Dokuments markiert sind. Ohne Zugriff auf die fertigen Dokumente kann diese Arbeit das Thema nicht vollständig abdecken.

Das Dokument NFV-SEC 024 wird bei Veröffentlichung das Dokument NFV-SEC 013 ersetzen und erweitern. Dies könnte zur Folge haben, dass Kapitel 3 dieser Arbeit (zumindest in Teilen) hinfällig wird, da Kapitel 3 zu großen Teilen auf NFV-SEC 013 basiert. Da NFV-SEC 024 momentan noch nicht referenziert werden darf, ein Grundverständnis des Themas jedoch wichtig ist, wurde das Kapitel trotz der baldigen, potentiellen Obsoleszenz in diese Arbeit aufgenommen. Für Aktualität des Informationsstands ist ein Verfolgen der beiden Work Items nahegelegt und ab Veröffentlichung zwingend erforderlich.

Zum Verfolgen der Entwicklung und potentiell geplanten Änderungen sind die Entwürfe der Dokumente öffentlich auf der Website von ETSI bereitgestellt. [33, 41]

Nach Veröffentlichung der Spezifikationen NFV-SEC 024 sowie NFV-SEC 025 müssen Lücken zwischen Sicherheitsimplikationen dieser, den Voraussetzungen aus NFV-SEC 014 und den Tests aus dem “General Requirements” - SCAS Dokument in einem „SCAS for MANO” - Dokument geschlossen werden.

# 8 Fazit

Eine große Neuerung in der fünften Generation der Mobilfunknetze ist die cloudbasierte Architektur und die damit einhergehende Virtualisierung von Netzwerkfunktionen. Aufgrund dessen können Netzwerkfunktionen deutlich schneller instanziiert, konfiguriert, skaliert sowie terminiert werden. Um diese dynamischen Netzwerkanpassungen automatisiert durchführen zu können, ist die Einführung einer Management- und Orchestrierungskomponente (MANO) notwendig. Diese weist den Netzwerkfunktionen die entsprechenden virtualisierten Netzwerkressourcen zu und skaliert die Leistung und Kapazität der Netzwerkfunktionen.

Diese wichtige Aufgabe geht jedoch gleichermaßen mit einer hohen Sicherheitsrelevanz einher, da eine Kompromittierung der MANO-Komponente effektiv das gleiche für sämtliche virtuellen Netzwerkfunktionen bedeuten würde.

Für einen Überblick und ein Verständnis der MANO-Komponente wurden in dieser Arbeit zunächst theoretische Grundlagen, Architektur und Funktionsweise von Network Function Virtualization und MANO zusammengefasst und erläutert. Das Management von virtuellen Sicherheitsfunktionen wurde im NFV-MANO Framework eingeordnet.

Anschließend wurde ein Überblick über die aktuelle Entwicklung des „SCAS for MANO“ – Dokuments gegeben sowie die Umsetzung der MANO-Zertifizierung mittels NESAS bewertet. Zur Erstellung des „SCAS for MANO“ – Dokuments herangezogene Spezifikationen wurden analysiert und die Ergebnisse der ETSI-Risikoanalyse erläutert. Zwei relevante Spezifikationen befinden sich jedoch noch in der Entwurfsphase und dürfen noch nicht inhaltlich zitiert werden.

Um festzustellen, welche der acht in der ETSI-Risikoanalyse festgestellten Sicherheitsvoraussetzungen noch in einem MANO-spezifischen SCAS-Dokument überprüft werden müssen, wurde das Ergebnis einer im Rahmen dieser Arbeit durchgeführten Gap-Analyse vorgestellt. Bei dieser wurde jede einzelne Sicherheitsvoraussetzung mit bereits existierenden Tests im „General Requirements“ – Dokument verglichen und geschlussfolgert, ob durch diese Tests die Sicherheitsvoraussetzung erfüllt ist oder ob diese noch nicht gänzlich überprüft wird.

Dadurch konnte gezeigt werden, dass von den acht Sicherheitsvoraussetzungen keine einzige bereits durch das „General Requirements“ – Dokument vollständig abgedeckt wird. Bei allen Voraussetzungen ist eine Diskrepanz vorhanden. Alle acht Sicherheitsvoraussetzungen müssen demnach im „SCAS for MANO“ – Dokument noch beachtet und überprüft werden.

Abschließend wurde eine der Sicherheitsvoraussetzungen mit Diskrepanz ausgewählt und ein Vorschlag für einen Testfall erarbeitet, mit welchem die Sicherheitsvoraussetzung überprüft werden kann sowie der Test am Beispiel von OpenStack erörtert.

# Literatur


[1] Bundesnetzagentur. „Bundesnetzagentur veröffentlicht Netzabdeckung mit 5G“. Bundesnetzagentur. Verfügbar unter: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2021/20211209_5GMonitoring.html (Zugriff am: 23. September 2022). [Online].

[2] European Telecommunications Standards Institute. „5G“. ETSI. Verfügbar unter: https://www.etsi.org/technologies/5G (Zugriff am: 25. September 2022). [Online].

[3] Bundesnetzagentur, „Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten - Liste der kritischen Funktionen nach § 109 Abs. 6 Satz 1 Nr. 2 TKG für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial“, August 2021. Verfügbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/ListekritischeFunktionen.pdf?__blob=publicationFile&v=3 (Zugriff am: 19. August 2022). [Online].

[4] M. Zolanvari, „SDN for 5G“, Oktober 2015. Verfügbar unter: https://www.cse.wustl.edu/~jain/cse570-15/ftp/sdnfor5g.pdf (Zugriff am: 22. Juli 2022). [Online].

[5] A. Maleki, et al., „An SDN Perspective to Mitigate the Energy Consumption of Core Networks“, Leeds, September 2017. Verfügbar unter: https://www.researchgate.net/publication/319876305_An_SDN_Perspective_to_Mitigate_the_Energy_Consumption_of_Core_Networks_-_GEANT2 (Zugriff am: 2. August 2022). [Online].

[6] C.-S. Li und W. Liao, „Software defined networks [Guest Editorial]“, *IEEE Communications Magazine*, Bd. 51, S. 113, 14. Februar

2013. Verfügbar unter: https://doi.org/10.1109/mcom.2013.6461194 (Zugriff am: 31. August 2022). [Online].

[7] D. Kreutz, et al., „Software-Defined Networking: A Comprehensive Survey“, IEEE, 2014. Verfügbar unter: https://arxiv.org/pdf/1406.0440.pdf (Zugriff am: 31. August 2022). [Online].

[8] European Telecommunications Standards Institute. „Network Functions Virtualisation“. ETSI. https://www.etsi.org/technologies/nfv (Zugriff am: 12. August 2022). [Online].

[9] Apis Training. NFV MANO Webinar. (22. Mai 2017). Verfügbar unter: https://www.youtube.com/watch?v=Sqpk37wKAh8 (Zugriff am: 13. August 2022). [Online-Video].

[10] Nokia. „Nokia confirms 5G as 90 percent more energy efficient“, Dezember 2020. Nokia. Verfügbar unter: https://www.nokia.com/about-us/news/releases/2020/12/02/nokia-confirms-5g-as-90-percent-more-energy-efficient/ (Zugriff am: 13. August 2022). [Online]

[11] *Network Functions Virtualisation (NFV); Architectural Framework*, GS NFV 002 v1.2.1, European Telecommunications Standards Institute, 2014. Verfügbar unter: https://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.02.01_60/gs_nfv002v010201p.pdf (Zugriff am: 30. September 2022). [Online].

[12] B. Chatras und D. U. Rauschenbach, „ETSI NFV Architecture & Interfaces“, Vortrag, Oktober 2016. Verfügbar unter: https://docbox.etsi.org/ISG/NFV/Open/other/Tutorials/201610-Tutorials-SDN_World_Congress-The_Haque/NFVIFA(16)0001303r5-ETSI_NFV_SDNWorldCongress_Tutorial_IFA_VNF_LCM.pdf (Zugriff am: 23. September 2022). [Online].

[13] *Network Functions Virtualisation (NFV); Use Cases*, GR NFV 001 v1.3.1, European Telecommunications Standards Institute, 2021. Verfügbar unter: https://www.etsi.org/deliver/etsi_gr/NFV/001_099/001/01.03.01_60/gr_NFV001v010301p.pdf (Zugriff am:

16. September 2022). [Online].

[14] *5G; System architecture for the 5G System (5GS)*, TS 123 501, European Telecommunications Standards Institute, 2020. Verfügbar unter: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.06.00_60/ts_123501v160600p.pdf (Zugriff am: 4. Oktober 2022). [Online].

[15] C. Flemming. „Set-Top-Box mit Smart TV: Deshalb lohnt sich ein Zusatzgerät“. Vodafone, 2022. https://www.vodafone.de/featured/tv-entertainment/set-top-box-mit-smart-tv-gruende-fuer-zusatzgeraet/#/ (Zugriff am 10. August 2022). [Online].

[16] T. Nguyenphu, „VNF Descriptor (VNFD) & VNF Package Overview“, Vortrag, April 2018. Verfügbar unter: https://docbox.etsi.org/ISG/NFV/Open/other/Tutorials/201805-Tutorials-NFV_World_Congress_San_Jose/RX14559_Layer123%20NFV_ZeroTouch_WC_April2018_VNFD_VNFPackage.pdf (Zugriff am: 27. August 2022). [Online].

[17] *Management and Orchestration; Network Service Templates Specification*, GS NFV-IFA 014 v4.2.1, European Telecommunications Standards Institute, 2021. Verfügbar unter: https://docbox.etsi.org/isg/nfv/open/Publications_pdf/Specs-Reports/NFV-IFA%20014v4.2.1%20-%20GS%20-%20Network%20Service%20Templates%20Spec.pdf (Zugriff am: 10. Oktober 2022). [Online].

[18] *Management and Orchestration; Report on Management and Orchestration Framework*, GR NFV-MAN 001 v1.2.1, European Telecommunications Standards Institute, 2021. Verfügbar unter: https://www.etsi.org/deliver/etsi_gr/NFV-MAN/001_099/001/01.02.01_60/gr_NFV-MAN001v010201p.pdf (Zugriff am: 12. Oktober 2022). [Online].

[19] *Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification*, GS NFV-IFA 005 v4.2.1, European Telecommunications Standards Institute, 2021. Verfügbar unter: https://docbox.etsi.org/isg/nfv/open/Publications_pdf/Specs-Reports/NFV-IFA%20005v4.2.1%20-%20GS%20-%20Or-Vi%20%20ref%20point%20Spec.pdf (Zugriff am: 15. September

2022). [Online].

[20] *Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification*, GS NFV-IFA 006 v3.5.1, European Telecommunications Standards Institute, 2021. Verfügbar unter: https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/006/03.05.01_60/gs_NFV-IFA006v030501p.pdf (Zugriff am: 15. September 2022). [Online].

[21] *Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification*, GS NFV-IFA 007 v3.5.1, European Telecommunications Standards Institute, 2021. Verfügbar unter: https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/007/03.05.01_60/gs_NFV-IFA007v030501p.pdf (Zugriff am: 15. September 2022). [Online].

[22] J. Sathyan, *Fundamentals of EMS, NMS and OSS/BSS*. New York: Auerbach Publications, 2013. Verfügbar unter: https://doi.org/10.1201/b15748 (Zugriff am: 18. September 2022). [Online].

[23] *M.3400 : TMN management functions*, M.3400 (02/00), ITU, 2007. Verfügbar unter: https://www.itu.int/rec/T-REC-M.3400/en (Zugriff am: 18. September 2022). [Online].

[24] *Management and Orchestration; Os-Ma-Nfvo reference point - Interface and Information Model Specification*, GS NFV-IFA 013 V2.7.1, European Telecommunications Standards Institute, 2019. Verfügbar unter: https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/013/02.07.01_60/gs_NFV-IFA013v020701p.pdf (Zugriff am: 15. September 2022). [Online].

[25] *Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification*, GS NFV-IFA 008 v4.2.1, European Telecommunications Standards Institute, 2021. Verfügbar unter: https://docbox.etsi.org/isg/nfv/open/Publications_pdf/Specs-Reports/NFV-IFA%20008v4.2.1%20-%20GS%20-%20Ve-Vnfm%20ref%20point%20Spec.pdf (Zugriff am: 15. September 2022). [Online].

[26] *Management and Orchestration; Report on Architectural Options*,

GS NFV-IFA 009 v1.1.1, European Telecommunications Standards Institute, 2016. Verfügbar unter: https://www.etsi.org/deliver/etsi_gs/nfv-ifa/001_099/009/01.01.01_60/gs_nfv-ifa009v010101p.pdf (Zugriff am: 17. September 2022). [Online].

[27] „Open Source MANO“. ETSI OSM. https://osm.etsi.org/ (Zugriff am 19. September 2022). [Online].

[28] „Open Source MANO 6.0 documentation“. ETSI OSM. https://osm.etsi.org/docs/user-guide/latest/01-quickstart.html#adding-vim-accounts (Zugriff am 19. September 2022). [Online].

[29] „How to Set Up Virtual Infrastructure Managers (VIMs) - Open Source MANO 6.0 documentation“. ETSI OSM. https://osm.etsi.org/docs/user-guide/latest/04-vim-setup.html#what-if-i-do-not-have-a-vim-at-hand-use-of-sandboxes (Zugriff am 20. September 2022). [Online].

[30] „Canonical Charmed OSM, NFV management and orchestration platform“. Canonical Charmed OSM. https://charmed-osm.com/ (Zugriff am 20. September 2022). [Online].

[31] *Security; Security Management and Monitoring specification*, GS NFV-SEC 013 v3.1.1, European Telecommunications Standards Institute, 2017. Verfügbar unter: https://www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/013/03.01.01_60/gs_nfv-sec013v030101p.pdf (Zugriff am: 1. September 2022). [Online].

[32] *Management and Orchestration; Architecture enhancement for Security Management Specification*, GS NFV-IFA 026 v3.4.1, European Telecommunications Standards Institute, 2020. Verfügbar unter: https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/026/03.04.01_60/gs_NFV-IFA026v030401p.pdf (Zugriff am: 1. September 2022). [Online].

[33] *Security Management Specification*, DGS/NFV-SEC024 Work Item, European Telecommunications Standards Institute. Verfügbar unter: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58648 (Zugriff am: 4. September

2022). [Online].

[34] GSM Association. „GSMA Network Equipment Security Assurance Scheme (NESAS)“. GSMA. https://www.gsma.com/security/network-equipment-security-assurance-scheme/ (Zugriff am 5. September 2022). [Online].

[35] Bundesamt für Sicherheit in der Informationstechnik. „Zertifizierung nach NESAS CCS-GI“. BSI. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-NESAS/NESAS-CCS-GI_node.html (Zugriff am 5. September 2022). [Online].

[36] *Catalogue of general security assurance requirements*, TS 33.117, 3GPP, 2021. Verfügbar unter: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2928 (Zugriff am: 12. September 2022). [Online].

[37] *5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)*, TS 33.512, 3GPP, 2022. Verfügbar unter: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3445 (Zugriff am: 12. September 2022). [Online].

[38] *Security Assurance Specification (SCAS) for NFV-MANO, SCAS for MANO*, DGS/NFV-SEC028' Work Item, European Telecommunications Standards Institute. Verfügbar unter: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=66802 (Zugriff am: 13. Oktober 2022). [Online].

[39] *'DGS/NFV-SEC028' Work Item Schedule*, DGS/NFV-SEC028, European Telecommunications Standards Institute. Verfügbar unter: https://portal.etsi.org/eWPM/index.html#/schedule?WKI_ID=66802 (Zugriff am: 13. September 2022). [Online].

[40] *NFV Security; Security Specification for MANO Components and Reference points*, GS NFV-SEC 014 v3.1.1, European Telecommunications Standards Institute, 2018. Verfügbar unter: https://

www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/014/03.01.01_60/gs_nfv-sec014v030101p.pdf (Zugriff am: 9. September 2022). [Online].

[41] *Secure End-to-End VNF and NS management specification*, 'DGS/NFV-SEC025' Work Item, European Telecommunications Standards Institute. Verfügbar unter: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59208 (Zugriff am: 4. September 2022). [Online].

[42] ONF. „XOS“. Open Networking Foundation. https://opennetworking.org/xos/ (Zugriff am 17. September 2022). [Online].

[43] Mirantis. „A review of OSM, Open-O, CORD, and Cloudify“. Mirantis. https://www.mirantis.com/blog/which-nfv-orchestration-platform-best-review-osm-open-o-cord-cloudify/ (Zugriff am 18. September 2022). [Online].

[44] Rakuten. „Edge Cloud“. Rakuten Symphony. https://symphony.rakuten.com/edge-cloud (Zugriff am 18. September 2022). [Online].

[45] Robin. „Robin Multi Data Center Automation Platform (MDCAP)“. Robin. https://www.robin.io/robin-multi-data-center-automation-platform-mdcap/ (Zugriff am 16. September 2022). [Online].

[46] Robin und H. Cheviry, „Unified orchestration and lifecycle automation for end-to-end 5G deployment“, 22. Juni 2021. Verfügbar unter: https://www.robin.io/blog/unified-orchestration-and-lifecycle-automation-for-end-to-end-5g-deployment/ (Zugriff am: 17. September 2022). [Online].

[47] Robin, „Designing Multi-access Edge Compute(MEC) Platforms“, 10. August 2021. Verfügbar unter: https://www.robin.io/white-paper/designing-multiacess-edge-compute-platforms/ (Zugriff am: 17. September 2022). [Online].

[48] European Union Agency for Cybersecurity, „NFV Security in 5G - Challenges and Best Practices“, Februar 2022. Verfügbar un-

ter: https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices (Zugriff am: 7. Oktober 2022). [Online].

[49] *Information security management*, ISO/IEC 27001, ISO. Verfügbar unter: https://www.iso.org/isoiec-27001-information-security.html (Zugriff am: 28. September 2022). [Online].

[50] X. Fu, B. Graham, D. Xuan, R. Bettati und W. Zhao, *Empirical and Theoretical Evaluation of Active Probing Attacks and Their Countermeasures*. Berlin, Heidelberg: Springer, 2004. Verfügbar unter: https://doi.org/10.1007/978-3-540-30114-1_19 (Zugriff am: 24. September 2022). [Online].

[51] H. Saljooghinejad und W. N. Bhukya, *Layered Security Architecture for Masquerade Attack Detection*. Springer, 2012. Verfügbar unter: https://doi.org/10.1007/978-3-642-31540-4_19 (Zugriff am: 24. September 2022). [Online].

[52] *Network Domain Security (NDS); Authentication Framework (AF)*, TS 33.310, 3GPP, 2022. Verfügbar unter: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2293 (Zugriff am: 25. September 2022). [Online].

[53] *Network Domain Security (NDS); IP network layer security*, TS 33.210, 3GPP, 2022. Verfügbar unter: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279 (Zugriff am: 25. September 2022). [Online].

[54] *The Transport Layer Security (TLS) Protocol Version 1.2*, RFC 5246, IETF, 2008. Verfügbar unter: https://www.ietf.org/rfc/rfc5246.txt (Zugriff am: 25. September 2022). [Online].

[55] *Protocols and Data Models; RESTful protocols specification for the management of NFV-MANO*, GS NFV-SOL 009 v3.3.1, European Telecommunications Standards Institute, 2019. Verfügbar unter: https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/009/03.03.01_60/gs_nfv-sol009v030301p.pdf (Zugriff am: 25. September 2022). [Online].

[56] Canonical. „MicroStack -OpenStack for the edge, micro clouds and developers“. microstack.run. https://microstack.run/ (Zugriff am 7. Oktober 2022). [Online].

[57] OpenStack. „Glance documentation v25.0.0.0rc2.dev2“. OpenStack Docs. https://docs.openstack.org/glance/zed/ (Zugriff am 10. Oktober 2022). [Online].

[58] OpenStack. „Nova documentation v26.0.0.0rc2.dev3“. OpenStack Docs. https://docs.openstack.org/nova/zed/ (Zugriff am 10. Oktober 2022). [Online].

[59] OpenStack. „Install and configure - Barbican v15.0.0.0rc3.dev1 documentation“. OpenStack Docs. https://docs.openstack.org/barbican/zed/install/install.html (Zugriff am 11. Oktober 2022). [Online].

[60] OpenStack. „Image Signature Verification - Glance v25.0.0.0rc2.dev2“. OpenStack Docs. https://docs.openstack.org/glance/zed/user/signature.html (Zugriff am 13. Oktober 2022). [Online].

[61] OpenStack. „Image Signature Certificate Validation - Nova v26.0.0.0rc2.dev3“. OpenStack Docs. https://docs.openstack.org/nova/zed/user/certificate-validation.html (Zugriff am 13. Oktober 2022). [Online].

[62] OpenStack. „Configuration Options - verify_glance_signatures - Nova v26.0.0.0rc2.dev3“. OpenStack Docs. https://docs.openstack.org/nova/zed/configuration/config.html#glance.verify_glance_signatures (Zugriff am 13. Oktober 2022). [Online].

[63] OpenStack. „Integrity life-cycle - Security Guide“. OpenStack Docs. https://docs.openstack.org/security-guide/management/integrity-life-cycle.html (Zugriff am 13. Oktober 2022). [Online].

Abbildungsreferenzen:

Abb. 1-8,10: Eigene Abbildung, Quellen entsprechend referenziert.

Abb. 9: Offizielle Robin MDCAP Architektur, [47 S. 6], modifiziert.

Abb. 11: Eigener Screenshot, Quelle entsprechend referenziert.

Abb. 12: Eigener Screenshot aus MicroStack / OpenStack. [56]

# Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mittweida, den 17. Oktober 2022

Eric Sabitzer