

Technology Enablers for 5G Networks – NFV Perspective

Dr. Faqir Zarrar Yousaf
Senior Researcher,
5G Networks Group,
NEC Laboratories Europe

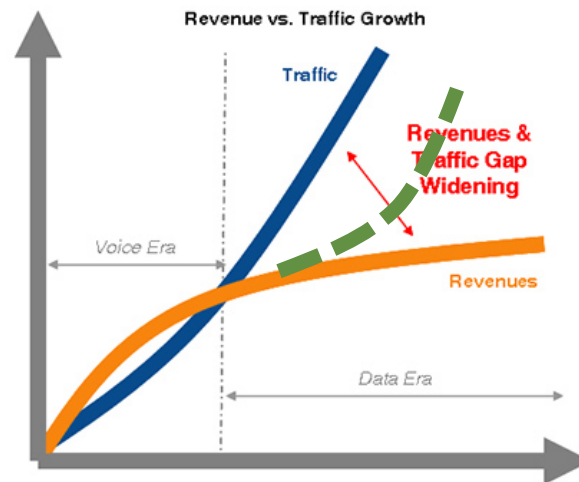
zarrar.yousaf@neclab.eu

Objective / Agenda

- The WHATs and WHYs of NFV
- ETSI ISG NFV Overview
- NFV key concepts – VNF and Network Service (NS)
- Overview of NFV Management and Orchestration (MANO) framework
- Overview of the ETSI NFV SEC WG

What & Why Network Function Virtualization (NFV) ?

NFV decouples the Network Functions (e.g., DNS, LB, FW, EPC) from the proprietary mission-specific hardware and run them on commodity servers as pure software entities → **Virtualized Network Functions (VNF)**



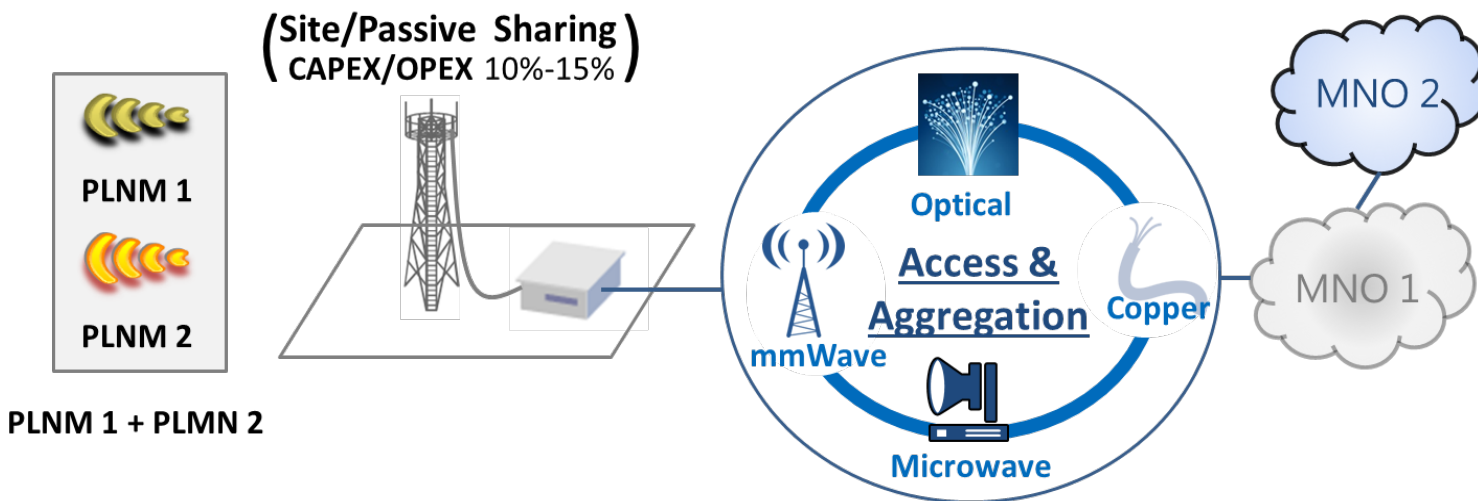
It's all about Money

1. Multi-tenancy → CAPEX / OPEX Reduction
2. On-demand resources / service provisioning
3. Fast-track (new) service innovation / provisioning
4. Energy and Resource efficient

Increased Revenues

CAPEX/OPEX saving of network sharing

	Radio Access Network (Spectrum and Active Sharing)	Mobile Backhaul (Transport)	Core Network (Evolved Packet Core)
CAPEX	25%-40%	10%-20%	15%-30%
OPEX	20%-30%	10%-15%	20%-25%



Capex Savings

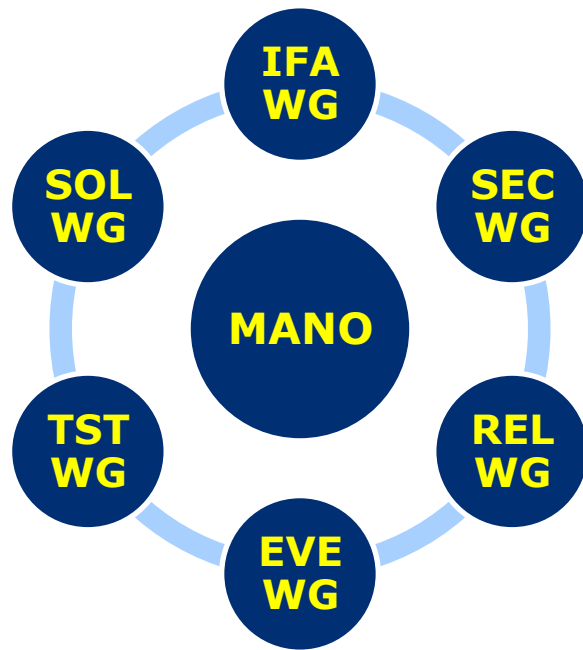
- Less equipment (and cables) through better sharing (slicing, multi-tenancy, multi-service)
- Cheaper equipment through HW commoditization

Opex Savings

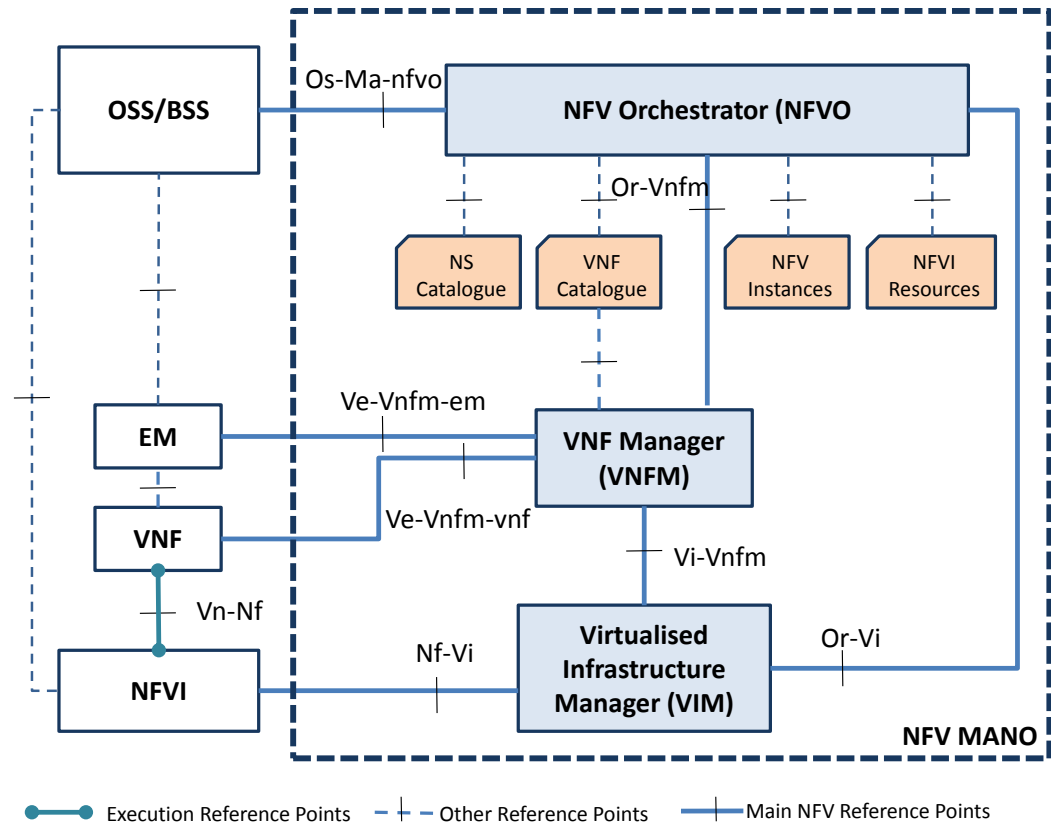
- Traffic demand based scale up and scale down options (energy reduction, efficient composition and allocation of network functions)
- Flexible and smooth network evolution via network programmability

ETSI ISG NFV Working Groups for MANO framework

ETSI ISG NFV Working Groups (WG)



ETSI NFV Management & Orchestration (MANO) Framework



IFA WG: Interfaces and Architecture WG

SEC WG: Security WG

REL WG: Reliability WG

EVE WG: Evolution & Ecosystem WG

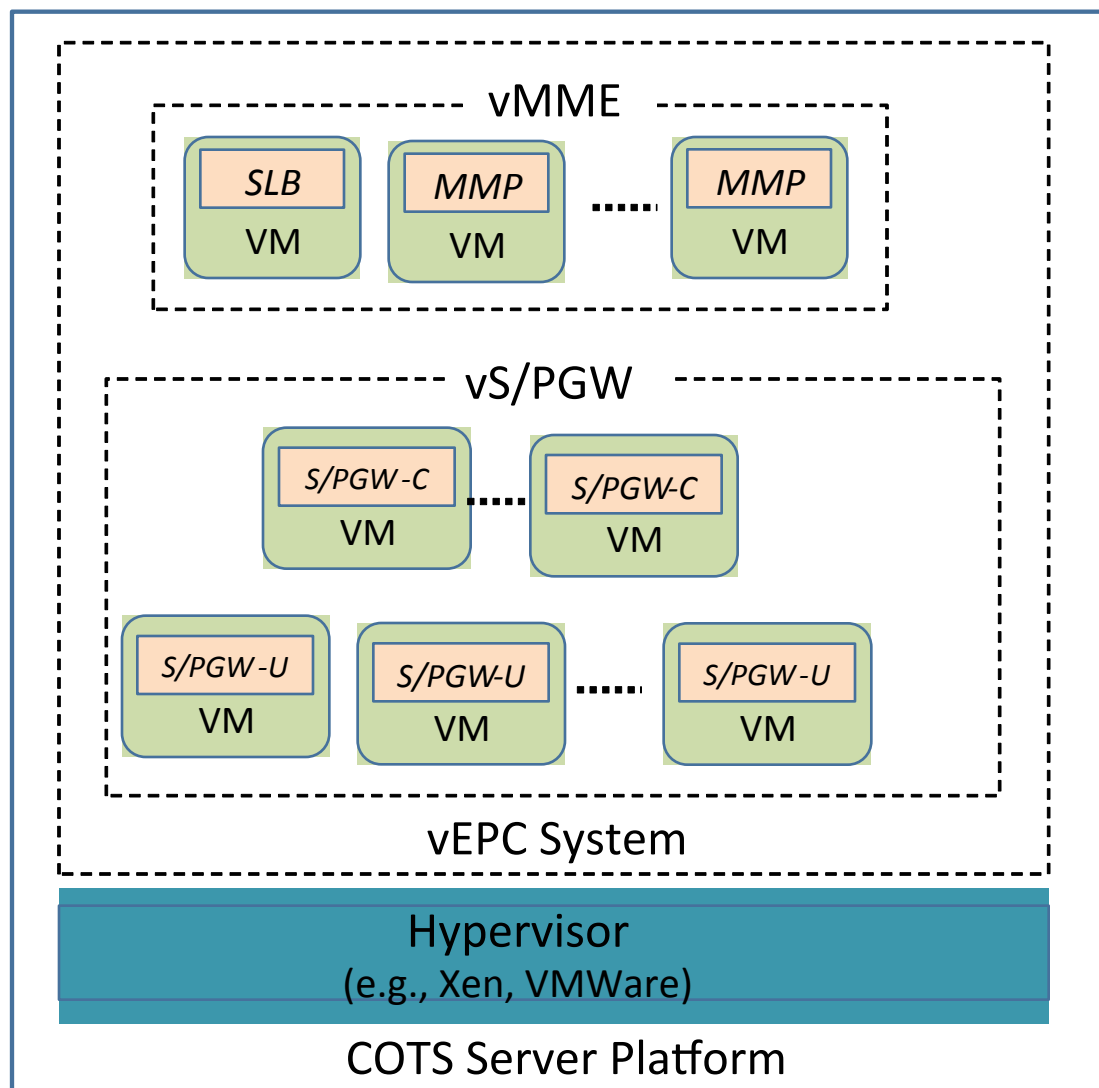
TST WG: Testing ,Implemntation and Open Source WG

NFV Concepts – VNF

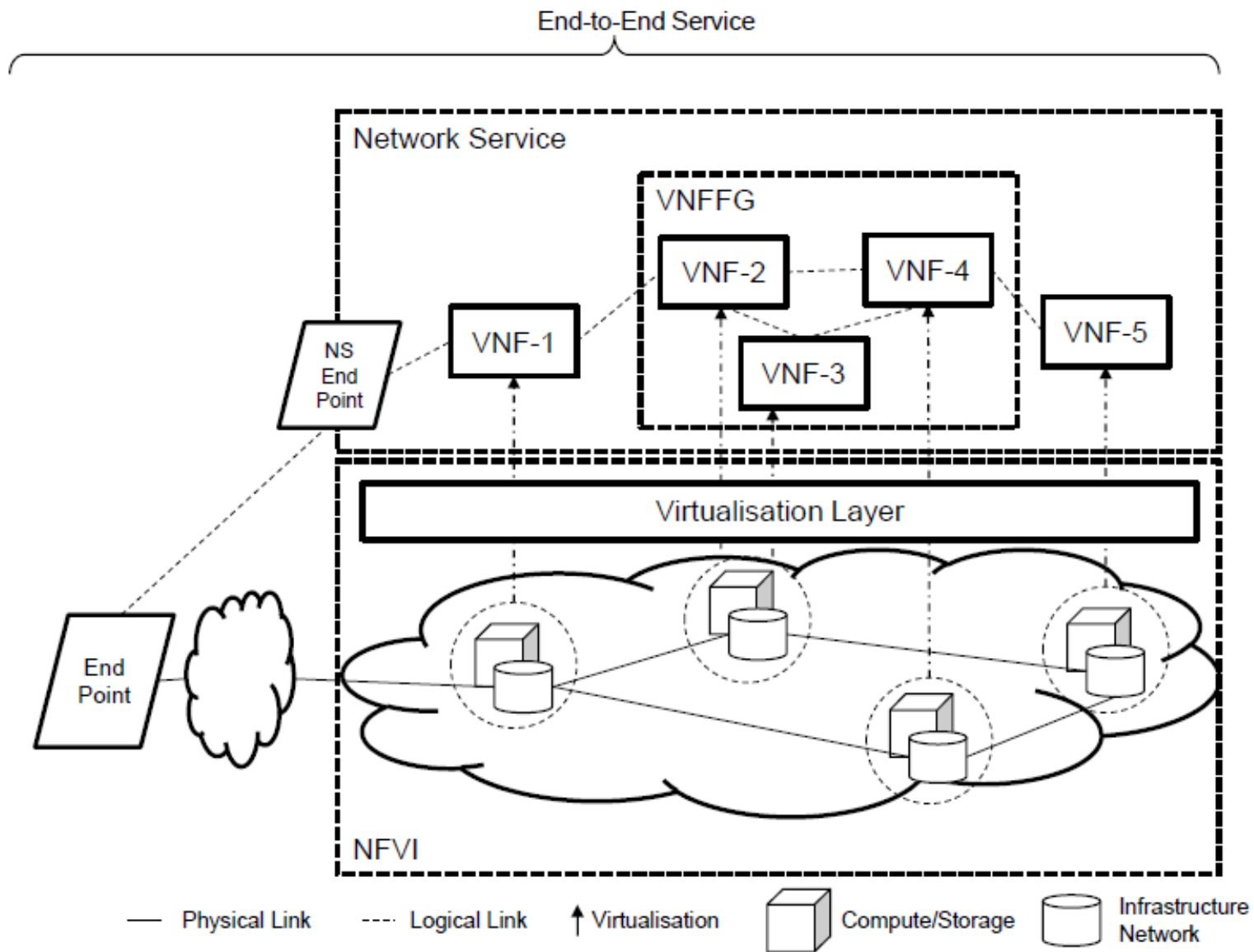
A virtualized EPC realized as VNFs

- vMME
- vS/P-GW

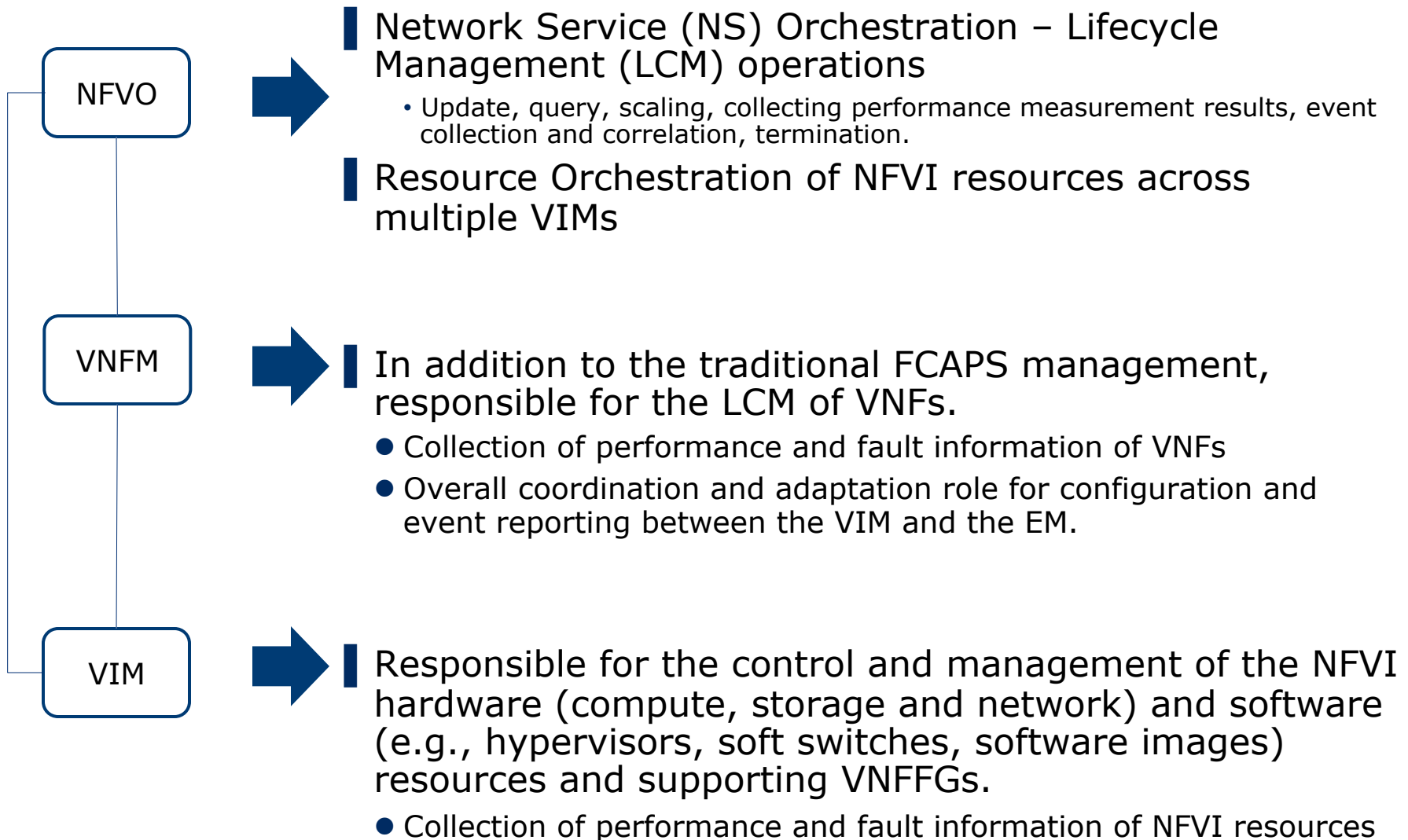
A VNF may be composed of multiple VNF Components (VNFC)



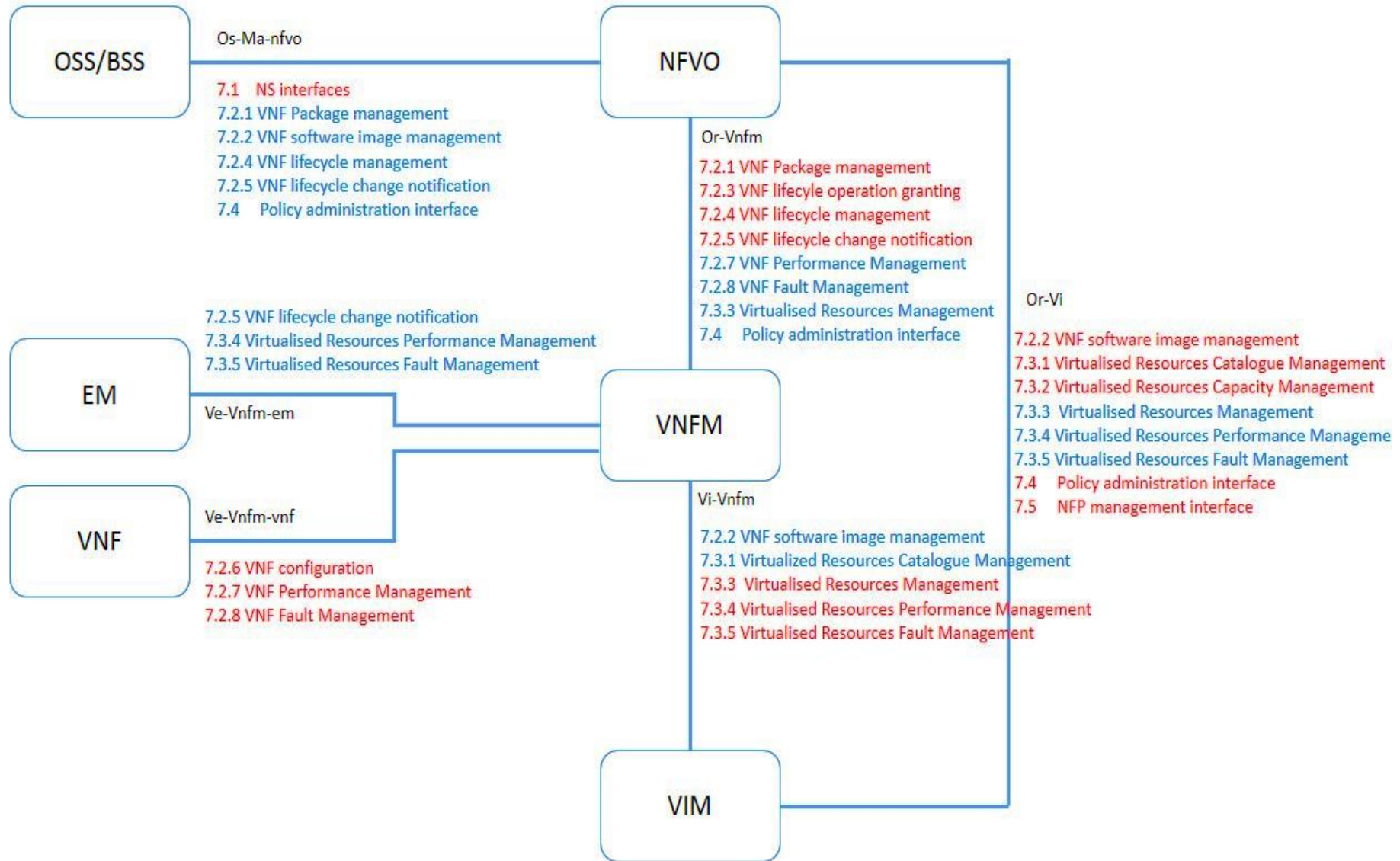
NFV Concepts – Network Service



Overview of NFV MANO Functions



Interface Mapping to ETSI NFV MANO Reference Points.



Responsibilities

- The SEC WG formed to address Security considerations for the MANO reference point.
- **Analysing threats to security** in virtualized environments and deriving **service and security requirements**.
- Identifying and specifying **best practice in areas of security** for NFV environments.
- Investigating **security enhancements** for NFV.
- Contributing to the security aspects of NFV demonstrators / proofs of concept.

Areas of Activity / Scope

- Information, network and communications security, including resilience, availability and performance isolation of NFV systems.
- Security of individual machines/processes and the security of large systems and networks.
- Security tools, controls and techniques to ensure security in an NFV environment.
- Appropriate measures for operational efficiency and features to support regulatory requirements, e.g. Lawful Intercept, Privacy and Data Protection.
- **Security at design-time, deployment-time and run-time.** → **DevOps**

DevOps for Network Function Virtualization

Development and Operations (DevOps)

- Collaboration and communication of both software developers and other IT professionals
- *Automation* of the process of software delivery and infrastructure changes

Agile Development

- Adaptive planning, evolutionary development, early delivery, and continuous improvement, and it encourages rapid and flexible response to change

Continuous Integration and Deployment (CI/CD)

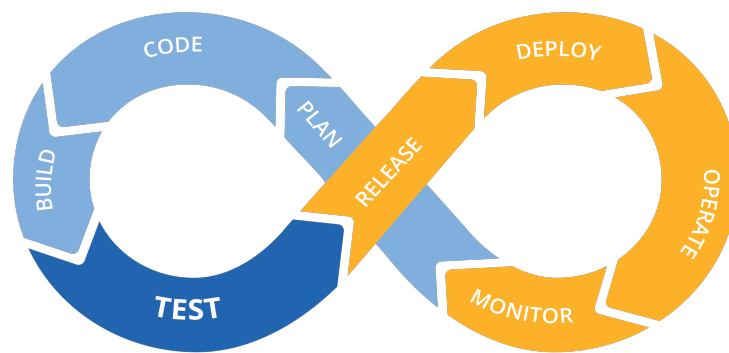
- Merging all developer working copies of code *several times* a day
- Automated testing and rollout of production service

Well established methods in software industry

- Especially for web-services

Imposes several challenges but also chances for telco operators

- Today, clear distinction between developers and operators
- Significant decrease in time-to-market

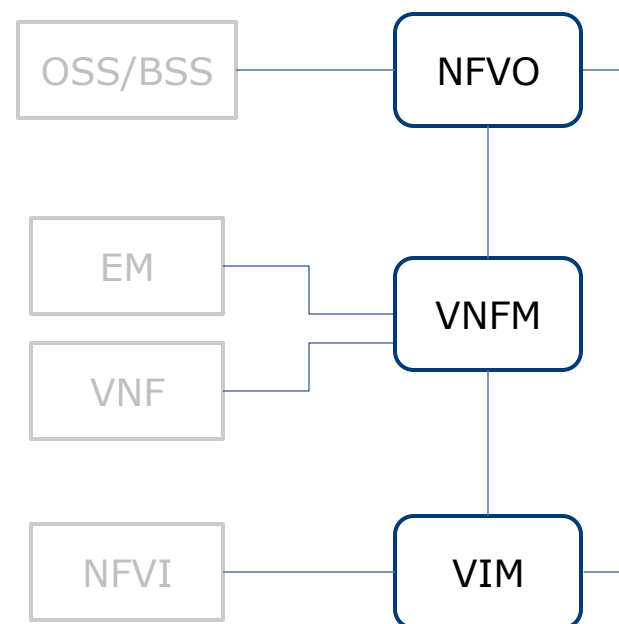


Threat Analysis (work-in-progress)

Threats / vulnerability & Response analysis for the various reference points and the respective interfaces

Manipulation of

- application data
- message requests/response
- Notifications
- stored data
- network services
- resources



Disruption of network services

Denial of Service

Misuse of Privileges

Eavesdropping/interception

Privacy concerns: Masquerading / Unauthorised access



SEC WG Active Work Items (WI)

- SEC003 – Security and trust guidance
- SEC005 – Certificate management report
- SEC007 – Attestation report
- SEC011 – Lawful Intercept (LI) architecture report
- SEC012 – System architecture for execution of sensitive NFV components – specification
- SEC013 – Security Management and Monitoring for NFV
- SEC014 – MANO Security specification.

*** for details please go to <https://www.portal.etsi.org>*

 **Orchestrating** a brighter world

NEC