

5G-TACTIC

5G Trusted And seCure network servICes

Towards 5G Open Source security – security validation of cloud-native MANO

Maksymilian Furmann, PCSS

WHAT'S PCSS

PCSS is a recognized partner on the international stage. We build our potential through cooperation with over 1,000 institutions from 60 countries across 6 continents. To date, we have completed nearly 400 research and structural projects (including dozens as a coordinator).

Leader in Artificial Intelligence and Quantum Technologies

Today, PCSS hosts Poland's AI factory: PIAST-AI. As one of the most important centers for AI development in Europe.

Parallel to this, within the PIAST-Q initiative, PCSS define the directions for quantum technology development.

Global e-Infrastructure Network

As the architect and operator of strategic infrastructure, PCSS designed and maintains:

- The PIONIER/PIONIER-Q national broadband network,
- The POZMAN Poznań Metropolitan Area Network,
- The High-Performance Computing Center.

We provide the scientific and economic community with access to HPC (High-Performance Computing) services, cloud computing, scalable data management systems, and the European Open Science Cloud (EOSC).

More: <https://www.psnc.pl/about/whats-pcss/>



PCSS Headquarters in Poznan



Poznańskie Centrum Superkomputerowo-Sieciowe
Poznan Supercomputing and Networking Center

PRESENTATION PLAN

A short roadmap for the talk — from motivation to continuous validation

1



Motivation and EU 5G security context

Why cloud-native MANO security validation matters

2



Security assurance methodology

How EU/ETSI requirements are used in 5G-TACTIC project

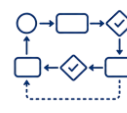
3



Open Source MANO as a case study

OSM role, architecture and integration with Kubernetes

4



Security validation workflow and scope

SCT, BVT, hardening and target of evaluation

5



Key observations from OSM testing

Operational risks, SCAS scripting and evidence analysis

6

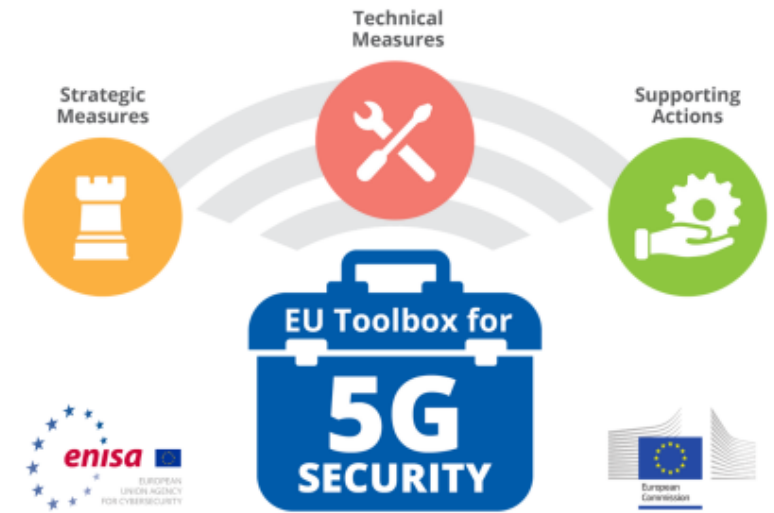


Continuous monitoring and re-validation

Moving from one-time testing to repeatable assurance

MOTIVATION: WHY THIS MATTERS

- MANO is a security-critical control component in 5G networks
- Cloud-native MANO introduces new risks across Kubernetes, containers, APIs and microservices
- Existing assurance specifications provide a baseline for NFV-based MANO, but do not fully address cloud-native MANO deployments
- Aligned with the EU 5G Security Toolbox, this work focuses on technical validation of risks related to insufficient security measures:
 - R1 – Misconfiguration of networks
 - R2 – Lack of access controls



EU 5G Security Toolbox: strategic, technical and supporting measures
Source: <https://www.enisa.europa.eu/news/enisa-news/member-states-report-on-eu-5g-toolbox-released-today>

Goal: bridge EU-level 5G security expectations with practical MANO security validation

5G SUPPORTING INFRASTRUCTURE

1. AI/ML platform

Protection of models, data, pipelines and decision-support mechanisms

2. MANO layer

Security of orchestration, lifecycle management, APIs and access control

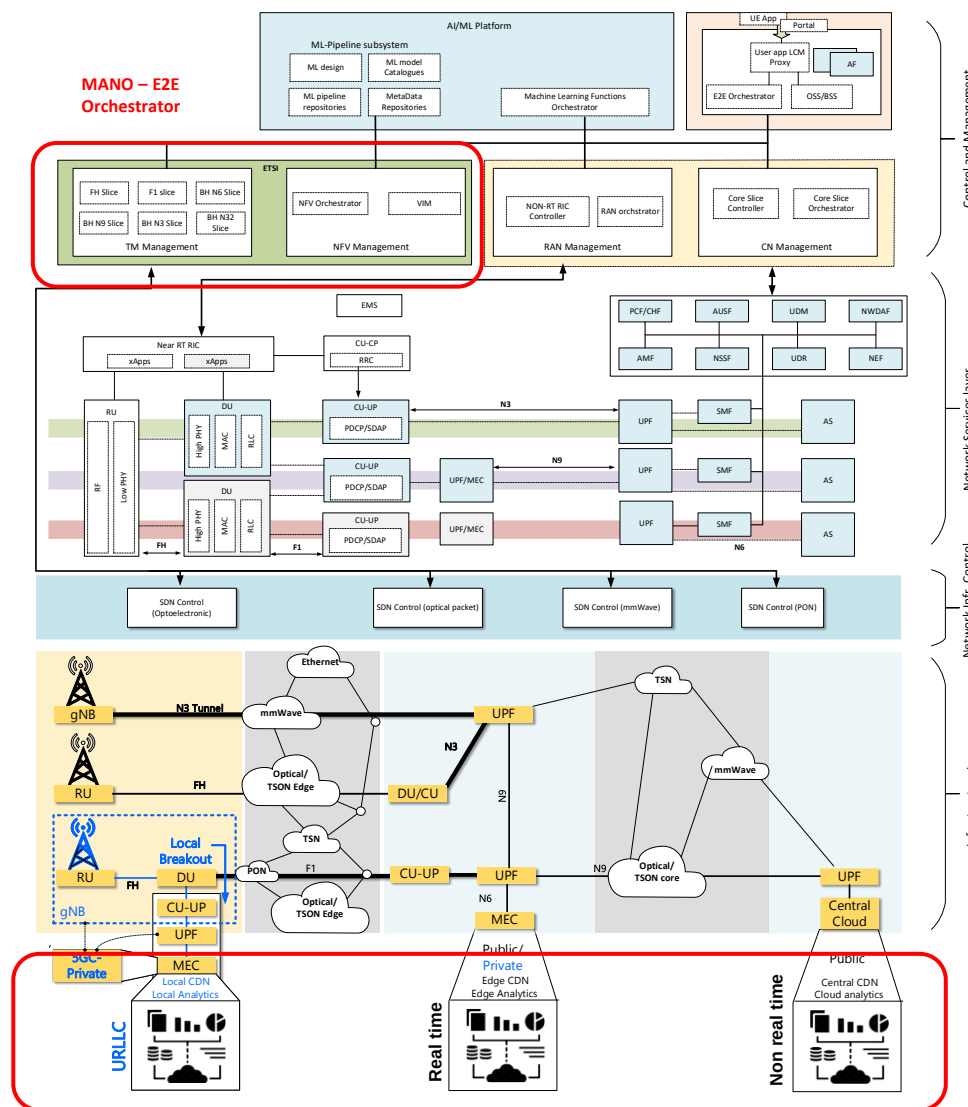
3. Network elements

Security of SDN-controlled transport, routers, switches and optical components

4. Compute infrastructure

Security of VNFs, CNFs, Kubernetes and virtualization platforms

The presented work focuses mainly on MANO security validation in cloud-native Kubernetes-based environments



ETSI TR 133 916 V16.1.0 (2022-01)



Universal Mobile Telecommunications System (UMTS);
LTE;
5G;
Security Assurance Methodology (SECAM)
for 3GPP network products
(3GPP TR 33.916 version 16.1.0 Release 16)

The methodology addresses risk scenarios and mitigation measures by translating security requirements into repeatable security activities

Reference inputs

1. SECAM

Security assurance methodology and test requirements

2. SCAS

Baseline for security testing

3. ENISA / EU 5G Toolbox

Risk scenarios and mitigation measures

Iterative security assurance process

STEP 1: Preparation and scope definition

Define the TOT/E based on relevant requirements

STEP 2: Testing and validation

Execute security checks and collect outcomes

STEP 3: Reporting and analysis

Identify findings, non-compliances and recommendations

STEP 4: Continuous improvement

Support for monitoring and re-validation

ETSI GS NFV-SEC 029 V5.2.1 (2025-03)



Network Functions Virtualisation (NFV) Release 5;
Security;
Security Assurance Specification (SCAS) for VM



CASE STUDY: OPEN SOURCE MANO

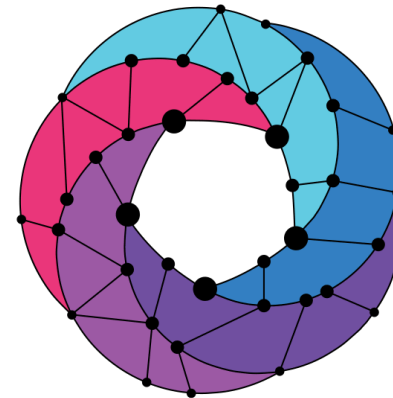
Open Source MANO (OSM) is an ETSI-aligned open-source platform for the management and orchestration of network services. It supports orchestration of **5G services**, including **network slice deployment** and lifecycle management of **VNFs and CNFs**.

Role of MANO in 5G

- Central component for deploying and operating 5G services
- Supports **lifecycle management (LCM)**
- Handles **instantiation, configuration, scaling, healing and termination**
- Automates **Day-0 / Day-1 / Day-2 operations**

Integration with infrastructure

- Interfaces with **VIM/CaaS platforms**, e.g. **OpenStack** and **Kubernetes**
- Manages compute, networking and storage resources through orchestration workflows



Open Source
MANO

Source: <https://osm.etsi.org/>

STEP 1: PREPARATION AND SCOPE DEFINITION

1. OSM analysis

OSM architecture, deployment model and available ETSI and OSM documentation

2. Testbed preparation

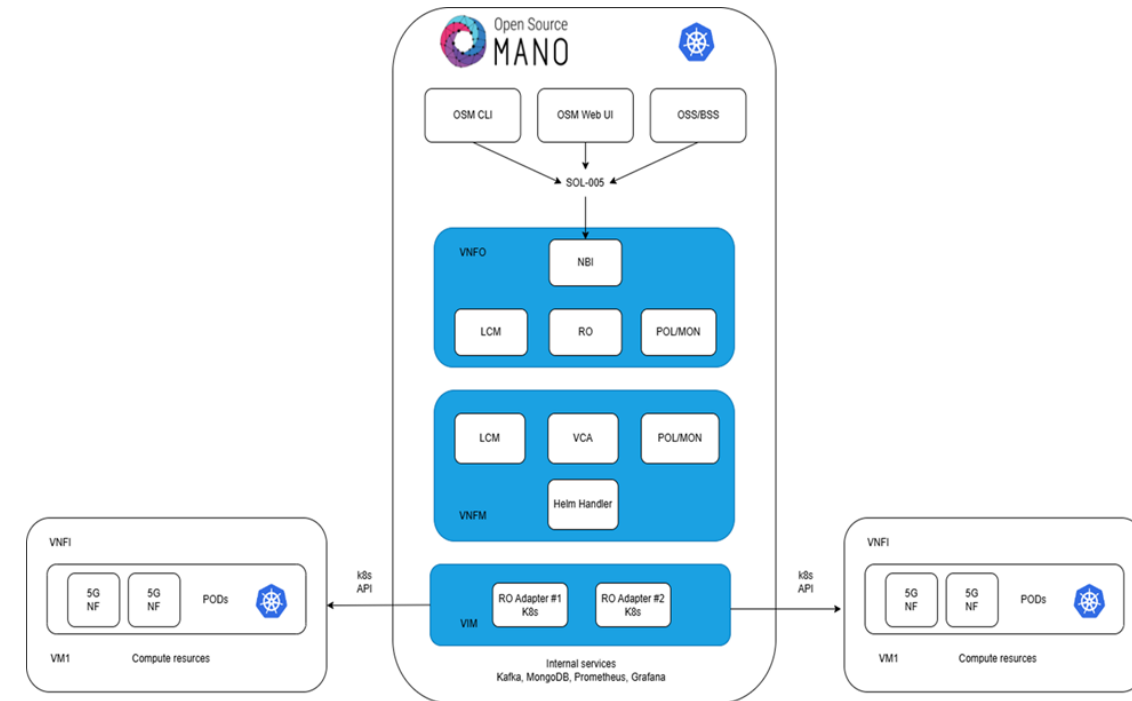
OSM-based cloud-native MANO integrated with Kubernetes clusters for CNF deployment

3. OSM TOT/E:

- **OSM management plane:** orchestration, LCM, user and role management
- **Interfaces and APIs:** GUI, REST/NBI, OAM, authentication and session handling
- **Kubernetes integration:** RBAC, namespaces, service accounts, policies
- **Network exposure:** ports, services and secure communication
- **Container layer:** image scanning, registry access

4. SCAS selection and adaptation

Adaptation of relevant Security Assurance Specification (SCAS) requirements to the OSM architecture and test scope



PCSS OSM-based cloud-native MANO testbed

STEP 2: TESTING AND VALIDATION

Security Compliance Testing (SCT)

Verifies compliance with applicable SCAS security requirements

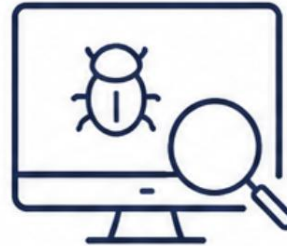


Scripts preparation

Preparation of supporting validation scripts to automate selected SCT checks

Basic Vulnerability Testing (BVT)

Uses FOSS tools to identify vulnerabilities on exposed interfaces



Tools selection

Selection of open-source testing tools
FOSS tools: Auditd, Cosign, Harbor, Trivy, Nmap, OpenVAS

Hardening

Reduces the attack surface through secure configuration, settings and protocol restrictions



Execution and evidence collection

Execution of security tests, collection of outcomes and identification of vulnerabilities or non-compliance

STEP 3: REPORTING AND ANALYSIS

Operational risks dominate over protocol-level issues

The main risks are related to configuration, access control and lifecycle management

SCT test scripts

SCAS were mapped to OSM components, interfaces and configuration settings, enabling reusable test scripts

Tool outputs need expert interpretation

FOSS tool provide useful evidence, but reports require filtering, correlation and contextual analysis

One-time testing provides only a snapshot

Cloud-native MANO continuously evolves through configuration changes, image updates, dependency changes, policy updates and new CNF deployments



STEP 4: CONTINUOUS IMPROVEMENT

One-time security testing provides only a snapshot of the current security posture; it does not guarantee that the system will remain secure after updates, configuration changes or new deployments

Centralized evidence repository

Stores logs, test results, reports and artifacts

Monitoring support

Security-relevant logs, metrics and events are observed

Re-validation

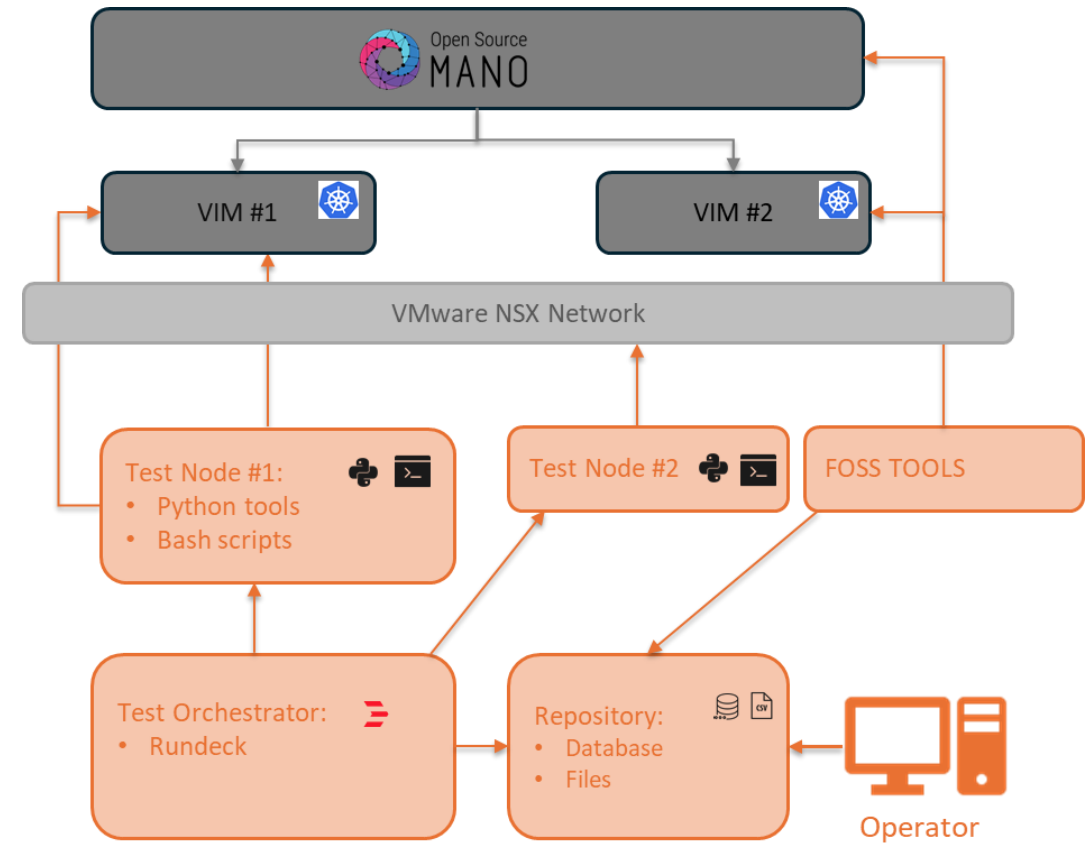
Tests are re-executed after changes or updates

Adaptation

Adapt security controls, evaluation tools and validation scripts to technological upgrades, new infrastructure entities and evolving threat landscapes

Findings analysis

Operator reviews results and identifies security gaps



CONCLUSIONS: FROM EU 5G TOOLBOX RISKS TO TECHNICAL VALIDATION

Planned platform functionalities are intended to support selected EU 5G Toolbox technical measures through repeatable validation activities:

TM01 - Ensuring the application of baseline security requirements

Validation of secure configuration and baseline checks

TM03 - Ensuring strict access controls

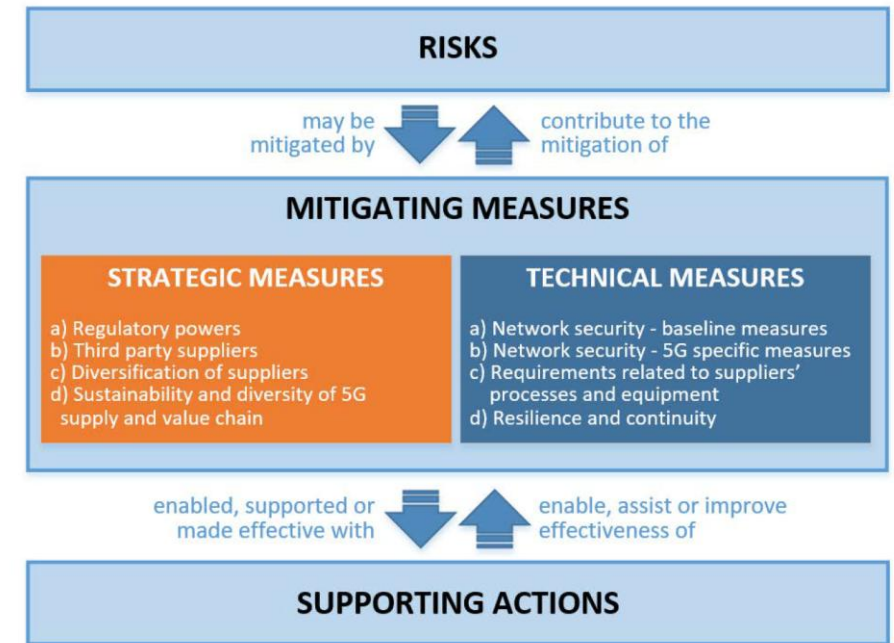
Checks of user roles, privileges, API authentication and RBAC

TM05 - Ensuring secure 5G network management, operation and monitoring

Evidence collection, monitoring support and re-validation of MANO operations

TM07 - Reinforcing software integrity, update and patch management

Image scanning, registry checks and update-related vulnerability validation



Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures

Source: <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>