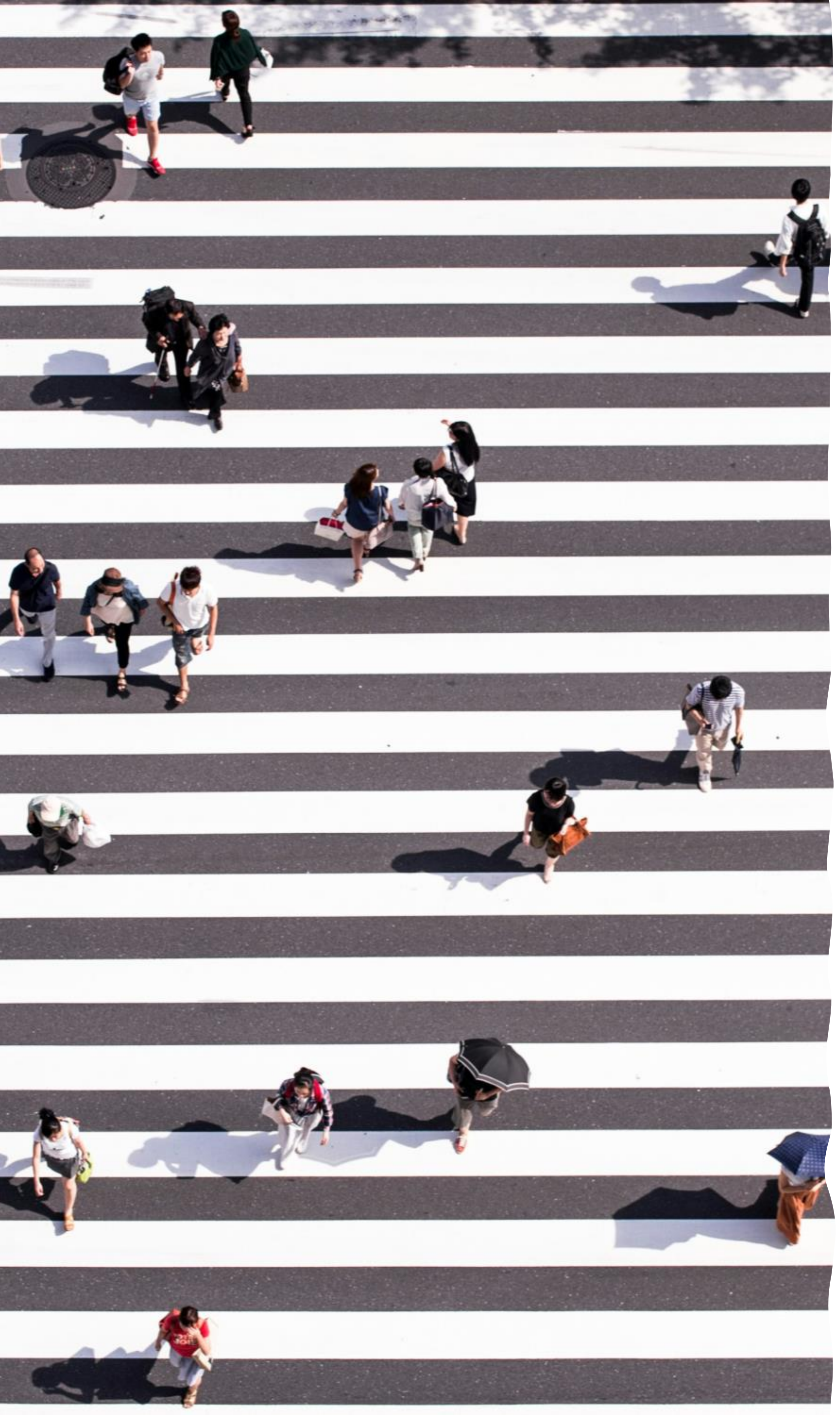
Assessing cybersecurity of public safety infrastructure

Filippo Berto, Marco Anisetti

Università degli studi di Milano

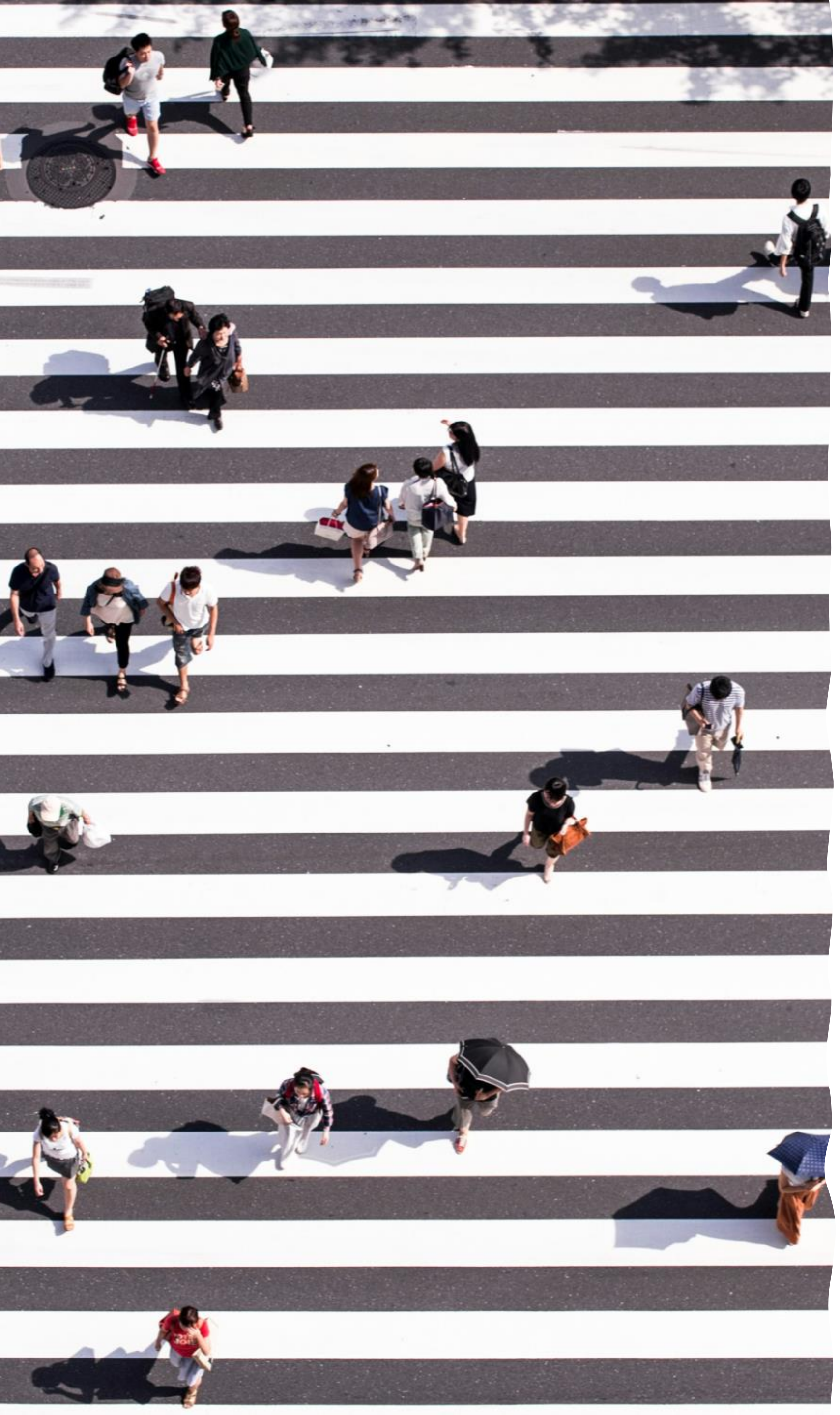
Overview

- Scenario
- Challenges
- Our Smart City Infrastructure
  - 5G-empowered Continuum
  - PNRR MUSA architecture
- The importance of Cybersecurity Governance
- Assess Moon Cloud DEMO



Scenario

- High interest in EU on multimodal solution for ensuring **Public Safety in Smart City** (e.g., H2020 Impetus project)
- State of the art solutions for city area monitoring are needed
  - **Vertical solutions** (specific, e.g., video surveillance)
  - **Holistic solutions** (horizontal, e.g., anomaly detection)



Scenario

- A Modern ICT Architecture for Smart City Safety is mandatory:
  - Scalable systems
  - Massive IoT
  - Data Lake
  - Big Data
  - AI/ML systems
- **Weaknesses in such architecture could have a devastating effect on Safety (e.g., cyberattack)**

Challenges: Weaknesses in Governance

Complex architecture supporting application workflows in the Edge to Cloud Continuum

Difficult to govern cybersecurity posture

Compliance with good practices and regulations

Security and privacy by design

Compliance with GDPR and AI act

Our Smart City Infrastructure (SmartCT)

- Distributed micro service-based architecture
- Data Lake and Big Data ecosystem
- Continuum based on 5G
- Support vertical applications dynamically deployed in the city Edge Cloud Continuum
- Assurance-aware design
  - Offers hooks for assessment/audit at every level
- **Based on EU PNRR MUSA Project Architecture**
- **Empowered with the Moon Cloud technology**

MULTILAYERED URBAN SUSTAINABILITY ACTION - MUSA

- Innovative ecosystem, collaboration of the 4 universities of Milan

- Aims to create a sustainable urban regeneration model that integrates environmental, economic and social aspects

- Involves academia, industry, local authorities and civil society to design a new vision of development with medium- and long-term positive impacts on the territory

- With an investment of 116 million euros from PNRR funds, MUSA represents a significant effort towards sustainable urban development in Milan

MUSA

MULTILAYERED URBAN SUSTAINABILITY ACTION

MULTILAYERED URBAN SUSTAINABILITY ACTION - MUSA

Objectives:

- Innovation Ecosystem
- Collaborative Effort
- Financial Backing
- Sustainable Development
- Public-Private Partnership
- Research and Innovation
- Urban Regeneration

MUSA

MULTILAYERED URBAN SUSTAINABILITY ACTION

MULTILAYERED URBAN SUSTAINABILITY ACTION - MUSA

Challenges:

- Urban Regeneration
- Big Data-Open Data in Life Sciences
- Deep Tech & Entrepreneurship
- Economic Impact and Sustainable Finance
- Sustainable Fashion, Luxury, and Design
- Innovation for Sustainable and Inclusive Societies

Microservices

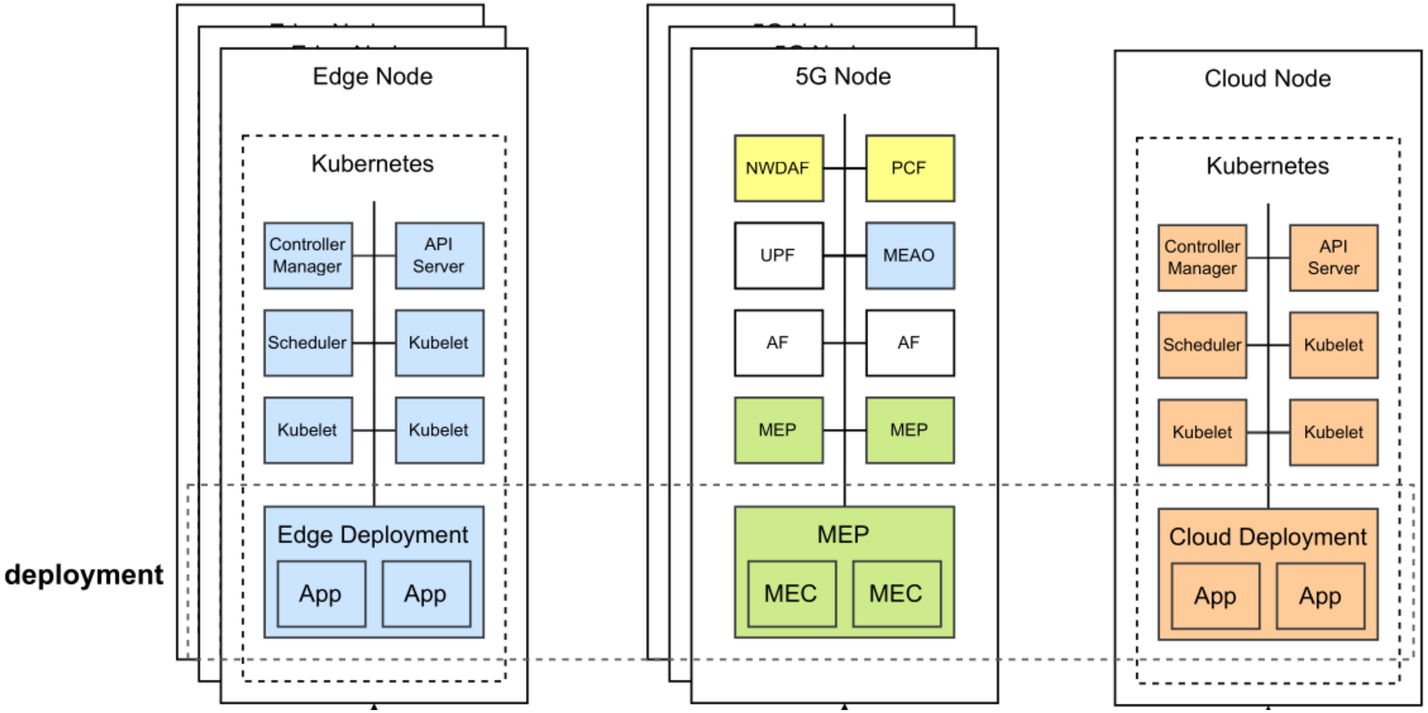
- Small scale services can be scaled individually on-demand
  - Enables horizontal scaling
  - Promotes geographical distribution
- Decoupling services through common interfaces
  - Increased specialization
  - Easier maintenance
  - Team-ownership
- Fine grained access and security controls
  - Policy-based access to resources and data
  - Stricter control on processes

Data Lake

- Centralized data management platform
- Allows Rule-Based or Policy-Based Access Control to data
- Manages:
  - Structured data (e.g., databases, CSVs)
  - Unstructured data (e.g., JSON, process logs)
  - Large binary files (e.g., AI/ML models, datasets)
- Advanced features
  - Access monitoring
  - Data lineage
  - Policy based data view transformation (e.g., filtering, anonymization)

5G Continuum

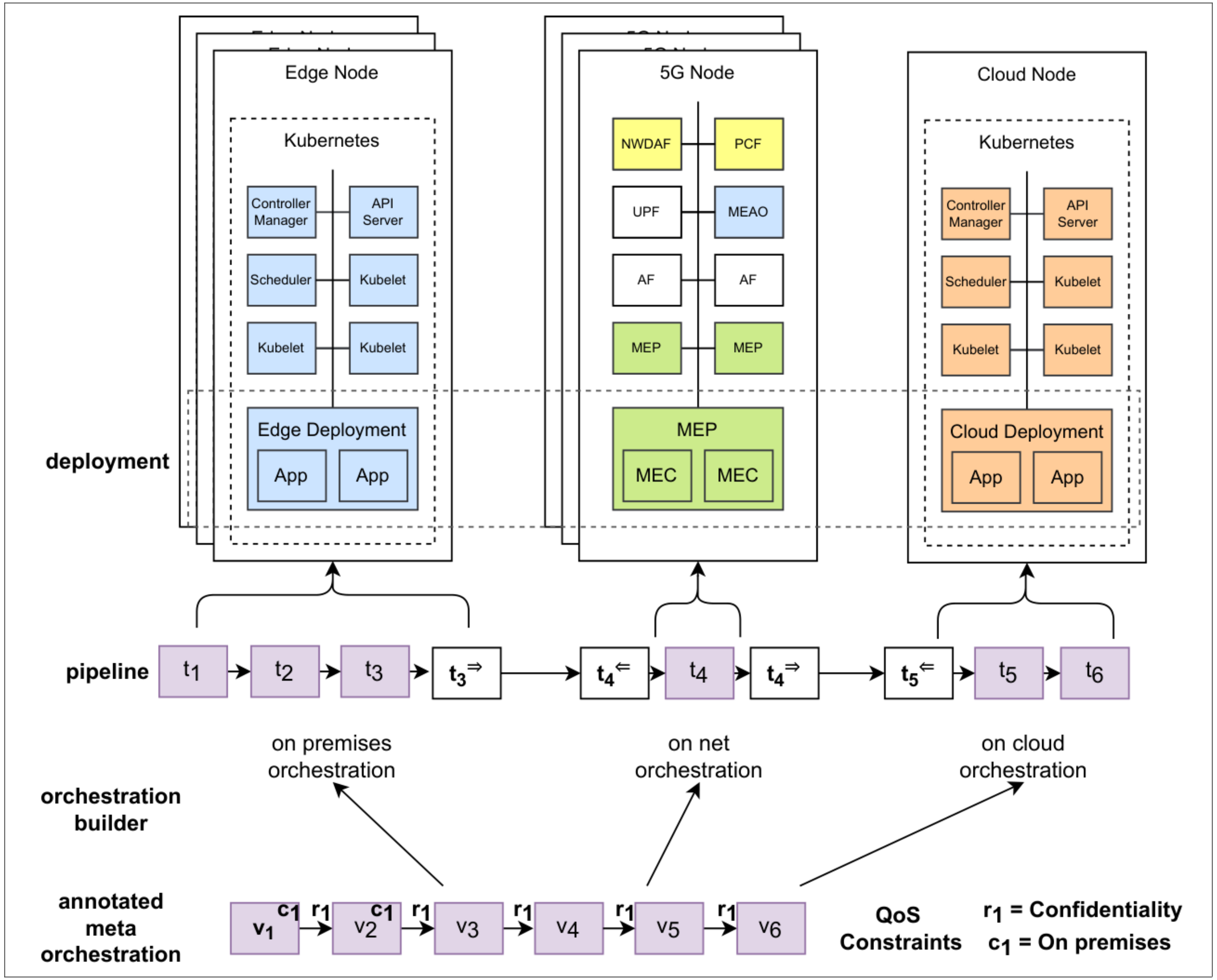
- Collaboration of several entities to provide a cohesive and distributed environment for service deployments
- Specialized deployment targets
  - Edge nodes for on-premises computation
  - 5G nodes for low latency services and massive IoT
  - Cloud nodes for performance intensive workloads
- Requires coordination of **configurations**, **services** and **networks**

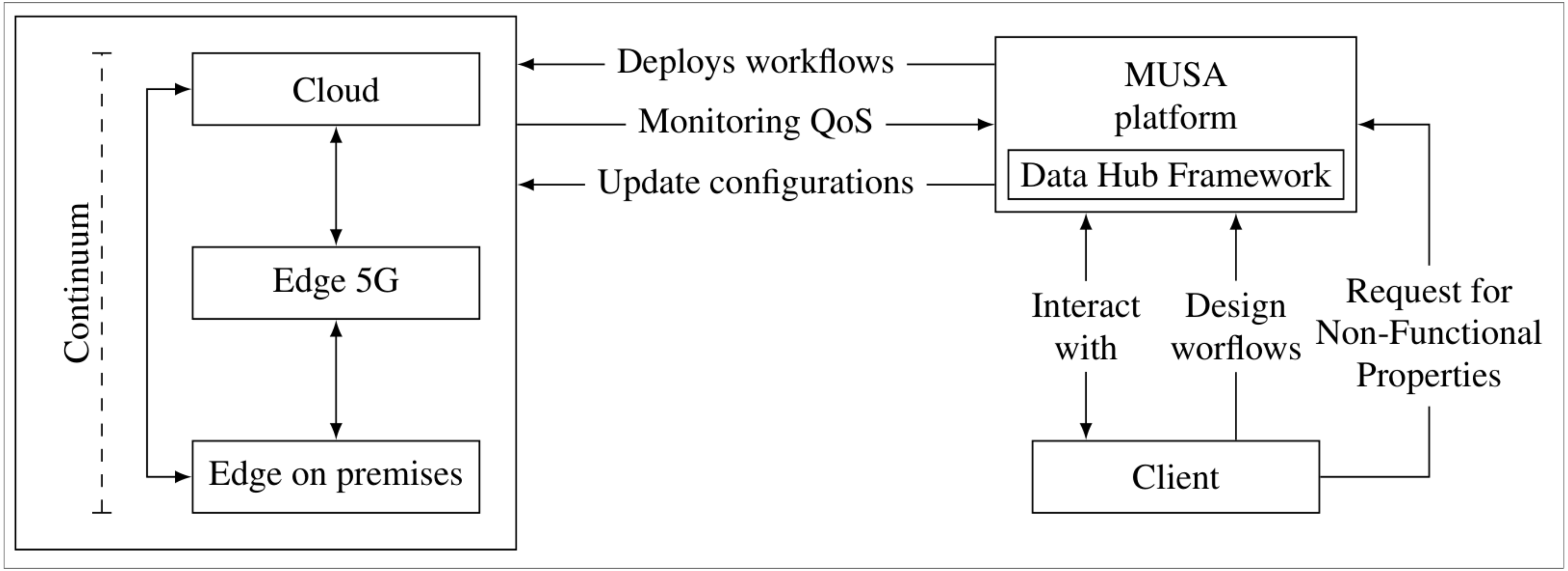


Example of Workflow in SmartCT 5G Continuum

Services and facilities are matched on:

- Services' functional requirements
- Users' non-functional requirements
- Facilities' capabilities





MUSA Deployment Architecture

The MUSA platform implements:

- Deployment Engine
- Data Lake
- Monitoring & Security Assurance

The platform manages all the aspects of the service deployment (e.g., life cycle, configuration, data)

Compliance with good practices and regulations

- Cybersecurity continuous assessment
  - New weaknesses threats and vulnerabilities
  - Platform and applications continuously evolving
- Regulatory compliance is Mandatory
  - AI compliance with AI act
  - Privacy compliance with GDPR
- **We adopted Moon Cloud as technology to ensure assessment and provide governance**

Moon Cloud

- Continuous **compliance assessment** and **assurance evaluation**
  - Targets ICT and infrastructures, enhancing operations with **security** and **performance assurance**

- Features:
  - Transparent **monitoring** of applications, enabling inspection and audit
  - Verifies **compliance** with standards
  - Centralized **security governance** specification
  - Faster and insightful reaction to incidents

Moon Cloud: Principal Features

Modern ICT Infrastructures

Integration with monitoring and profiling

Automated application security analysis

Data policy checking

AI/ML Based Applications

Integration with training pipelines

Model poisoning and pollution detection

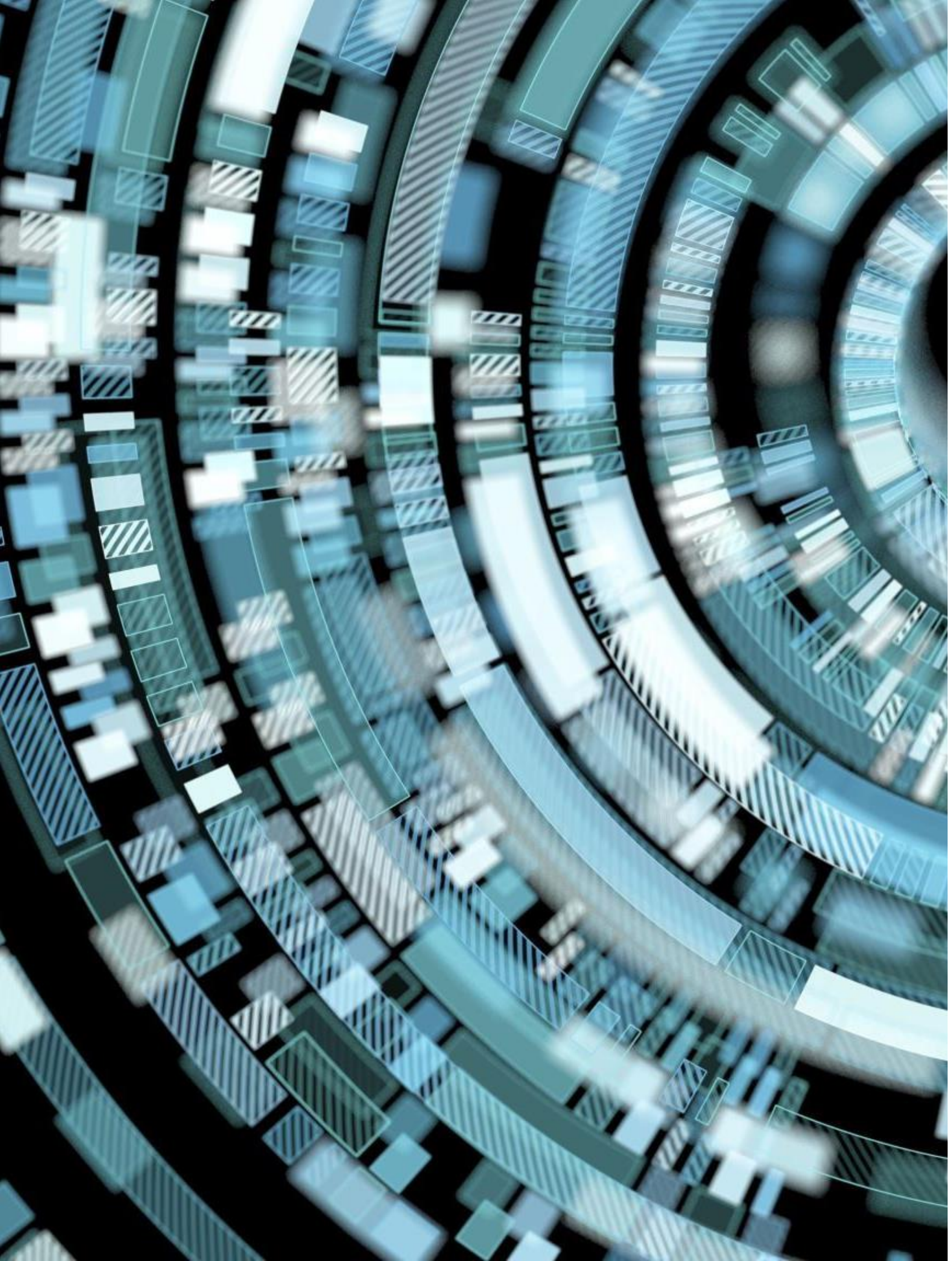
Dataset lineage monitoring and inspection

Edge to Cloud Continuum

Transparent monitoring

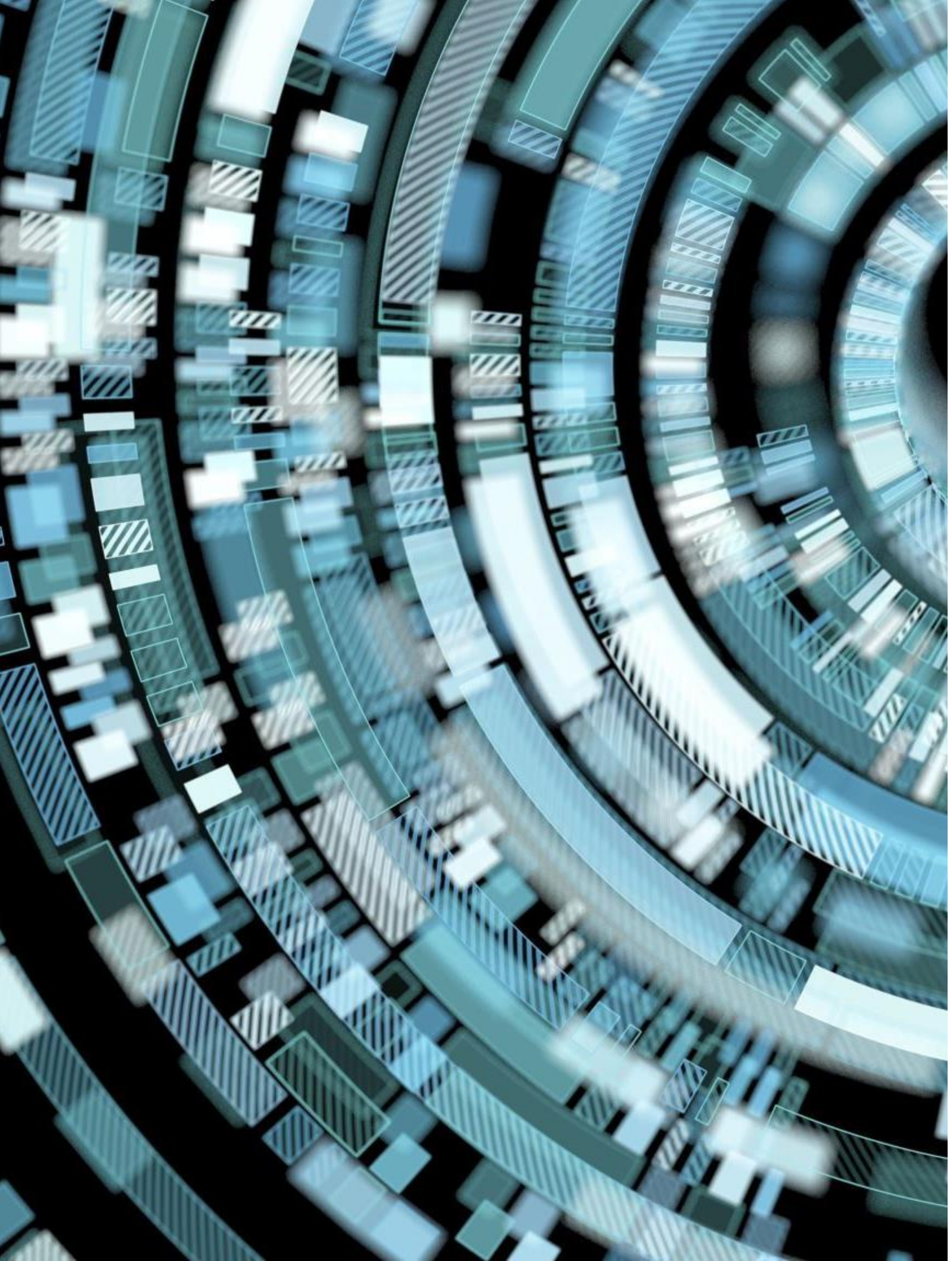
Agent-based monitoring

Continuous non-functional requirements checking



Moon Cloud Architecture

- **Based on models and evidences:** Template-based customization that can be easily adapted to customers' needs, evidence-based compliance assurance.
- **Fully automatic and customizable:** Moon Cloud offers a platform allowing full customization of compliance and assurance as a service.
- **Covers all (cloud stack) layers:** The evaluation deeply inspects all the aspects affecting the system. A deep dive in the hidden part of the security and performance iceberg.
- **Integrates pre-existing solutions:** Third-party monitoring and testing tools, existing certification and compliance solutions can be easily integrated within Moon Cloud.



Moon Cloud Architecture

- **Continuous testing and monitoring:** Assurance and compliance are guaranteed via non-invasive continuous monitoring and testing.
- **Non-tamperable system: Secure collection of monitoring evidence via** non tamperable probes.
- **Assess AI/ML models: The evaluation deeply inspects all the aspects** affecting the system including AI/ML models. A deep dive in the hidden part of the iceberg.

Cybersecurity Governance with Moon Cloud

Tutorial

The Targets

The entire SmartCT platform including applications and components

- IoT devices and Edge nodes
- Safety-oriented vertical applications (e.g., video-based weapon detection)
- Data Lake (ETL format)
- Platform Frontend
- External Cloud Services
- Platform Backend
  - Platform services (e.g., authentication service)
  - Holistic application services (e.g., anomaly detection)
- The development process pipelines of both applications and the SmartCT platform itself

The Targets (2)

All the targets are managed through the Moon Cloud Inventory, organized in:

- Projects
- Zones
- Targets

The **correctness** and **freshness** of the information in the inventory if **crucial for security**

Moon Cloud Assessment Activities

- Evaluations on the **platform during development stages**
- Evaluations on the **platform in operation**

The scope is to guarantee compliance with

  - Cybersecurity best practices
  - Privacy (e.g., GDPR)
  - AI act compliance

Carried out via Testing, Monitoring, Configuration Checking, and manual declarations of compliance

Hello World: Assessment Tutorial

Availability assessment:

- We register a target in a zone
- We register eventual credentials to connect to the target
- We create and evaluation
- We monitor the results

Any questions?

Assessing SmartCT Platform

Assessing SmartCT Platform in Operation

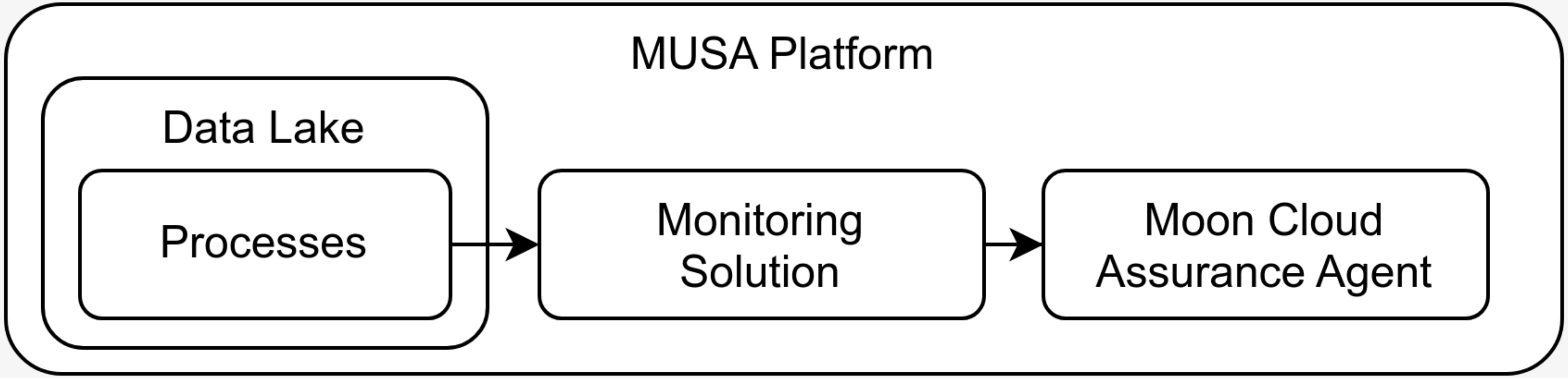
Data Lake: Observability

Observability of the platform enables inspectability

- Monitoring of the system's state
- Anomaly detection

Enhance the system with Non-functional property monitoring

- Availability
- Security
- Privacy



Data Lake: Observability

Data Lake:
Security Assessment

Active security assessment of the platform

Automatic tentative of exploitation using attack frameworks (e.g., Metasploit)

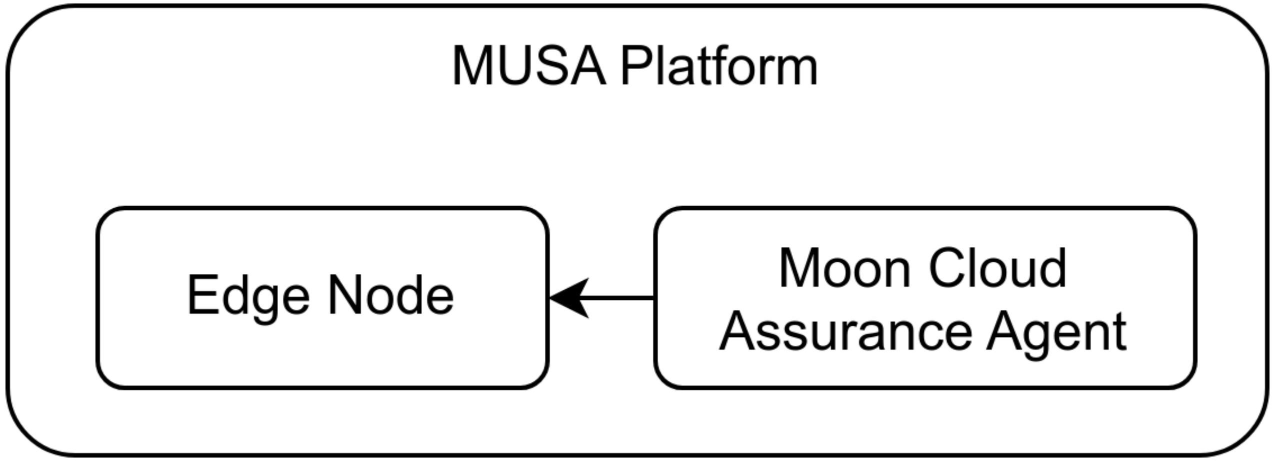
Enhances the platform security by checking its attack surface for vulnerabilities

Edge Nodes: Security Auditing

Deployment of security auditing tools on the target edge nodes

The Moon Cloud agent scans the node and checks for security issues and misconfigurations

Enhances the security level of the target, hardening against malicious actors



Edge Nodes: Vulnerability Assessment

The Moon Cloud agent runs vulnerability assessment tools on the target

The tool scans the node and checks whether any known vulnerability is applicable to the target

Enhances the security level of the target, identifying security risks

```
"scripts": {
    "start": "electron .",
    "dev": "rollup -c -w",
    "build": "rollup -c"
},
"keywords": [],
"author": "",
"license": "ISC",
"devDependencies": {
    "electron": "8.2.1",
    "electron-reload": "1.5.0",
    "concurrently": "5.1.0",
    "@rollup/plugin-commonjs": "11.0.0",
    "@rollup/plugin-node-resolve": "7.0.0",
    "rollup": "1.20.0",
    "rollup-plugin-livereload": "1.0.0",
    "rollup-plugin-svelte": "5.0.3",
    "rollup-plugin-terser": "5.1.2",
    "svelte": "3.21.0"
},
"dependencies": {
    "cron": "1.8.2",
    "node-notifier": "7.0.0",
    "rollup-plugin-scss": "2.4.0"
```

Edge Nodes:
Static Analysis

Deployment of static analysis tools on the target edge nodes

The Moon Cloud agent scans the node and checks for security issues and misconfigurations

Checks for misconfigurations and errors in the system files

Edge Nodes:
Source Code Analysis

Deployment of static analysis tools on the target edge nodes

The Moon Cloud agent scans the node and checks for security issues and misconfigurations

Checks for misconfigurations and errors in the system files

Edge Nodes:
Analysis of Docker Images

Security analysis of Docker images in the registry

The Moon Cloud agent scans the image checking for vulnerabilities and misconfigurations

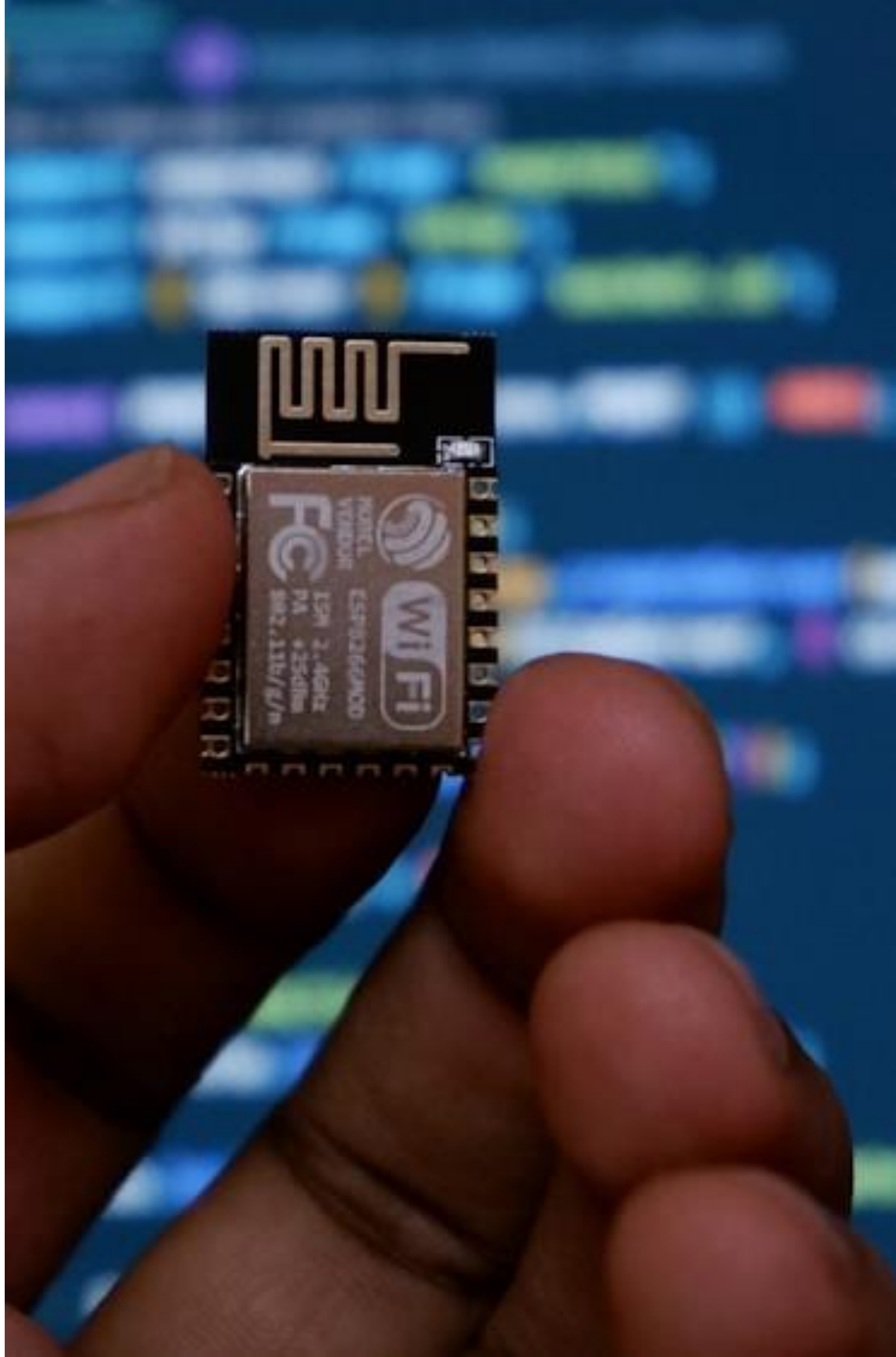
The tool guarantees higher level of security providing vulnerability reports, checks on the image signature and misconfiguration

IoT Devices: Availability

Request for availability checks on managed IoT Devices in the network

The Mon Cloud agent tries to contact the target device and retrieves usage statistics

Simplifies inventory management and hardware maintenance



IoT Devices: Vulnerability Assessment

IoT devices are common target of attacks, becoming part of botnets

Moon Cloud aims at limiting the security risks by preventively assessing the vulnerabilities of the targets

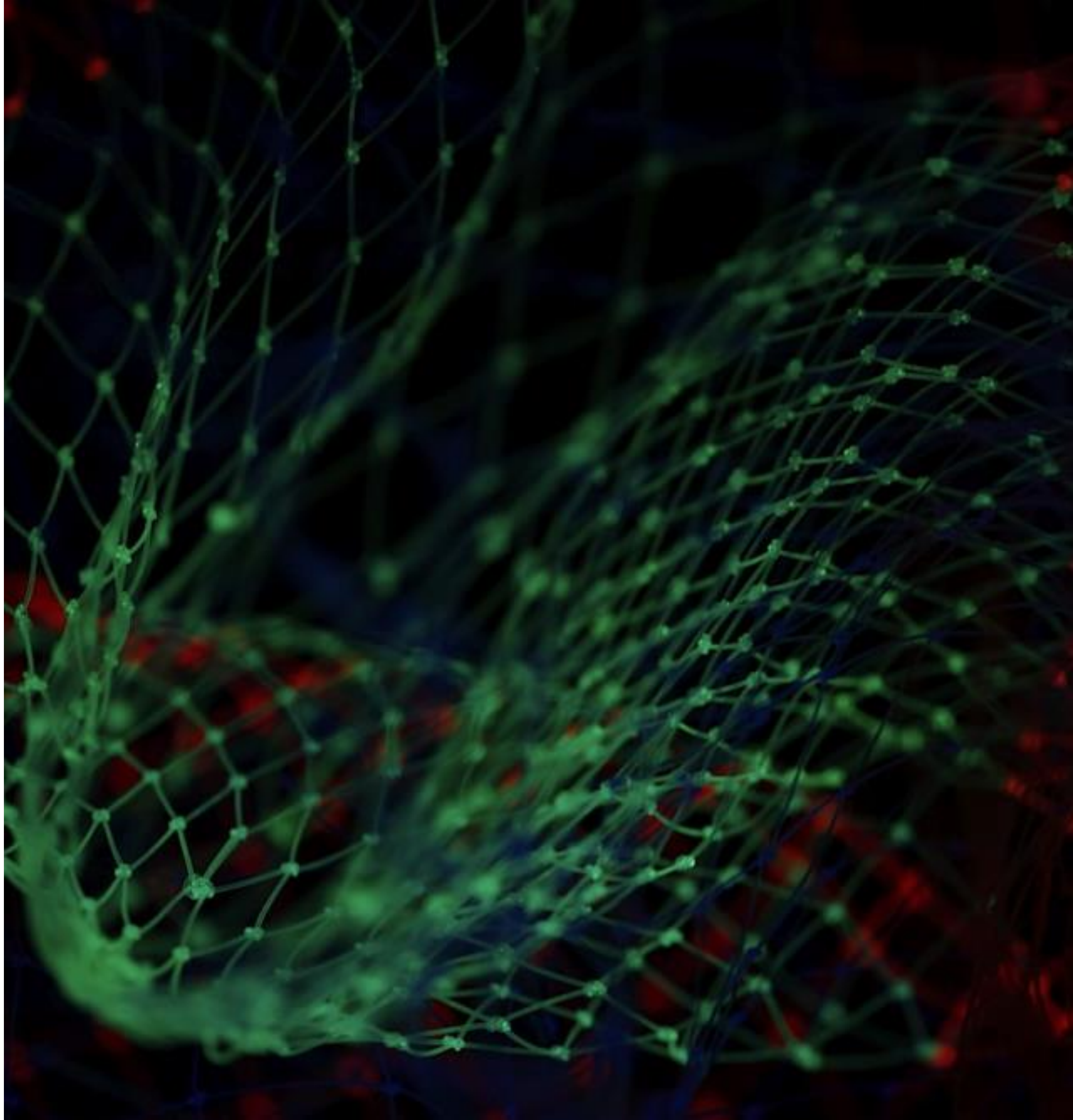
The Moon Cloud agent uses vulnerability scanning tools to automate the security checks against IoT devices

Machine Learning: Dataset Evaluation

ML-based workflows require datasets with advanced properties.

Moon Cloud analyzes the dataset verifying metrics, e.g., class balance, noise, k-anonymity, ...

The Moon Cloud agent automates the checks, running them when the dataset changes



Machine Learning: Compliance Assessment

ML-based applications must follow strict regulations

Moon Cloud provides a question-based assessment of workflow goals and implementation

Assessment updates can be requested automatically

Machine Learning: MLOps

CI-CD integration of ML security and quality assessment

Moon Cloud integrates with GitHub and GitLab CI platforms to inject additional checks on workflow code and datasets

Machine Learning: Performance Check

Integration in ML worflows of non-functional properties checking on the produced models

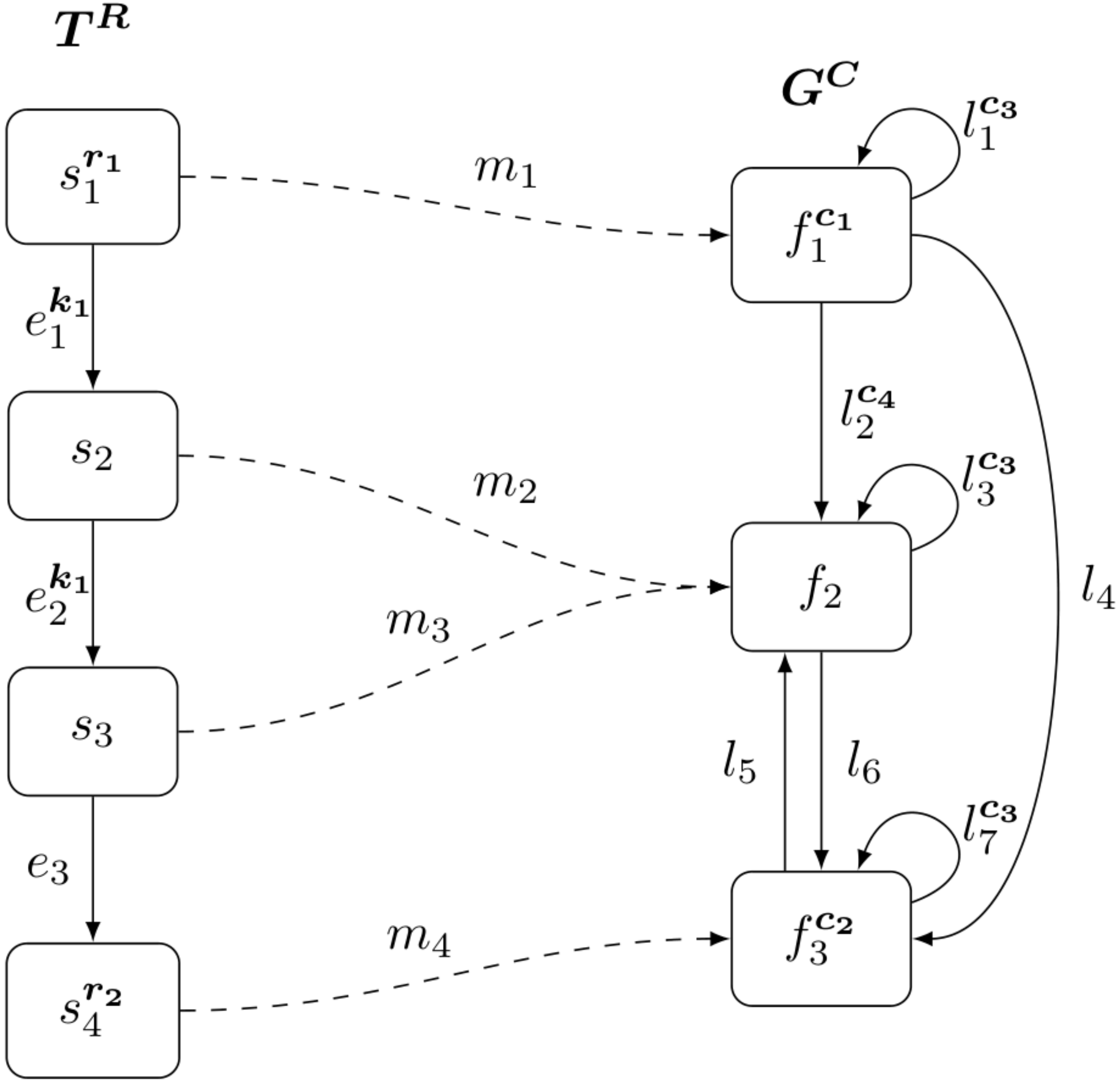
Moon Cloud automates the property assessment by checking the output of several metrics. E.g., accuracy, precision, recall, ...

The agent connects to the computing node where the model is stored, requests for a metric evaluation and checks the results

Any questions?

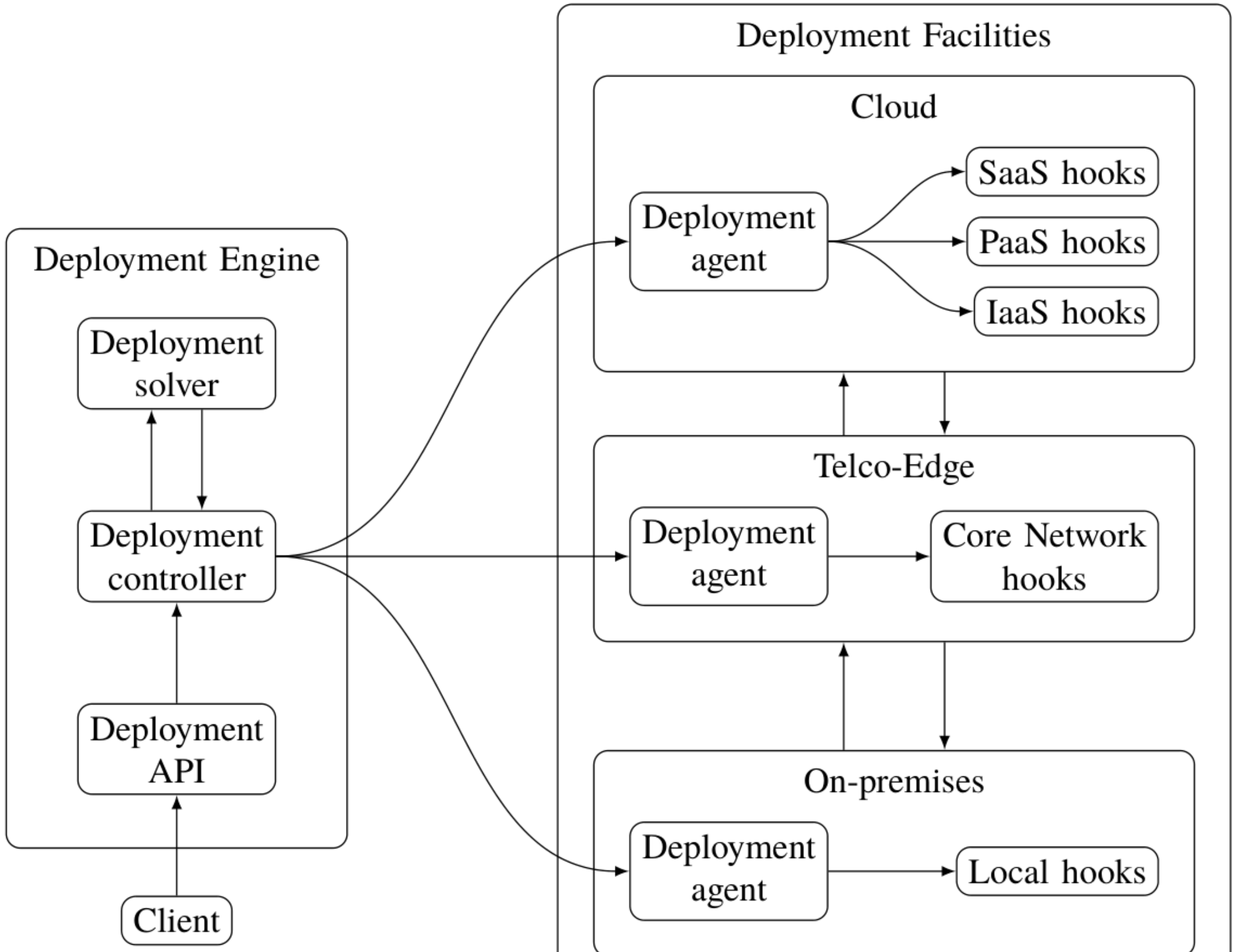
Deployment in the 5G Continuum

- Deployments templates are annotated with the user non-functional requirements
- We consider service execution requirements (e.g., security and location) and link requirements (e.g., latency and bandwidth)



Deployment in the 5G Continuum

- A deployment engine tries to match the user non-functional requirements with the deployment facilities properties
- When a solution is found, the deployment engine uses the facilities deployment hooks to deploy the services

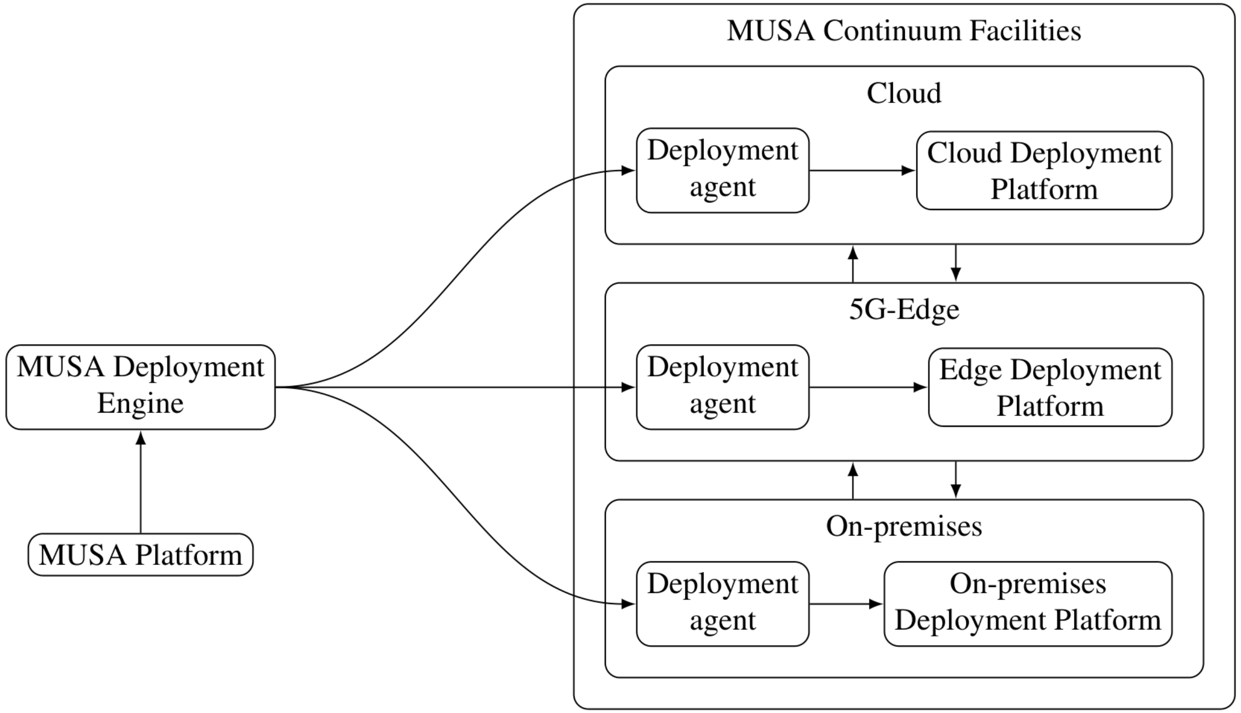


Deployment flow using the MUSA platform

The user defines a template of the deployment, with **non-functional requirements**, through the **MUSA platform**

Deployment Agents in each node are instructed by the **Deployment Engine** to update their configuration

The deployment facilities are federated, allowing transparent integration of their services and configurations


MUSA Continuum Facilities
Cloud
Deployment agent
Cloud Deployment Platform
5G-Edge
Deployment agent
Edge Deployment Platform
On-premises
Deployment agent
On-premises Deployment Platform
MUSA Deployment Engine
MUSA Platform