
LF
NETWORKING
LFN Developer & Testing Forum

LF NETWORKING

LFN Developer & Testing Forum

Operational Security Assurance for Open Source 5G Mobile Networks

Margaret (Maggie) Cogdell
Laboratory for Advanced Cybersecurity Research (LACR)
National Security Agency

Anti-Trust Policy Notice

LFN NETWORKING
LFN Developer & Testing Forum

- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrustpolicy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

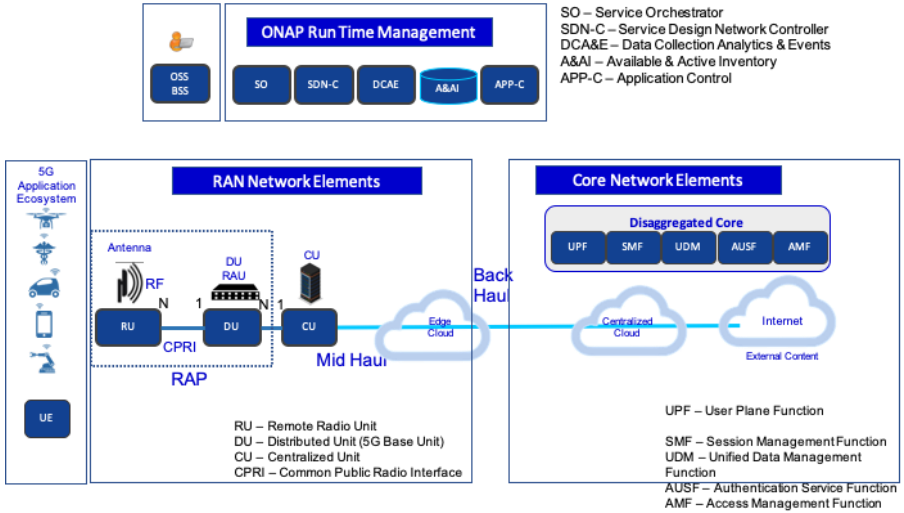
ONAP & AI/ML

- Goal: *Improve the monitoring capabilities of ONAP for our customers*
- Objectives
  - ONAP orchestration & management security
  - Identify how threats would manifest in performance metrics
  - Detect and/or classify core network traffic anomalies

Approach

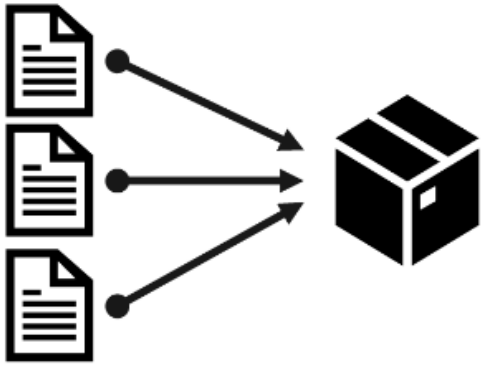
- 5G Core: Create prototype of meaningful performance and fault management metrics for 5G Core

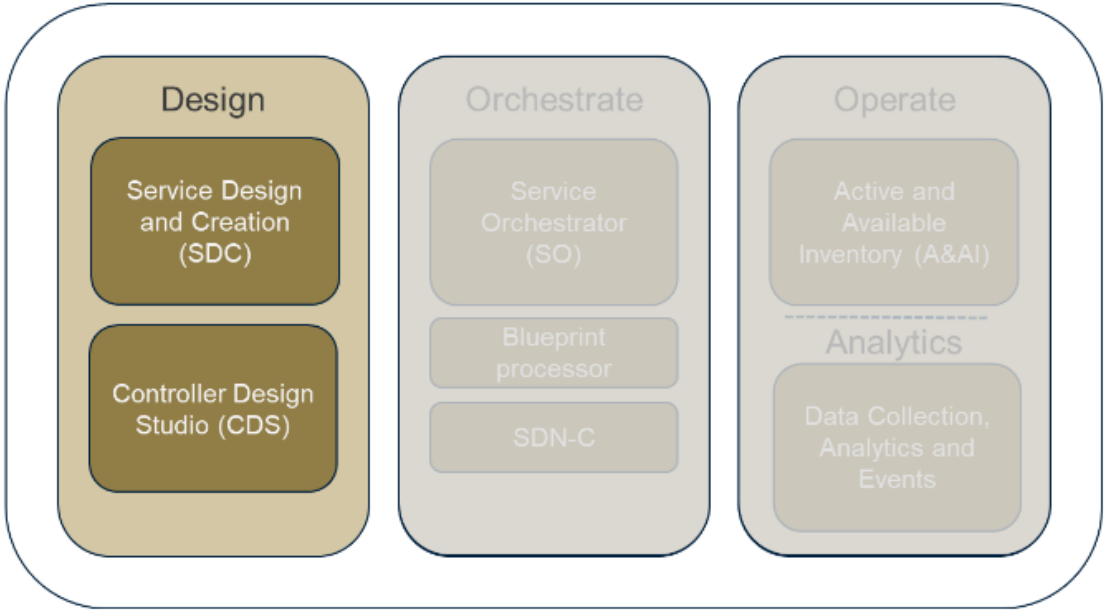
- ONAP/Core integration: Define & implement performance metric collection from the Core and relay counters to ONAP / DCAE (Data Collection Analytics, and Events) via VES (Virtual Event Streaming) adapter



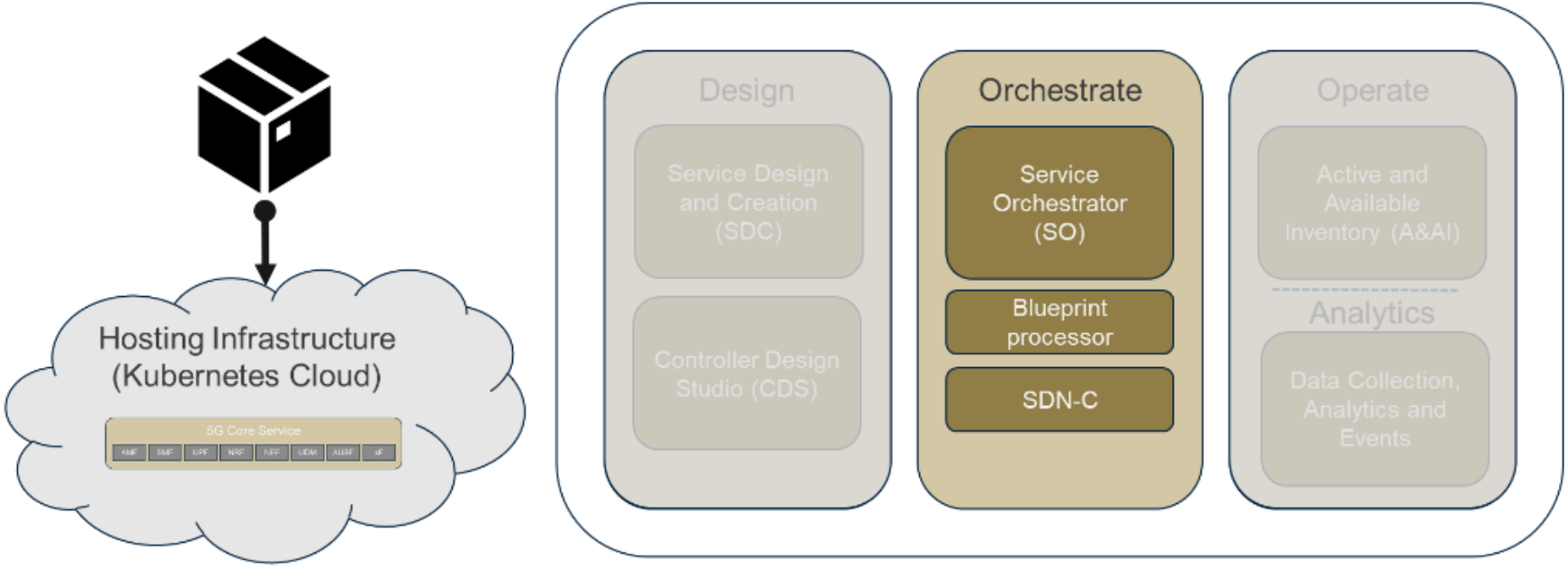
Source: https://docs.onap.org/en/jakarta/guides/onap-developer/architecture/onap-architecture.html

ONAP Overview – Service Onboarding & Design

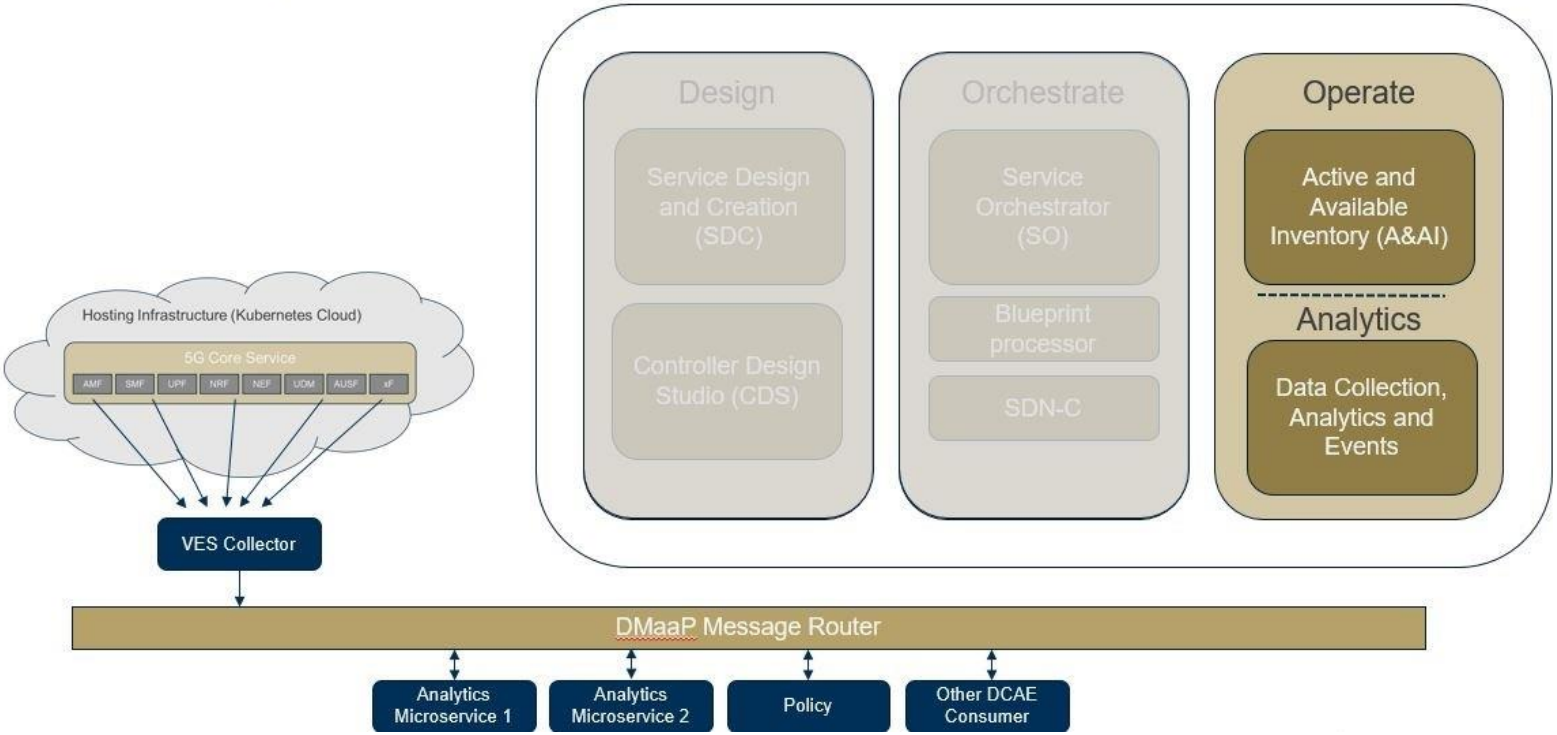




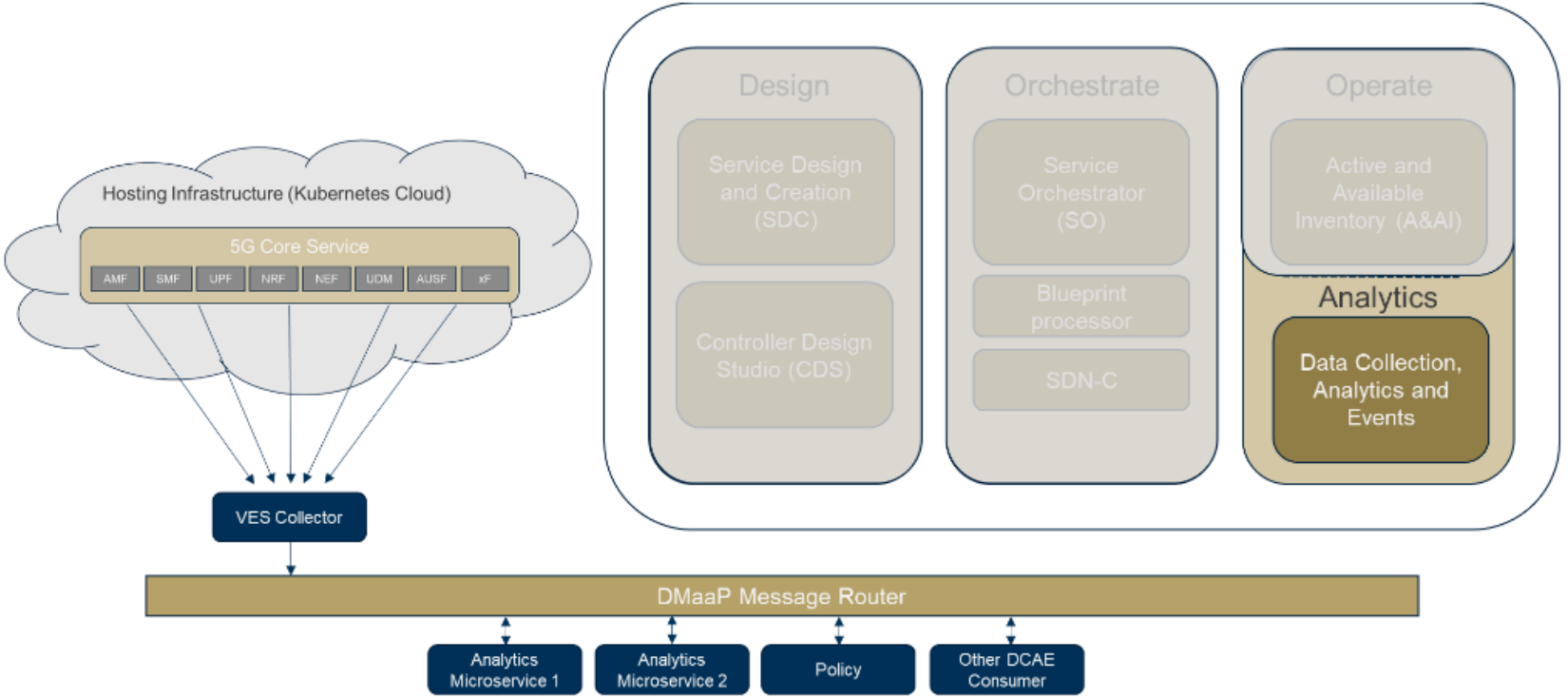
ONAP Overview – Service Orchestration



ONAP Overview – Operation & Monitoring



ONAP Overview – 5G Core Metric Export Approach



Hurdles of Implementation

- Lab testbed
- DCAE & NWDAF

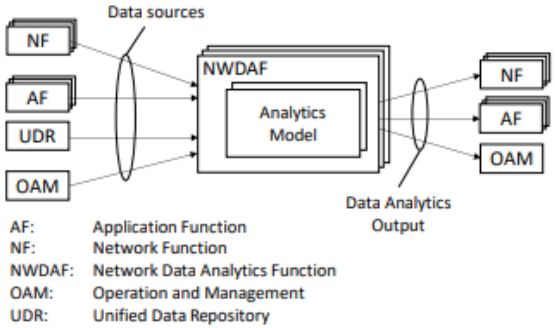


Image taken from: "5G Evolution: A View on 5G Cellular Technology Beyond 3GPP Release 15"

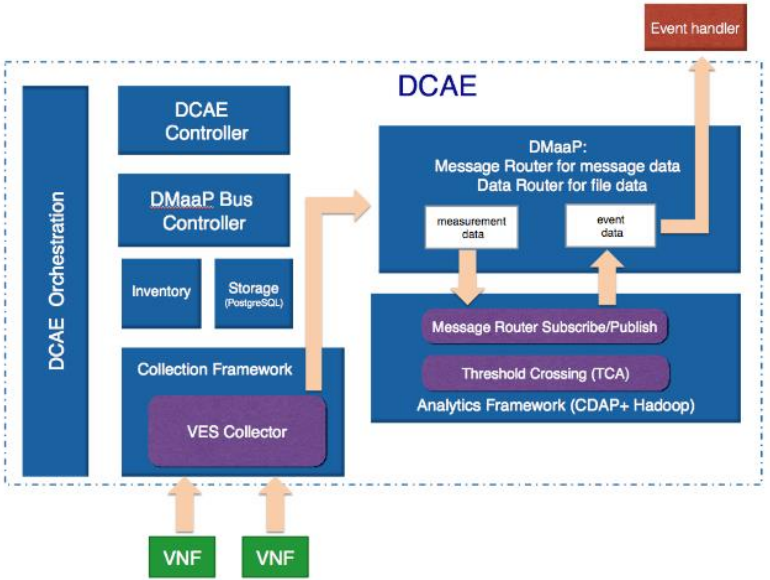


Image taken from: https://wiki.onap.org/pages/viewpage.action?pageId=1015831

Changes to 5G Core

- UPF
  - Incoming and outgoing data traffic on the N6 interface - This data is between the core and and external data network (e.g. the Internet)
  - Number of incoming General Packet Radio Service (GPRS) Tunneling Protocol (GTP) data packets on the N3 interface, from (R)AN to UPF
  - Number of outgoing GTP data packets of on the N3 interface, frc
- AMF
  - Number of initial registration requests
  - Number of successful initial registrations
  - Number of successful mobility registration updates
  - Number of authentication requests
  - Number of failed authentications due to parameter error
  - Number of authentication rejections
- SMF
  - Number of PDU session creation requests
  - Number of successful PDU session creations
  - Number of failed PDU session creations

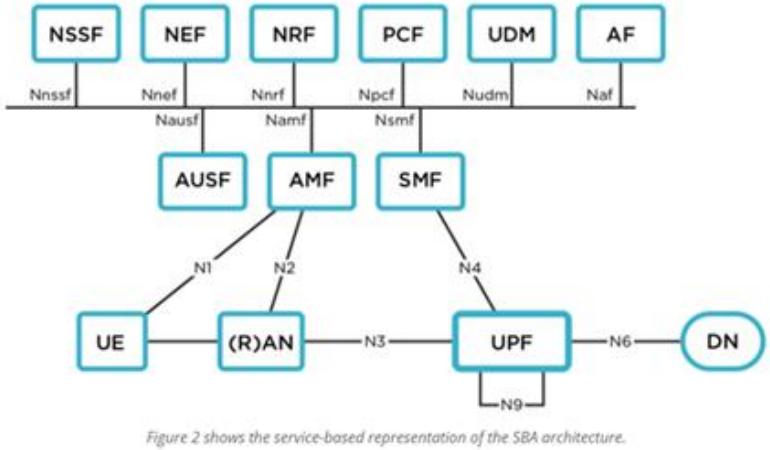


Image from: https://emblasoft.com/images/blog/n3-in-the-5g-sba.png

ONAP Components for Data Collection and Events (DCAE)

- DCAE Collectors
  - VES Collector
  - Bulk Performance Measurement (PM)
- DCAE Analytics
  - KPI computation
  - MS Threshold Crossing Analysis
  - Holmes (Alarm event processing)

Next Steps

5G Network

- Integrate AI/ML techniques
- Machine learning for secure 5G Networks - Identified 3 potential scenarios for investigation
  - Abnormal behavior thresholds
  - DDoS detection
  - Logistics tracking
- Completed creation of initial counters within the 5G Core to enable collection of performance data

AI/ML for 5G Security & Decision-Making

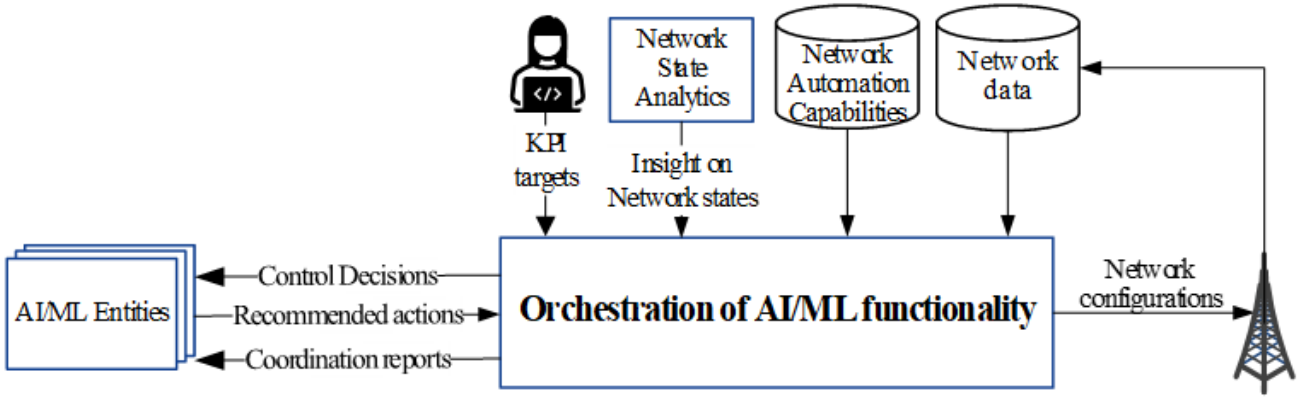


Figure 5.N.1: Orchestrating AI/ML

Image taken from: 3GPP TS 28.908 V0.4.0 (2022-08)

- AI applications to 5G
- Deep Reinforcement Learning (RL) for improved SDN controller decision-making
- Supervised/Unsupervised Machine Learning (ML) uses for improved cybersecurity

ML Methods for 5G Network Security*

LFN NETWORKING
LFN Developer & Testing Forum

- General ML for 5G categories of methods:
  - Supervised/Unsupervised/Self-Supervised ML for 5G traffic classification, clustering, & prediction of malicious and/or anomalous activity
  - Reinforcement learning for SDN dynamic decision-making and response, such as routing changes, to mitigate effects of attacks

Function	ML Technique	Objective
Network planing, management and monitoring	• K-means clustering; • Deep neural network; • Reinforcement Learning; • SVM.	• Clustering users and service requirements; • Routing and forwarding decisions; • Resource optimization; • Parameter configuration; • Forecasting resource usage.
Fault detection and security	• Principal component analysis; • Logistic regression; • Deep neural network.	• Classification of users and applications; • Anomaly detection; • Predicting unusual behaviour.

* - Table reference from: Domeke, A., Cimoli, B. & Monroy, I.T., “Integration of Network Slicing and Machine Learning into Edge Networks for Low-Latency Services in 5G and beyond Systems”, *Applied Sciences*, 2022, 12, 6617,

Community Feedback

- How would we add security monitoring functions to ONAP and the 5G Core?
- What other metrics should be considered to improve security and continuity of service?
- In Software Defined Networking applications, Machine Learning objective functions attempt to optimize routing paths. What's the equivalent capability to obtain that outcome for the Core?
- Potential 5G Core Machine Learning objective functions:
  - Efficient resource allocation for network slices
    - Drawing from the "route learning" for SDN, learning more efficient selection of and routes to slice resources
    - Helpful in mitigating DDoS attacks
  - How to create trust scores for 5G core services and hosting infrastructure (hypervisor + container orchestrator)?


LF
NETWORKING
LFN Developer & Testing Forum

LF NETWORKING

LFN Developer & Testing Forum

Backup Slides

Service Lifecycle

- Design service in SDC/CDS (blueprints, etc.) for basic, static deployment. A more comprehensive deployment solution can be created to include scaling and automatic configuration with a significant development effort required.
- Use Service Orchestrator to instantiate service
- Service communicates monitoring info directly to DCAE collectors.
- NFs (Network Functions) send data to DCAE via PM files (or VES events)
- PM (Performance Measurement) data processed by analytics microservice, and any outputs made available to policy or other services on DMaaP

ONAP Components for Service Design and Orchestration

- A&AI – Active and Available Inventory is the central database for managed components, infrastructure, services
- SO – The Service Orchestrator component acts on managed environment with workflows to act on, create, modify, destroy network services
- SDC – Service Design and Creation enables onboarding network components, and to design and build services
- CDS – The Controller Design Studio allows creation of controller blueprint archives and automated configuration files for VNFs/CNFs (Day 0/1/2)
- SDNC – Software Defined Network Controller contains microservices to generating VNF and VF names that are used by the CDS controller blueprint processor

Platform Architecture Diagram Honolulu Release

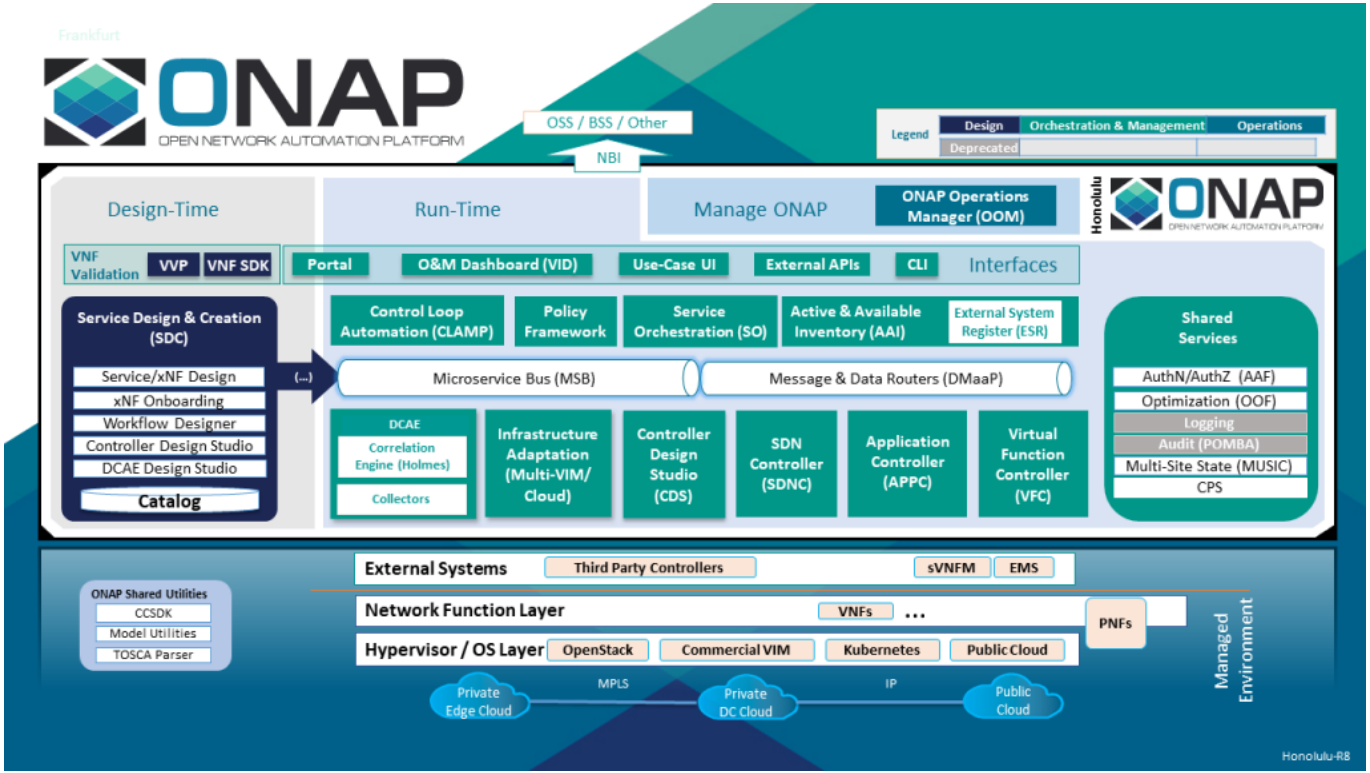


Image taken from: https://www.onap.org/architecture

Diagram of VES

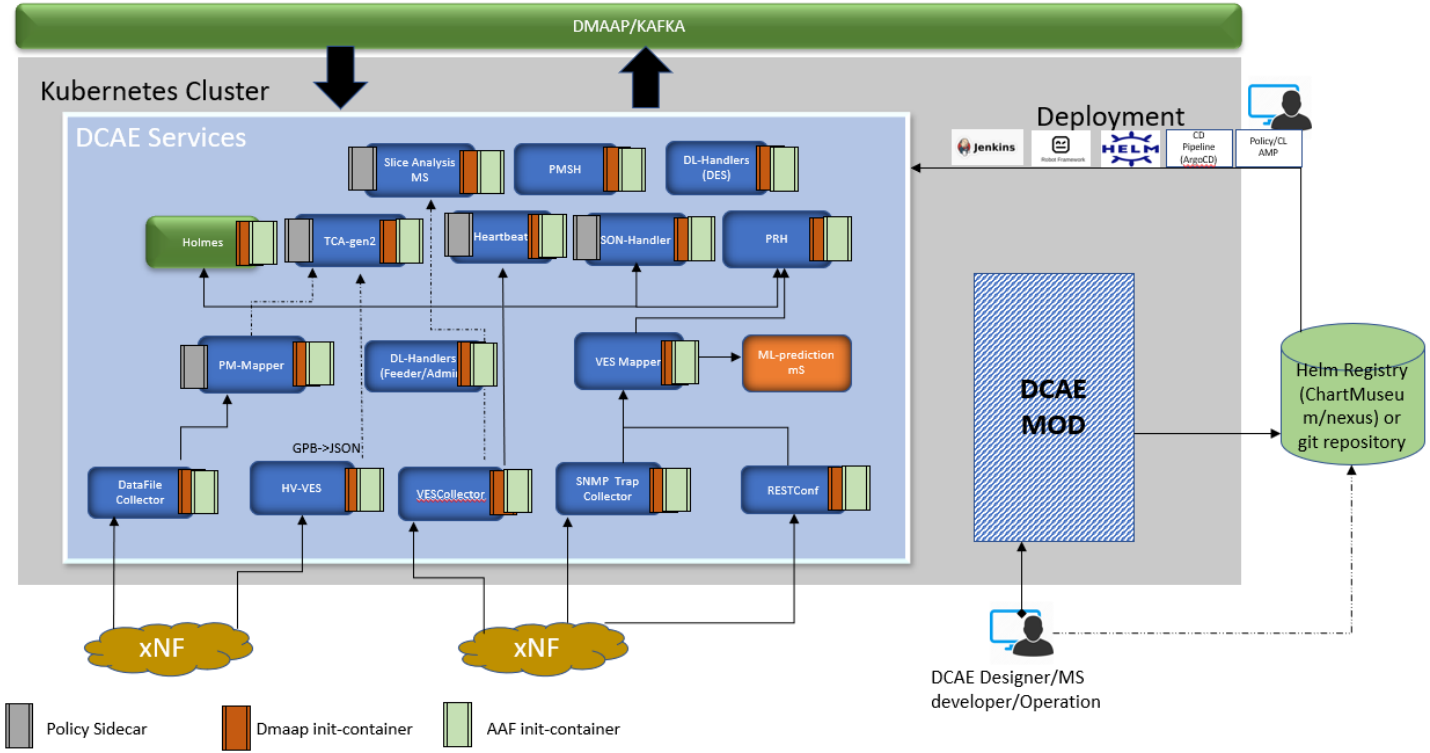


Image taken from: https://docs.onap.org/projects/onap-dcaegen2/en/latest/sections/architecture.html