Input to Akraino Edge Stack Project for 2020

by Ike Alisson

November 4th, 2019

Table of Content

AKRAINO EDGE STACK

1. Input summary (Purpose) to Akraino Edge Stack for 2020 Goals

As individuals will continuously generate Data and store, invoke and/or trigger Data to their Private and Public Clouds (to offer for AI/ML Model training, Manufacturing of Consumer and Industrial Goods (3D Printing), E-commerce/Health Services etc.), initially, for densely populated areas, such as shopping malls, schools, business offices, residential apartment areas/buildings in order to meet the dynamic shift in Data throughput/volume traffic and preserve (for AI/ML Training Models) the Data Granularity (Nature, Pattern, Characteristics) to be able to re-configure the units at the Edge as:

- IoT unit (IP-anchor node, UE-relay, CPE, IoT GW, Actuators)

  and/or

- small-cell BTS unit (compatible with O-RAN from O-RAN Alliance and/or TIP O-RAN and/or SCF (Small Cell Forum) O-RAN.

Using HW SoC (System on a Chip, GPP) that is COTS (Commercially of the Shelf) e. g. DANOS (white-box switch blueprint) Project and supporting simultaneously several Wireless Access Technologies (such as 3GPP & Wi-Fi 802.11ax through 5G CUPS and UDR & UDM and 3GPP Rel 16 ATSSS - Access Traffic Steering, Switching and Splitting) and O-RAN small cell configuration(from O-RAN Alliance or TIP O-RAN and/or O-RAN SCF (Small Cell Forum).

AKRAINO EDGE STACK

2. Criteria/Principles

To assure de-coupling of HW (COTS white-box switches) & SW and Multi-Vendor inter - operability and Solution Scalability being Vendor independent through:

- Data-centric rather than Process-centric Services that:
  - Enable dynamic End-to-End (E2E) communication
  - Intent-based, driven by Policy
  - Use Common Data Repository for all layers

AKRAINO EDGE STACK

3.1 3GPP 5G "Mobility" re-definition as ground for IoT UCs proliferation

”Mobility” Paterns Re-defined/Diversified in 5G - UEs categorized/defined as:

A) Stationary during their entire usable life (e.g., sensors embedded in infrastructure)
B) Stationary during Active Periods, but **Nomadic between activations** (e.g., Fixed Access),
C) Mobile within a Constrained & Well-Defined Space/Area
(**Spatially Restricted** e.g., in a Factory or Stadion or Airport),
D) Fully Mobile (WAN).

- to enable the offloading of IP Traffic from the 5G Network onto traditional IP routing Networks via **an IP anchor node (and UE configured as UE relay)** close to the Network Edge

(ETSI ISG MEC Group renamed "MEC" on 2017-03-28 from “Mobile Edge Computing” to “Multi- access Edge Computing”

- as UE moves, changing the IP anchor node needed in order to reduce
  - IP Traffic Load,
  - End-to-End latency
  - Better User Experience

- Seamless access to both 3PGG and non - 3GPP Network Access Technology (e.g WiFi, Bluettooth &..)

5G introduces also Dynamic Subscriber Management via GSMA Standardised eUICC OTA Solution Platform (SM-DP & SM- SR Platform)

AKRAINO EDGE STACK

3.2 5G/LTE-M for IoT with Wi-Fi Gen 6 (802.11ax) synergy to comply with 3GPP 5G Service Availability & Reliability - 1

SoC - System on Chip supporting:

3GPP LTE-M for IoT
- 1Gb/s UL + DL
- PSM,
- eDRX,
- TAU

and

Wi-Fi 802.11ax (HEW Gen 6) on OFDMA
- 1024 kB/s (4x256 QAM) with
- MU-MIMO &
- TWT

Figure 1 below provides an overview of the architecture for LTE-M (and NB-IoT) in a roaming scenario as described by 3GPP:

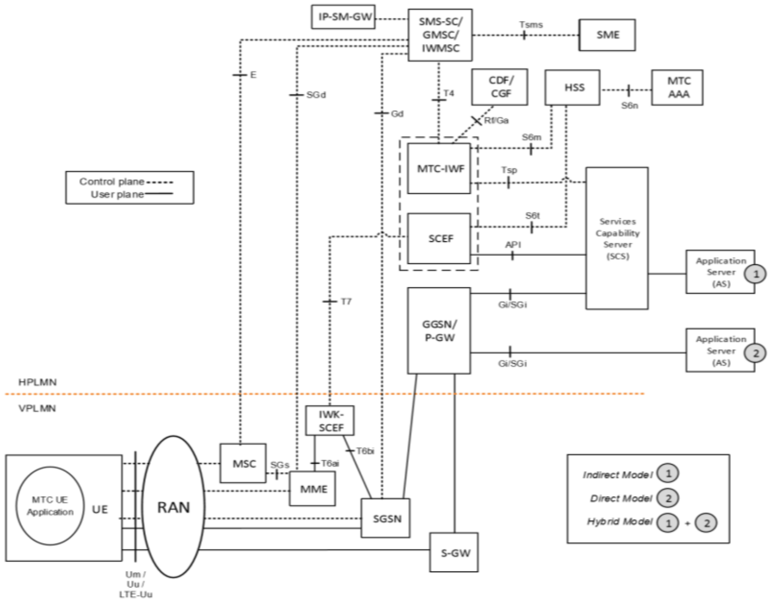


Figure 1: 3GPP Architecture for Machine Type Communication (NB-IoT and LTE-M Roaming)

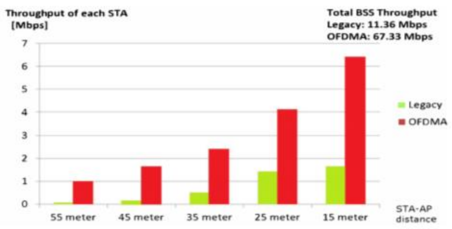


Fig. 1. OFDMA gain in the overlapped network scenario [21].

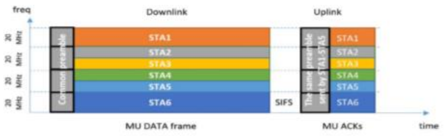


Fig. 2. An example of OFDMA transmission in 802.11ax.

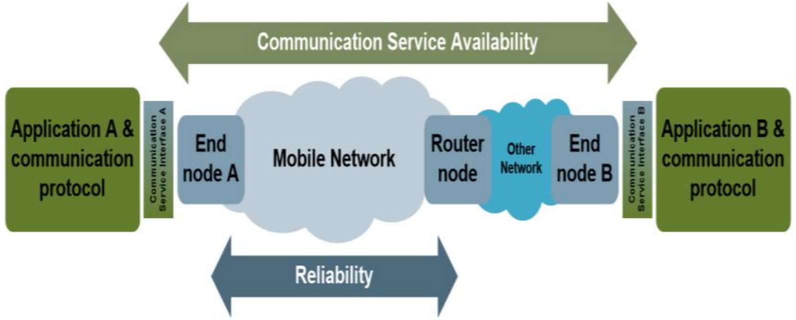


Figure C-4: Example in which communication service availability and reliability have different values. Packets are delivered over a daisy chain of a mobile network and another network (e.g., IEEE 802.11n based). Reliability is evaluated for the mobile network only, while communication service availability depends on the performance of both networks.

This scenario is not in scope for this specification, since it pertains to the particular deployment of a mobile network, but we discuss it nonetheless, as this example provides valuable insight for network operators.

This scenario describes unicast communication from application A to B. The packets are handed over from the application to the communication network at the communication service interface A, and the packets are then transmitted to the end node B. In this example, the packets are transmitted over two daisy-chained networks—one mobile network according to 3GPP specifications, and another network, e.g. a network based on IEEE 802.11n. As in the other examples above, communication service availability is measured between the two communication service interfaces, but the reliability is only measured between end node A and the router node. This has implications for, e.g., the maximum communication latency allowed for each network. In case the agreed end-to-end latency between the service interfaces is, for instance, 100 ms, and the 802.11n network has a latency of 30 ms, the maximum allowable latency for packages in the mobile network is 70 ms (NOTE). So, if the latency in the mobile network exceeds 70 ms, the communication service availability is 0%, despite the agreed QoS stipulating a larger end-to-end latency, i.e. 100 ms.

NOTE: The transit time through the router node is not considered here. It is assumed to be very small and much less than 100 ms.

AKRAINO EDGE STACK

3.2 5G/LTE-M for IoT with Wi-Fi Gen 6 (802.11ax) synergy - 2

On the Network side, with CUPS & 3GPP Rel 16 ATSSS - Access Traffic Steering, Switching & Splitting Function, there is embedded support for 3GPP & non-3GPP (Wi-Fi) Access Technologies convergence

For simplicity, Fig.3. depicts the case, where all UP services for different applications are controlled by the same CP service. However, it is also possible to have a set of CP services that are dedicated for controlling a certain set of UP services. Depending on SLAs and specific customer demands an inclusion of additional CPSs provided by 3rd parties in the framework of collaboration/partnerships may be enabled using service exposure capabilities and correspondingly designed APIs.

A typical example is Authentication and Authorisation (AA). For cellular networks, SIM-based authentication is utilized, and for fixed access networks, a line-ID or/and username and password is utilized. A network service, which is associated with an access network over which the request was initiated, is addressed and the UP is configured appropriately. The Network Services may work together through a common set of data for the customer or will configure the same UP, or will address other common network services, such as for monitoring, QoS configuration, or for an execution of common policies.

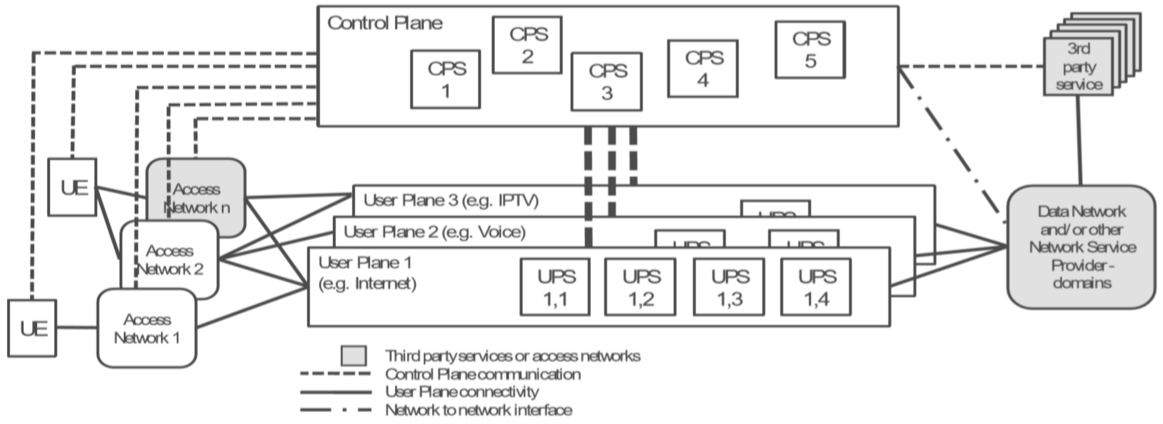


Fig.3. : Potential architecture for the use of different User Planes controlled by one Control Plane

The following Figure 6.1-3 depicts the ATSSS roaming architecture in the case of HR with N3IWF in the same PLMN as 3GPP access.

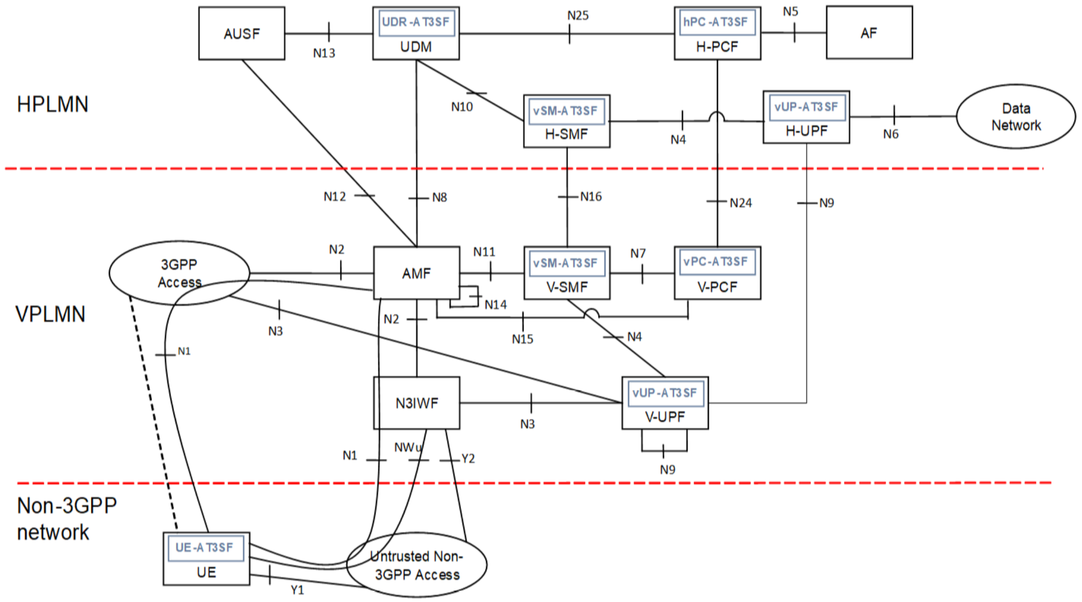


Figure 6.1-3: Roaming ATSSS architecture - HR scenario with N3IWF in same the PLMN as 3GPP access

NOTE 1: For example, the UE or the UPF may trigger the traffic splitting per packet for non-GBR service when the RTT on both accesses are on the same level, e.g. RTT1 for 3GPP is 20ms, RTT2 for non-3GPP is 25ms. The sender may gradually increase the bandwidth on each access until the RTT for this access is impacted or close to the latency threshold, e.g. 100Mbps with RTT1=20ms for 3GPP access, 200Mbps with RTT2=25ms for non-3GPP access, then keeping the routing ratio 3GPP:non-3GPP =1:2 to obtain 300Mbps with RTT=25ms.

ATSSS	Access Traffic Steering, Switching and Splitting
AT3SF	Access Traffic Steering, Switching and Splitting Function
GBR	Guaranteed Bit Rate
MA-PDU	Multi-Access Packet Data Unit
RTT	Round Trip Time

AKRAINO EDGE STACK

3.2 5G/LTE-M for IoT with Wi-Fi Gen 6 (802.11ax) synergy - 3

Scenario 1: Figure 3-1 shows an example deployment for convergence of enterprise Wi-Fi network with the 5G core network. Enterprise Wi-Fi network has a number of devices such as laptops, workstations, tablets, security camera and mobile phones connected over Wi-Fi access to a Wi-Fi AP. The enterprise Wi-Fi access network (including Wi-Fi AP and Wireless LAN Controller (WLC)) is integrated with a 5G Core network deployed by a mobile network operator. Devices connected over enterprise Wi-Fi access can access services provided by 5G core network. Some of these devices accessing 5G core network services over enterprise Wi-Fi may only support Wi-Fi radio and may not include 3GPP identity or SIM credentials on the device. Some other devices support both Wi-Fi and 5G radios and can have dual connectivity over both Wi-Fi and NR access links within the enterprise environment.

In this scenario an enterprise device supporting both radios may roam seamlessly between the enterprise Wi-Fi network and a 5G RAN managed by the mobile operator while it continues to access the enterprise network services. The mobile network operator could have certain level of visibility of and input to policy settings and network manageability of enterprise Wi-Fi access network. The enterprise IT organization could have the ability to request 5G core network resources for enterprise users.

Scenario 2: In this scenario the mobile network operator deploys and owns both the enterprise Wi-Fi access as well as the cellular 5G RAN and 5G Core. The 5G Core network sets network management related policies on the enterprise Wi-Fi network, as in Scenario 1. Devices operating in the enterprise Wi-Fi deployment can be Wi-Fi only devices (with or without 3GPP identity or SIM credentials on the device) or devices with both Wi-Fi and cellular radios. Devices supporting both radios can seamlessly roam between enterprise Wi-Fi and 5G radio access networks operated by the mobile network operator, and access relevant enterprise/5G network services using either one of the access networks.

Scenario 3: The enterprise owning the enterprise Wi-Fi network also deploys and owns a private 5G Core network to provide 5G core functionality to devices in the enterprise network. The enterprise sets network management related policies for the operation of enterprise Wi-Fi and 5G network. These policies may be defined in the 5G Core, as in other scenarios. Devices operating in the enterprise Wi-Fi deployment can be Wi-Fi only devices (with or without 3GPP identity or SIM credentials on the device) or can support both Wi-Fi and cellular radios. Devices supporting both radios can seamlessly roam to a PLMN (Public Lane Mobile Network) operator deployed 5G access network, per business agreements. Such dual radio devices can access enterprise network services while connected over PLMN operator 5G RAN.

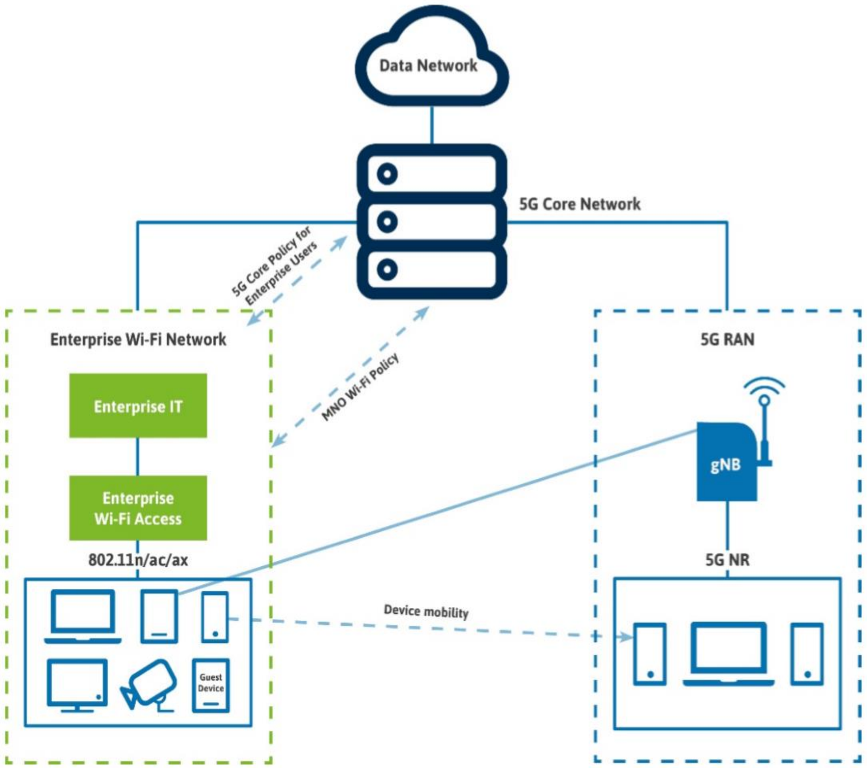


Figure 3-1 Example Deployment for Convergence of Enterprise Wi-Fi with 5G

3.2 5G/LTE-M for IoT with Wi-Fi Gen 6 (802.11ax) synergy UDR & UDM - 4

Common Data Repository through
UDR - Unified Data Repository and
UDM - Unified Data Management

Figures 4-1 shows the data storage architecture for the 5GC:

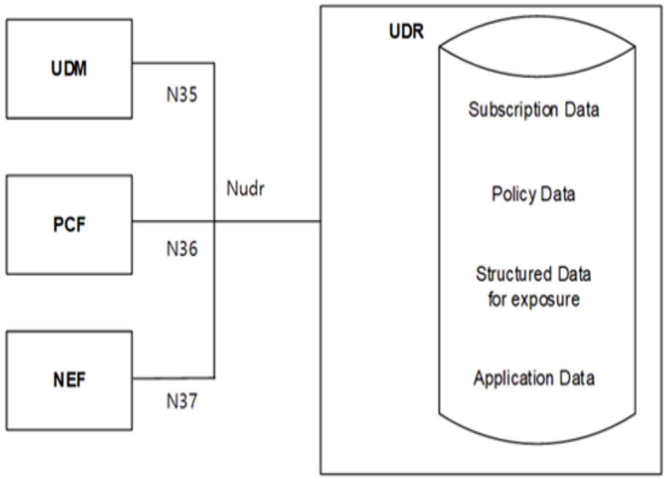


Figure 4-1: Data storage architecture

The Nudr interface is used by the network functions (i.e. UDM, PCF and NEF) to access a particular set of the data stored in the UDR.

Within the 5GC, the UDM – Unified Data Management, offers Services to the AMF- Access and Mobility Management Function , SMF - Session Management Function, SMSF - Short Message Service Function, NEF - Network Exposure Function , GMLC - Gateway Mobile Location Centre, NWDAF - Network Data Analytics Function and AUSF - Authentication Server Function via the Nudm Service based Interface (see 3GPP TS).

Figure 4.1-1 provides the reference model (in service based interface representation and in reference point representation), with focus on the UDM.

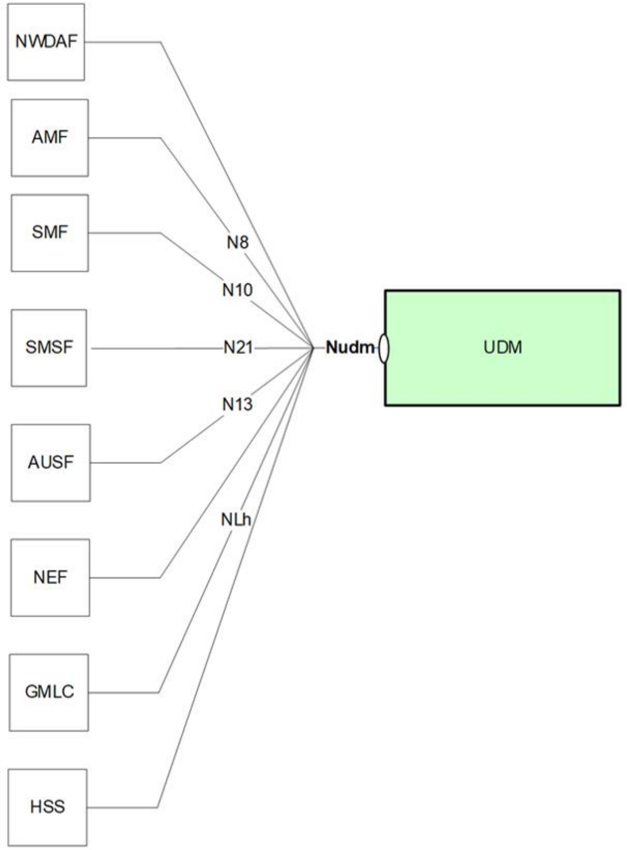


Figure 4.1-1: Reference model – UDM

AKRAINO EDGE STACK

3.2 5G/LTE-M for IoT with Wi-Fi Gen 6 (802.11ax) synergy - KP (Knowledge Plane) & AMC (Autonomic Management & Control) - 5

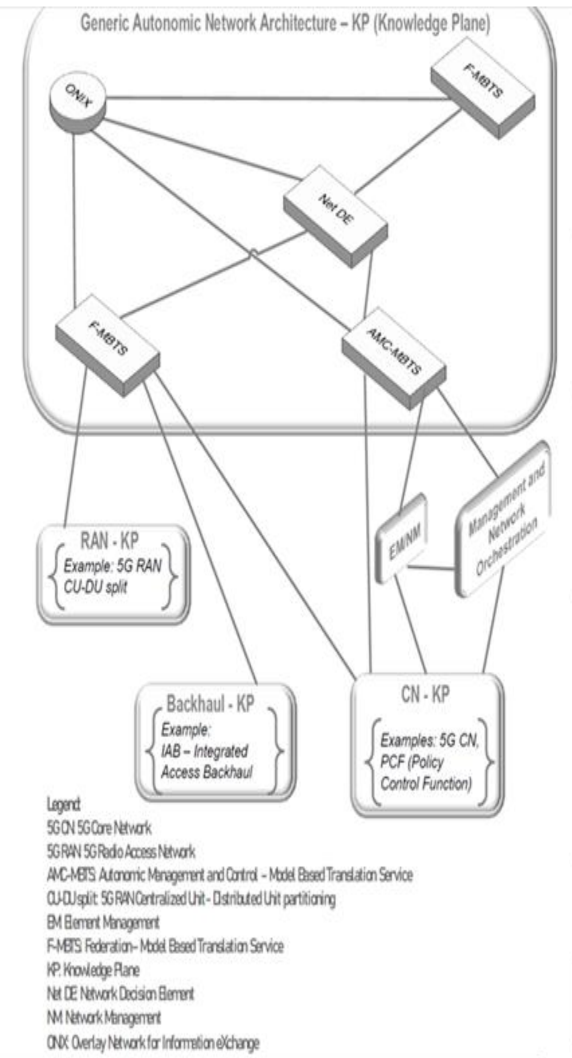


Fig.7. Exemplification of AMC KP in a 5G mobile access system

- The network analytics functions performed by interworking modularized Autonomic Managers (AMs) using the and associated shared Knowledge Bases (KBs), which execute as software with real-time and predictive analytics as loadable modules or applications, shall be supported.
- Multi-Layer autonomics, such as the abstraction levels at which autonomic and cognitive capabilities can be embedded, shall be supported. For example, this multi-layer architecture includes E2E Service Orchestrator, SDN controllers, OSS, NFVO, VNFM, VIM, EM, virtualization layer as a multi-tenant platform

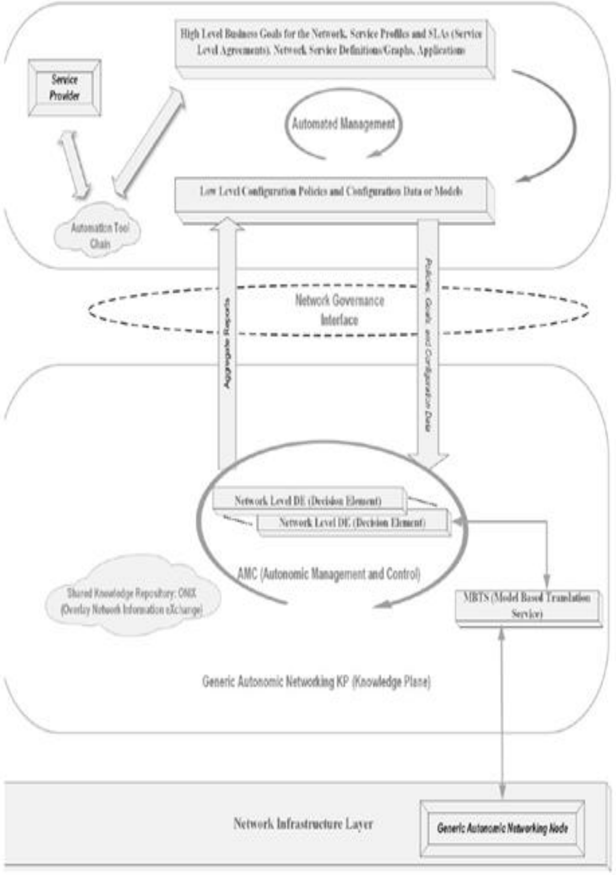


Fig.5. Illustration of entities in an autonomic management and control environment

Autonomic Management is distinct relative to **Automated Management**. The former emphasizes ***Learning, Reasoning, & Adaptation***, while the latter focuses on **Efficient Workflow Implementation & Automation of the Processes** involved in the Creation of Network Configuration and Monitoring Tasks.

Automated Management provides input to the **AMC**. Indeed, **AMC** must exhibit a **Network Governance Interface** through which the input that governs the **Configuration of an Autonomic Network** should be provided. **AMC** exposes **Views & Reports** to the **Automated Management Process**.

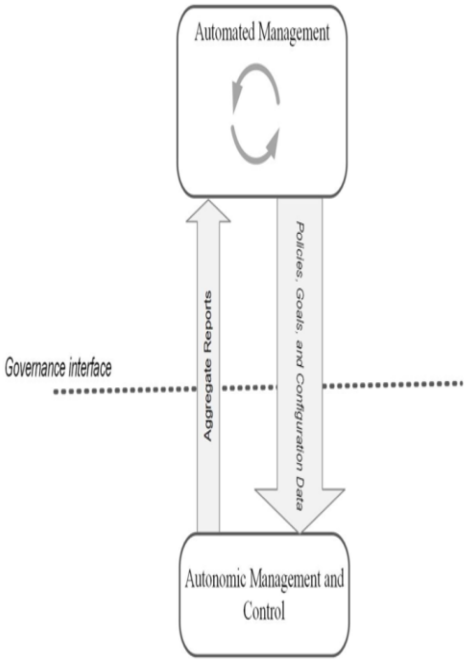


Fig.4. Automated Management vs Autonomic Management illustration (their interaction and complementarity)

The Cognitive Capabilities embedded within a DE (Decision-making Element also referred as AM-Autonomic Manager element) utilize AI & ML Models of Learning & Responding to Dynamic Shifts in the System & Environmental Contexts, through slow and fast feedback control loops. The DEs are part of the KP (Knowledge Plane) in the AMC Framework with various relationships & interfaces associated with a variety of Human Stakeholders that represent Diverse Roles & Functional Responsibilities. The Consumer of DEs could interact with Vendors/Suppliers for Changes or Updates, via a related Catalog or Marketplace of Advertised Deployable AI & ML Models, utilized within a DE (Decision-making Element).

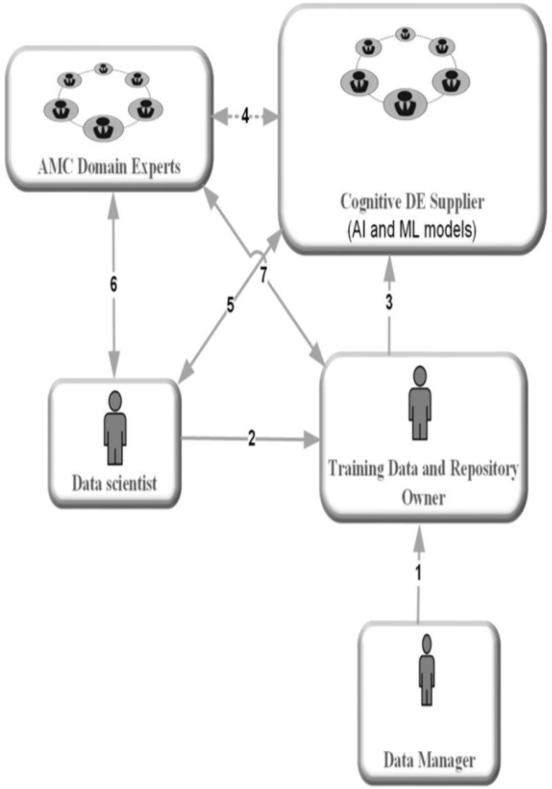


Fig.6. Stakeholder interfaces and relationships with a cognitive AMC framework

AKRAINO EDGE STACK

3.3 LF DANOS Project white-box switch blueprint

- AT&T will deploy 60,000 dNOS 5G Routers compliant with the white box (run on Vyatta NOS Linux) DANOS Project specification
  - white box blueprint "decouples HW from SW" so any organization can build its own compliant systems running other SW. The white box spec appears to be OS agnostic.

The software architecture of dNOS envisions three high level layers; the base operating system, the control and management plane, and the data plane. The key functional components and their interfaces are depicted in Figure 2.

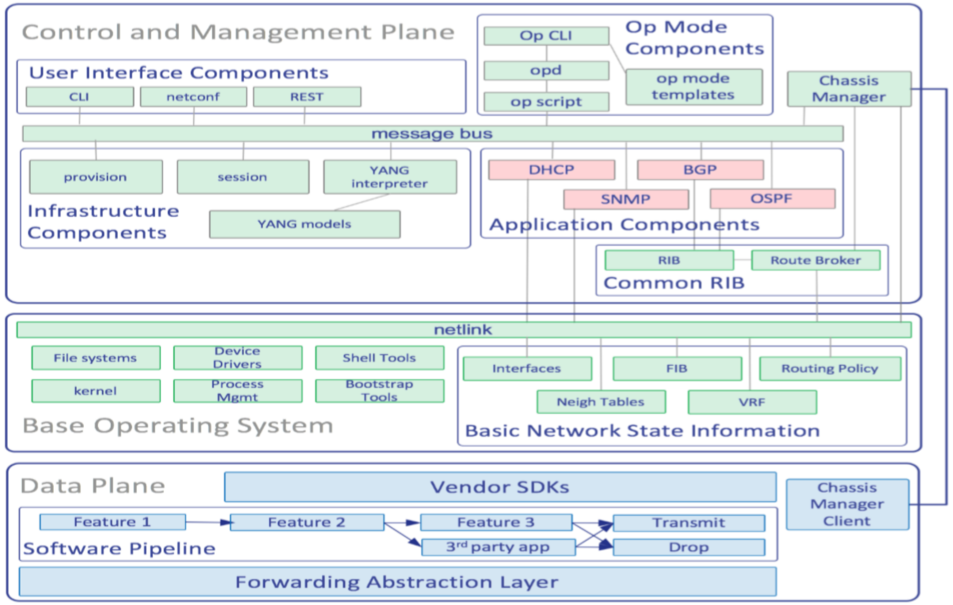


FIGURE 2 - DNOS SOFTWARE ARCHITECTURAL OVERVIEW

Colors correspond to layers represented in Figure 1

2 Key Functional Components of dNOS

The following is an abstract representation of the functional components in the system.

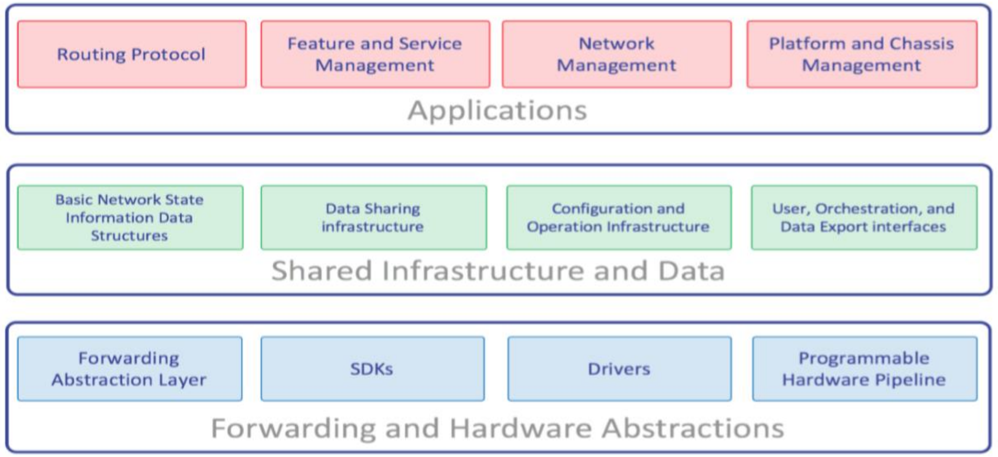
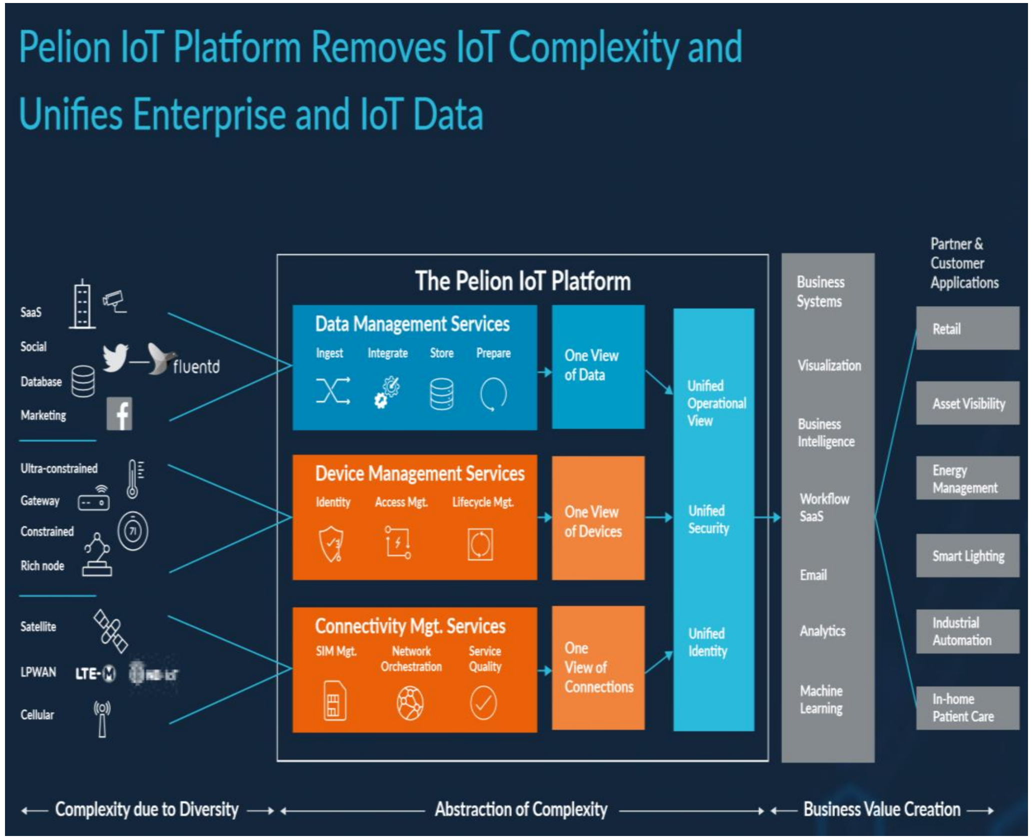


FIGURE 1 - DNOS FUNCTIONAL LAYERS AND COMPONENTS

AKRAINO EDGE STACK

3.4 Arm SoC and Arm Pelion IoT Connectivity Management Platform

- Arm Cortex - M is a SoC for IoT
- Arm Pelion IoT Platform is a Platform for Device & Connectivity Management handling eSIM with UICC profiles managed OTA via GSMA Standardized Platform (SM-DP & SM - SR).
- Arm applies also Flexible Access Business Model enabling to use Arm's HW & SW for free during testing and selection analysis of the HW & SW



Alternatively, Flexible Access provides access to a wider range of IP products, support, tools and training for unlimited design time and with payment due only at the point of manufacture. The licensing model includes a wide range of Cortex-A, Cortex-R and Cortex-M CPUs, Mali GPUs, Corstone foundation IP package, System IP, Security IP and Artisan physical IP libraries.

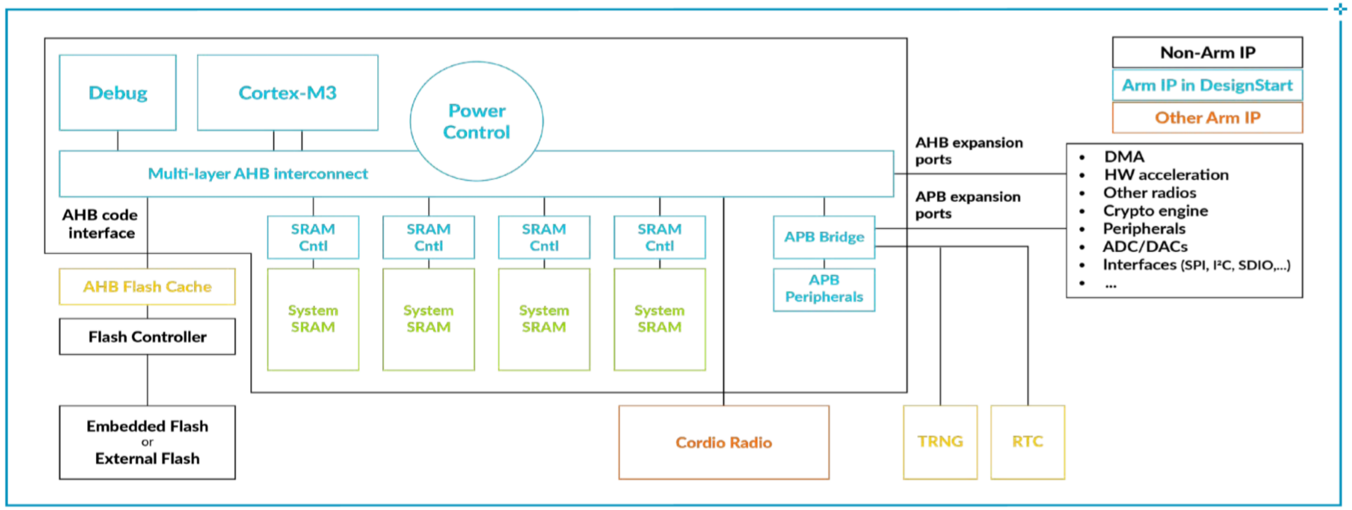


Figure 4: *SSE-050 subsystem block diagram*

AKRAINO EDGE STACK

3.5 vRAN/O-RAN from Wind River/Intel (Akraino vRAN blueprint)

As Wind River/Intel had already provided to Akraino a blueprint for vRAN Solution by integrating ALTIOSTAR RAN Solution (for vRAN), the latter (ALTIOSTAR) is also Compliant with O-RAN Specifications from TIP (Telecom Infra Project - Facebook) O-RAN Specification written/led by Vodafone and Telefonica and deployed in selected markets e.g. UK, Turkey, Africa).

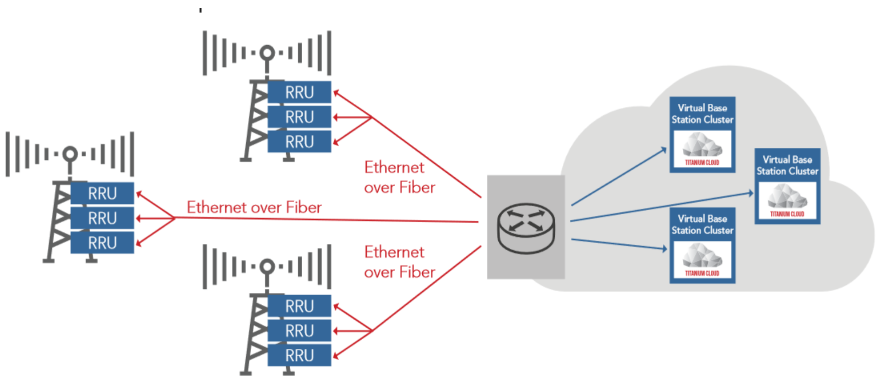


Figure 4. Virtual RAN

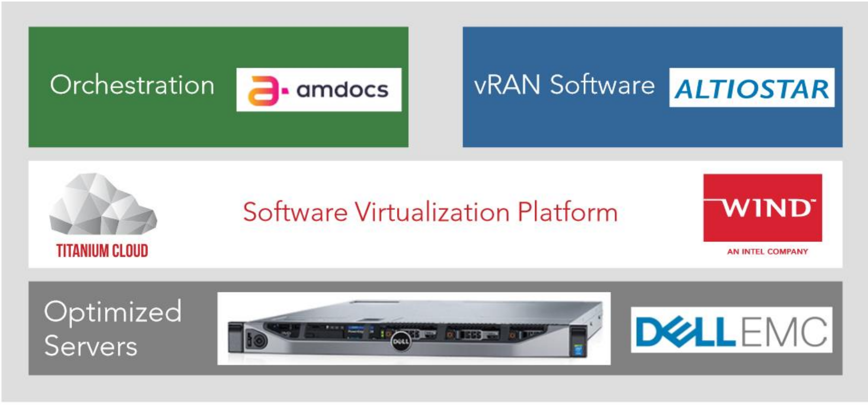


Figure 5. Introducing an end-to end solution for vRAN

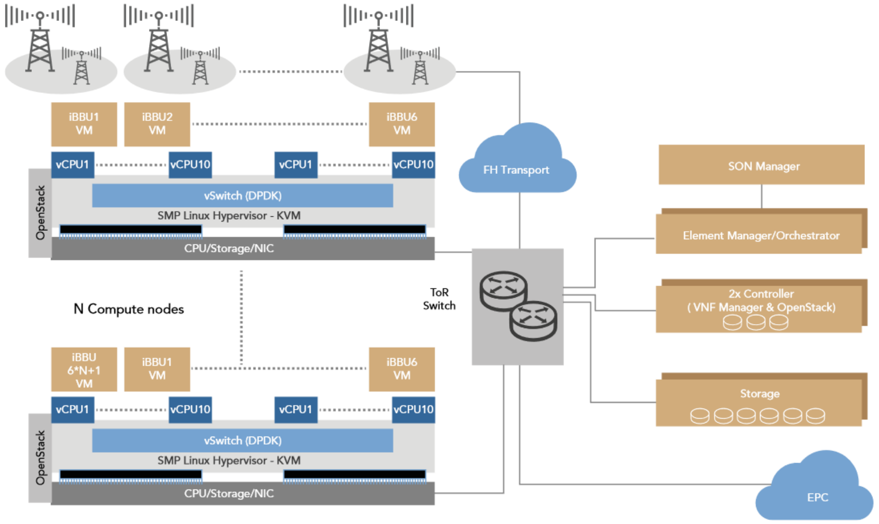


Figure 6. NFV architecture on commercial off-the-shelf hardware

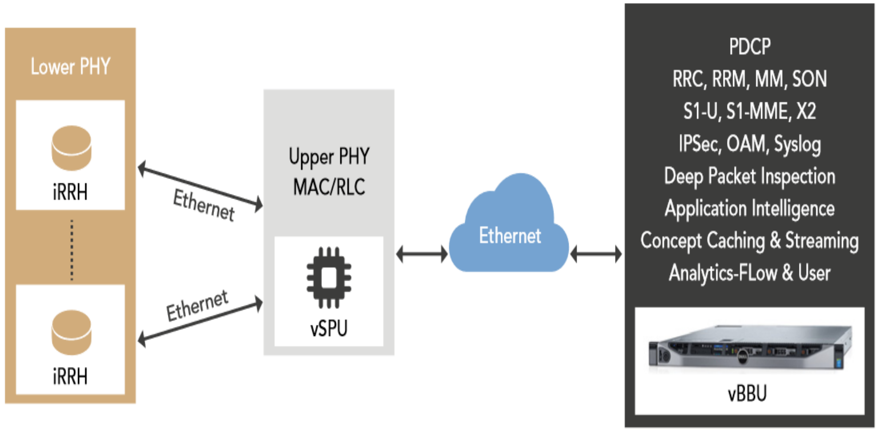


Figure 7. Altiostar vRAN architecture: Functional split options

AKRAINO EDGE STACK

3.6 SCF (Small Cell Forum) nFAPI Specification for O-RAN 3GPP backwards compatible with 3GPP (4G & 3G) Specifications

- SCF (Small Cell Forum) provided specification for O-RAN that is backward compatible to 3GPP RAN 3G Specification
- Some of the involved Companies contributing to the preparation of the Specification (that already participate at LF Akraino) are:
- Intel, Nokia, Qualcomm

- Link to SCF Specification from June 2019: [Small_Cell_Forum_222_5G_O_RAN_FAPI_PHY_SPI_Specification_10_0_June_2019.pdf]

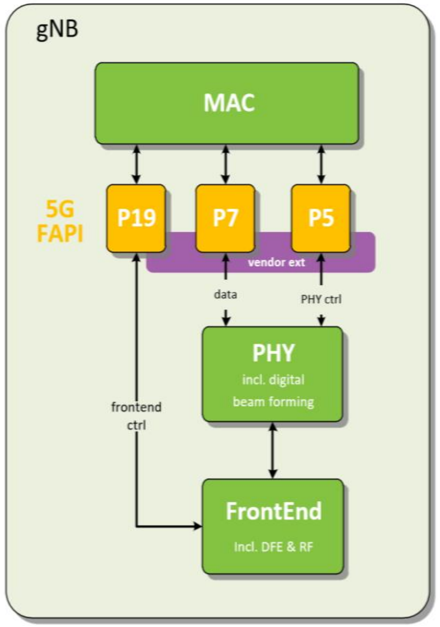


Figure 1-2 5G FAPI Architecture

The introduction of 5G nFAPI with MAC and PHY residing in different physical locations, a central unit (CU) and distributed unit (DU), is outside the scope of this document version.

4. Summary:

If the units on the Edge interchangeably can be designed/configured from Data-centric Services Management point of view and interchangeably be turned/re-configured as IoT units and/or small-cell BTS and then, with the CN KP (Knowledge Plane) and AMC (Autonomic Management and Control), provide Service and Management Automation handled from (2) main Criteria:

1. Preserve/retain and use of Data Granularity (Nature/Pattern/Characteristics) for AI/ML Model building for providing/offering of Personalized Services and Goods (Health, Banking, Household goods manufacturing, 3D Printing Personalized goods etc.)

2. Data volume throughput dynamic adaptation (with regard to the former above) can/will also be automated and therein assure the Network and Service Availability, Quality, Reliability and Security.

AKRAINO EDGE STACK