ETSI TR 103 747 V1.1.1 (2021-11)

Core Network and Interoperability Testing (INT/WG AFI); Federated GANA Knowledge Planes (KPs) for Multi-Domain Autonomic Management & Control (AMC) of Slices in the NGMN® 5G End-to-End Architecture Framework

Reference
DTR/INT-00165

Keywords
artificial intelligence, slicing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Core Network and Interoperability Testing (INT).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document provides a mapping and evaluation of architectural components for autonomic network management & control developed/implemented in the EU-funded SliceNet Project to the ETSI AFI Generic Autonomic Networking Architecture (GANA) model - an architectural reference model for autonomic networking, cognitive networking and self-management. It serves to provide useful insights to implementers of ETSI GANA Knowledge Plane (KP) Platforms on approaches that can be taken in implementing ETSI GANA Knowledge Plane Platforms and how to federate them for E2E (Cross-Domain) Autonomic Management and Control (AMC) operations across network segments such as Radio Access Networks (RANs), Transport Networks and Core Networks. It goes further to discuss how to address the AMC Requirements specified in NGMN® E2E 5G Architecture by a way of providing insights on how ETSI GANA KP platforms in an E2E 5G Architecture can address the AMC requirements, while leveraging experiences gained in SliceNet Project in implementing GANA autonomic/cognitive management and control software components for 5G network slices.

1 Scope

The present document presents a plausible approach to implementing Federated GANA Knowledge Planes (KPs) Platforms for E2E Multi-Domain Federated Autonomic Management and Control (AMC) of 5G Network Slices in NGMN® E2E 5G Architecture, using components prototyped and implemented in the European Union (EU) funded SliceNet Project (Grant Agreement N° 761913). The present document produces and leverages a mapping of architectural components for autonomic network management & control developed/implemented SliceNet Project to the ETSI TC INT AFI Generic Autonomic Networking Architecture (GANA) model - an architectural reference model for autonomic networking, cognitive networking and self-management. The mapping identifies the components that were prototyped in Slicenet Project that can be used to implement specific GANA Functional Blocks (FBs) for Autonomics and their associated Reference Points (Rfps), while providing the illustrations that help implementers of GANA autonomics in 5G networks. Other aspects covered in the present document are:

- A Study of GANA aligned AMC Requirements in the NGMN® 5G E2E Architecture in order to provide answers on how the approach presented in the present document can help implementers of GANA AMC solutions for 5G.
- Providing useful insights to implementers of ETSI GANA Knowledge Plane (KP) Platforms on approaches that can be taken in implementing ETSI GANA Knowledge Plane Platforms and how to federate them for E2E (Cross-Domain) Autonomic Management and Control (AMC) operations across network segments such as Radio Access Networks (RANs), Transport Networks and Core Networks.
- Providing insights on leveraging experiences gained in SliceNet Project in implementing GANA autonomic/cognitive management and control software components for 5G network slices.

The mapping of the components to the GANA model concepts serves to illustrate how to implement the key abstraction levels for autonomics (self-management functionality) in the GANA model for the targeted wireless networks context, taking into consideration the work done in ETSI TR 103 495 [i.26].

It also shows how GANA can be implemented using the components developed in SliceNet project as an example.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI White Paper No.16 GANA: "Generic Autonomic Networking Architecture Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services".

NOTE: Available at http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp16_gana_Ed1_20161011.pdf.

[i.2] ETSI TS 103 195-2 (V1.1.1): "Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management".

NOTE: Available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=50970.

[i.3] ETSI 5G PoC on 5G Network Slices Creation, Autonomic & Cognitive Management & E2E Orchestration-with Closed-Loop (Autonomic) Service Assurance for the IoT (Smart Insurance) Use Case.

NOTE: More information at https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals.

[i.4] White Paper No.1 of the ETSI 5G PoC: "C-SON Evolution for 5G, Hybrid SON Mappings to the ETSI GANA Model, and achieving E2E Autonomic (Closed-Loop) Service Assurance for 5G Network Slices by Cross-Domain Federated GANA Knowledge Planes".

NOTE: More information at https://intwiki.etsi.org/images/ETSI_GANA_in_5G_PoC_White_Paper_No_1_v1.28.pdf.

[i.5] ETSI TR 103 473 (V1.1.2): "Evolution of management towards Autonomic Future Internet (AFI); Autonomicity and Self-Management in the Broadband Forum (BBF) Architectures".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103400_103499/103473/01.01.02_60/tr_103473v010102p.pdf.

[i.6] ETSI TR 103 404: "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Autonomicity and Self-Management in the Backhaul and Core network parts of the 3GPP Architecture".

[i.7] ONAP® Open Source Project: "ONAP Architecture Overview".

NOTE 1: Available at https://www.onap.org/.

NOTE 2: Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

[i.8] BBF CloudCO Open Source Project.

NOTE: Available at https://www.broadband-forum.org/cloudco.

[i.9] OPNFV® Open Source Project.

NOTE 1: Available at https://www.opnfv.org/.

NOTE 2: Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

[i.10] ONOS Open Source Project.

NOTE: Available at https://onosproject.org/.

[i.11] OpenDayLight® Open Source Project.

NOTE 1: Available at https://www.opendaylight.org/.

NOTE 2: Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

[i.12] ETSI OSM (Open Source MANO).

NOTE: Available at https://osm.etsi.org/.

[i.13] ACUMOS ®: "An Open Source AI Machine Learning Platform".

NOTE 1: Available at https://www.acumos.org/.

NOTE 2: ACUMOS® is a registered trademark of LF Projects, LLC.

[i.14] White Paper No.3 of the ETSI 5G PoC: "Programmable Traffic Monitoring Fabrics that enable On-Demand Monitoring and Feeding of Knowledge into the ETSI GANA Knowledge Plane for Autonomic Service Assurance of 5G Network Slices; and Orchestrated Service Monitoring in NFV/Clouds".

NOTE: Available at ETSI_5G_PoC_White_Paper_No_3_2019_v1.19.pdf.

[i.15] White Paper No.2 of the ETSI 5G PoC: "ONAP Mappings to the ETSI GANA Model; Using ONAP Components to Implement GANA Knowledge Planes and Advancing ONAP for Implementing ETSI GANA Standard's Requirements; and C-SON - ONAP Architecture".

NOTE: Available at ETSI_5G_PoC_White_Paper_No_2_Final_v7.3.pdf.

[i.16] ETSI 5G PoC Report on Specifications of Integration APIs for the ETSI GANA Knowledge Plane Platform with Other Types of Management & Control Systems, and with Info/Data/Event Sources in general.

NOTE: Available at https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals.

[i.17] ETSI TS 129 520 (V16.6.0): "5G; 5G System; Network Data Analytics Services; Stage 3 (3GPP TS 29.520 version 16.6.0 Release 16)".

[i.18] ETSI TS 128 533 (V15.0.0): "5G; Management and orchestration; Architecture framework (3GPP TS 28.533 version 15.0.0 Release 15)".

[i.19] 5G End-to-End Architecture Framework by NGMN® Alliance: "P1-Requirements and Architecture: NGMN® 5G E2E Architecture Framework v3.0.8".

NOTE: Available at https://www.ngmn.org/publications/5g-end-to-end-architecture-framework-v3-0-8.html.

[i.20] White Paper No.4 of the ETSI 5G PoC: "ETSI GANA as Multi-Layer Artificial Intelligence (AI) Framework for Implementing AI Models for Autonomic Management & Control (AMC) of Networks and Services; and Intent-Based Networking (IBN) via GANA Knowledge Planes (KPs)".

NOTE: Available at ETSI_5G_PoC_White_Paper_No_4_v3.1.pdf.

[i.21] White Paper No.6 of the ETSI 5G PoC: "Generic Framework for Multi-Domain Federated ETSI GANA Knowledge Planes (KPs) for End-to-End Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Networks/Services".

NOTE: Available at ETSI_5G_PoC_White_Paper_No_6.pdf.

[i.22] ETSI GS AFI 002 (V1.1.1): "Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture (An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management)".

[i.23] SliceNet Project Deliverable D5.7: "Framework for Cognitive SLA and QoE Slice Management", December 2019.

NOTE: Available at https://doi.org/10.18153/SLIC-761913-D5_7.

[i.24] SliceNet Project Deliverable D5.5: "Modelling, Design and Implementation of QoE Monitoring, Analytics and Vertical-Informed QoE Actuators, Iteration I.

NOTE: Available at https://doi.org/10.18153/SLIC-761913-D5_5.

[i.25] SliceNet Project Deliverable D5.6: "Modelling, Design and Implementation of QoE Monitoring, Analytics and Vertical-Informed QoE Actuators, Iteration II".

NOTE: Available at https://doi.org/10.18153/SLIC-761913-D5_6.

[i.26] ETSI TR 103 495: "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Autonomicity and Self-Management in Wireless Ad-hoc/Mesh Networks: Autonomicity-enabled Ad-hoc and Mesh Network Architectures".

[i.27] White Paper No.5: "Artificial Intelligence (AI) in Test Systems, Testing AI Models and ETSI GANA Model's Cognitive Decision Elements (DEs) via a Generic Test Framework for Testing GANA Multi-Layer Autonomics & their AI Algorithms for Closed-Loop Network Automation".

NOTE: Available at ETSI_5G_PoC_White_Paper_No_5.pdf.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AFI	Autonomic Future Internet
AIOPS	Artificial Intelligence for IT Operations
AMC	Autonomic Management & Control
AMF	Access and Mobility Management Function
AN	Autonomous Network
API	Application Programming Interface
AUSF	AUthentication Server Function
BBF	BroadBand Forum
CN	Core Network
CP	Control Plane
CPS	Control Plane Services
CPSR	Control Plane Service Register
CPU	Central Processing Unit
CRUD	Creation/Configuration, Read, Update and Delete
C-SON	Centralized Self Organizing Network
CSP	Communications Service Provider
DB	DataBase
DDCM	Data-Driven Control and Management
DE	Decision making Element
DP	Data Plane
DSON	Distributed SON
DSP	Digital Service Provider
E2E	End-to-End
EMS	Element Management System
EPC	Evolved Packet Core
EPS	Edge Packet Service
FCAPS	Fault, Configuration, Accounting, Performance, Security
FGE	Forward Graph Enabler
GANA	Generic Autonomic Network Architecture
GW-C	GateWay-Control plane
GW-U	GateWay-User plane
IBN	Intent-Based Networking
ICT	Information and Communications Technology
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPC	Inter PoP Connection

ISG	Industry Specification Group
IT	Information Technology
JSON	Java Script Notation Object
KB	Knowledge Base
KP DE	Knowledge Plane Decision-making Element
KP	Knowledge Plane
KPI	Key Performance Indicator
LL-MEC	Low-Latency MEC
MANO	MANagement and Orchestration
MAPE-K	Monitor-Analyze-Plan-Execute over a shared Knowledge
MB	MegaByte
MBTS	Model-Based Translation Service
MDAS	Management Data Analytics Service
MEC	Mobile Edge Computing
ML	Machine Learing
NBI	Northbound interface
NE	Network Element
NF	Network Function
NFV	Network Function Virtualisation
NFVO	NFV Orchestrator
NGMN®	Next Generation Mobile Networks
NMR-O	NFV MEC RAN Orchestrator
NRF	Network Repository Function
NS	Network Slice
NSO	Network Service Orchestrator
NSP	Network Service Provider
NSS	Network Sub-Slice
NSSF	Network Slice Selection Function
NSST	Network Slice Subnet Templates
NST	etwork Slice Template
NWDAF	Network Data Analytics Function
OAI	OpenAirInterface
ONAP	Open Network Automation Platform
ONIX	Overlay Network for Information eXchange
OOB	Out-Of-Band
OODA	Observe-Orient-Decide-ACT
OSA	One Stop API
OSM	Open Source MANO
OSS	Operations Support Systems
OVS	Open Virtual Switch
P&P	Plug & Play
PAP	Policy Administration Point
PCF	Policy Control Function
PCI	Policy Catalogue & Inventory
PCM	Policy Control Manager
PCS	Proactive Control Scheme
PDP	Policy Decision Point
PF	Policy Framework
PGW	Packet Gateway
PNF	Physical Network Function
PR	Policy Recommender
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
REST	Representational State Transfer
RNIS	Radio Network Information Service
SBA	Service Based Architecture
SBI	Service Based Interface
SDK	Software Development Kit
SDN	Software Defined Networks
SDO	Standards Development Organizations
SGW	Serving GateWay

SLA	Service Level Agreement
SMF	Session Management Function
SNMP	Simple Network Management Protocol
SON	Self Organizing Networks
SS-O	Service and Slice Orchestrator
TAL	Tactical Autonomic Language
TCAM	Ternary Content Addressable Memories
UDM	Unified Data Management
UE	User Equipment
UI	User Interface
UP	User Plane
UPF	User Plane Function
VIM	Virtual Infrastructure Management
VLAN	Virtual LAN
VNF	Virtual Network Function
WAN	Wide Area Network
WG	Working Group
WIM	WAN Infrastructure Manager

4 Principles for Autonomic Networking and Autonomic Management & Control (AMC), and Enablers

4.1 Overview on Autonomics Principles and Enablers for Autonomic Networking, Autonomic Management & Control (AMC), and Autonomous Networks

Autonomic systems rely on an autonomic elements which regularly sense the possible sources of change through sensors, reason about the current situation and arrange adaptations through actuators. Autonomous networks focuses on the definition of closed loops (MAPE-K, OODA, cognitive loop, etc.) or controllers as enablers for autonomy in future networks. The Autonomous Networks aims to define fully automated innovative network and services for vertical industries' users and consumers, supporting self-configuration, self-healing, self-optimizing and self-evolving network infrastructures. Autonomous Networks incorporate a simplified network architecture, autonomous domains and automated intelligent business/network operations for the closed control loop, offering the best-possible user experience, full lifecycle operations automation/autonomy and maximum resource utilization. One of the Key inseparable features of an autonomic system is a need of continuous monitoring.

Self-manageability in GANA is achieved through instrumenting the network with autonomic Decision-making-Elements (DEs), which automate network operations by implementing control loops. Such control loops operate using the knowledge regarding events and the state of network resources.

The GANA model defines a generic Autonomic Management and Control (AMC) framework and structure within which to specify and design autonomics-enabling functional blocks for any network architecture and its management architecture. Autonomic Management & Control is about Decision making elements (Des) as autonomic functions with cognition introduced in control and management plane. Cognition is seen as learning and reasoning used to effect advanced adaptation in Decision making Elements. Control is about control-logic as the core of DE that realizes a control-loop in order to adjust network resources/parameters or services. From an architecture perspective, AMC Framework and 3GPP Hybrid-SON (Self Organizing Network) model are compatible with each other. Both shares common design principles on enabling implementers of autonomics algorithms to combine centralized and distributed control of network resources, parameters and services. Federation of AMC allows knowledge exchanging, sharing, interaction and collaboration among KPs with each KP platform governing and controlling the behaviour of an autonomic system.

The following concepts and paradigms help implementers of ETSI GANA autonomics in understanding important taxonomy of terms and concepts that related in this area of the drive to smart and self-driving networks:

- **Autonomic Network (AcN)--concept:** An Autonomic Network either refers to the Network Infrastructure made up of Network Elements/Functions (NEs/NFs) that exhibit autonomics (control-loops) in their behaviors, or is the inclusion together of Network Infrastructure with some level of autonomics (control-loops) in NEs/NFs and its associated Management and Control architecture that also exhibits autonomics (Control-Loops) at that higher level. A Multi-Layer AcN's property of being "autonomic" (also called "**autonomicity**" (a paradigm) in ETSI Standards such as [i.2]), relates to **Hierarchical (nested) and Interworking Control-Loops introduced at various Abstraction Levels (from NE/NF level) up into the Management & Control Systems Level of the Network**.

NOTE: On the journey to implementing an Autonomous Network (AN) with certain degree of autonomy, the starting point is designing the network as an Autonomic Network (AcN) as the foundation. The science of Control-Loops (called "**Autonomics**") is key enabler for achieving the property of being autonomous, and that an AcN is expected to evolutionarily "maximize" the property of being "autonomous" in as far as the "**Degree and Measure of Operations Tasks that can be performed by the autonomic network (AN) without direct human involvement in the decision and actions**".

- **An Autonomous Network (AN)--concept: An AN is a network that exhibits a property called Degree of Autonomy that** pertains to the Degree and Measure of Operations Tasks that can be performed by an Autonomic Network (AcN) without direct human involvement in the decision and actions, thanks to Autonomics (the science of Control-Loops) in-built in the AcN as the enablers for the autonomous behavior (an operational property of the autonomic network). The Degree of Autonomy is associated with Maturity Levels for Autonomy that are increasingly attained by the Autonomic Network (AcN) over time, thanks to the Evolution of the Autonomics (Control-Loops) by enrichment of automation in network and services management and control intelligence in the Control-Loops to maximize the autonomic network's property of being Autonomous. In ICT networks, AN is to be governable by Human Operator through inputs such as business goals and policies and other governance inputs such an Intents, Service Level Agreements (SLAs) for services to be delivered by the AN.

- **Automated Management (a paradigm):** It is about **workflow reduction and automation** i.e. **automation of the processes** involved in the creation of network and/or service configuration inputs using specialized task **automation tools (e.g. scripts, automated workflow management tools, network planning tools, policy generators for conflict-free policies, intents, goals, Service Level Agreement (SLAs), etc.)** such that the Inputs can be provided by the Human Operator to the Autonomic Network (AcN) or Autonomous Network (AN) to govern its operation. The Inputs (high-level inputs), also called Governance Objectives/Goals for the AcN/AN are further operated upon by the AcN/AN to further derive detailed low-level configuration data and actions that are then applied by the AcN/AN on its own to self-configure and execute other self-* operations such as self-optimization, self-diagnosis, self-repairing/healing, self-protection during its operation. The AcN/AN exposes an interface called the **Governance Interface** through which the **Automated Management realm** provides the Governance Inputs (Objectives/Goals) to the AcN/AN. The same Governance Interface of the AcN/AN is used by the AcN/AN to provide feedback to the Human (through Tools of the Automated Management realm) in form of Reports that provide insights such as how the AcN/AN is fairing in fulfilling the Objectives, or feedback in form escalations that the AcN/AN would like the Human Operator to get involved in the decisions on how to handle certain situations the AcN/AN has encountered.

- **Autonomic Management and Control (AMC) -a paradigm:** It emphasizes **learning, reasoning, and adaptation** using control-loops that also take into consideration the feedback knowledge obtained from network and services monitoring**. Automated Management** provides Input (Governance Inputs) to the Autonomic Management & Control (AMC) of Networks and Services Domain ("area/space"). [i.1] and [i.2] define the AMC paradigm as the interworking of nested and hierarchical control-loops and associated logics introduced in the Management Plane, in the Control Plane, and also in the converged (non-disaggregated) Management Planes and Control Planes (as there are such cases). Indeed, Autonomic Management & Control should exhibit a network Governance Interface through which the input that governs the configuration of an Autonomic Network (AcN) should be provided by the human operator. Thanks to automation tools and mechanisms (Automated Management), by using a high-level language, the operator can define the features of the network services that should be provided by the underlying network infrastructure. Such a business language that can help the operator express high level business goals required of the network may be modelled by the use of an ontology to add semantics and enable machine reasoning on the goals. The human operator defined features relate to business goals, technical goals and some input configuration data that an autonomic network is supposed to use as operational targets (which may flexibly be changed or modified by the operator at any time) for network resources and parameters configurations.

- In the relationship of the two properties of an AcN/AN (of being "autonomic" and being "autonomous"), one can realize that the science of Control-Loops (called "**Autonomics**") is key enabler for achieving the property of being autonomous, and that an AcN is expected to evolutionarily "maximize" the property of being "autonomous" in as far as the "**Degree and Measure of Operations Tasks that can be performed by the Autonomic Network (AcN) without direct human involvement in the decision and actions**". That means that evolving the Autonomics (Control-Loops) of the AcN by enrichment of automation in management, control and associated intelligence in the Control-Loops, **Maximizes** the AcN's property of being Autonomous (but while still remaining governable and controllable by humans-particularly for telecommunication and IT networks meant to serve business customers of network providers). Two Dimensions for Autonomics Evolution of the AcN are:

  1) Market Place Driven Evolution of Decision-making-Elements (DEs) for Autonomics enables onboarding better DEs with better Algorithms;

  2) Algorithmic Evolution of DEs' AI Algorithms for Autonomics.

  The "evolution" takes different paces in deployed AcNs of various organizations. Therefore, **Evolutionary Autonomic Networks** are characterized by the ability to **evolve in maximization of the property of being "Autonomous" (degree of Autonomy** in operations tasks**)** by enriched automation using Control-Loops, to reach an extent by which the human operators see themselves focused mainly on providing Governance Inputs (such as Business Objectives, SLAs, Goals, Policies and Intents) to the Network while experiencing a drastic reduction of involvement in any burdens involving tasks such as security management/control, fault-management and Network Optimization processes for the network (thanks to autonomics features such as self-repair, self-healing, self-protection and self-optimization, self-awareness, by the network on its own).

For more details on taxonomy harmonization in this space and enablers for the paradigms, the following sources provide useful insights [i.20], [i.1] and [i.2].

4.2 Closed Control-Loop(s)

Traditional networks based on human labour-intensive, time and resource-consuming management tasks, carried out by operations teams, should be conducted autonomously by following a much more efficient, intelligent and automated machine-oriented approach. Network transformation and the evolution from the traditional communications industry to the digital services industry demands a paradigm shift in the way networks are planned, deployed and operated.

The evolution to the digital services industry imposes additional challenges on the agility, flexibility and robustness needed to manage the lifecycle of services and underlying resources. In the digital services industry, service innovation cycles are becoming much shorter, service activation is expected to be instantaneous, and services are supposed to be always available and highly responsive. Due to these requirements, the digital services industry is incompatible with human dependencies on service activation, optimization and recovery situations.

The ongoing network transformation towards Network Functions Virtualisation (NFV) and Software-Defined Networks (SDNs) is becoming a reality and will result in a significantly improve in agility, flexibility and cost efficiency to manage network functions, which are the foundations to trigger a paradigm shift in the way network operations are planned, deployed and managed, called cognitive network management. This approach consists of implementing machine-based intelligence to support the creation of autonomous processes to manage complex networking scenarios.

One of the main impacts of this paradigm is the significant reduction of operational costs. Proactive and reactive actions are automated to resolve or mitigate networking problems, thereby minimizing the human effort in maintenance and troubleshooting tasks, and leading to significant Operational Expenditure (OPEX) reduction.

Three key capabilities is to be provided to create a **closed control loop solution** able to support the implementation of autonomous and intelligent cognitive processes:

- **Automated network monitoring:** the key challenge is to build transversal and automated monitoring capabilities crossing all network domains. These can be achieved through the automated deployment of virtualized probes in the network infrastructure to facilitate system-wide distributed monitoring. Collected information has to feed data analysis algorithms, like data analytics, data mining or Machine Learning (ML), in order to create key indicators that may translate to:

  1) service affecting conditions (e.g. network failures, performance bottlenecks, security breaches, intrusions);

  2) conditions that may evolve to service affecting issues in the future;

  3) non-optimal service delivery to specific users, i.e., detection of cases where the service topology being used to deliver a service to end users can be optimized in order to minimize allocated resources or the service QoS.

- **Cognitive framework:** the ability to define high level tactical corrective and preventive measures to respond to the diagnosed conditions. Tactical measures may correspond to reactive actions to fix or mitigate existing network issues or may correspond to proactive actions to prevent the evolution of the diagnosed condition to an effective service-affecting anomaly. These actions typically correspond to services and/or network functions lifecycle management requests (e.g. automated instantiation, configuration, scalability, reconfiguration of connectivity logical topology, etc.).

- **Automated and dynamic service provisioning:** automated and intelligent processes to manage the lifecycle of services and network functions. These comprise the dynamic selection of the best locations and resources for services deployment (or migration) considering the requirements associated with the specific service instance being provisioned (for instance the contracted QoS). This process also includes the provisioning of the key performance indicators to be produced for the service instance.

4.3 Introduction to the ETSI GANA Reference Model for Autonomic Networking, Cognitive Networking and Self-Management

This clause introduces the ETSI GANA Reference Model to provide a basis for the objectives described in the scope of the present document.

The ETSI Generic Autonomic Networking Architecture (GANA) Reference Model is an Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services standardized by ETSI [i.1], [i.2], [i.22], which defines a generic Functional Blocks (FBs), their associated reference points, and messages passed through those reference points. Figure 1 presents the snapshot of the ETSI GANA Reference Model and the aspect of Multi-Layer Autonomics' Cognitive Algorithms for Artificial Intelligence (AI) and the levels of abstractions of self-management functionality. Self-management functionality is a logic (component) that implements a control-loop as the core driver of the self-management behavior in terms of orchestration and/or (re)-configuration of entities that need to be orchestrated, managed and dynamically (re)-configured by the logic to meet certain objectives.

GANA Knowledge Plane (KP) is an Intelligent Management and Control Functional Block which is an integral part of AMC. KP consists of multiple DEs.

Looking more closely at Figure 1, the KP level autonomics is considered as the "Macro-level" autonomics (control-loops for dynamic adaptation of behavior and state), while autonomics introduced in the Network Elements/Functions (NEs/NFs) is considered as "Micro-level" autonomics.

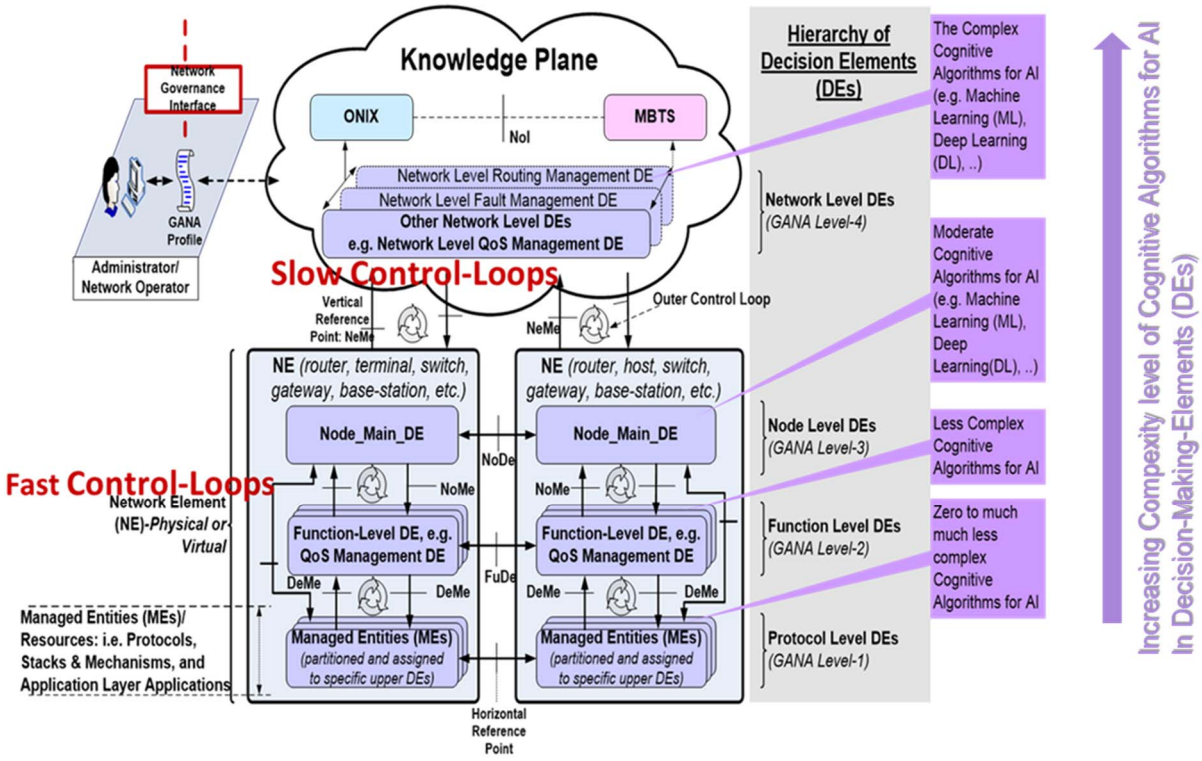

Figure 1: Snapshot of the GANA Reference Model and Autonomics Cognitive Algorithms for Artificial Intelligence (AI), and illustration of the notion of increasingly varying complexity of AI from within an NE up into the Knowledge Plane level

The three key Functional Blocks of the GANA KP are summarized below (in reference to Figure 1):

- **GANA Network-Level DEs:** Decision-making-Elements (DEs) whose scope of input is network wide in implementing "slower control-loops" that perform policy control of lower level GANA DEs (for fast control-loops) instantiated in network nodes/elements. The Network Level DE are meant to be designed to operate the outer closed control loops on the basis of network wide views or state as input to the DEs' algorithms and logics for Autonomic Management and Control (AMC) (the "Macro-Level" autonomics). The Network-Level-DEs (Knowledge Plane DEs) can designed to run as a "micro service".

- **ONIX (Overlay Network for Information eXchange):** is a distributed scalable overlay system of federated information servers). The ONIX is useful for enabling auto-discovery of information/resources of an autonomic network via "publish/subscribe/query and find" mechanisms. DEs can make use of ONIX to discover information/context and entities (e.g. other DEs) in the network to enhance their decision making capability. The ONIX itself does not have network management and control decision logic (as DEs are the ones that exhibit decision logic for Autonomic Management and Control (AMC)).

- **MBTS (Model-Based Translation Service):** which is an intermediation layer between the GANA KP DEs and the NEs ((Network Elements)-physical or virtual)) for translating technology specific and/or vendors' specific raw data onto a common data model for use by network level DEs, based on an accepted and shared information/data model. KP DEs can be programmed to communicate commands to NEs and process NE responses in a language that is agnostic to vendor specific management protocols and technology specific management protocols that can be used to manage NEs and also policy-control their embedded "micro-level" autonomics. The MBTS translates DE commands and NE responses to the appropriate data model and communication methods understood on either side. The value the MBTS brings to network programmability is that it enables KP DEs designers to design DEs to talk a language that is agnostic to vendor specific management protocols, technology specific management protocols, and/or vendor specific data-models that can be used to manage and control NEs.

Remark: More detailed descriptions of the GANA Model are found in [i.1] and in [i.4], [i.15], [i.14] and in the specification itself ETSI TS 103 195-2 [i.2].

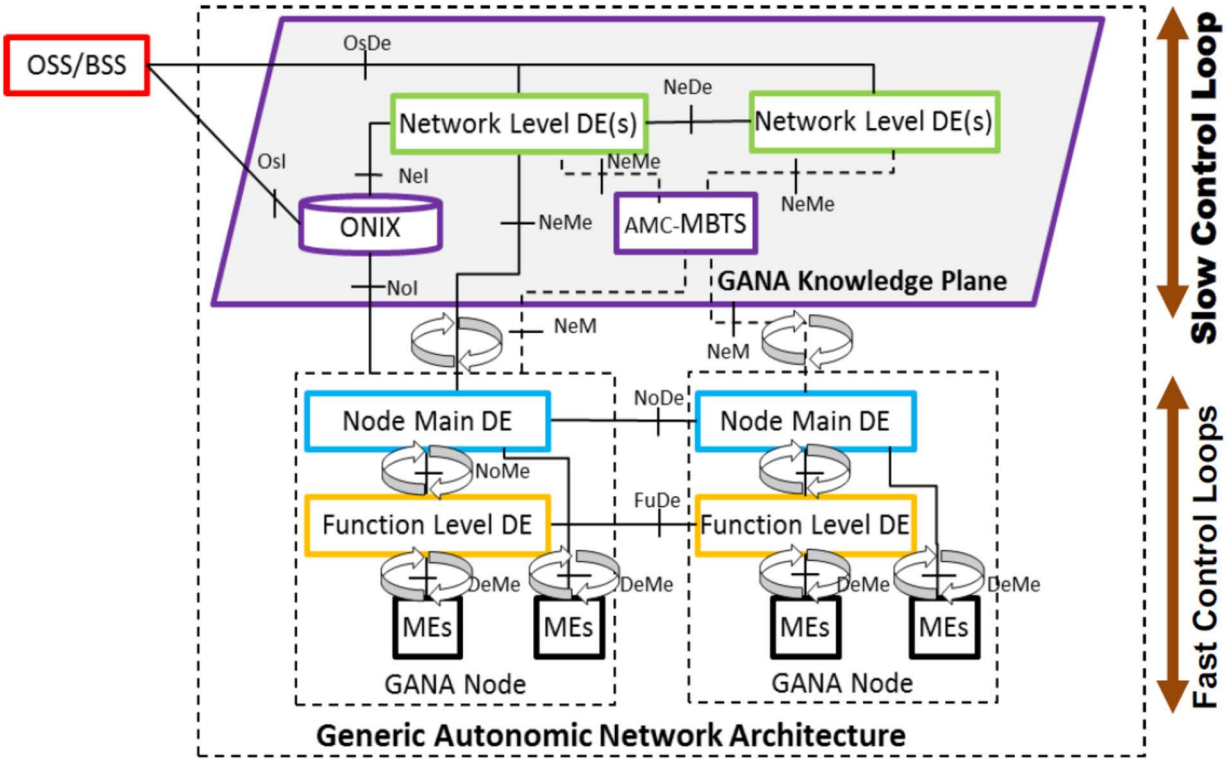

Figure 2: GANA Reference Model with link to OSS/BSS

GANA as a Hybrid Model for Multi-Layer Autonomics and associated Multi-Layer AI Algorithms are characterized as follows:

- GANA is a Hybrid Model: It guides and offers flexibility to implementers on the choice to implement certain autonomics as distributed software and algorithms within certain Network Elements/Functions (NEs/NFs), i.e. "Micro Autonomics", while being able to also choose to implement some algorithms as centralized algorithms in the KP Platform ("Macro Autonomics").

- Hybrid SON Model is compatible with GANA: Hybrid SON (C-SON (Centralized SON) & DSON (Distributed SON)) are considered as an implementation of the GANA Model for the RAN.

According to the ETSI GANA Knowledge Plane (KP) concept, a Knowledge Plane (KP) Platform views various management and control systems such as SDN Controllers, OSS, Orchestrators, EMS's/NMS's and NFV MANO Components as event data sources and also as components or systems through which the Knowledge Plane can dynamically program the underlying network infrastructure. As illustrated on Figure 3, other data sources may be used in implementing the Knowledge Plane. The figure illustrates the various kinds of APIs that may be required to integrate the ETSI GANA Knowledge Plane (KP) Platform with OSS/BSS, Orchestrators, Production Network SDN Controllers, NMS/EMS, NFV MANO, SDN Controllers for OOB (Out-Of-Band) Monitoring Fabrics, Traffic Probing & Analytics Platforms, Telemetry Data Lakes, and Big Data Analytics Apps, Ticketing Systems, and other types of Info/Data/Event Sources that should feed the target GANA KP Platform with data, information, or events. These aspects are further illustrated in clause 3.5 of [i.21]. ETSI TS 103 195-2 [i.2] specifies APIs that should enable to integrate ETSI GANA KP, SDN, NFV, E2E Orchestration, Big-Data driven analytics for AMC, and OSS/BSS systems (or configuration management systems in general). More details on this subject are found in [i.16], [i.15], [i.14]. [i.15] presents an approach to implementing a KP Platform using the ONAP open source software, and [i.15] also discusses how other open source products such as [7], [8], [9], [10], [11], [12] and [13] can be used in implementing a KP Platform that integrates with other management and control systems depicted on Figure 3, such as SDN controllers, NFV MANO stacks, etc.

NOTE: In the case of the 3GPP 5G Architecture, functions such as the Network Data Analytics Function (NWDAF) [i.17] and the Management Data Analytics Service (MDAS) [i.18] need to be integrated with KP Platform so that events and KPIs data from the functions can be used by KP DEs in their autonomic operations.

Figure 3 presents the Integration of the GANA KP with various management and control systems through which the Knowledge Plane can selectively program the network; and KP integration with Event Sources, Data Sources and Info/Knowledge Sources. More details on this subject are found in [i.21]).

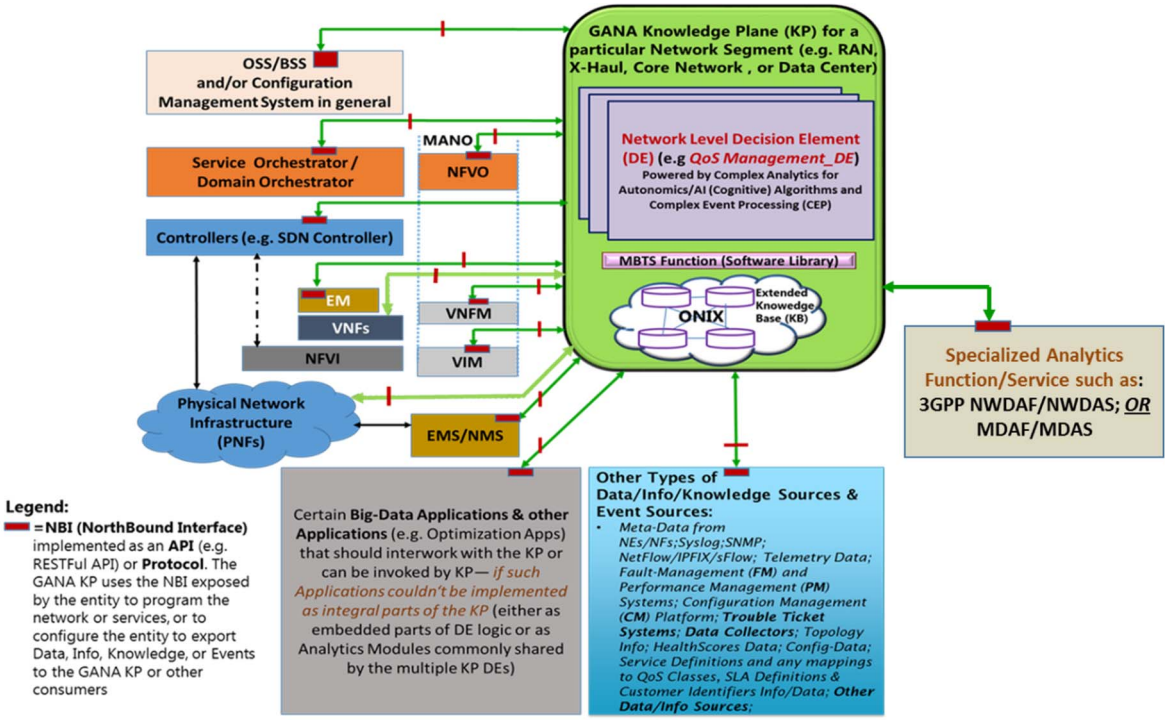

Figure 3: Integration of the GANA Knowledge Plane (KP) with various management and control systems through which the Knowledge Plane can selectively program the network; and KP integration with Event Sources, Data Sources and Info/Knowledge Sources

Figure 4 presents the need for collaboration or coordination of Autonomic Functions (DEs) on certain actions or aspects that are better addressed through collaboration/coordination (more details can be found in [i.14]).

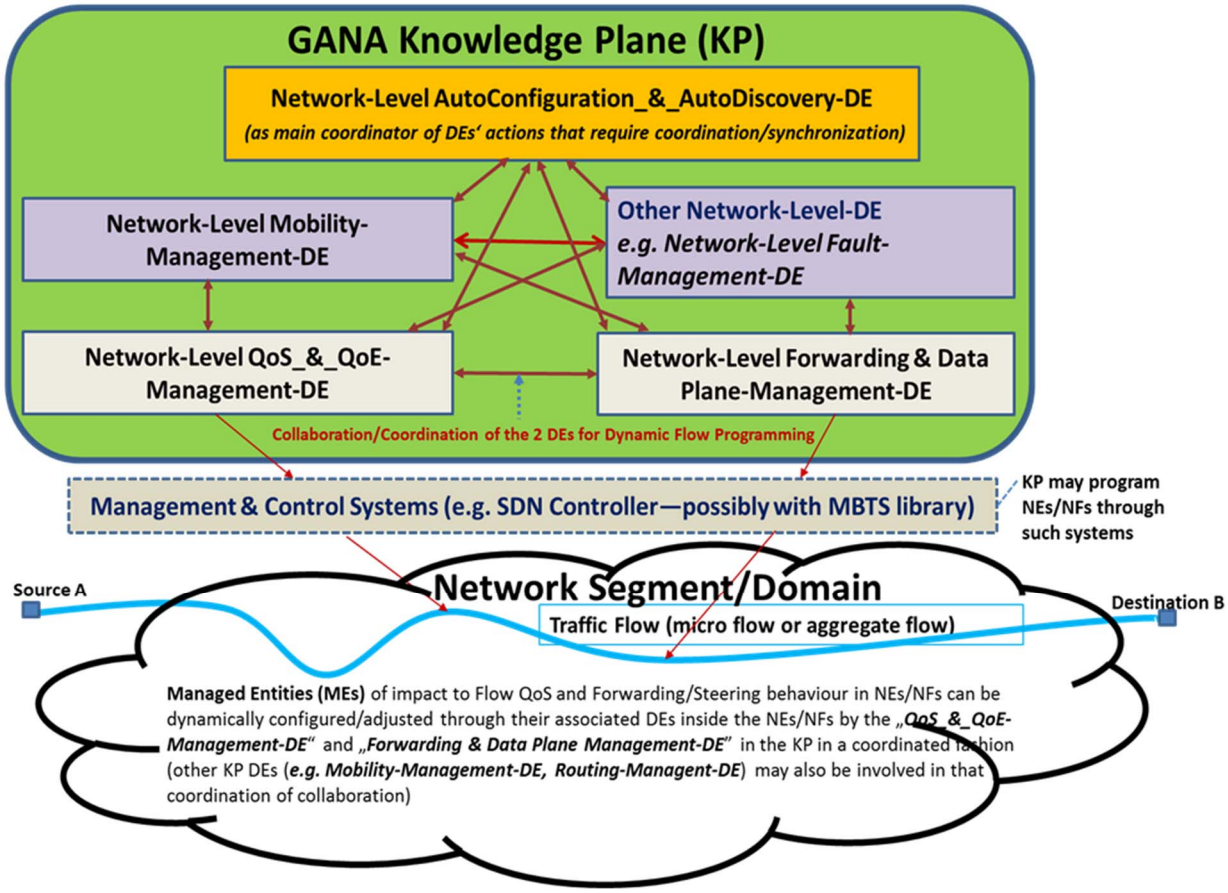

Figure 4: Need for collaboration or coordination of Autonomic Functions (DEs) on certain actions or aspects that are better addressed through collaboration/coordination

Figure 5 presents DE Coordination by a Superior/Designated cDE, and how "Intent" as Input should be handled in the ETSI GANA Framework (more details can be found in [i.20]).

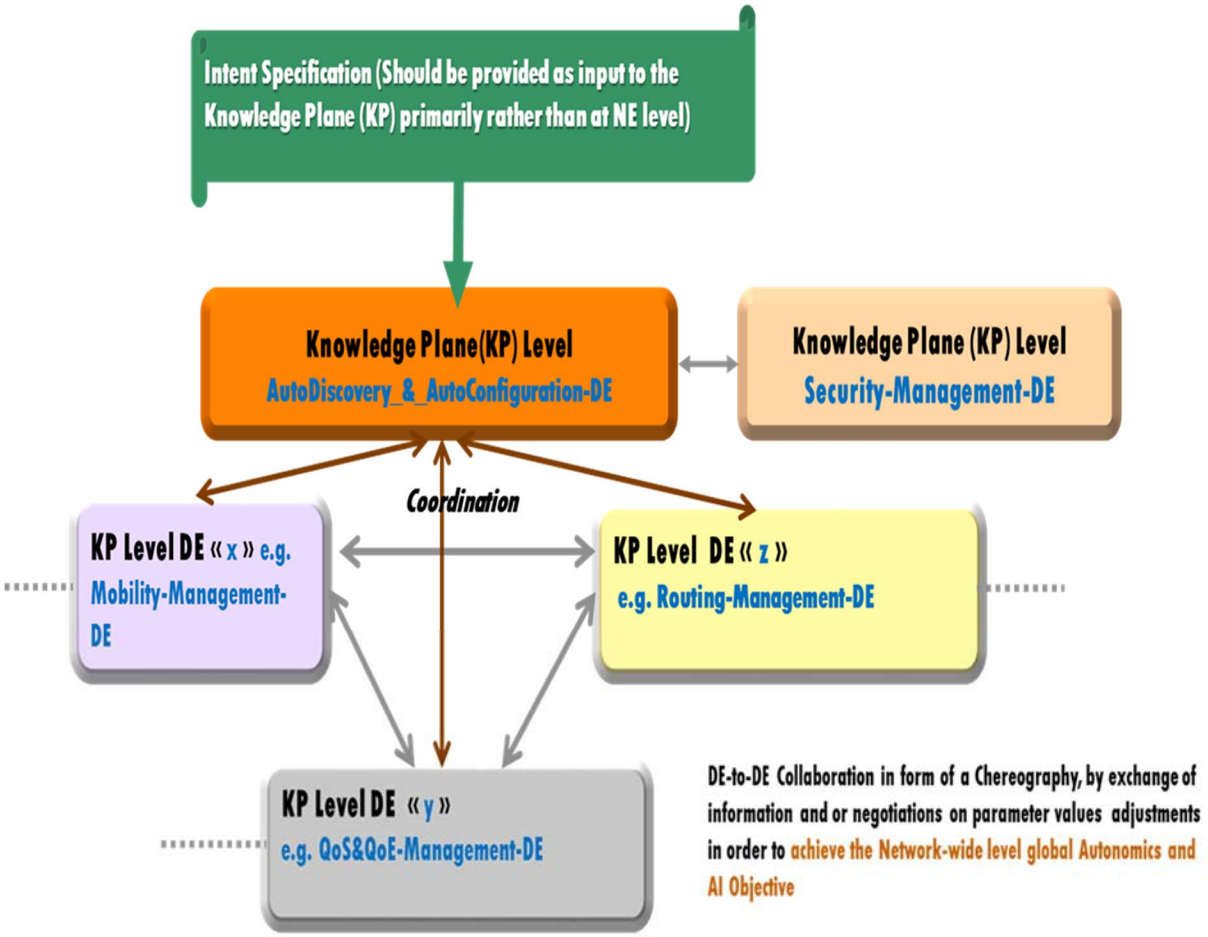

Figure 5: DE Coordination by a Superior/Designated cDE, and how "Intent" as Input should be handled in the ETSI GANA Framework

Figure 6 presents DE Coordination by a Superior/Designated dDE, and how "Intent" as Input should be handled in the ETSI GANA Framework (more details can be found in [i.20]).

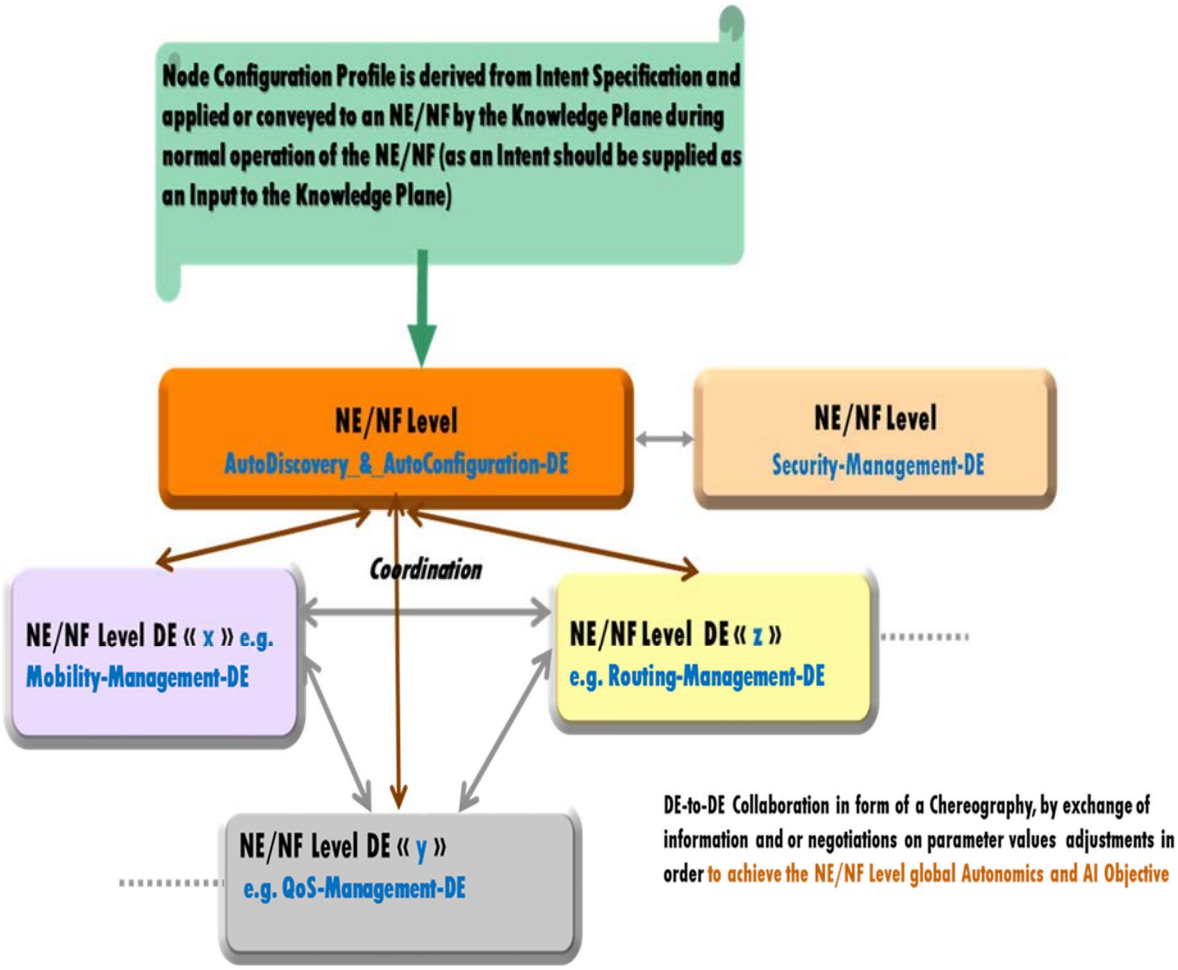

Figure 6: DE Coordination by a Superior/Designated dDE, and how "Intent" as Input should be handled in the ETSI GANA Framework

Figure 7 presents an elaboration on KP DEs interactions in exchanging information/knowledge that enable the coordinating KP DEs to use the information in their decisions on adaptively (re)-configuring their respective Managed Entities (MEs) - when considering the Security-Management-DE (more details in [i.21]).

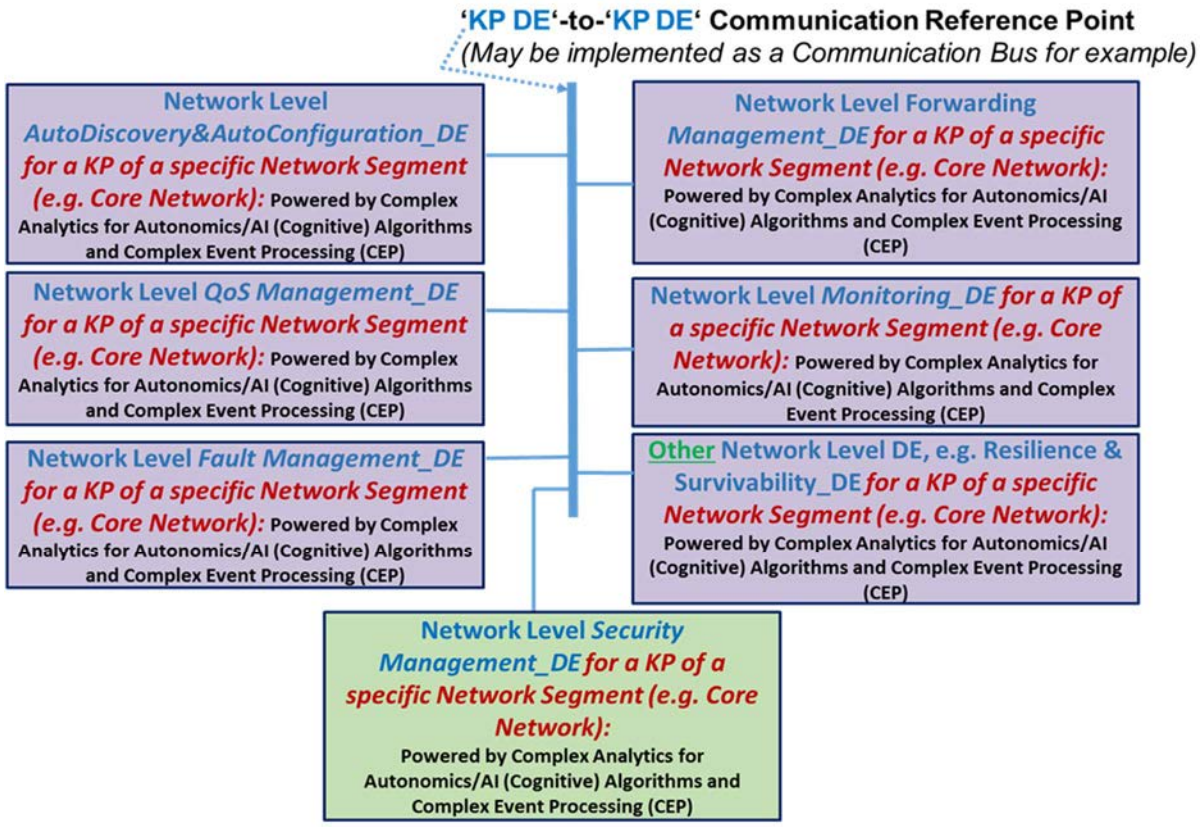

Figure 7: Elaboration on KP DEs interactions in exchanging information/knowledge that enable the coordinating KP DEs to use the information in their decisions on adaptively (re)-configuring their respective Managed Entities (MEs) -
when considering the Security-Management-DE

Figure 8 presents an Illustration of part of the Framework for Addressing Stability of Control-Loops in GANA described in [i.1]: Design for Stability Principles and Run-Time Stability Principles for Coordination/Synchronization/Orchestration among DEs. More details on this subject are found in [i.20].

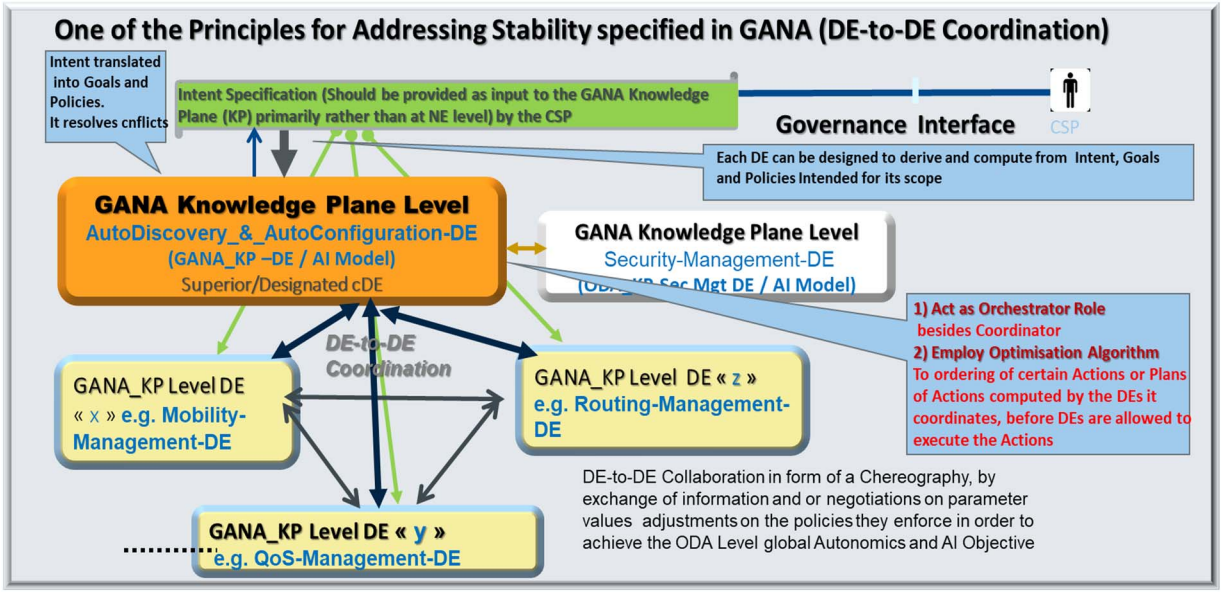

Figure 8: An Illustration of part of the Framework for Addressing Stability of Control-Loops in GANA described in: Design for Stability Principles and Run-Time Stability Principles for Coordination/Synchronization/Orchestration among DEs

As described in ETSI TS 103 195-2 [i.2], the GANA model fused various principles of autonomic networking and management and control models into the Hybrid Model that combines and accommodates the various best principles in a unified way.

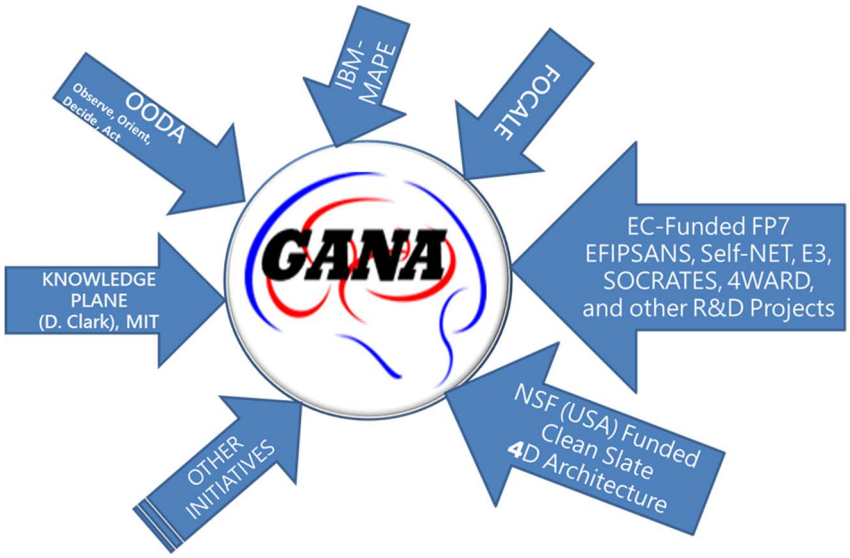

Figure 9: ETSI GANA as a Holistic & Unifying Model for AMC (Autonomic Management & Control) that fuses together the well-established models for AMC

4.4 Federation of GANA Knowledge Planes Framework

Figure 10 is a snapshot of the Framework for Federation of GANA KP Platforms described in ETSI TS 103 195-2 [i.2].

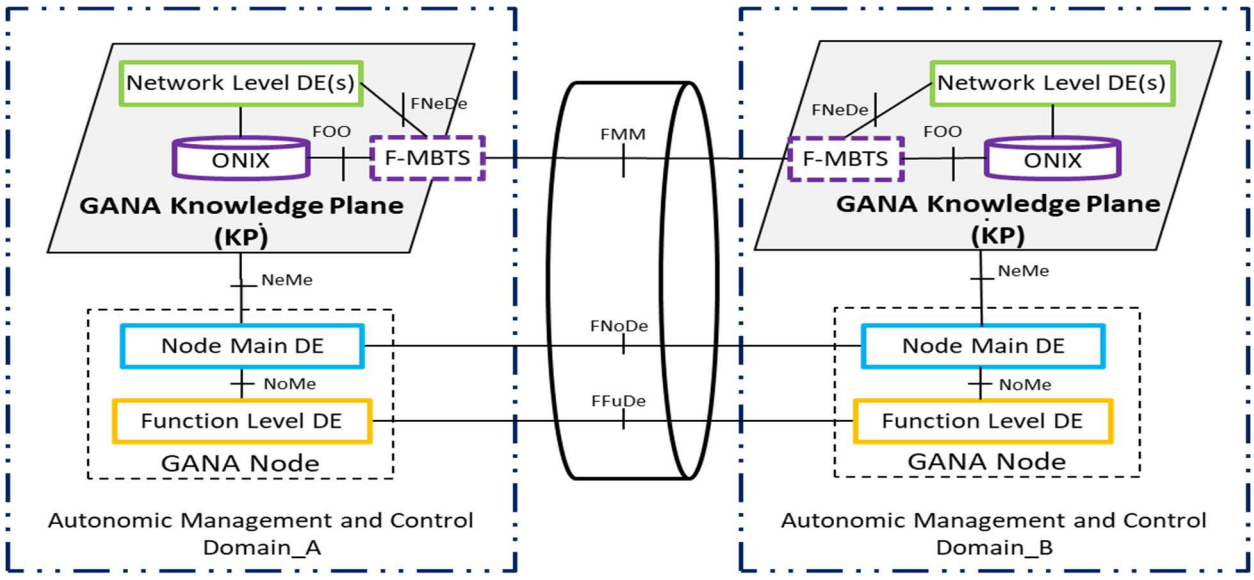

Figure 10: Snapshot of the Framework for Federation of GANA KP Platform

Among the various cases of GANA instantiations onto different types of network architectures and their associated management and control architectures being carried out by ETSI, an example of a GANA Instantiation onto a particular Network Architecture and its associated Management & Control Architecture in which Federated Autonomics is considered is presented in Figure 11. Other cases of Federated GANA autonomics are illustrated in GANA instantiations onto BroadBand Forum (BBF) architecture Scenarios [i.5]. [i.5] presents the case of Federated/Interworking GANA Knowledge Planes (KPs) for BBF (BroadBand Forum) Domain and 3GPP Domain.

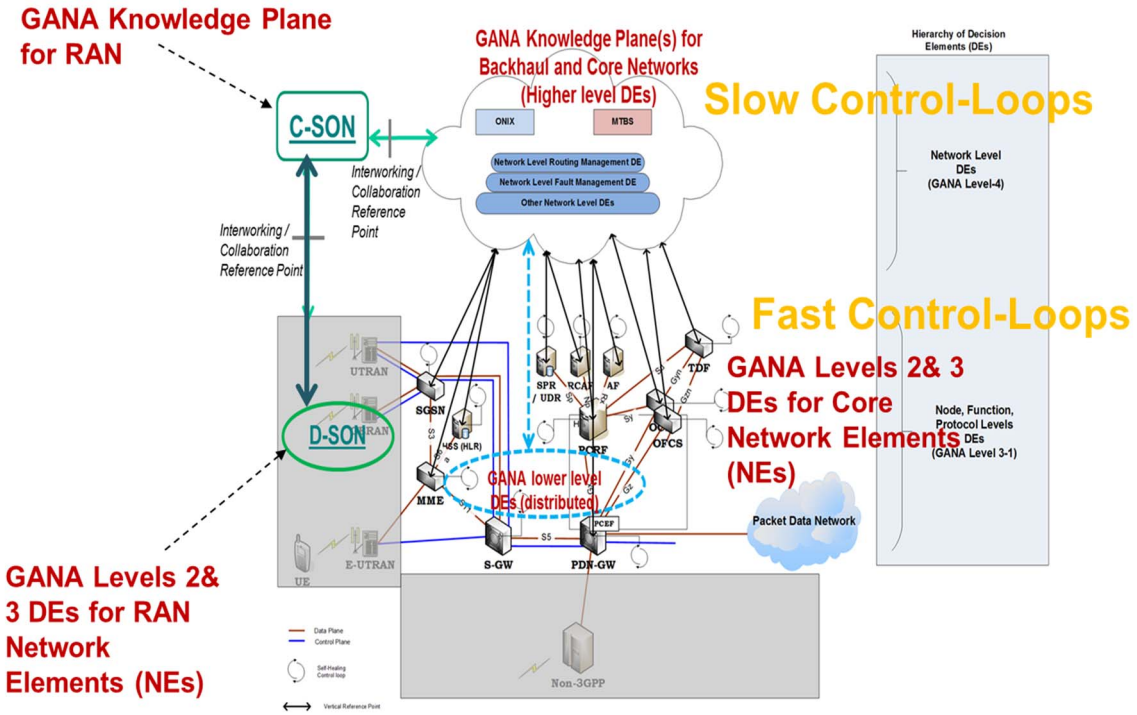

Figure 11: Instantiation of GANA onto 3GPP EPC Core & Backhaul Network [i.6] and Federated/Interworking GANA Knowledge Planes for RAN-, Backhaul - and 3GPP EPC Core Networks complemented by low level autonomics

4.5 AMC Requirements in the NGMN® 5G E2E Architecture, and need for Knowledge Plane Federations for E2E AMC in NGMN® E2E 5G Architecture

[i.19] provides details about the NGMN® E2E 5G Architecture with the various Autonomic Networking and AMC Requirements in the NGMN® E2E 5G Architecture. The ETSI GANA Model and its concept of the GANA Knowledge Plane (KP) as a platform for implementing AMC were adopted by NGMN® deriving specification of Requirements for Autonomic Networking and AMC in the NGMN® 5G E2E Architecture (section 6.4 of [i.19]).

The nature of the Autonomic Networking and AMC Requirements in the NGMN® 5G E2E Architecture [i.19] can be characterized as follows:

- Autonomics and AMC Requirements pertaining to Fast Control Loops in Network Elements/Functions (NEs/NFs).
- Autonomics and AMC Requirements pertaining to Slow Control Loops in GANA Knowledge Plane Level.
- Federated E2E decision making across autonomic domains by the way of Federated Knowledge Plane (KP) Platforms for specific network segments/domains.

For example, Figure 7 in [i.19] provides an exemplification of GANA AMC KP in a 5G mobile access system.

NOTE 1: Clause 9 of the present document gives focus to Autonomics and AMC Requirements pertaining to Slow Control Loops in GANA Knowledge Plane Level and Federated E2E decision making across autonomic domains by the way of Federated Knowledge Plane (KP) Platforms for specific network segments/domains.

According to the NGMN® 5G E2E Architecture Framework [i.19], various types of common and generic information may be exchanged by federated KPs, and such information should include the following types of information as further discussed in [i.21]:

- Synchronization of actions across multiple KPs [i.2]: This is required, for example, to realize an effective E2E federation of Orchestrated Closed-Loop Security Management and Control (adaptive security enforcement and defense) in network infrastructure segments and across multiple domains (Technologically and/or administratively diverse domains). Examples of such domains are network segments (domains) such as Radio Access Network (RAN), X-Haul Transport Network (i.e. Fronthaul, Midhaul, Backhaul, etc.), "Multi-Access Edge Computing" (MEC) site or Core Network. E2E autonomic security management and Control should be achievable through a federation of KPs for the various network segments (domains) associated with a given E2E scope. In this case, each KP policy controls the AuFs (Autonomic Functions), meaning DEs, running in certain NEs/NFs within the network segment governed within the scope of the associated KP. The KP level AuF called the Security Management-DE implements the security policies for self-protection and self-defense of associated NEs/NFs and for securing a network zone under the responsibility of the DE, complemented by NE/NF level DEs required to realize 'fast control loops' within the NEs/NFs, in accordance with the generic autonomic networking principles [i.1].

- Security event information (regarding a description of a detected security incident): An example is detected threats that may impact a peer domain, which could trigger an investigation of the detected threat that is identified by the collaborating KPs. The exchange of such security threats detection or predictions information may result in the KPs collaboratively negotiating an adaptation strategy (self-adaptation without human involvement) for adjusting security enforcement policies that each KP then applies to realize self-protection and self-defense for its associated network segment/domain against the detected or predicted threat(s). For example, there may be some security threats detected in the access network domain by the KP for the access network that could have impact on X-Haul transport network domain as a peer domain or may have impact on the core network as the peer domain in terms of impact scope of the security threat(s).

- Trust model (e.g. a reputation-based trust model) between the Autonomic Management and Control (AMC) administrative domains: An example of such a trust model would be a kind of trust model that spans across autonomously managed and controlled domains, with the associated network infrastructure segments and their associated KPs, where each particular network segment has a KP.

- Security related SLA (Service Level Agreement) violation detection: The detection of an SLA violation, requires the associated KPs to initiate a resolution through a collaboration across the KPs to resolve the SLA discrepancies by reacting to resolve the detected discrepancies for an alignment with the configured SLA clauses in the SLA contracts that were established by the associated domain owners or stakeholders/partners.

Remark: The Information that needs to be exchanged on a KP-to-KP Federation Reference Point, as well as the messages and communication means should be candidate for standardization (e.g. in ETSI TC INT AFI WG).

NOTE 2: Clause 9 of the present document discusses how to address the AMC Requirements specified by NGMN® in its E2E 5G Architecture that need to be addressed by network segment specific GANA Knowledge Plane (KP) platforms and their need.

4.6 The Value of Autonomics in Network Slicing

The provisioning of Network Slices (NSes) with proper Application Level Quality of Experience (QoE) guarantees is seen as one of the key enablers of future 5G-enabled networks. However, it poses several challenges in the slices management that need to be addressed for efficient End-To-End (E2E) services delivery, including estimating QoE Key Performance Indicators (KPIs) from monitored metrics and reconfiguration operations (actuations) to support and maintain the desired quality levels. SliceNet has designed and is implementation s cognitive slice management that leverages autonomic principles powered by Machine Learning (ML) techniques to proactively enablers' remedial actuations to maintain the network in the required state to assure E2E QoE, as perceived by the vertical subscribers.

5 SliceNet Architecture

5.1 Overview

SliceNet addresses various challenges in AI/ML-based autonomous network monitoring, control and management for future networks such as 5G and beyond networks. SliceNet allows AI and ML technologies to be deployed flexibly wherever appropriate in the system framework and distributed over different administrative domains belonging to various service providers.

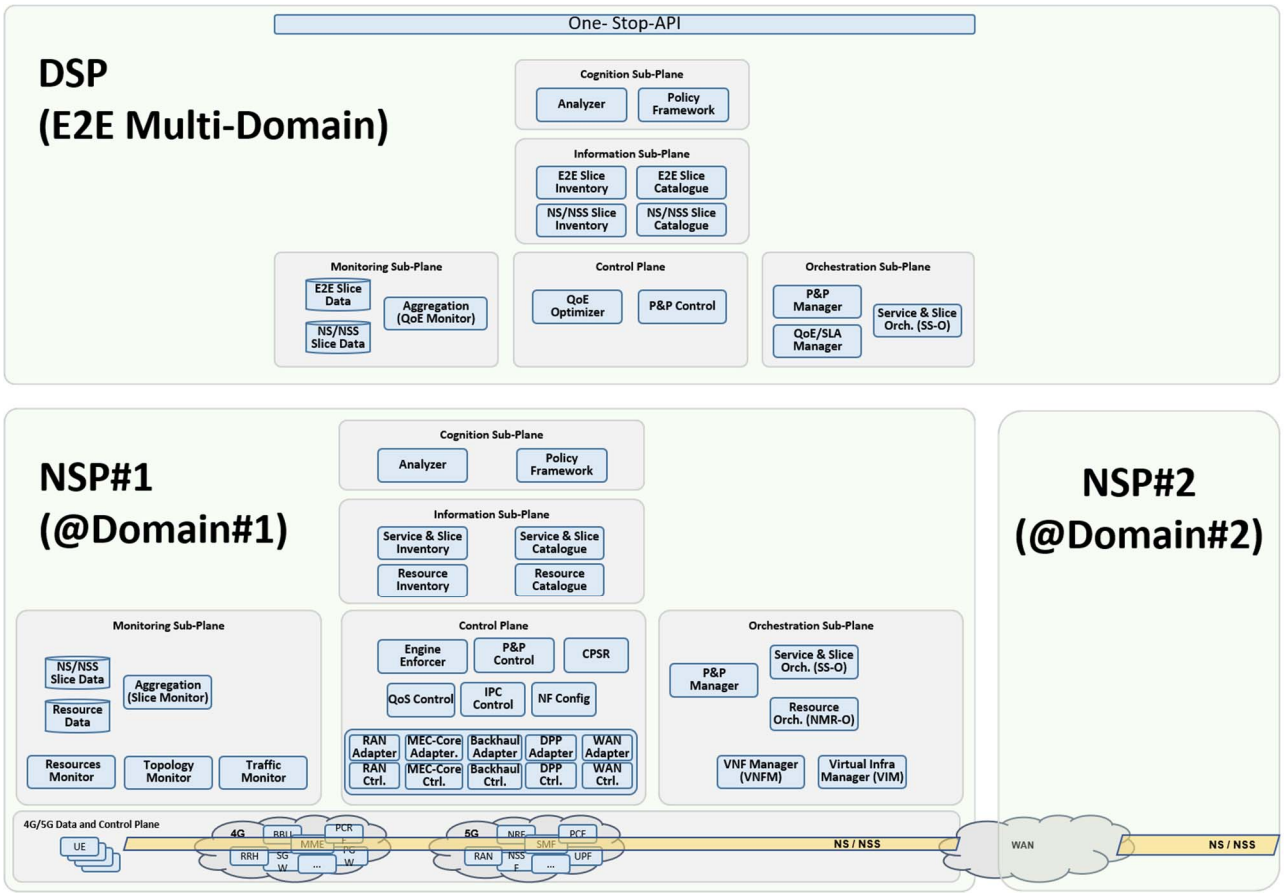

Figure 12: SliceNet framework architecture overview

Figure 12 shows an overview of the SliceNet framework architecture. It is highlighted that SliceNet supports the differentiation of various business roles in 5G architecturally, in line with the vision of 3GPP. Specifically, SliceNet focuses on enabling the role of Digital Service Provider (DSP) to deal with E2E multi-domain network slicing and services, on top of multiple domains administered by corresponding Network Service Providers (NSPs). In each DSP and NSP domain, two major planes, Management plane and Control plane, are concerned. The management plane consists of four sub-planes: Monitoring, Cognition, Information, and Orchestration.

These Management sub-planes and the Control plane, when interworking with each other, provide a cognitive autonomous control loop, analogous to the conventional MAPE-K (Monitor-Analyze-Plan-Execute with shared Knowledge) loop, in each DSP or NSP domain respectively. The cognitive autonomous control loop in a DSP domain handles cognitive management and control for E2E multi-domain network slices and services and is primarily concerned with the vertical's QoE and SLA (Service Level Agreement), whilst that in an NSP domain deals with cognitive operation and QoS control for intra-domain Network Slices (NS) or Network Sub-Slices (NSS). An NSS is created over a network segment such as RAN (Radio Access Network), MEC (Multi-access Edge Computing), Backhaul, Core Network, etc.

SliceNet is compatible with virtualized 4G/LTE (Long-Term Evolution) and 5G networks, which are considered sliceable thanks to the SliceNet overlay Control plane on top of 4G/5G data plane and control plane. This further facilitates multi-domain network slicing over not only the emerging 5G networks but also existing virtualized 4G networks for extended service coverage. Finally, a One-Stop API (Application Programming Interface) layer exposes the whole system to verticals.

5.2 Control Framework

The main purpose of the Control Plane is to provide the Slice control context by a set of configuration endpoints exposing technology and implementation-agnostic control APIs towards slice management and orchestration components.

The Control Plane is thought to handle tasks for the enforcement of network functions configuration rules and policies governing the run time operations of Radio Access Network (RAN) RAN, Core Network (CN), Mobile Edge Computing (MEC), Backhaul and Wide Area (WAN) network segment.

The functionality is composed by a set of loosely-coupled components called Control Plane Services (CPS) and Adapters interacting directly each other by a Service Based Interface (SBI) within a Service Based Architecture (SBA) framework.

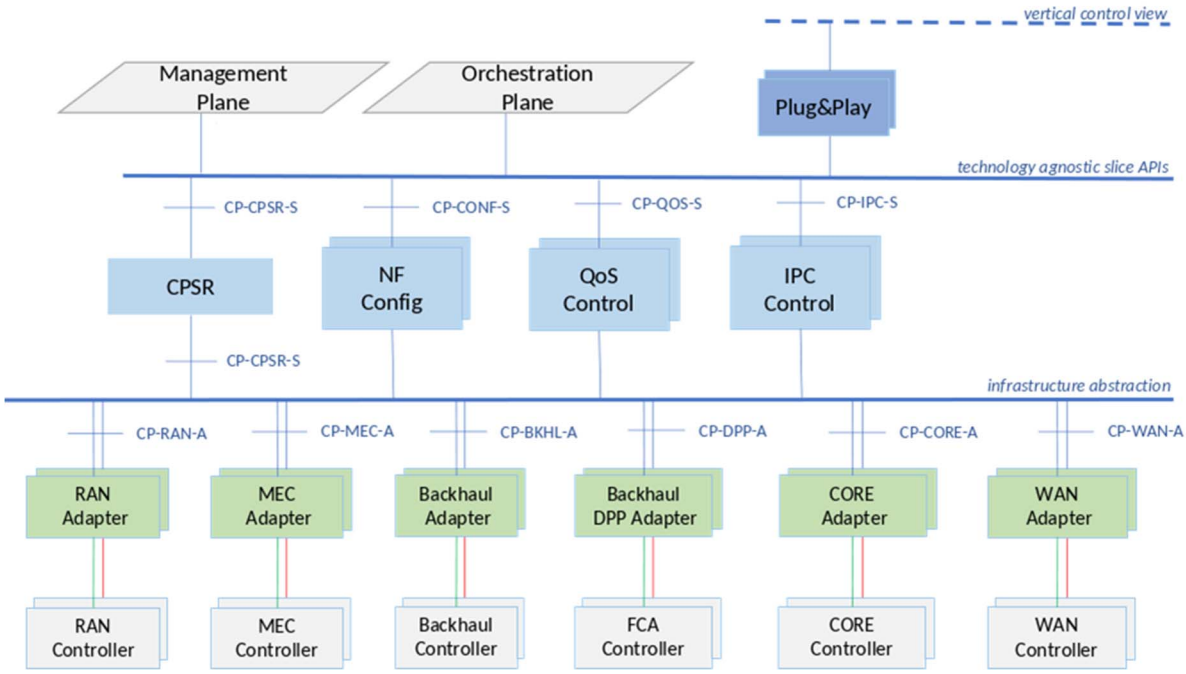

Figure 13: Control Plane Architecture

Figure 13 shows the Control Plane Architecture that is Service Based and adopt a layered approach with a set of abstractions level:

- Infrastructure layer abstraction: Adapters are introduced to expose technology agnostic primitives to upper layer by abstracting heterogeneous vendors technologies of the NSP infrastructure pillars (RAN, MEC, Core, Backhaul, WAN).
- Slice control layer abstraction: Slice CP Services are introduced to expose a Slice control context to upper layer by abstracting NSP Slice composition in terms of both technology and network pillars.
- Slice customization layer abstraction: Plug & Play is introduced to enable customized slice view and control to Verticals by further abstracting the Slice control layer.

The SBA framework is implemented by the Control Plane Service Register (CPSR) component.

Adapters can easily be onboarded to support newly added infrastructure pillars so to allow dynamic architecture expansion and interoperability.

Each Control Plane Service (CPS) is instantiated per Slice enabling isolation, scalability and resource optimization while offering specific configuration and control capabilities APIs as described below.

QoS Control

The QoS Control Service is responsible to enforce dynamic QoS setting for each slice towards the underlying network segments (RAN, CN, MEC, Backhaul, WAN) according to the input parameters in the exposed interfaces.

The request to set the QoS constraints can be on a per-slice basis or for an IMSI and optionally for the EPS bearer IDs associated with a slice. In principle, the request to set the QoS constraints is deployed to all network segments depending on the slice composition.

The QoS CPS exposes **APIs** for the following operations to its service consumers:

- *Set QoS constraints*, to allow indication of quantitative QoS parameters per slice to be enforced towards the wanted network segment. Included parameters are:
  - SliceID, it is the Unique ID of the slice.
  - SegmentId is optional, if it is not defined the QoS constraints will be enforced on all active sessions for all network segments.
  - UserEqId and epsBearerId are optional, if they are not defined, QoS enforces QoS constraints on all active user sessions for the specific slice.
  - QoS constraints are mandatory. It can be included: qosDirName (Upload/Download), qosDirValue (e.g. 50), qosUnitScale (e.g. MB).

In case the set QoS constraints is directed towards the WAN network segment, the QoS constraints include the per-flow and per-network-device forwarding rules with QoS attributes to be enforced at domain border devices in order to interconnect sub-slices belonging to different administrative domains:

- *Set Priority*, to allow change of priority for a traffic type flow associated to a slice within the back-haul data plane. Included parameters are:
  - SliceID, the Unique ID of the slice.
  - PriorityValue, Identify the priority value of the traffic flows.

NF Config Control

The NF Config Control Service is responsible to enforce the configuration operations towards the Network Functions composing the slice. Depending on the slice template/design that is instantiated a number of operations are expected to be available per slice. These operations are not limited to a predefined subset. Several operations can be defined and catalogued so that they can be included.The NF Config Control service analyses the requested operation and execute it in the context of a defined workflow among those configured during instantiation.

The NF Config CPS exposes **APIs** for the following operations to its service consumers:

- *Set NF configuration*, to allow set, update and removal of specific NF configurations. Included parameters are:
  - Request, POST/PUT/DELETE.
  - Request body, NF ID/address, config parameter name, current value to be applied for the parameter name.

IPC Control

The IPC (Inter PoP Connection) Control Service is responsible, for each slice instance, to deliver a proper interconnection of the slice Network Functions (i.e. mostly VNFs and MEC applications) deployed in different segments and domains, namely edge (e.g. MEC) and Core ones allowing geographically distributed slice Network Functions to be properly interconnected according to their end-to-end forwarding graph descriptor.

The **IPC Control** exposes **APIs** for the following operations to its service consumers:

- *Provision InterPoP Connection*s, to create a new interPoP connection among two or more PoPs where the Network Functions (i.e. VNFs and MEC applications) of a given slice have been deployed and provisioned.
- *Update InterPoP Connections*, to dynamically update an existing interPoP connection, mostly intended for on-demand modification of one or more of the constraints related to the network connectivity for the given slice, like QoS parameters but also endpoint traffic identification attributes (e.g. IP addresses or VLAN identifiers) if applicable.
- *Remove InterPoP Connections*, to delete an existing interPoP connection, e.g. as a consequence of an overall slice decommissioning/termination operation.

A general descriptor of an InterPoP Connection, received and processed by the IPC CPS, contains the slice identifier and the list of InterPoP paths to be interconnected through the Backhaul network:

- Slice Id: univocally identifies the slice through the backhaul network.
- InterPoP Paths: are the set of paths across the backhaul network. Each InterPoP path consists of:
  - a pair of endpoints: an endPoint on the PoP consists basically of an IP address and an encapsulation identifier (e.g. VLAN) to identify the per-slice incoming/outgoing traffic;
  - a set of constraints: bandwidth and latency to evaluate along the path interconnecting the endpoints.

5.3 Cognitive management

5.3.0 Introduction

The SliceNet Cognition Plane adds Machine Learning (ML) capabilities to the established Monitor-Analyse-Plan-Execute governed by a Knowledge-base (MAPE-K) control loop to implement an autonomic E2E slice management and control. The proposed architecture covers the entire loop, including cognition-based monitoring to obtain QoE KPIs, a ML pipeline for the analysis phase, and an actuation framework. The SliceNet Cognition Plane embraces the MAPE-K approach for automated and autonomic management; MAPE-K is a loop of **M**onitor-**A**nalyse-**P**lan-**E**xecute governed by a **K**nowledge-base that encapsulates policies, rules, algorithms, etc. SliceNet is designed to support ML for the Monitoring and Analysis steps, as well as for creating new Knowledge. SliceNet QoE Monitoring, separates the acquisition of monitoring data from the processing of that data and transforming it into NS QoE metrics. The Analysis step uses the acquired knowledge to assess the NS QoE and possible impact on corrective actions; this is done by both inferring learned cognitive models and by applying more traditional automated management methods. The Planning and Execution steps (termed *Actuation*) are governed through a Policy Framework (PF). Actually, the Policy Manager located at the SliceNet Cognition Plane, together with the policy decision and enforcement points, which can be located in several architecture locations (e.g. management, control and data planes), are responsible for the policy-driven behaviour of the system. SliceNet employs a Data-Driven Network Operations methodology, a.k.a. AIOPS (Artificial Intelligence for IT Operations). Network analysis applications react to collected operations data (both raw and processed) and generate new metrics and signals (e.g. QoE metrics and QoE-aware insights) that in turn trigger network operation actions. With this methodology, most components interact only with the data store, acting as consumers and producers. This approach minimizes the direct interfaces, provides flexibility, and easier integration of cognitive tools. It also allows existing techniques to be used with little change, as the outputs of the cognitive tasks can be treated as advanced sensor metrics; indeed, this is how SliceNet's QoE sensors are implemented. The main components of the Cognition Plane and its relation to the other SliceNet planes are shown in figure 14. The figure details only the SliceNet logical components that have significant interaction with the Cognition Plane; other components of the SliceNet logical architecture are hinted by empty boxes.

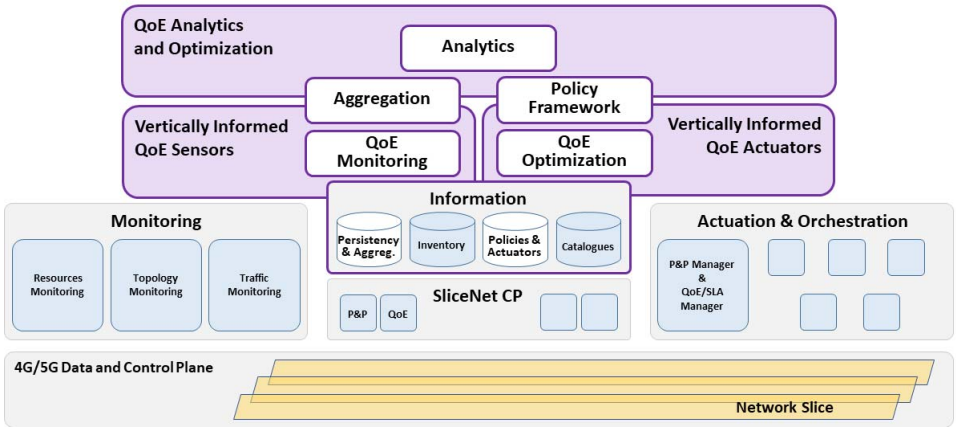

Figure 14: Cognition Plane overview

Vertical informed sensors provide *QoE monitoring* capabilities and prepare *aggregated data* from the ML-based analytic processes. Although monitoring utilizes information from several sources, it has direct interfaces only with the persistent data stores, simplifying the interfaces and following a Data-Lake approach.

Analytics and optimization tasks process the QoE sensor data to provide cognitive insights that enable the vertical-informed actuation. Analysis is applied first to historical data to learn new models and derive new policies and optimization parameters. At run-time, similar analysis is applied to verify and refine the learned models. Finally, the learned models are inferred in near-real-time to provide concrete input signals for actuation. SliceNet defines an actuation framework with the core goal of maintaining and optimizing the perceived QoE by vertical customers. To this goal, the actuation framework focuses on determining the required changes to E2E NSes that support the verticals' services, while taking charge of enforcing such changes. The actuation framework is designed with two main components in mind, namely, the Policy Framework (PF) and the QoE optimizer. The PF is a rule-based policy engine, in which rules define what actions are executed in response to system and NS events. The QoE optimizer is the responsible for all (re-)configurations necessary to maintain the QoE of a specific E2E NS. Thus, given the rules specified by the PF, and gathered monitoring data, the QoE Optimizer triggers the necessary actions to carry out the desired actuations. The PF and QoE Optimizer get their input from both analytics and external monitoring data to determine when and how actuations should be carried out. Then, the actual actuation is triggered by timely collaborations across functions at different layers. In a nutshell, the rules defined by the PF are translated into operations that the QoE Optimizer can trigger/execute. These trigger/executions are abstractions of the Operations exposed by execution points (mainly, control and orchestration layers). Traditional Operations Support Systems (OSS) are evolving towards more flexible, agile and service-oriented management platforms. This can be achieved through policies, which can be seen as high-level directives that convey what the software components should do under certain conditions. SliceNet's QoE Optimizer component is responsible for triggering the desired actions (Execution from the MAPE-K loop) within the actuation framework. The actions are meant to maintain the quality of a particular E2E NS deployed on the underlying infrastructure, which may encompass several NSPs/segments/domains. As such, the QoE Optimizer is designed as a module that will be instantiated per E2E NS. A QoE Optimizer instance will have a specific actuation scope tailored to its NS, at the DSP level, since it is necessary to gain visibility of all elements/NSSes that intervene and may affect the quality of the delivered NS.

5.3.1 Cognitive Control Loop

As described above, SliceNet follows the MAPE-K for automated management of network QoE. SliceNet employs a Proactive Control Scheme (PCS) in managing the run-time lifecycle of a NS, while utilizing cognitive methods to maintain the desired SLA.

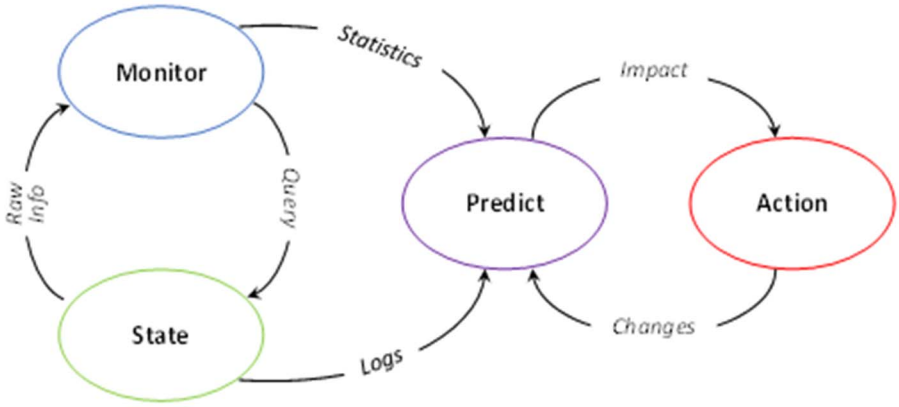

Figure 15: Proactive Control Scheme

Monitor and **State** generate the data required for analysis. The monitoring component is continuously querying the current **State**, in order to extract raw data about the NS, including resource telemetry, topology, and traffic metrics. **Monitor** component generates calculated KPIs by processing the data as network statistics and by applying aggregations at different levels (e.g. per cell, per slice, etc.). Another important role of the **Monitor** is to enrich its raw input data (e.g. labelling the raw data). The analytics and ML are encapsulated in the **Predict** component. It further enriches the data, adding insights, predictions, and impact analysis, to allow proactive management with better system diagnostics and prognosis. The enrichment information is added to the monitored data as an extra source for the **Action** component. This approach allows the Cognition Plane to support both real-time and near-real-time models, in which the **Action** component may react immediately to time-sensitive metrics and utilize the results of more complex analytics for proactive actions. The **Action** component has a dual role, as both an internal ML control loop; and a network control loop for taking network actions. The ML control loop can imply actions such as (re-)validating a ML model in use. The changes caused by actions are fed back to **Predict** alongside raw data like logs and processed statistics in order to maintain ML models, thus closing the loop and allowing for consecutive iterations of the monitor-predict-action cycle.

5.3.2 Knowledge & Monitoring

SliceNet employs a Knowledge-Centric, Data-Driven approach to network operations. All data sources are logically merged into one data store and analysis outcomes are shared through the same data store. Multiple data sources are logically merged to provide all the required information for QoE management. Control Plane (CP) and Data Plane (DP) sensor outputs are collected and persisted to support traditional monitoring through parsing, transformation, and aggregation. However, this data is also used for ML model training and for extracting QoS metrics.

5.3.3 Analysis

ML pipeline defined for SliceNet's Cognition Plane architecture is depicted on Figure 14. As a starting point, and external to the pipeline, there is a data discovery and gathering phase, this is where input for ML occurs. Logically, this step represents a data source from the pipeline point of view. Internally, it is divided into six different functional areas, covering all phases from data collection to the ML models' lifecycle:

- **Ingest data:** this module enables the pipeline to read data and its responsibility is divided into two components:
  - **Readers:** data input can be multiple files containing observations or streaming data. Each reader abstracts the medium source of the observations and their nuances.
  - **Normalization modules:** data normalization is the process of combining, merging, and cleaning, according to the knowledge gathered from the data analysis. Includes removing duplicate observations, removing invalid and/or badly formed data.
- **Data analysis:** the initial analysis serves the purpose of gaining data insights and further problem contextualization. This module runs statistical queries (i.e. counting, averaging, grouping), to check if the dataset is balanced, incomplete or how to focus its modelling.

- **Transform data:** data transformation depends on data analysis and problem objectives. This module transforms the data into ML-ready. This is where features are extracted and their normalization (e.g. ordinal, one-hot encoding) happens.
- **Create model:** ML algorithms, which can cover the classification, prediction or clustering ML areas, are applied in this phase. This is where models are effectively trained, optimized (i.e. hyper-parameter tuning) and their testing strategies are put in place: cross-validation, feature importance analysis, dimensionality reduction and so on.
- **Deploy model:** during the training/testing phase, if a model shows significant fitness metrics values it can then be deployed into production and start being used to predict, classify or cluster data in the real-time problem domain.
- **Monitor and maintain model:** deployed models can lose their effectiveness over time, especially when the data domain is too volatile and dynamic, this means that certain models may be unfit for usage since they no longer properly represent the real world. When models show fitness metrics that are below the configured acceptable values, they are archived, and a re-training task is scheduled to update them. As identified in Figure 16, when such a situation occurs, the process reverts back to step 4, the "**Create model**" phase.

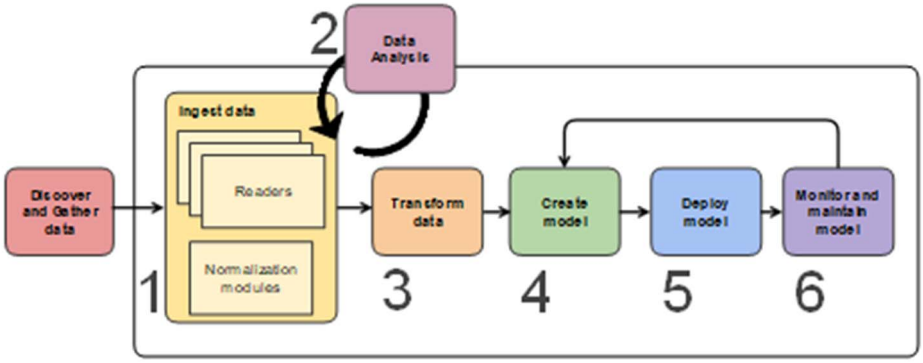

Figure 16: ML pipeline architecture

The Cognition Plane architecture uses data processing applications not only to process data for training, but also to infer the learned models at slice run-time. The orchestration and life-cycle management of cognition-plane applications has similarities with the orchestration and management of the slice CP and DP VNFs, as exercised through the Network Function Virtualization (NFV) Management and Orchestration (MANO) architecture.

SliceNet introduces a Data-Driven Control and Management (DDCM) loop [i.24], which employs prediction-based decision policies and network services, customized for slices. Figure 17 depicts the DDCM loop and illustrates the process of cognitive and autonomic network control. It also shows how to apply the cognitive control process pattern of PCS through the DDCM loop, focusing on the overall Cognition Plane. DDCM is a combination of analytic techniques and modelling approaches on top of SliceNet's CP and DP, making it possible to actuate over the physical network infrastructure domain (e.g. RAN, CN). Network slicing over a cognitive control and management-ready architecture allows operators to create customized control and management models for different slices. The definition of these functions and their parametrization are specified within the slice template during the creation of the slice instance, with the orchestration system creating all control, management and cognition artefacts associated to the NS.

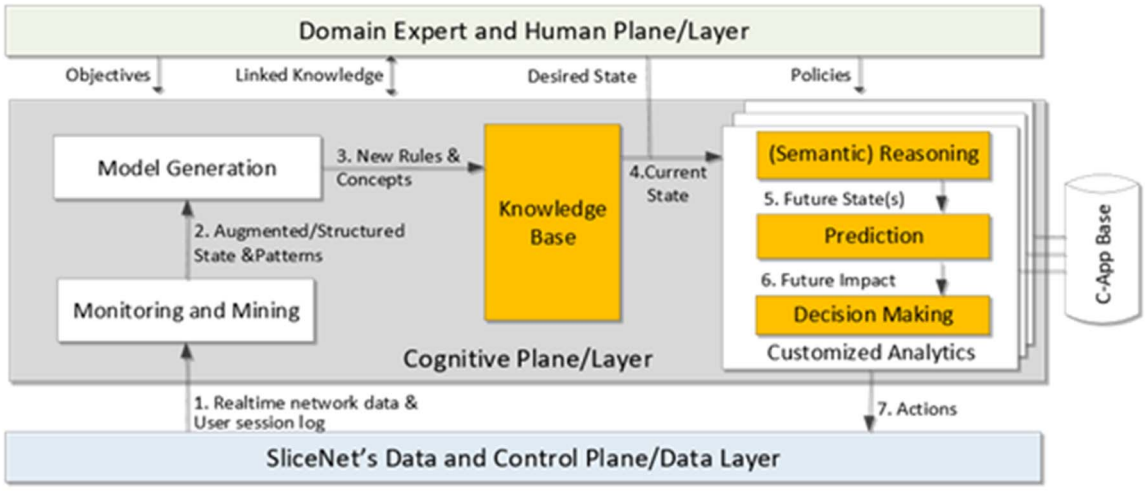

Figure 17: Cognition Plane entailing Data-Driven Control and Management loop

The steps of the DDCM loop over the Cognition Plane, depicted in Figure 17, are described as follows:

- **Real-time network data & User session logs** are monitored from DP and CP.
- **Monitoring and Mining** consists of the **Monitoring** module that extracts and arranges raw data from heterogeneous sources; and the **Mining** module that performs a chain of certain mining operations on raw data, such as data cleaning, pre-processing and transformation, in order to prepare data for a later analysis stage, for example in some data-set D.
- **Model Generation** is a module that works on the previously obtained data-set D. This data-set is the descriptor of the current network state used to discover new semantic rules and concepts which will be added into a KB as new updates. It is worth noting that the discovered knowledge can be encoded in a description model such as an ontology that is suitable for knowledge representation. Any proper statistical and analytics techniques can be used for this module to select the most appropriate data features and their inter-relations. For example, the network input variables which affect network KPIs (e.g. throughput) are defined and the most effective ones are selected as the most appropriate data features out of the high dimensional (in terms of number of features) dataset. Traditional supervised ML and statistical analysis algorithms can also be used to define how the pre-defined effective network input variables affect network KPIs.
- **Current network state** from the KB and **desired state** from **Domain Expert and Human Plane** are sent to **Customized Analytics**. The desired state is deduced out of the services-based objectives, policies and the linked knowledge from other network domains.
- **Reasoning** module checks and determines if the current state of the network is following the targeted optimization goal (network KPIs) and predefined policies. It goes through the updated KB, and extracts the respective inferences, which define the **future states** of the network. In this way, the decision maker is able to assess how far the current network state is from the desired state (global network optimization goals).
- After this, the **Prediction** module predicts the future impact of the inferred future state of the network. By using proper ML algorithms, such as regression algorithm, the future states' input data variables can be mapped to some functions, which predict their future real impact.
- Finally, the **Decision-maker** defines a vector of control actions including a set of network configurations and parameter settings, and sends them to their respective controllers.

Control Applications (C-Apps), performing different network control operations (e.g. mobility management, handover management, policy and charging), provide an abstraction layer over the underlying network and controllers to facilitate the RAN and CN programmability, as well as the interaction with SliceNet DP and CP. Note that C-Apps, residing in C-App Base, includes all "Reasoning", "Prediction" and "Decision-maker" modules, having a set of predefined APIs between them, and translates high-level/technology-agnostic policies and service definitions to low-level/technology-dependent ones RAN and the Evolved Packet Core (EPC). The functionalities of such C-Apps may be encapsulated within the multiple SliceNet CP adapters (RAN, CN, backhaul), which implement the logic necessary to translate the agnostic operations that are defined within SliceNet's CP to technology specific ones to be configured onto the several network segments.

The described Cognition Plane involving DDCM loop can be followed, as a baseline approach, by all centralized and distributed network management and control solutions (for slices and services) to make global and local control decisions and satisfy network optimization goals.

5.3.4 Planning & Execution

SliceNet defines an actuation framework, which covers both planning and execution phases, with the core goal of maintaining and optimizing the perceived QoE by vertical customers.

The actuation framework is designed with two main components in mind:

- The Policy Framework (PF) component is a rule-based policy engine, in which rules define what actions are executed in response to system and NS events.
- The QoE Optimizer component is responsible for all (re-)configurations necessary to maintain the QoE of a specific E2E NS. Thus, given the rules specified by the PF, and monitoring data gathered both from the SliceNet monitoring stack (specifically, the QoE Monitoring) and verticals' feedback (through the P&P controller), the QoE Optimizer triggers the necessary actions to carry out the desired actuations.

Interactions from the analytics at the cognition plane as well as actuation systems at the NSP (the TAL Engine, as depicted in the picture), are enabled thanks to the centralized Data Lake at the DSP level, which collects all data sources for them to be ready for consumption by the Actuation Framework, more specifically, the QoE Optimizer module. While the planning, decision and trigger of the actions is done within the core actuation framework (PF and QoE Optimizer), the actual execution of the actions is carried out by specific functions at both SliceNet CP and orchestration layer.

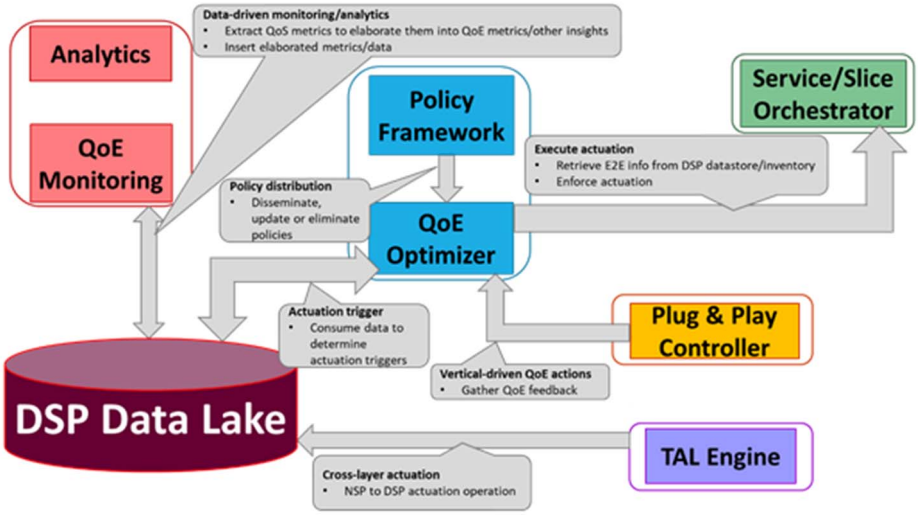

Figure 18: Logical architecture of the Actuation Framework

SliceNet's PF design and software implementation is partially aligned with ONAP Policy Subsystem. Since ONAP is already working on a policy-driven operational management architecture and therefore developing a Policy Subsystem, it was decided to experiment and adopt some of their software components. Other PF components that are not under development in the ONAP Policy Subsystem are currently under development in SliceNet. The PF enables the service designer and/or system operators to **manage the entire policies lifecycle** that is, allowing the policies Creation/Configuration, Read, Update and Delete (CRUD) operations. Policies are stored in the **Policy Catalogue & Inventory (PCI)** logical component. Policies administration capability that is, after policies are on-boarded to the PCI, the system operator should be able to activate the policies deployment on the SliceNet architecture components that should run and execute them, these components are known as Policy Decision Points (PDPs). The policy deployment/distribution capability is delivered by the Policy Administration Point (PAP) component. Policy monitoring feature is delivered by the **Policy Context Manager (PCM)** logical component. Since the PCI, PAP, PCM and PR logical components are responsible for the policies management, they are grouped in the **Policy Manager** logical component [i.23] and [i.25].

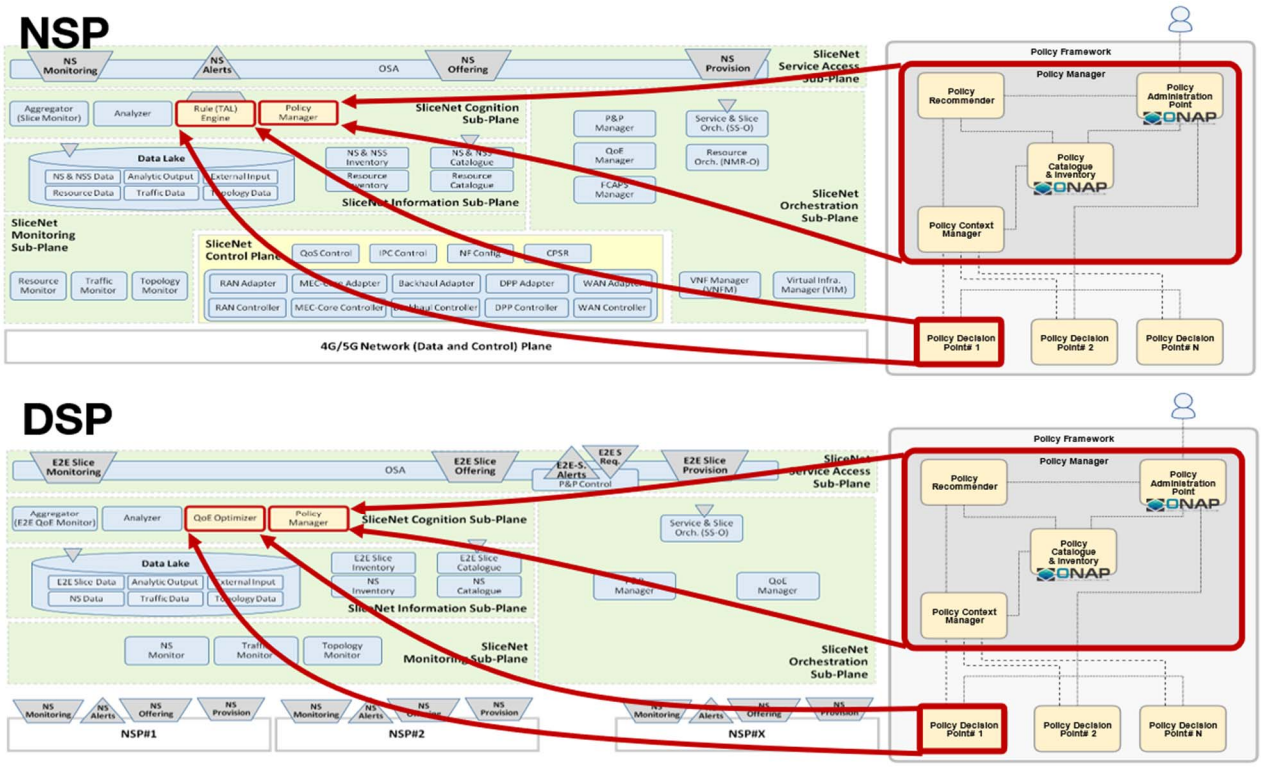

Figure 19: Mapping of SliceNet and ONAP Policy Framework architecture

PCI and PAP components are inherited from ONAP Policy Subsystem, whereas the PDPs are developed within SliceNet. In order for the PDPs to receive the policies, they should subscribe policy notifications from the PAP. The notifications are sent through a web socket in JSON format.

5.4 Slice management

SliceNet assumes that multidomain provisioning of slices involves several players from more than one layer. It considers the NSP as the lower level of slice provisioning with its offering being available for reservation and utilization under the DSP logic. DSP is considered as the mediator between vertical and network. The processing of the request applied by the DSP aims at resolving an adequate synthesis of NSP resources that can support the service level requirements posed by the vertical. In this context SliceNet has adopted a vertical (i.e. slice user) centric approach that aims at abstracting technology and domain related enablers towards the provision of services tailored to the needs of the topmost user of the infrastructure. In a given NSP domain there are specific technology components that are expected to be deployed or engaged in slice provisioning. Those components can be either virtualized or physical resources for which it is assumed that there is an NSP specific orchestration approach to be followed during slice or sub-slice commissioning. Among these resources there can be a variation of sensing or actuation capabilities. Those capabilities are subject to be processed in the context of the DSP slice request processing. For example, upon a slice template request which involves specific service resilience requirements, a DSP might be searching among the NSPs offerings for those resources that provide CPU utilization and temperature monitoring information so that a DSP defined mitigation policy can be implemented/enforced. The DSP is not aware how these metrics are collected, e.g. as SNMP or Ceilometer counters, but it only states that these should be available for higher level analytics processing. Similarly, the DSP might be requiring that particular configuration options should be available as actuation/mitigation options. For example, the option of certain flow acceleration or blocking should be available. Again, the DSP only needs to know that this option is available by a particular NSP without knowing that this is implemented as specific NFs configuration or as an SDN related configuration.

This concept allows targeting management functionalities in an abstract way by giving room for the development of several alternatives that serve the same purpose. Those alternatives can be onboarded in the form of monitoring and actuation descriptors that are focusing on separation of autonomic and cognitive management from measurement and metric collection as well as from the orchestration/enforcement processing of the mitigation reactions. Thus, autonomic or cognitive procedures are abstractly defined on the basis of available metrics and operations, whereas measurement collection and action enforcement are resolved and applied in the context of the protocols defined for the involved resources. An NSP, being aware of the capabilities of the resources it is federating, maintains a catalogue repository of the offerings by associating the monitoring and actuation options with the resources. Additionally, from the inventory repository allocated resources are possible to be associated with their types. The catalogued and inventory part of the information is expected to be hosted in the Information sub-plane. Inventory information can be also retrieved either directly by the Information sub-plane or through references from information kept at the Orchestration sub-plane.

In this respect P&P has been designed on the basis of the provisioning of vertical oriented exposure of the delivered slice. This requires that specially crafted plugs are available that allow verticals activate those relating to their business. Each of the plugs provides a northbound exposure that fits the needs of the slice owner whereas it is able to process, in southbound, the platform specific information as this is maintained via the layered and multidomain FCAPS enablers. FCAPS framework is also provided in an abstraction fashion starting from the pillar technologies per NSP domain and spanning up to inter-domain aggregations as administered by the DSP domains. The overall governance of the several domain enablers and abstractions is applied through the One Stop API that spans vertically from NSP to Vertical and provides role based views of the artifcacts that have to be administered under a producer consumer relationship between overlayed roles.

In practice FCAPS allows NSP domain to abstract its domain specific technologies with respect to actuation and sensing capabilities and expose these as offerings through the One Stop API towards DSPs. DSPs can consume the monitoring information as this arranged per slice via the NSP Data Lake implemented as a time series Influx DB as well as invoke actuation information through the layered orchestration entities. DSPs maintain higher level slice counters and metrics, in their own Data Lakes, as these have been made available through exposure functions instantiated per slice and specially allocated Kafka topics. At the level of DSP, Data Lake information is subject to be processed by Cognitive, QoE and P&P functionalities that have been activated per slice to deliver higher level and novel FCAPS strategies. Beyond the bottom-up approach for the delivery of slice specific metrics and due to the vertical centric approach it was considered important to allow verticals contribute to the Data Lake information for the exploitation of service metrics that the user endpoints are able to produce. In this respect the vertical tailored UI view provided by P&P and OSA is augmented to create slice specific endpoints that expose the existing P&P options towards more automated (UI less) procedures to contribute to the slice segment of the DSP Data Lake and trigger cognitive and QoE functions via direct quantitative vertical feedback. OSA allows therefore slice owners to indicate which P&P functions should be exposed as REST endpoints that can be invoked by metric and counter agents deployed in vertical UEs and collecting valuable metrics from the user domain.

5.5 Orchestration

The proposed multi-domain orchestration is based on a cross-layer combination of three levels of orchestration logics, namely for vertical services, NSs and slice resources. These levels of orchestration logics are implemented in three different functional modules which are mapped to the business roles identified in clause 5.1: the Service Orchestrator at the DSP level, the Slice Orchestrator at the NSP level and the Resource Orchestrator at the NSP level. While the combination of the Service and Slice Orchestrators builds the SS-O (Service and Slice Orchestrator), the Resource Orchestrator is defined and described hereafter as NMR-O.

Figure 20 shows how these orchestration function modules relates each other to build the proposed multi-domain orchestration architecture for 5G vertical services and Network Slices. In practice, each NSP domain offers a set of Network Slices to one or more DSP domains. The Slice Orchestrator within each NSP domain is responsible to expose single domain Network Slices, managing their lifecycle (instantiation, configuration, runtime operations) leveraging on the capabilities offered by the NMR-O for the NSP domain resource orchestration (at network, NFV and MEC level). In turn, each DSP offers to verticals E2E Network Slices, spanning across multiple NSP domains, in the form of 5G vertical services.

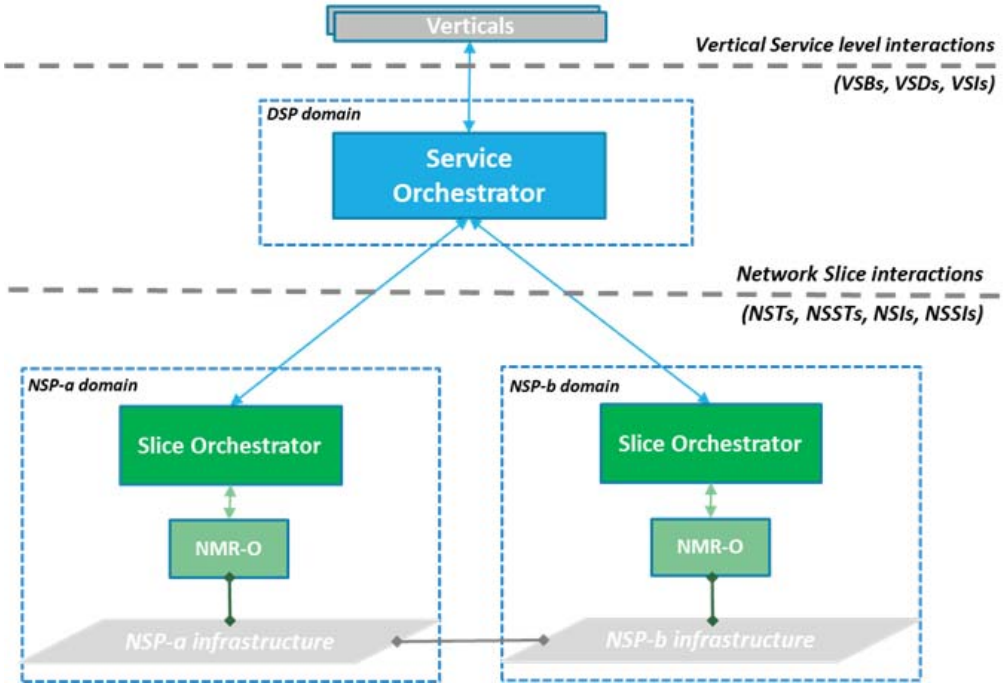

Figure 20: SliceNet multi-domain orchestration high level approach

As said, the SS-O functionalities are implemented by the combination (and interaction) of the Service and Slice Orchestrators, which respectively reside in the DSP and NSP domains.

The Service Orchestrator at the DSP level provides orchestration of vertical services as requested by verticals and takes care to map these into E2E Network Slices which are composed by single-domain Network Slices offered by one or more NSPs. Therefore, it manages the lifecycle of E2E Network Slices and coordinates the Slice Orchestrators. In terms of vertical service and E2E NS management features offered by the Service Orchestrator, they can be summarized as follows:

- interaction with verticals for service offer exposure and customization;
- collection of Network Slice offers from NSPs, in the form of Network Slice Templates (NSTs);
- lifecycle management of vertical services, mapped to E2E Network Slice and composed by single domain Network Slices;
- maintenance of up to date vertical service and E2E Network Slice instance status and features;
- coordination of multi-domain actuation operations for runtime optimization of E2E Network Slices.

On the other hand, the Slice Orchestrator is responsible for the coordination of single-domain Network Slices lifecycle, thus interacting with the NMR-O resource orchestrator for the actual creation and configuration of slice resources. The Slice Orchestrator is deployed at the NSP level, and it manages single administrative domain Network Slices while, in terms of management logics, it operates at a finer resource granularity with respect to the Service Orchestrators within the DSPs, since it coordinates the actual resources in the NSP physical and virtual infrastructure. As part of its single-domain Network Slice management responsibilities, the Slice Orchestrator provides the following main functionalities:

- interaction with DSPs for single domain NS offer exposure, including slice components and capabilities;
- onboarding and maintenance of NSTs;
- lifecycle management of Network Slice instances, including mapping and translation of Network Slice instance requirements into resource constraints and operations;
- maintenance of up-to-date Network Slice instances status and characteristics;
- coordination of single-domain actuation operations for runtime optimization of Network Slice instances.

The main work element of the NMR-O is the Network Service, which is basically a set of virtual and physical functions and configurations that are configured at the infrastructure of the NSP and work in a coordinated way to provide a more complex functionality to the NS. Hence, the NMR-O receives Network Service requests from the SS-O at NSP level through the NBI. The core of the NMR-O is implemented by Open Source MANO. In NMR-O functional architecture, OSM is expected to provide the orchestration of the VNFs composing the network services requested from the SS-O. In this regard, the NSO forwards the network service-related operations received through its NBI to the OSM NBI. Upon the reception of these requests, OSM contacts the Virtual Infrastructure Manager(s) of the NSP to allocate and configure the computational and network resources to provide the network service(s).

6 Impact of MEC, Network Slicing and Hardware Acceleration to the SliceNet Concepts and Principles

6.1 Impact of Virtualization

The urge to increase significantly the operational efficiency in service delivery and the agility to create and manage new services lead the traditional communication service providers to begin the adoption of the cloud computing paradigm as a foundation to its service infrastructure. In this context standardization bodies, and specially ETSI, started to define new network and service architectures, using cloud computing to promote the evolution from traditional networks (built over traditional network appliances providing network functions over dedicated specialized hardware - network ossification), to new generation networks where the trend is to decouple network functions (software) from the supporting infrastructure and to deploy those functions in geographically distributed telecom data centres (living networks).

NFV aims to transform network architectures by implementing network functions in software that can run on common purpose virtualized infrastructure built on top of industry standard hardware. Benefiting from IT Cloud Management evolution, especially the evolution in VIM (Virtual Infrastructure Management) platforms (e.g. OpenStack), the evolution towards an NFV enabled service architecture will lead to the creation of a new service environment, built over a mesh of micro data centres, the new service platforms. These platforms, including advanced virtual infrastructure management platforms, will provide enhanced agility for new services creation and management, being also a contributor for costs reduction due to use of common purpose hardware. At present time, the creation of a new service requires the setup of an engineering project to coordinate and govern the configuration of several distinct network elements (appliances) and the creation of specific service logic in proprietary service delivery and control platforms. Additionally, the management of this distributed service intelligence over several network appliances requires the setup of complex management processes.

All this together compromises the agility to launch new services. The migration of service logic to software functions hosted by data centres, the VNF's (Virtual Network Function), will allow the service provider to reduce significantly the operational impact of launching new services. At first, developing a set of software components is, in principle, much more agile and fast than to create new functions in several network appliances (or to deploy new appliances altogether) and additionally will bring much more flexibility to create new functions. Second, but not least important, the virtual infrastructure management capabilities provided by the new service platforms will support through API's (Application Programming Interface) full automated management of the VNFs. This will not only contribute to implement automated management processes (deployment, provisioning, supervision, etc.) but will provide new tools that will streamline the implementation of new service management scenarios like service personalization, service optimization (e.g. service load dynamic adaptation, dynamic QoS management) and service healing (e.g. service replacement and/or reconfiguration to bypass anomalies). On the other hand, this evolution movement will impose new requirements on the traditional operations management processes, creating the need to explicitly manage new service elements like virtual compute, virtual networking and virtual network functions.

6.2 Impact of MEC

SliceNet exploits the interplay between Multi-access/Mobile Edge Computing (MEC) and Software-Defined Networking (SDN) in exploring and demonstrating coordinated network programmability through an ecosystem of network applications and SDK. Given the open specifications of MEC for vendor implementation, the SDN concept is applied in SliceNet MEC system called Low-Latency MEC (LL-MEC) with OpenFlow and FlexRAN protocols. LL-MEC provides an ETSI-aligned MEC platform and also acts as a CN controller providing a clean separation between Control Plane (CP) and User Plane (UP) or Data Plane (DP) in the CN.

Figure 21 shows the schematic diagram of LL-MEC. The MEC application manager lays the foundation for the upper-most layer and provides the programming interfaces (Mp1) for applications to be developed. Standing in the middle layer, the MEC platform includes two main core components, namely Radio Network Information Service (RNIS) and Edge Packet Service (EPS), which manage RAN and CN network services based on the C-plane and D-plane Application Programming Interfaces (APIs) from the abstraction layer respectively. At the bottom-most layer, the eNodeBs and OpenFlow-enabled switches comprises the Data Plane with the information abstracted by the FlexRAN and OpenFlow protocols and exposed through abstraction API (Mp2). The proposed MEC platform operates on a software-defined mobile network consisting of multiple LTE eNodeBs and OpenFlow-enabled switches, whether it is physical or software. Figure 21 depicts the application of LL-MEC to 4G. As seen in the figure, the control and Data Plane are separated, which without loss of generality also applies to 5G. In order to simplify the annotation in the figure, the Control Plane and Data Plane of SGW and PGW are respectively annotated as X-GW-C and X-GW-U, which represent the UPF and to some extend SMF in 5G-CN architecture. As specified by ETSI, the Mp1 and Mp2 reference points are the interfaces between layers.

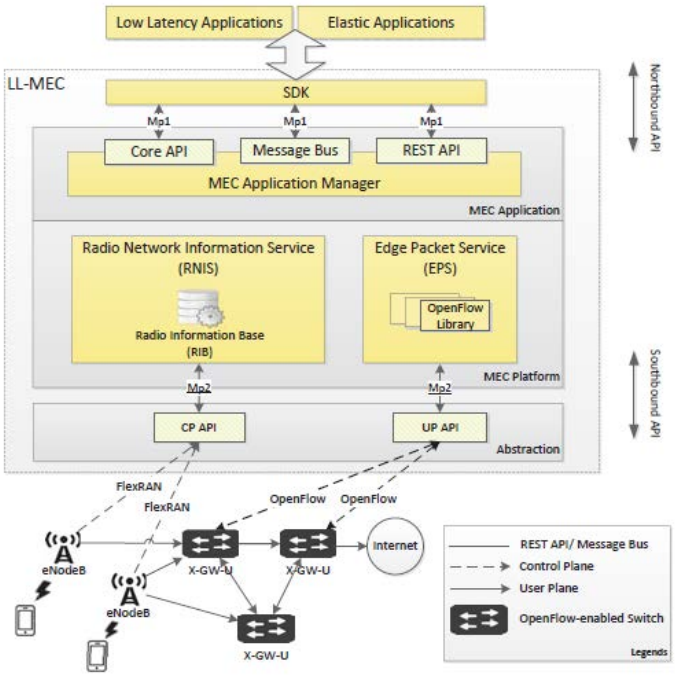

Figure 21: Schematic diagram of LL-MEC

6.3 Impact of Network Slicing

Figure 22 shows an example of 5G network slicing, In this example, each of the network slices has dedicated network functions e.g. UPF, SMF, NRF, PCF while several common NFs (e.g. AMF, NRF, NSSF, UDM, and AUSF) can be shared among the network slices.

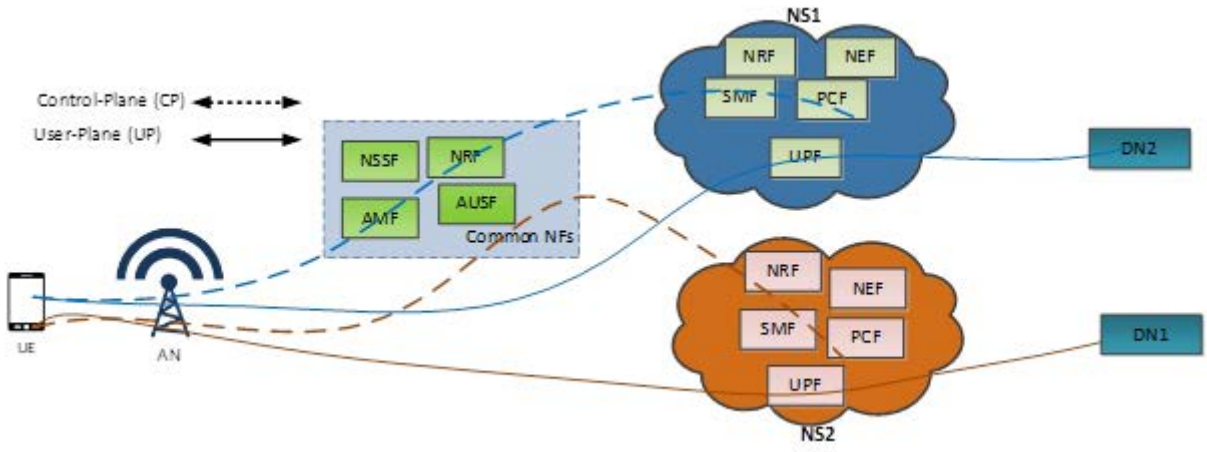

Figure 22: 5G network slicing

SliceNet achieves End-to-End (E2E) network slicing for 4G/5G networks. Figure 23 below shows a deployment example for the SliceNet Infrastructure which is based on the OAI, Mosaic-5G FlexRAN and LL-MEC platforms. This infrastructure offers the following features:

- A RAN runtime slicing system, which enables the dynamic creation of slices with QoS support, while providing functional and resource isolation among different slices (e.g. verticals).
- LL-MEC platform leverages the SDN principle to separate user plane processing from its control logics at the edge and core networks to enable user plane programmability as per slice requirements.

Dedicated core networks on per slice basis enabling isolation among different slices.

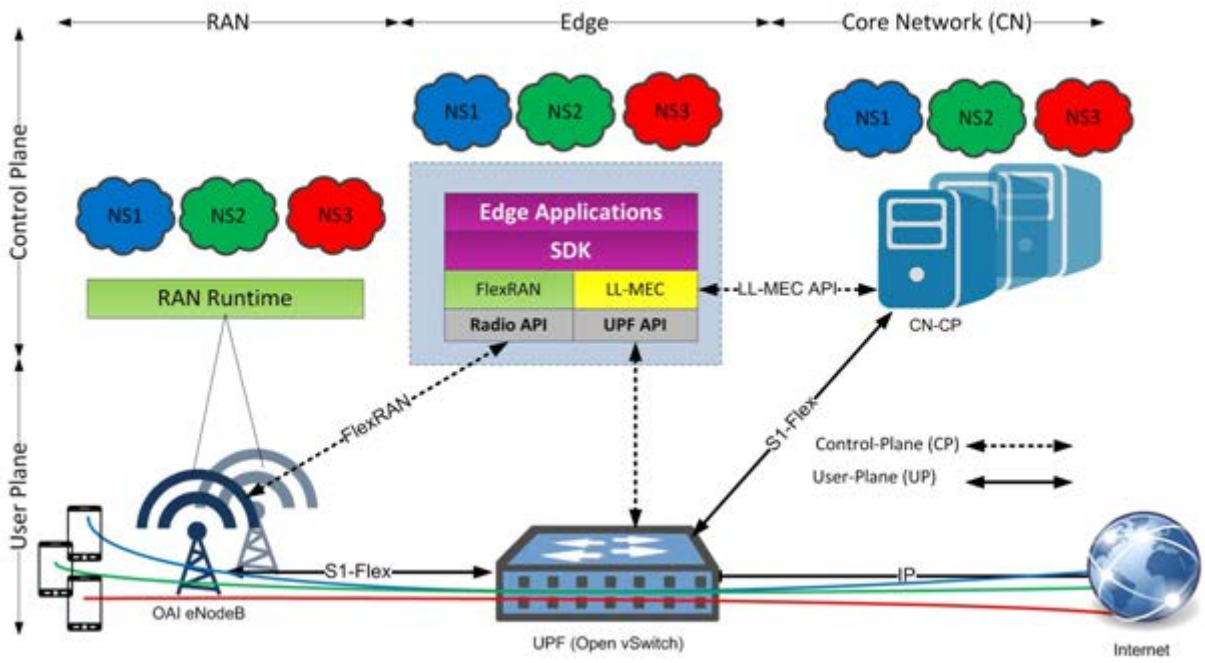

Figure 23: E2E network slicing

Furthermore, in the MEC-to-CN segment, data plane network slicing can be applied to ensure the QoS of the network slice instance over this wired network. A programmable software data path together with a flexible definition of network slices, will allow controlling traffic in 5G infrastructure, as a means to control the QoS of the slices. This is especially important in architectures where user mobility and tenant isolation are essential requirements and have to be supported both at the same time. From the NSP point of view, these requirements are key aspects and they imply the use of nested encapsulation. It is also necessary to isolate the performance of different 5G users belonging to different tenants and to isolate the performance of the different tenants using the same physical infrastructure. In summary, in a 5G scenario, a "Programmable Software Data-Path" has to offer fine-grained control over 5G flows, allowing slicing at 5G user-level to provide simultaneous control of users, tenants, and infrastructure. Given the above mentioned 5G requirements, the SliceNet programmable software-based data path based on the Open Virtual Switch (OVS) provides novel mechanisms designed and prototyped in the context of this project to contributing to controlled performance in 5G traffic:

- 5G flow specification: Low-level implementable and flexible specification of a 5G Network Slicing definition according to different criteria such as Tenant or User identifier, and others.
- QoS requirements: For each defined 5G Network Slice, QoS control is enforced to allow performance tenant isolation and 5G user isolation.
- Dynamic configuration of a slice:Change in real time any of the parameters of a 5G Network Slice definition and its QoS associated, through actuations including setting new bandwidth, redirecting traffic, dropping traffic, etc.

6.4 Impact of Hardware Acceleration

An extension to softwarised data plane in SliceNet is hardware-based programmable data plane. Through hardware acceleration for traffic engineering, the performance of data plane network slicing can be significantly enhanced. The Figure 24 shows such a hardware-acceleration based programmable data plane for traffic classification and control.

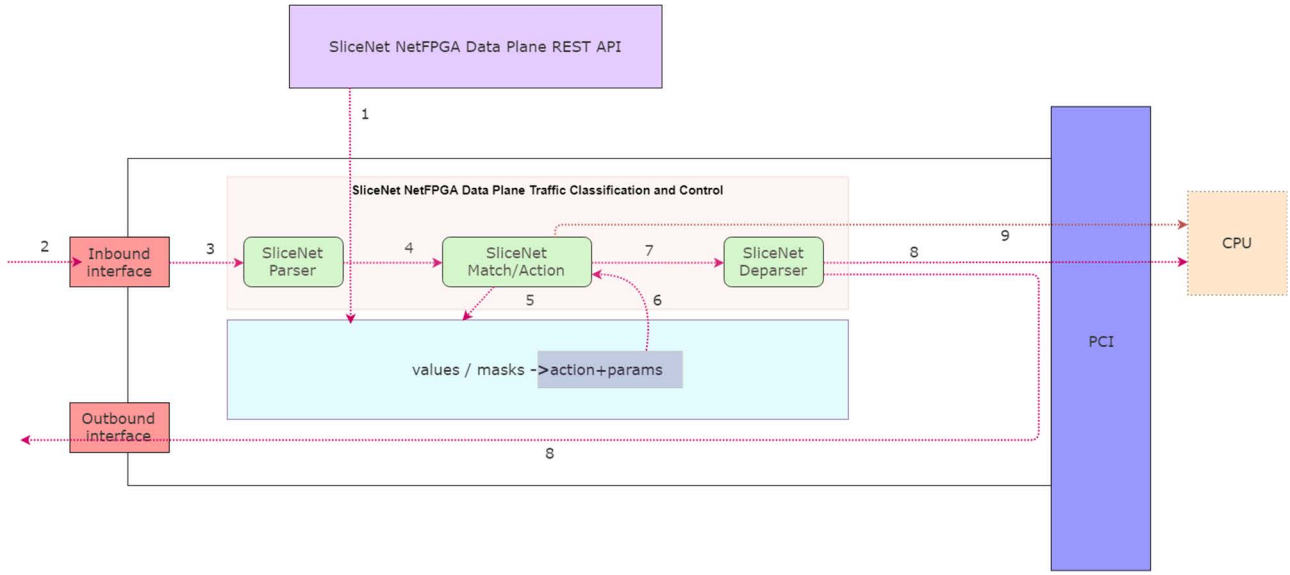

Figure 24: Hardware-acceleration based programmable data plane

The operations of this prototyped hardware programmable data plane are as follows:

1) The traffic classification rules are inserted in the hardware platform's Ternary Content Addressable Memories (TCAM) table through a REST API.

2) An inbound packet arrives at the hardware platform.

3) The packet is sent to the Parser for classification.

4) Once the packet has been classified based on its headers, it is sent to the Match/Action component.

5) In the Match/Action component, the TCAM table is checked.

6) If there is any rule that matches the packet, the "action data" will be received by the Mach/Action (step 6).

7) Match/Action applies to the packet the action received in the "action data" of the rule (step 6) and it is sent to the Deparser component.

8) The Deparser builds the packet that is going to be sent to the PCI or to the outbound interface depending on the specific action.

9) The digest data will be sent to the CPU for further processing.

7 GANA in ETSI 5G PoC Implementations by the Industry

This clause describes the framework ecosystem shown below which corresponds to the discourse where GANA Autonomics are being built and demonstrated to the industry. This ecosystem is 5G network slice-centric; meaning the stakeholders are assigned roles of slice consumer or customer and slice producer/provider. Resource management (including allocation, provisioning, monitoring, guaranteeing, and adapting) is governed by GANA AMC (Autonomic Management and Control Paradigm) and uses slices as main instruments of leverage. Whether CSPs, ISVs (Independent Software Vendors), Hardware Vendors, Manufacturers, or End-Customers, all stakeholders get their interactions and service transactions organized using 5G slices with end-to-end capabilities) and those slices are orchestrated by the Autonomic Network (AN) in the shown ecosystem to form the workflow of the scenario use-cases and shape the behaviour the GANA Autonomic Management and control components (with capabilities related to AI and ML). The guidelines for behavioural modelling come from high-level policies, objectives (which may be formulated as intents), which are then broken down into smaller objectives and actions by the AN in line with the GANA AMC.

Figure 25 presents the Ecosystem that is the basis for the ETSI INT AFI WG 5G PoC on 5G Network Slices Creation with ETSI GANA Autonomic & Cognitive Management of 5G Slices & E2E Orchestration and the Consortium. The depiction of the high-level design principle of the 5G PoC ecosystem and associated actors/roles relationships and interactions that are described in [i.4].

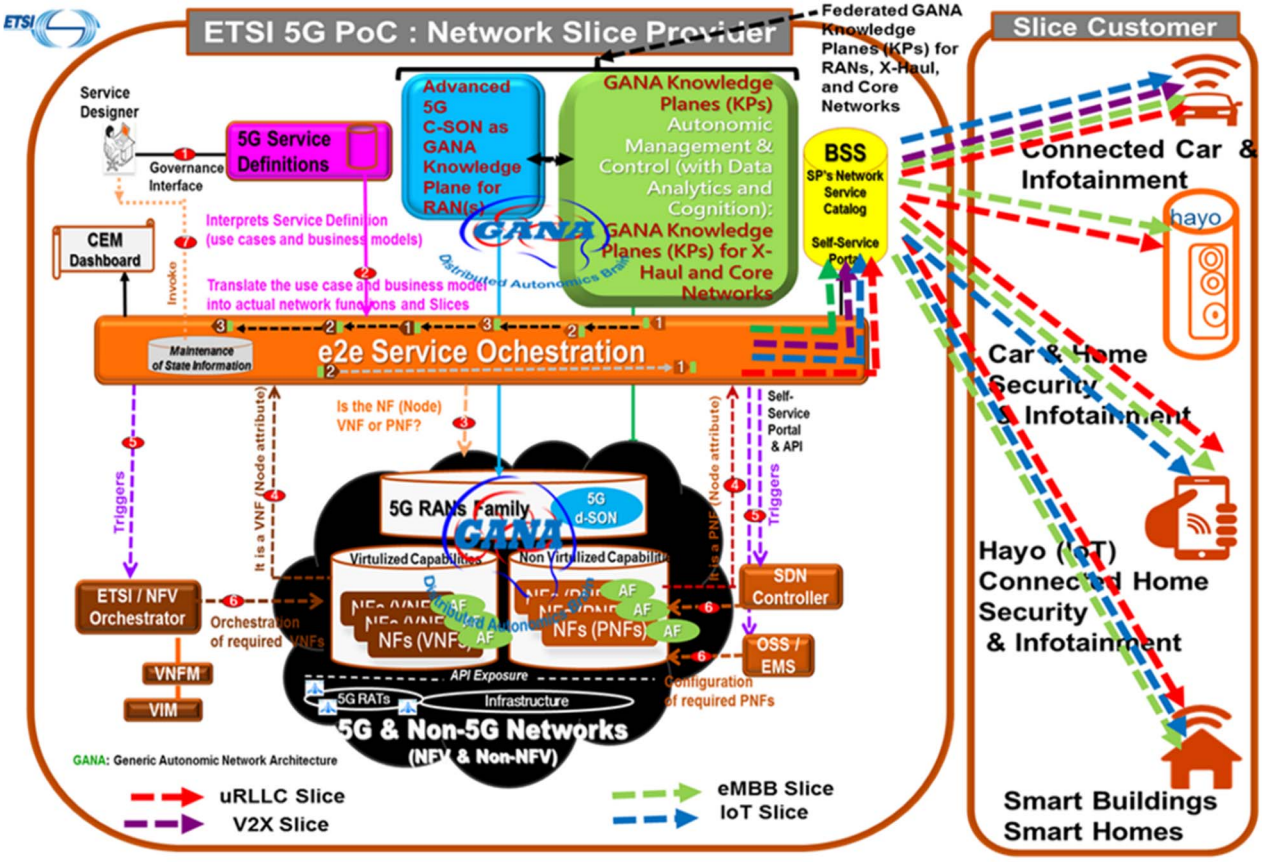

Figure 25: The Ecosystem that is the basis for the ETSI INT AFI WG 5G PoC on 5G Network Slices Creation with ETSI GANA Autonomic & Cognitive Management of 5G Slices & E2E Orchestration and the Consortium

It is describes for instance architectural frameworks defined in GANA in [i.4] and [i.15], e.g. C-SON as GANA Knowledge Plane for RAN.

While leveraging GANA Autonomics and demonstrating different capabilities of various stakeholders in this discourse, the ETSI PoC (Proof of Concept) series instrument has been used within TC INT AFI in different show-cases (PoC series instances) as outlined below:

- ***ETSI PoC Demo Instance No.1:*** *Autonomic Service Assurance for IoT in Smart Insurance and related use-cases. Through closed-loop automation, assuring and guaranteeing service QoS, SLA, and KPI requirements to be maintained and eventually monetized, thanks to GANA Autonomics, and demonstrating the feasibility of the use-case selected and the gained leverage were fully achieved objectives.*

- ***ETSI PoC Demo Instance No.2:*** *C-SON Evolution for 5G, Hybrid SON Mappings to the ETSI GANA Model, and achieving E2E Autonomic (Closed-Loop) Service Assurance for 5G Network Slices by Cross-Domain Federated GANA Knowledge Planes. The alignment and compatibility of the GANA Autonomics framework and model with H-SON which is a key technology used and endorsed in 3GPP shows a high-potential SDO alignment and synergy showcased in the PoC.*

- ***ETSI PoC Demo Instance No.3:*** *Programmable Traffic Monitoring Fabrics that enable On-Demand Monitoring and Feeding of Knowledge into the ETSI GANA Knowledge Plane for Autonomic Service Assurance of 5G Network Slices; and Orchestrated Service Monitoring in NFV/Clouds.*

- ***ETSI PoC Demo Instance No.4:*** *Generic Framework for Multi-Domain Federated ETSI GANA Knowledge Planes (KPs) for End-to-End Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Networks/Services.*

- ***ETSI PoC Demo Instance 5 (in preparation):*** *ETSI GANA as Multi-Layer Artificial Intelligence (AI) Framework for Implementing AI Models for Autonomic Management & Control (AMC) of Networks and Services; and Intent-Based Networking (IBN) via GANA Knowledge Planes (KPs) and Artificial Intelligence (AI) in Test Systems, Testing AI Models and ETSI GANA Model's Cognitive Decision Elements (DEs) via a Generic Test Framework for Testing GANA Multi-Layer Autonomics & their AI Algorithms for Closed-Loop Network Automation.*

A detailed list of documents, whitepapers, and PoC descriptions can be found at https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals.

Figure 26 presents the 3GPP Hybrid-SON Model Mappings to the ETSI GANA Model.

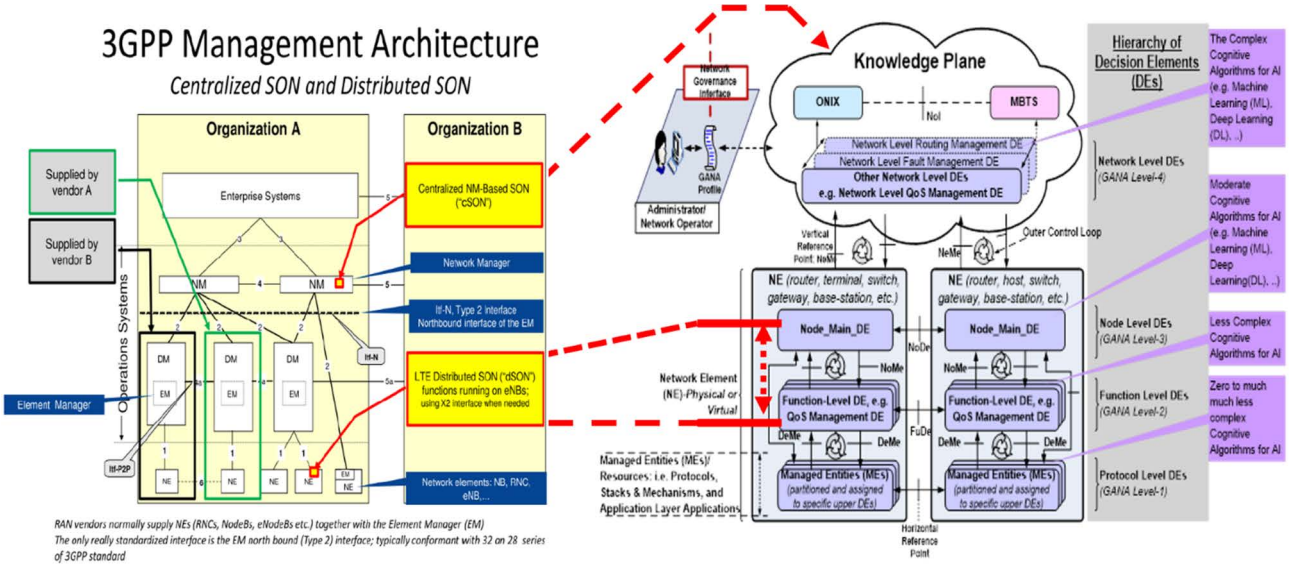

Figure 26: 3GPP Hybrid-SON Model Mappings to the ETSI GANA Model

Figure 27 presents an Illustration of SON Functions Mappings to the ETSI GANA Model, D-SON mapped to GANA Levels 2 & 3 DEs Implementation.

SON Function	GANA DE Specialization as SON Function(s)
Plug & Play; CCO; ANR; RACH Optimization	Auto-Configuration-DE
Cell Degradation Management; COC	Fault-Management-DE; Resilience&Survivability-DE
ES (Energy Saving)	Auto-Configuration-DE
H00; MRO	Mobility_Management_DE
LBO (MLB?); APO	QoS_Management_DE

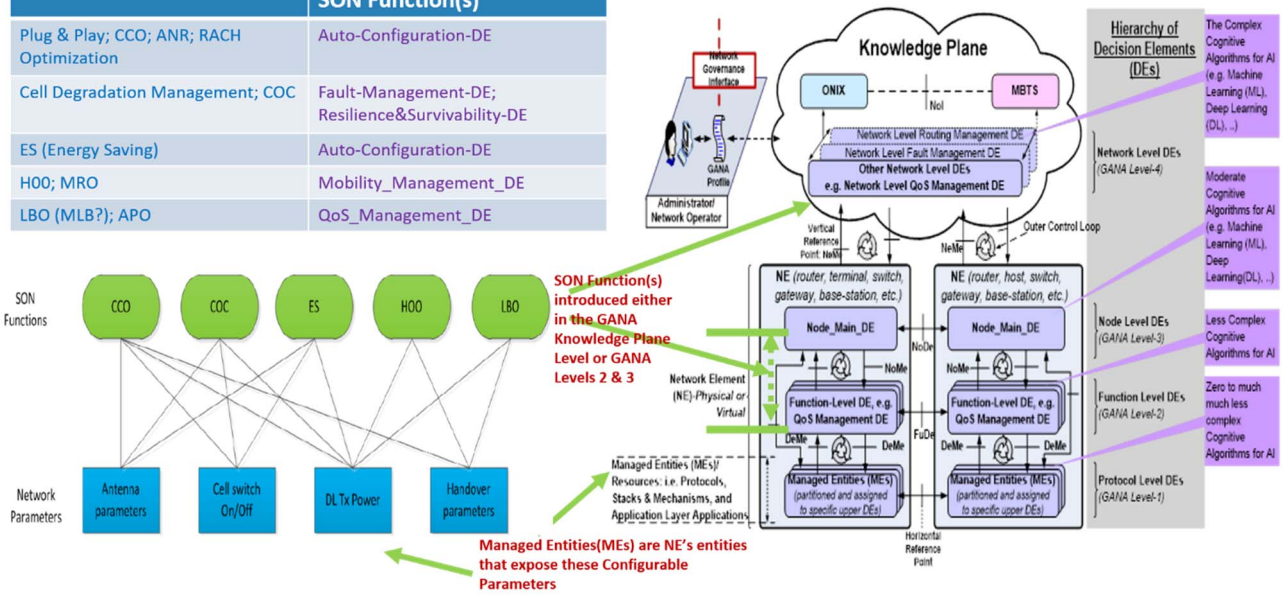

Figure 27: Illustration of SON Functions Mappings to the ETSI GANA Model, D-SON mapped to GANA Levels 2 & 3 DEs Implementation

The following diagrams provide an illustration of Federation of GANA Knowledge Planes (KPs) for E2E Autonomic (Closed-Loop) Service & Security Assurance of 5G Slices, a case called "**Horizontal Federation of GANA KPs**". Figure 30 provide an illustration of Federation of GANA Knowledge Planes (KPs) for E2E Autonomic (Closed-Loop) Service & Security Assurance of 5G Slices, a case called "**Vertical or Hierarchical Federation of KPs**". More details on this subject can be found in [i.21].

Figure 28 presents a Framework for E2E Autonomic(Closed-Loop) Service Assurance of Network Services through the Federation of GANA Knowledge Planes (KPs) for various segments: RAN (C-SON), Front-/Backhaul, Core Network, etc., and complemented by lower level autonomics in Network Elements (NEs) or Network Functions(NFs). More details on this subject can be found in [i.4].

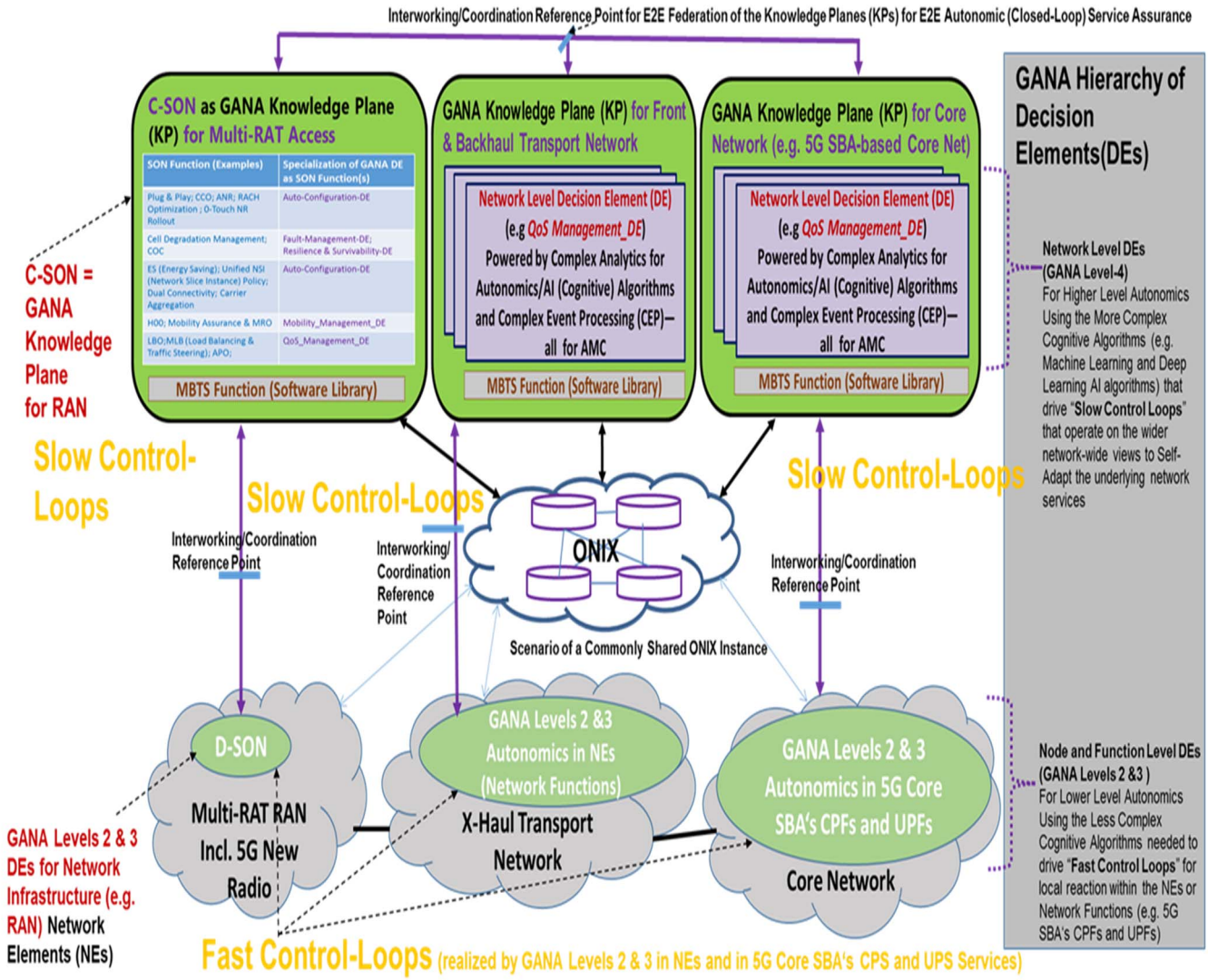

Figure 28: Framework for E2E Autonomic (Closed-Loop) Service Assuranceof Network Services

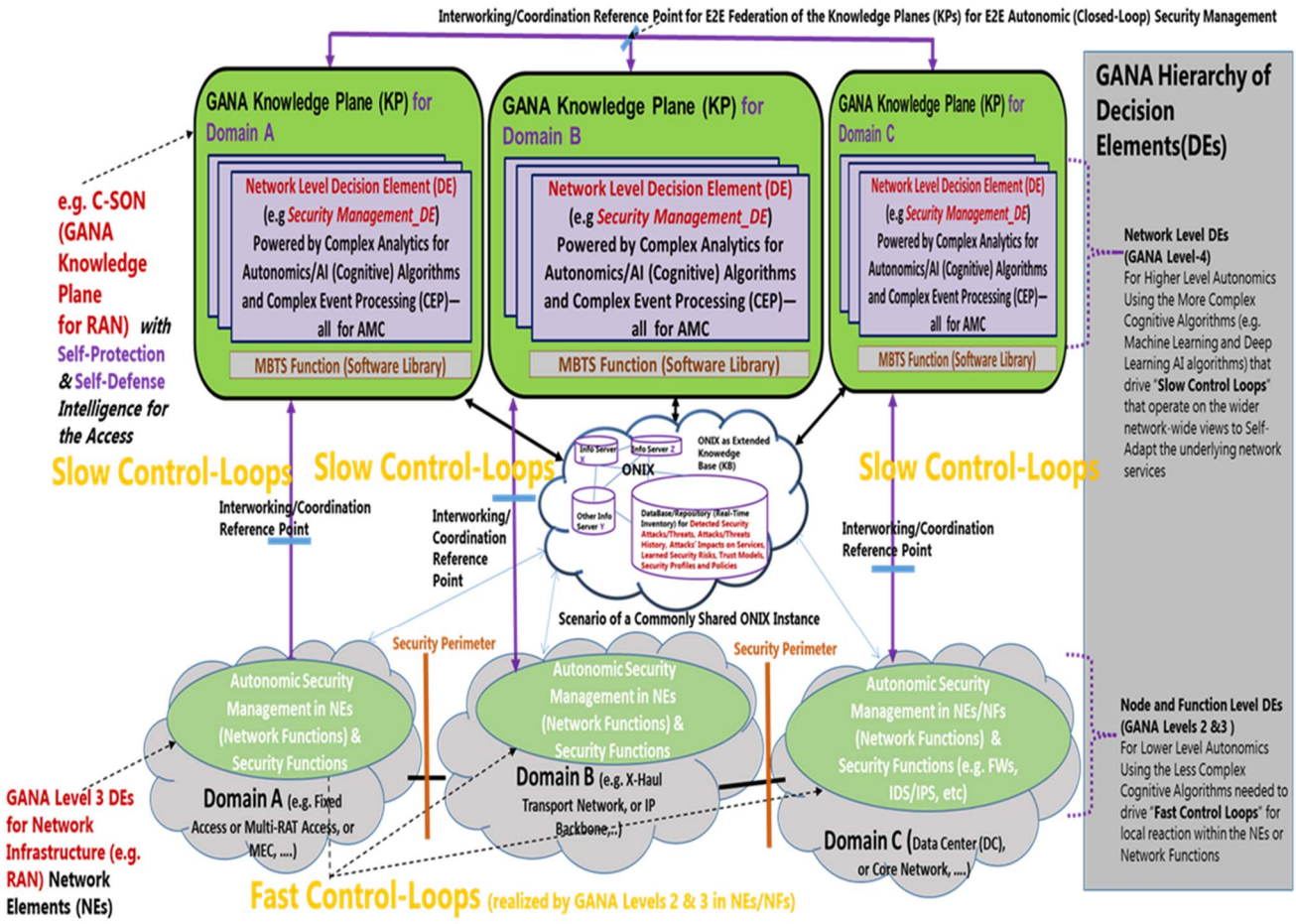

Figure 29: Option-A GANA: Knowledge Planes Horizontal Federation

Figure 30 presents the Option-B (Vertical/Hierarchical Federation), by which the GANA Knowledge Plane (KP) Platforms for the specific network segments federate vertically through an overlay umbrella Hierarchical GANA Knowledge Plane (KP) Platform that receives information from the lower level KPs and coordinates the lower level KPs. More details can be found in [i.21].

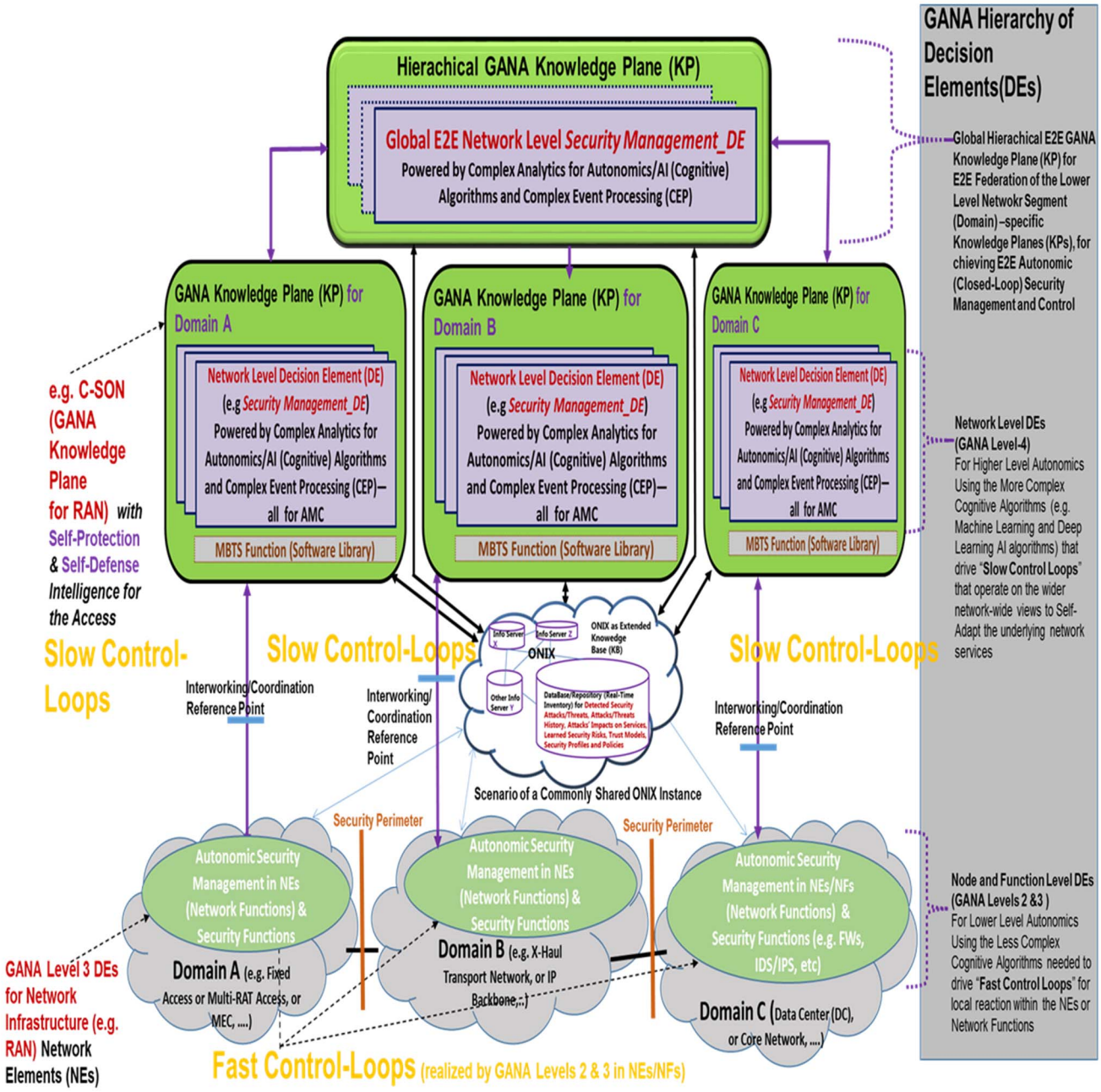

Figure 30: Option-B: GANA Knowledge Planes *Vertical*/Hierarchical Federation

Figure 31 presents the Option-A (Horizontal Federation of Knowledge Planes Platforms) in Inter-Network Segments KP Domains model (within a single Organization Scenario). More details on this subject can be found in [i.20].

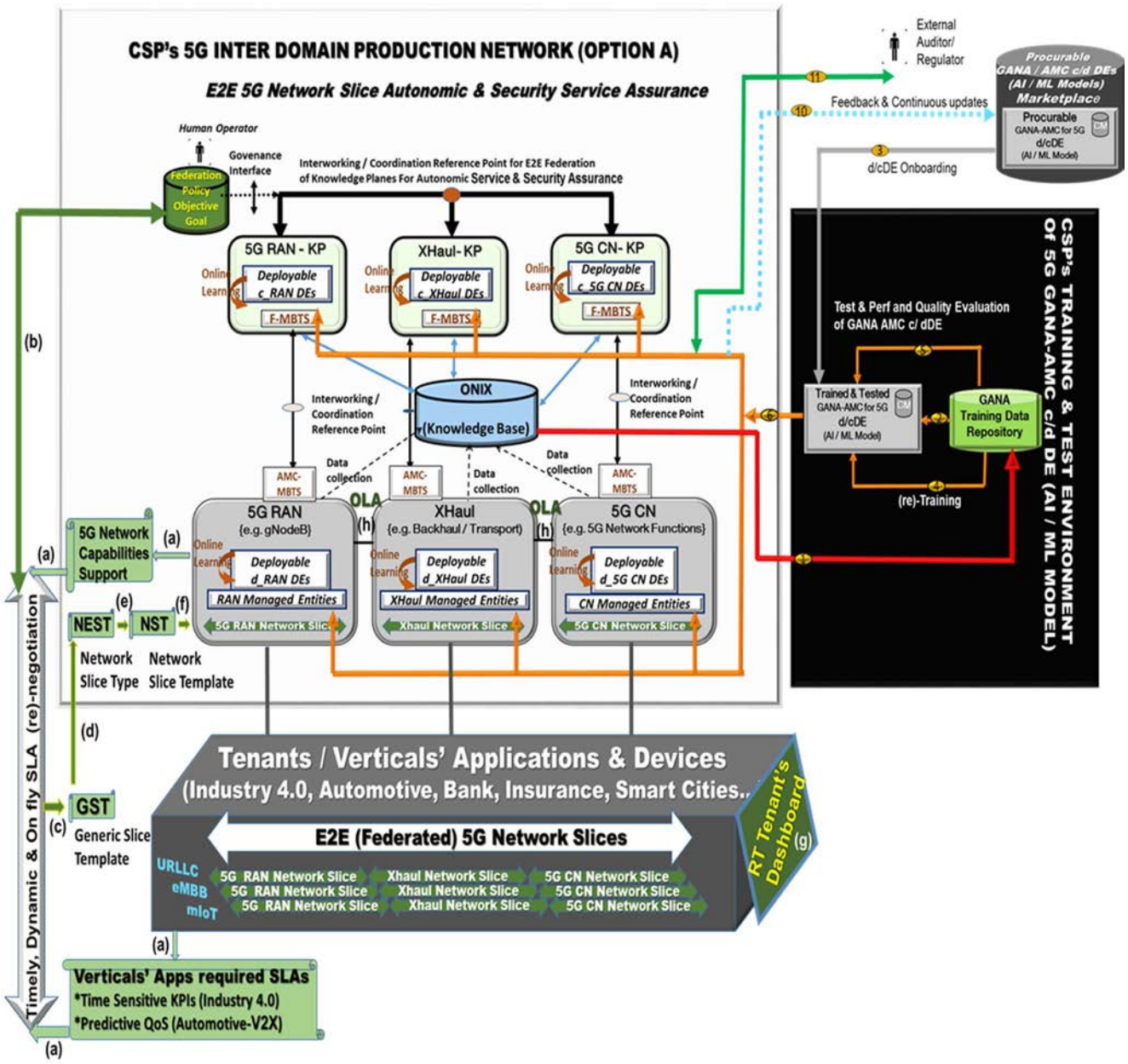

Figure 31: Option-A (Horizontal Federation of Knowledge Planes Platforms) in Inter-Network Segments KP Domains model (within a single Organization Scenario)

Figure 32 presents the Option-B (Hierarchical/Vertical Federation of KP Platforms) in Inter-KP Domains model (within a single Organization Scenario). More details on this subject can be found in [i.20].

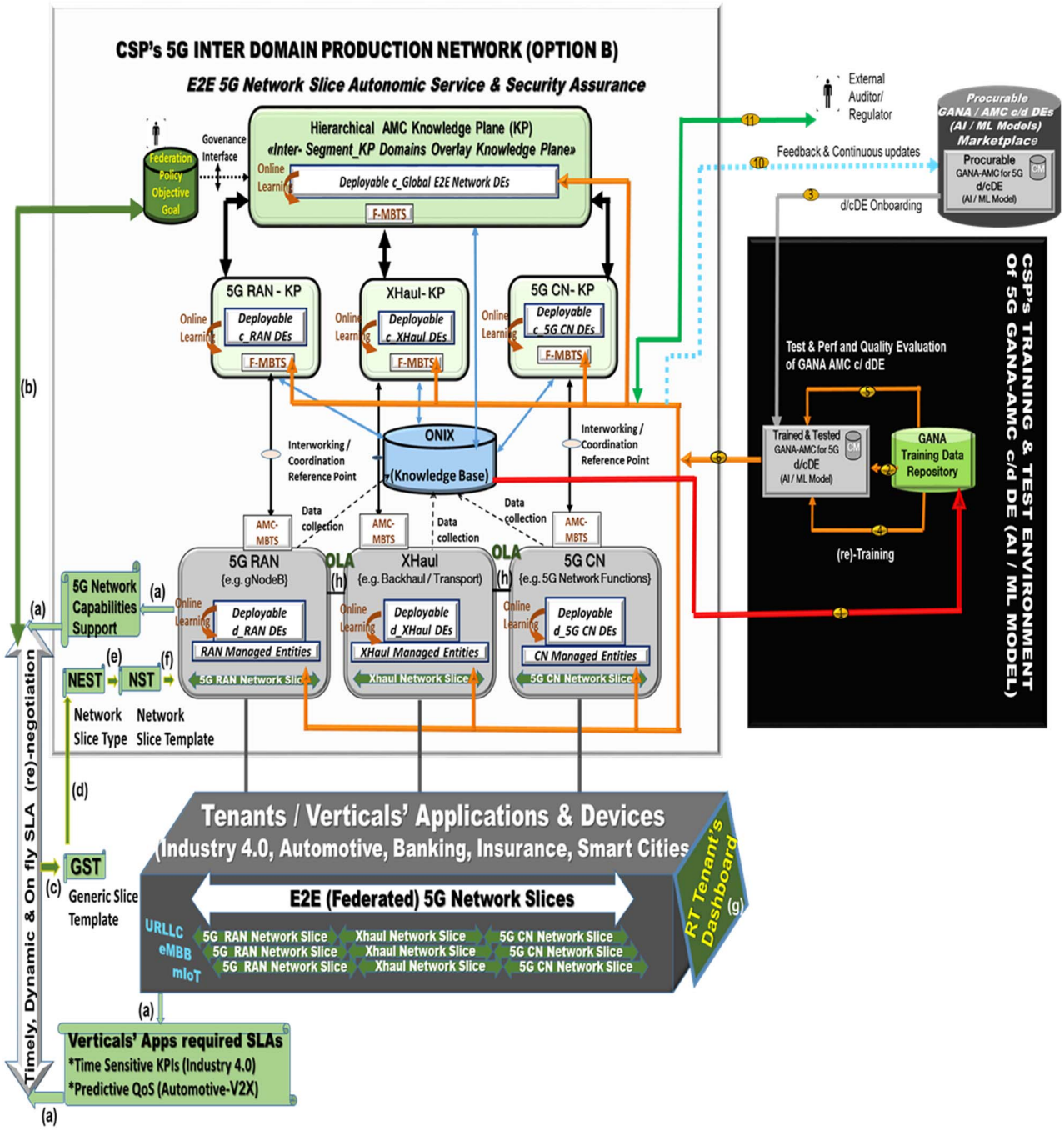

Figure 32: Option-B (Hierarchical/Vertical Federation of KP Platforms) in Inter-KP Domains model (within a single Organization Scenario)

Figure 33 presents Option-B (Hierarchical/Vertical Federation of Knowledge Planes Platforms) in Inter-Operator KPs federation model (Multi Organization Scenario). More details on this subject can be found in [i.20].

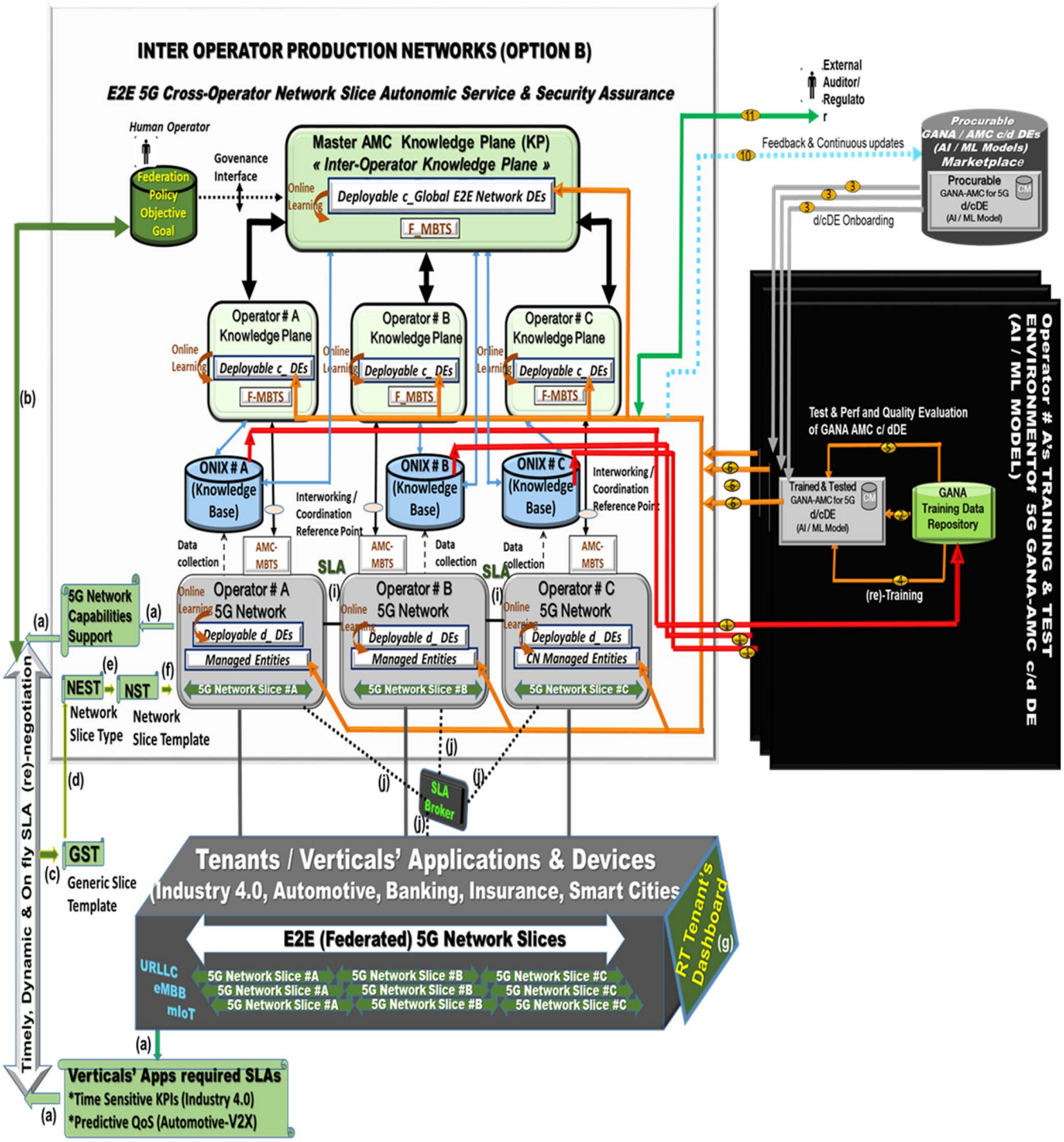

Figure 33: Option-B (Hierarchical/Vertical Federation of Knowledge Planes Platforms) in Inter-Operator KPs federation model (Multi Organization Scenario)

Figure 34 presents an illustration of Knowledge Plane (KP) driven "Open-Loop" and "Closed-Loop" (Autonomic) Service and Security Assurance for SDN Environments, with the capability of the Security Management-DE and the Monitoring-DE of the KP in being able to collaborate in triggering On-Demand Traffic Monitoring in the Network for Analytics of Suspected Traffic. More details on this subject can be found in [i.21].

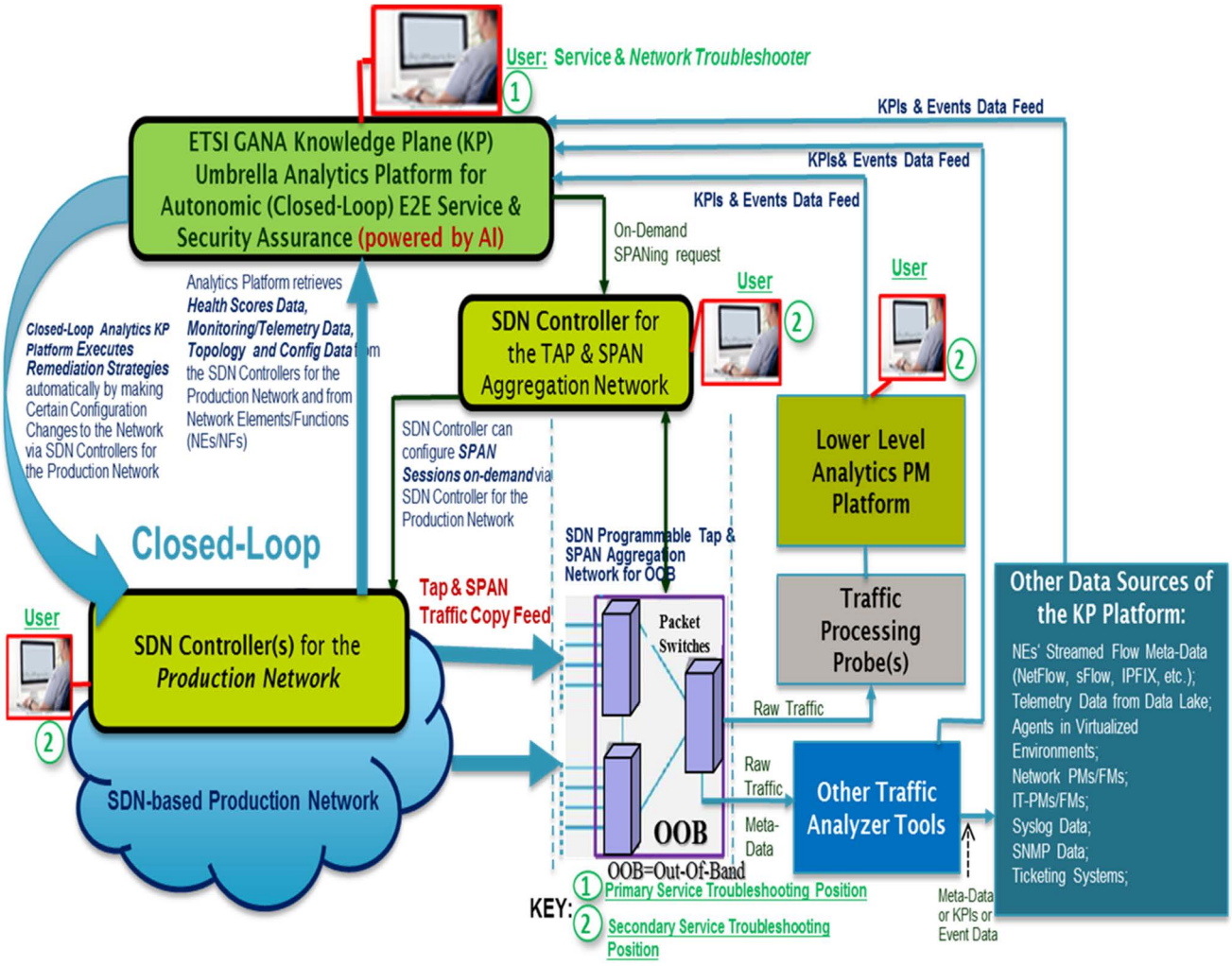

Figure 34: Knowledge Plane (KP) driven "Open-Loop" and "Closed-Loop" (Autonomic) Service and Security Assurance for SDN Environments

The following are some of the 5G PoC White Papers that have been published and are available for downloading at this PoC site: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals:

- ***White Paper No.1:*** *C-SON Evolution for 5G, Hybrid SON Mappings to the ETSI GANA Model, and achieving E2E Autonomic (Closed-Loop) Service Assurance for 5G Network Slices by Cross-Domain Federated GANA Knowledge Planes: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals.*

- ***White Paper No.2:*** *ONAP Mappings to the ETSI GANA Model; Using ONAP Components to Implement GANA Knowledge Planes and Advancing ONAP for Implementing ETSI GANA Standard's Requirements; and C-SON - ONAP Architecture: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals.*

- ***White Paper No.3:*** *Programmable Traffic Monitoring Fabrics that enable On-Demand Monitoring and Feeding of Knowledge into the ETSI GANA Knowledge Plane for Autonomic Service Assurance of 5G Network Slices; and Orchestrated Service Monitoring in NFV/Clouds: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals.*

- ***White Paper No.4:*** *ETSI GANA as Multi-Layer Artificial Intelligence (AI) Framework for Implementing AI Models for Autonomic Management & Control (AMC) of Networks and Services; and Intent-Based Networking (IBN) via GANA Knowledge Planes (KPs): https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals.*

- ***White Paper No.5:*** *Artificial Intelligence (AI) in Test Systems, Testing AI Models and ETSI GANA Model's Cognitive Decision Elements (DEs) via a Generic Test Framework for Testing GANA Multi-Layer Autonomics & their AI Algorithms for Closed-Loop Network Automation: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals.*

- ***White Paper No.6:*** *Generic Framework for Multi-Domain Federated ETSI GANA Knowledge Planes (KPs) for End-to-End Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Networks/Services: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals.*

8 Mapping of SliceNet architecture components to GANA Concepts and Architectural Principles, How to use the SliceNet components to implement GANA Components

8.1 General Mapping of SliceNet Architectural Concepts and Principles to GANA Concepts and Principles

This clause provides a mapping between functional components of the GANA and the SliceNet architectures. It is worth noting that the two architectures have been designed independently. In a bottom up approach the following aspects of mapping to the ETSI GANA are identified:

- SliceNet deploys technology adaptors in the context of Control Plane and Monitoring Descriptors in the context of FCAPS framework over network elements to support agnostic management and can be correlated with MEs at GANA Level-1.

- SliceNet Control Plane and FCAPS Framework components operate on top of the adaptors and monitoring descriptors to allow for proper enforcement of actions and unified retrieval of monitoring that is subject to domain specific processing and policies realized by the processing applied through the Tactical Autonomic Language (TAL or Rule) Engine and any local domain deployed Cognitive Modules. This resembles the Fast Control Loops delivered by GANA Level-2 and GANA Level-3 components. It is worth highlighting here that the separation per NE is applied in SliceNet at the level of adaptors and monitoring descriptors whereas the Fast Control Loops are delivered per Slice including all resources allocated in a particular domain. The latter maps, therefore, to any horizontal interaction as it can be found in GANA through the Horizontal Reference Points.

- Local domain processing in SliceNet can be exposed (through the appropriate TAL scripts) to Multi domain SliceNet components, where cross domain information is subject to processing by Cognitive, Plug and Play (vertical exposure) and Policy artifacts. The synthesis of this interdomain FCAPS and Control is modular and defined in the Slice capabilities that in turn rely on single Domain offerings. The very specific activation of the artifacts is subject to Vertical decision. The Cognitive, Plug and Play (vertical exposure) and Policy artifacts, once provisioned, provide the MBTS equivalent processing that leads to actuation towards the separate domains through Orchestration services. In the role of ONIX, SliceNet provides a Slice design options at the level of DSP where Cognitive, Plug and Play (vertical exposure) and Policy offerings are registered along with their dependencies on underlying (single domain) federated resources that are orchestrated based on the dependency resolution during provisioning phase.

- The KP DEs can employ the ONAP Policy Framework to distribute the KP generated policies to the specific targets that are policy controlled by the KP DEs. SliceNet's PF design and software implementation is partially aligned with ONAP Policy Subsystem as described in clause 5.3.4.

8.2 Autonomic networks and General GANA integration with SDN, NFV, Data Analytics Applications, Orchestrators, and Other Management and Control Systems

Network Function Virtualization (NFV) and Software-Defined Networking (SDN) are two key enabling technologies and principles for softwarisation in 5G networks, especially 5G network slicing. Softwarisation and virtualization with resource isolation overlay on top of shared physical resources is the key to create many different logic networks (network slices), each with a set of different network characteristics, designed for different vertical sectors. The adoption of technologies such as NFV and SDN are driving the wider utilization of practices such as control and data plane separation as well as workflow and process automation. Interoperability is a key in SliceNet and is enabled by the adoption of standard APIs and standard control and management architectures (e.g. at the SDN and NFV level) when applicable. Service components like network functions (either physical or virtual) are abstracted at different layers and across domains following the SDN and NFV principles to hide the infrastructure complexity to the vertical actors and customers. SliceNet Plug &Play control enable from a slice provider perspective to activate a specific per-slice SDN and NFV control functions needed to accommodate the vertical requirements, in terms of network functions composition, as well as performance and QoE. In particular, each Plug & Play instance should be able to plug specific drivers and plugins (while abstracting their logics and complexity) for SDN controllers, NFV MANO tools and even programmable PNFs and VNFs) running in the programmable E2E infrastructure (spanning from RAN to MEC and core networks).

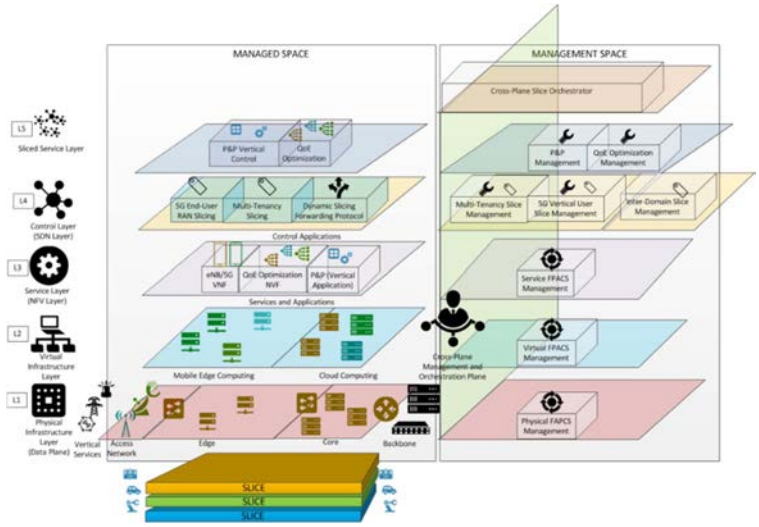

Figure 35: Five layer SliceNet managed domain

Figure 35 depicts a simplified view on SliceNet managed domain layers. The first layer (L1) is the Physical Infrastructure Layer, representing the 4G/5G physical infrastructure deployments. The Virtual Infrastructure (L2) is partially available in some latest 4G deployments or 5G prototypes, where cloud computing technologies are utilized and the emerging Mobile Edge Computing paradigm is being investigated to push virtualized resources to the edge of the network. The Service Layer (L3) comprises all the services (mainly NFV services in SliceNet) running on top of the underlying infrastructure. The Control Layer (L4) is decoupled from the Service Layer following the SDN paradigm to gain a holistic, logically centralized control of the physically distributed services. Finally, the Sliced Service Layer (L5) is a new layer introduced by SliceNet as a novel extension of the multi-tenant concept now embracing the SDN world. This layer provides a novel plug & play functionality of the control plane so that it is customized and isolated for a particular vertical customer of the infrastructure differentiating itself from the common control plane for all the users of the infrastructure.

Each SliceNet control service aims to provide specific slice configuration capabilities, following an SBA approach, in terms of:

- Inter-PoP forward graph configuration, mostly focusing on inter PoP network configuration (i.e. cross and inter pillar) to be combined with intra-PoP forwarding graphs that are normally offered by NFV and MEC MANO functions (via specialized VIM capabilities) in the context of NS support. Forward Graph Enabler (FGE) intents to account for the role of WIM Manager and remain compliant with ETSI MANO specifications. In this way the component is expected to be forward compliant with future NFVO implementations that support WIM Management.

- PNF, VNF and 4G/5G (either user or control) NF configuration.
- Inter-domain connectivity, focusing on user traffic classification and forwarding beyond 4G/5G Core pillars.
- UE Session QoS Control.
- Data Plane Programmability for quality based user traffic management that takes advantage of packet processing and acceleration techniques.

AMC, SDN, NFV, E2E orchestration of services and resources, and Big Data analytics applications for network management & control constitute the complementary networking paradigms for evolving future networks.

The AFI GANA Reference Model takes into consideration the impact of virtualization on network architecture.

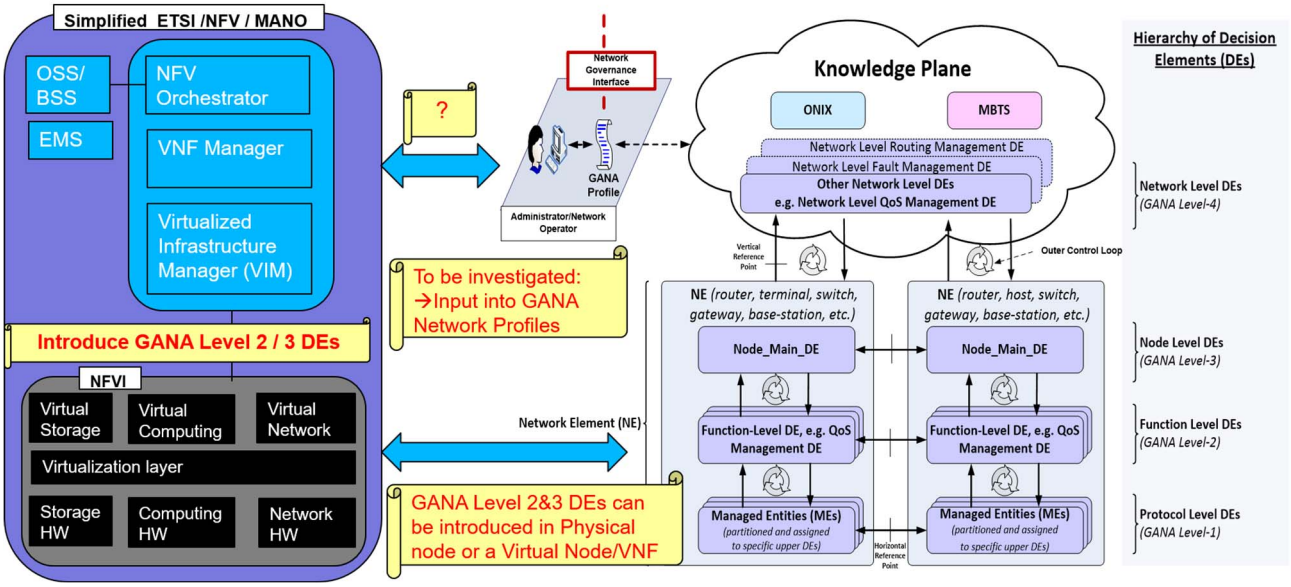

Figure 36: Impact of Virtualization on GANA Reference model: mapping to ETSI ISG NFV MANO

Clause 4.3 of the present document presents some aspects of GANA integration with SDN, NFV, Data Analytics Applications, Orchestrators, and Other Management and Control Systems. However, various aspects of General GANA integration with SDN, NFV, Data Analytics Applications, Orchestrators, and Other Management and Control Systems are addressed in various other documents published by ETSI and White Papers published by the 5G PoC Project [i.3]. The following are some of the resourceful documents that address this subject.

- ETSI 5G PoC Report [i.16].
- White Paper No.1 [i.4].
- White Paper No.6 [i.21].
- ETSI TR 103 473 [i.5]provides a link between SDN, NFV, GANA with consideration of BBF and 3GPP network domains.

8.3 SliceNet mapping to GANA Network Level (Knowledge Plane (KP) Level) Autonomics

As explained previously, inside its architecture SliceNet has designed and prototyped a Cognition Sub-Plane that incorporates ML techniques to gain insights about the underlying network infrastructure and deployed slices. Together with the incorporated actuation framework and the designed Data Lake, it enables network management systems with cognitive-based operations for quality-aware management of network slices. In this regard, SliceNet's Cognition Sub-Plane acts as the Knowledge Plane (KP) defined within GANA's architecture. Figure 37 depicts a simplified view of the SliceNet architecture, only showcasing the relevant components for the current discussion. In this regard, the figure illustrates how the multiple Cognition Sub-Plane components as well as the Monitoring Sub-Plane are mapped to GANA's architecture, more specifically to its KP and related components.

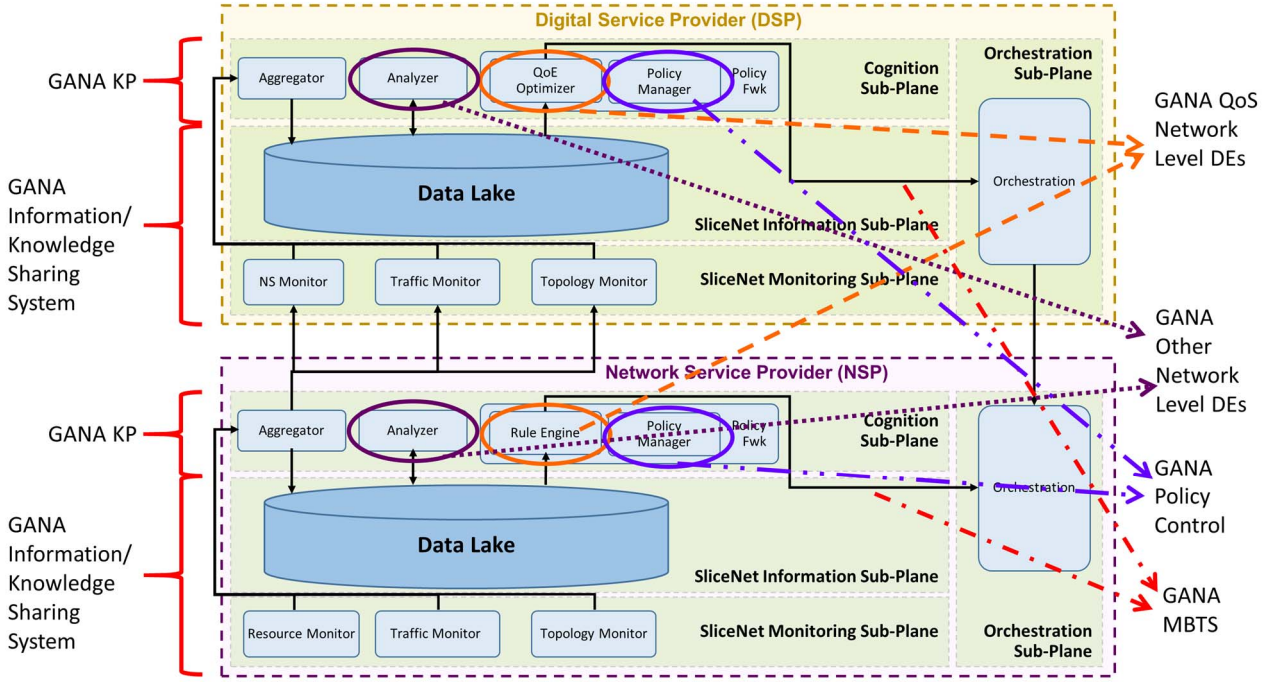

Figure 37: Mapping between SliceNet Cognition Sub-Plane and GANA Knowledge Plane and related elements

Indeed, SliceNet's Cognition Sub-Plane matches the functionalities of GANA's KP, as both implement an entity in which reasoning, learning and adaptation procedures take place in order to govern another entity which focuses on the efficient implementation and automation of configuration and provisioning work-flows. In the case of SliceNet, the derived insights are employed to govern the behaviour of the Orchestration Sub-Plane at both levels (DSP and NSP), which is the responsible to coordinate the operation of the underlying network system.

Both SliceNet's Cognition Sub-Plane and GANA's KP need to be nurtured by copious amounts of data in order to execute the functionalities related to learning and reasoning. In this regard, SliceNet's Data Lake is employed to enable the sharing of information across multiple modules of the Cognition Sub-Plane and across layers/roles. The Data Lake instances centralize the monitoring information coming from the Monitoring Sub-Plane, which keeps track of relevant Key Performance Indicators (KPIs), metrics and alerts related to the health and performance of deployed network slices. Such approach perfectly matches the Information/Knowledge Sharing System defined in GANA, as the main purpose of this framework also relates to the sharing of data between layers and components of the KP.

The key components of GANA's KP are the network Decision Entities (DEs), which are elements that given the inputs disseminated from the automated management layer (i.e. the KP), autonomously take decisions for self-configuration, self-healing, self-diagnosis, etc. of the network layer. In this regard, SliceNet also has defined decision elements inside the architecture of its Cognition Sub-Plane, the QoE Optimizer and the Rule Engine, which are distributed between the multiple roles of the SliceNet architecture. In GANA's nomenclature, both QoE Optimizer and Rule Engine implement network level QoS DEs, dedicated to functions to govern operations for QoS management and control of the network. Both modules receive information from the information sharing system (the Data Lake in SliceNet) and according to them, contact the governed system (the Orchestration Sub-Plane in SliceNet) to enforce operations to maintain optimal QoS levels. More specifically, the Rule Engine is focused on fault, performance and optimization enforcement at the NSP level to while the QoE Optimizer purpose is the maintenance of end-to-end Quality of Experience (QoE) levels for the deployed network slice for which it is responsible for.

Both entities are governed through policies distributed from a Policy Administrator. These policies indicate under what circumstances (an event and its value), what action should be enforced towards the governed system in order to maintain overall optimal quality levels. In this regard, SliceNet's Policy Administrator implements GANA's policy control, which is a system based on policies that establishes the rules under which the multiple network level DEs should behave when interacting with the governed system. Thus, both SliceNet and GANA follow a policy-based approach that, rather than an imperative approach, follows a more declarative methodology, in which the policies and the DEs specify the "when" and "what" of the actions of the governance system (Cognition Sub-Plane/KP), while the "how" is left to the discretion of the governed system.

To enable the interaction between these DEs and the governed system (i.e. the Orchestation Sub-Plane), SliceNet has defined an interface between the QoE Optimizer/Rule Engine and the orchesrator at their level. This interface allows for them to express what is the required action to be executed and the essential parameters for the action (e.g. an increase of bandwidth and the percentage to be increased), while the exact work-flow and operations to materialize the action is executed by the orchestrator. This type of interface implements the Model-Based Translation Service (MBTS) of GANA's architecture, as they serve similar purposes. The MBTS in GANA is a service that allows the multiple DEs to interact with the automated management system (i.e. the governed system) without the need to know the low-level network details of the carried operations, since these are treated by the underlying orchestration and control planes. As such, both SliceNet and GANA follow an agnostic approach for the communication of the DEs and the governed system, simplifying the exchange of operations between the two groups of entities.

Aside from these QoS Network Level DEs, SliceNet also defines other entities that may act as network level DEs. This is the case of the ML models executed within the Analyser at the Cognition Sub-Plane. These modules act as advanced monitoring and sensing functions of the underlying network system and deployed slices, extracting data from the shared Data Lake and inserting back elaborated events that provide insights about their status. These elaborated events may then be used to trigger the QoS Network Level DEs i.e. the QoE Optimizer and the Rule Engine. While ML models do not execute any kind of decision in regards of configuration of the network of slices, they produce valuable information which can influence on the behaviour of QoE/QoS-related configuration operations. In this regard, the multiple ML models defined in SliceNet can be understood as Other Network Level DEs in GANA's nomenclature, since they do not fall into a classic network level category (such as QoE or routing), but contribute towards the general decision making of the Cognition Sub-Plane/KP.

To summarize, the difference between the SliceNet and GANA approaches, aside from the separation/aggregation of some functionalities, resides in the specialization of SliceNet's Cognition Sub-Plane, which focuses on the management of network slices rather than general network management. Nevertheless, the two approaches are perfectly compatible, highlighting the alignment of SliceNet with 5G architecture standards.

8.4 How to implement a GANA Knowledge Plane (KP) for a specific network segment using the SliceNet Intelligence Framework

As stated earlier (mapping clause) Cognitive, Plug and Play (vertical exposure) and Policy artifacts at the level of DSP domain, deliver an equivalent of the GANA KP that is deployed per instantiated multidomain slice. The approach to implement such a KP equivalent in SliceNet Framework is the following:

- Technology specific components per domain (network resources, frameworks, and controllers) are abstracted by means of FCAPS descriptors in the context of monitoring and by Control Plane adaptors in the context of actuations. FCAPS descriptors are onboarded to the relevant FCAPS manager whereas adaptors are activated and registered dynamically with the Control Plane Registry (CPSR).

- Both sensing and actuation capabilities are selected and correlated with the slice templates (NST and NSST) onboarded resources in the orchestrator to provide a set of augmented descriptors.
- Augment NST/NSSTs are dynamically advertised to DSP orchestrator from NSP orchestrators
- At the DSP level, the augmented slice templates provide the available monitoring and actuation options from all the NSPs. This allows DSP orchestrator to resolve the NSTs among the underlying NSPs based on the interest on the available offerings.
- The offerings are listed for DSP developers who design Cognitive, Plug and Play (vertical exposure) and Policy components and register these with the relevant dependencies on NSP offerings (as discovered through slice templates).
- Cognitive, Plug and Play (vertical exposure) and Policy components implement the KP processing agnostic to underlying technologies and focused on High Level Management of the infrastructure towards specific service delivery goals.
- Cognitive, Plug and Play (vertical exposure) and Policy components are catalogued once registered to be subject to inclusion in slice features.
- Slice features are thereafter subject to selection by Vertical as high-level management options.
- Selected features indicated which Cognitive, Plug and Play (vertical exposure) and Policy components to be activated at the DSP level. Their dependencies drive selection of underlying NSTs and NSSTs (among NSPs) and NSP slice(s) provisioning drives the instantiation of FCAPS and Control Plane artifacts according to previously annotation.
- Provisioned monitoring artifacts ensure the flow of relevant information from NSPs DataLakes (through TAL/Rule Engine) to DSP DataLakes where it is consumed (separated and isolated per slice) by the Cognitive, Plug and Play (vertical exposure) and Policy artifacts. Actuation decisions follow the opposite route and are propagated through orchestrator to CP elements for enforcement.

9 Addressing the AMC Requirements in the NGMN® 5G E2E Architecture

The content of this clause follows from a study of the NGMN® 5G E2E Architecture White Paper [i.19] to extract the AMC Requirements and analyse and comment on how the implementations oriented aspects presented in clause 7 and clause 8 can guide the implementer in addressing the AMC Requirements.

The NGMN® also defines as one of the key requirements for 5G systems the concept of Autonomic Networking (AuN). Given the complexity of 5G systems, in which multiple network technologies and service requirements coexist, it is essential to push the concept of AuN from an E2E perspective for automating the configuration, management, operation and self-awareness of 5G systems. For this, in NGMN®, [i.19], NGMN® introduces the need for Autonomic Management and Control (AMC) in the overall E2E 5G network architecture. It proposes a framework in which an underlying network infrastructure layer is governed by another entity that provides insights about the overall system and then enforces actions to the infrastructure layer. In this regard, NGMN® divides the said entity into two different roles (Figure 38 below (right)). First, an Automated Management layer, in which reasoning, learning and adaption procedures take place. Then, the created insights are distributed to an AMC layer, which focuses on the efficient implementation and automation of configuration and monitoring workflows.

The key elements of the AMC layer are the GANA Knowledge Plane (KP) Decision Elements (DEs), which, given the inputs disseminated from the Automated Management layer (e.g. policies), autonomously take decisions for self-configuration, self-healing, self-diagnosis, etc. of the network layer. Lastly, a common Knowledge Base (KB) is present for the sharing of data between the layers. SliceNet's Cognition Sub-Plane combines both layers capabilities, in which insights are gained through specialized analytical functions, overall behaviours are defined thanks to policies and (re-)configurations that are determined through the capabilities of a dedicated DE, namely the QoE Optimizer. The difference between the two approaches, aside from the separation/aggregation of roles, resides in the specialization of SliceNet's Cognition Sub-Plane, which focuses on the management of NSes rather than general network management. Nevertheless, the two approaches are perfectly compatible, highlighting the alignment of SliceNet with 5G architecture standards.

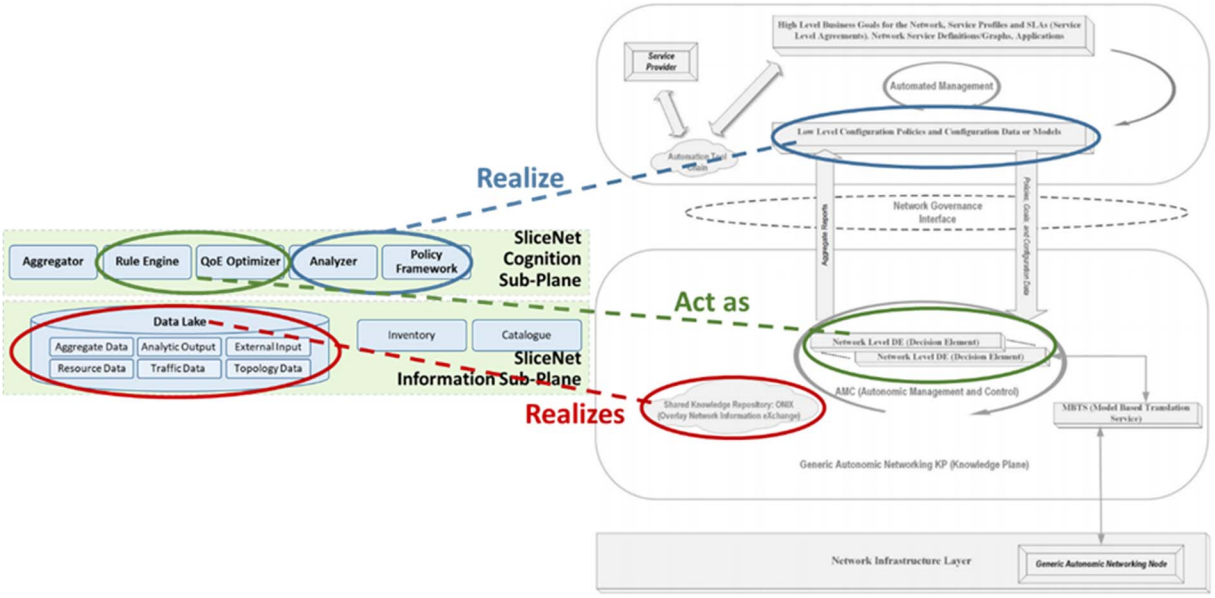

Figure 38: Mapping between SliceNet's Cognition Sub-Plane and NGMN® AMC framework

ML provides an algorithmic approach for AMC to learn, adapt, and improve continuously based on feedback control loop. ML is a pivotal technology within AMC, where the E2E system behaviour is adjusted in response to a perception of the E2E system environment and the processed information, experience, and intelligence within the KP.

The SliceNet's Cognitive sub-plane also uses AI/ML techniques to drive the operational aspects for services, network slices and the underlying network infrastructure resources. The intelligence it provides is distributed among its inner modules. In this plane, data training is performed in order to achieve a specific model that is later applied. Integration of AI/ML techniques into end-to-end network slice management and orchestration is essential to achieve an autonomous closed-control loop network.

10 Conclusion

The present document has provided useful insights to implementers and solution suppliers for ETSI GANA Knowledge Plane (KP) platforms for AMC of specific 5G network segments such as Radio Access Network (RAN), X-Haul Transport and Core Network. There present document indeed provides a plausible approach to implementing Federated GANA Knowledge Planes (KPs) Platforms for E2E Multi-Domain Federated Autonomic Management and Control (AMC) of 5G Network Slices in NGMN® E2E 5G Architecture, using components prototyped and implemented in the European Union (EU) funded SliceNet Project (Grant Agreement N° 761913). As described in the present document, the insights to implementers should also consider the results from the ETSI 5G PoC White Papers and Demo materials publicly available at https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals.

The insights are based on the following perspectives:

- Requirements for Autonomic Networking and AMC in NGMN® E2E 5G Architecture [i.19]. The ETSI GANA Model and its concept of the GANA Knowledge Plane (KP) as a platform for implementing AMC were adopted by NGMN® deriving specification of Requirements for Autonomic Networking and AMC in the NGMN® 5G E2E Architecture [i.19].

- NGMN® and ETSI TC INT AFI WG Agreement on the fact that Knowledge Plane (KP) Platforms for AMC need to be *disaggregated*, meaning that KP Platforms should designed and implemented for specific network segments as domains (e.g. RAN, X-Haul Transport, Core Network). Both NGMN® and ETSI TC INT AFI WG are in agreement that *E2E Autonomic (Closed-Loop) Service and Security Management & Control in 5G* is to be achievable by way of Federation of the Knowledge Plane-Level Security-Management-DEs across multiple network segments/domains (RAN, X-Haul Transport, Core Network), following the principles for federated AMC outlined in the NGMN® 5G E2E Architecture Framework [i.19]. According to the NGMN® E2E 5G Architecture [i.19], E2E Autonomic (Closed-Loop) service assurance should be achievable through a federation of Knowledge Planes (KPs) that implement components for AMC intelligence for specific network segments (viewed as domains). There are many advantages to implementing disaggregated Knowledge Plane (KP) Platforms. For example, the ICT infrastructure for a specific network segment may be supplied to a CSP (or even to an enterprise's network(s) environment) by a supplier that should not necessarily be the supplier of the autonomics software or (autonomic-) management and control platforms for the network segment (infrastructure). And also, a CSP or an enterprise may desire to have Solutions suppliers for Autonomics software (e.g. GANA DEs), AMC Platforms like KP Platforms or Management and Control Systems for specific ICT network segments to not be the same supplier for all the network segments or the underlying infrastructures-for various reasons (e.g. to allow for competitive solutions sourcing). This way, disaggregation avoids the problems of "vendor-lockin" for a CSP or enterprise and it also enables for competition and innovations among solution suppliers. Unlike the approaches being taken in 3GPP on analytics platforms that do not follow disaggregation approaches.

This work and the insights for AMC implementation have been facilitated by the fact that the ETSI GANA Model is a Multi-Layer Artificial Intelligence (AI) Framework for Implementing AI Models for Multi-Layer Autonomic Management & Control (AMC) of Networks and Services. GANA as a Hybrid Model for Multi-Layer Autonomics and associated Multi-Layer AI Algorithms exhibits the following characteristics:

- GANA is a Hybrid Model (ETSI White Paper No.16 and ETSI TS 103 195-2 [i.2]):
  - It guides and offers flexibility to implementers on the choice to implement certain autonomics as distributed software and algorithms within certain Network Elements/Functions (NEs/NFs), i.e. "Micro Autonomics", while being able to also choose to implement some algorithms as centralized algorithms in the KP Platform ("Macro Autonomics").
- Hybrid SON Model is compatible with GANA (more details in White Paper No.1 of 5G PoC [i.4]):
  - Hybrid SON (C-SON (Centralized SON) & DSON (Distributed SON)) are considered as an implementation of the GANA Model for the RAN.

Annex A: Bibliography

- 5G security recommendations: "Package #2: Network Slicing", by NGMN® Alliance: 27-April-2016.
- ODA TM Forum's Open Digital Architecture (ODA): "IG1167 ODA Functional Architecture Vision R18.0.0 (Intelligence Management Function Block)".
- 5G security - Package 3: "Mobile Edge Computing/Low Latency/Consistent User Experience: by NGMN® Alliance", 20 February 2018, by NGMN® 5G security group.
- ODA TM Forum's Open Digital Architecture (ODA): "IG1177 ODA Intelligence Management Implementation Guide: R18.5.0" (IG1177 Release 18.5, December 2018).
- IBM White paper: "An architectural blueprint for autonomic computing", MAPE-K, June 2005.
- Andrew Lerner: "AIOps Platforms", Gartner Blog, August 2017.

NOTE: Available at https://blogs.gartner.com/andrew-lerner/2017/08/09/aiops-platforms/.

- N. Miloslavskaya, A. Tolstoy: "Big Data, Fast Data and Data Lake Concepts", Elsevier Procedia Computer Science, vol. 88, pp. 300-305, October 2016.

History

Document history		
V1.1.1	November 2021	Publication