ETSI AN Whitepaper - Unlocking Digital Transformation with Autonomous Networks

Presented by:

For: TMF AN MSDO online session

24/04/2023

Agenda

- 1. OCG AN Introduction/ Agenda (Nick Sampson / Ton Brand)
- 2. ETSI AN whitepaper: scope, general aspects and recommendations (Luigi Licciardi)
- 3. AN activities in:
  - a. ISG ENI (Ray Forbes)
  - b. ISG ZSM (Nurit Sprecher)
  - c. TC INT/AFI (Ranganai Chaparadza, Benoit Radier)
  - d. ISG MEC (Dario Sabella)
  - e. ISG F5G (Yi Lin)
- 4. Q&A

© ETSI 2023. All rights reserved.

ETSI AN whitepaper: scope, general aspects and recommendations

Overview from Autonomous Networks perspective

Presented by: Luigi Licciardi

Unlocking Digital Transformation with Autonomous Networks

ETSI perspectives and major achievements

ETSI White paper No. 56

Authors

Aldo Artigiani (Huawei), Christian Berghoff (Federal Office for Information Security), Tayeb Ben Meriem (IPv6Forum), Ranganai Chaparadza (IPv6 Forum), Bruno Chatras (Orange), Ray Forbes (Huawei), Muslim Elkotob (Vodafone), Antonio Gamelas (Altice/PT), Taras Holoyad (Federal Network Agency), Luigi Licciardi (Huawei), Yi Lin (Huawei), Diego Lopez (Telefonica), Faraz Naim (Accenture), Yoshiro Nakajama (NTT DoCoMo), Marie-Paul Odini (HPE), Luca Pesando (TIM), Benoit Radier (Orange), Dario Sabella (Intel), Nick Sampson (Orange), Nurit Sprecher (Nokia)

Editors : Anthony Brand (ETSI), Luigi Licciardi (Huawei)

1. Executive Summary
2. Autonomous Network
   - 2.1. A view of Autonomous Networks
   - 2.2. Autonomous Networks framework and principles
   - 2.3. Common enablers
3. ETSI activities on Autonomous Networks
   - 3.1. ISG ENI
   - 3.2. ISG ZSM
   - 3.3. ISG NFV
   - 3.4. TC MTS
   - 3.5. TC INT WG AFI
   - 3.6. ISG IPE
   - 3.7. ISG MEC
   - 3.8 ISG F5G
   - 3.9.ISG SAI
   - 3.10. Further key topics to address
4. Mapping of ETSI activities related to AN
5. ICT ecosystem initiatives on AN
6. Recommendations
7. Summary
8. References

Scope: To present the key role of AN focusing on ETSI major achievements, deliverables and recommendations across the several ISGs and TCs relating to AN.
It reports the activity mapping and progress organized by arguments.
It is addressed to a large audience, including managers and vertical partners. *

* Deep technical details and deliverables can be found in the Reference chapter.

© ETSI 2023. All rights reserved.

A view of Autonomous Networks

An **Autonomous Network** is a network that self operates according to the business goals with no human intervention beyond the initial supply of input (e.g., intent, goals, policies, certain configuration data) by human operator. It is capable of self-management operations (e.g., self-configuration, self-diagnosis, self-repair, self-healing, self-optimization, self-protection) of its resources, functions/applications and services. Its self-management operations are enabled by capability to auto- discover operational information and act on it.

Autonomous Networks AAA properties:

- **Automatic** – the ability to self-control the internal resources and operations, as well as to bootstrap and operate without manual intervention.
- **Aware** – the ability to monitor its operational context, performance and internal states to assess if its current operation serves defined and agreed goals.
- **Adaptive** – the ability to change its operations to cope with temporal and spatial changes in operational context on short and long terms. In other words, the ability to adapt its behavior by changing its decisions in order to maintain agreed operational delivery values.

The degree of autonomy of Autonomous Networks varies from low levels of automation capabilities (L0 to L3) to fully matured autonomous capabilities (L4- L5).

© ETSI 2023. All rights reserved.

Mapping of ETSI activities related to AN

	AN topics / ETSI Groups	TC INT AFI WG	ISG ENI	ISG ZSM	ISG F5G	ISG MEC	ISG NFV	ISG IPE	ISG SAI	TC MTS
1	Terms & definitions	●	◕	○			○		○	
2	Use cases & requirements	●	◕	●	◕	○	●	●		
3	Architecture / framework	●	◕	●	◕	◔	◔		◑	●
4	Levels of autonomy/autono-micity	●	●	○	◔					
5	Cognition	●	◕	◔			◔			
6	Self-X properties	◕	◔	◔			◔			
7	Governance interface	●	◕	◔	◔		○			
8	Intent-driven management [2]	◕	◔	◔	◔		◔			
9	Policy Control Management Framework(s)	●	◕	○			●			
10	AN services, functions and resources Life-cycle management	◑	○		○	◔	◑			
11	Closed control loop automation	●	◕	◑			◔			
12	Analytics and intelligence (including AI topics)	◕	◕	◔	○		◔		◔	
13	Knowledge representation (e.g. information models & Ontologies) & management	◑	◔	○			○			
14	ANs federation and Inter-AN coordination	◕		◑	◔	◔	○		◔	
15	APIs and data models	◑	◑	◔	◔		○			
16	Robustness, trustworthiness, traceability	◑		◔			○		◑	
17	Security/privacy	◑	○	◕	○	○	○		●	●
18	Testing framework and methodology	◑	○	○			○		◑	●
19	Metrics and KPIs	◕	◕		○		○			◑
20	PoCs	●	◕	◔	○		○		◔	

The table legend (an empty table entry shows the AN aspect is not considered by the ISG/TC):

- ○ Under consideration
- ◔ Started
- ◑ Stable
- ◕ Under revision / enhancement
- ● Published / completed

© ETSI 2023. All rights reserved.

Autonomous Networks Enablers and External Interfaces

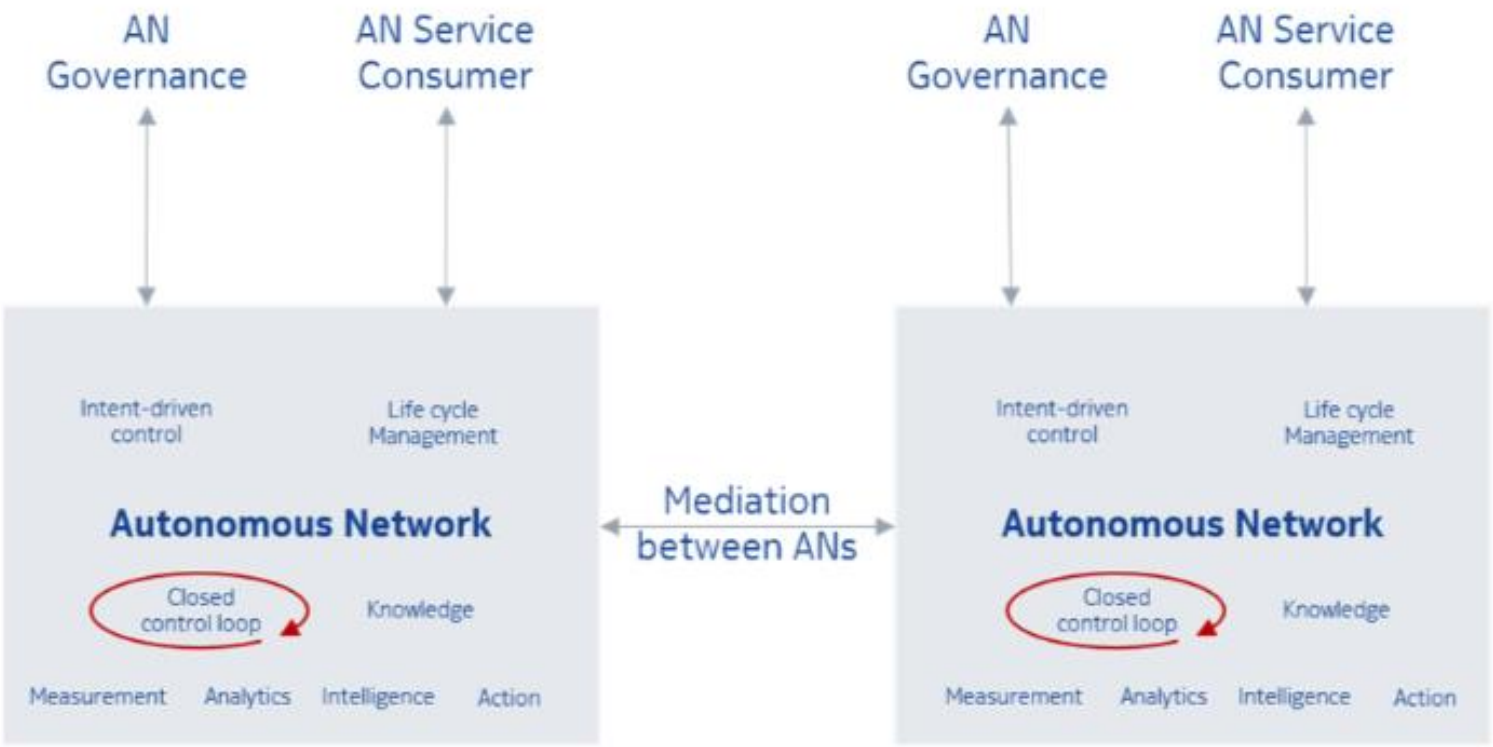


Figure 1: An example of a high-level illustration of Autonomous Networks' enablers and external interfaces

- Autonomous network governance interface
- Intent-based network control
- Closed control loop
- Analytics and intelligence
- Knowledge
- Inter-AN mediations

- Automation and autonomic behavior to enable the **Self-X Concept**: self-configuration, self-healing, self optimization, self-awareness, self-knowledge.
- **Cognitive Systems** to augment human decision-making and action processes, based on Context-awareness. Statistics, analytics, predictions, recommendations and commands are sent to manage entities.

© ETSI 2023. All rights reserved.

Ecosystem Initiatives on Autonomous Networks

- Significant effort and relevant initiatives are active across the industry ecosystem on Autonomous Networks and Network Automation.

- Industry cooperation and coordination are essential for harmonization, widespread interoperability and consistent behaviors across a multi vendor ecosystem.
- AN multi SDO Table successfully organized online workshops to share results and present ideas, architectures, solutions.

© ETSI 2023. All rights reserved.

Autonomous Networks Security (Faraz Naim)

Building a consistent level of security policies, procedures and Minimum Baseline Security Standard (MBSS) for all network elements is extremely important to minimize risks.

There is a need for *centralized Identity governance* for Resource management and user access.

Lack of centralized security configuration and weak access management procedures may cause network exploitation of applications and systems, which can lead to unauthorized access of user data, log files and manipulation of AI/ML models.

A **Unified Framework** is required to prevent attacks on the AI/ML model:

- A *centralized Assurance* procedure must be used to evaluate and assess the AI/ML model before moving it to production
- Usage of methods to clean the training dataset from suspicious samples
  (AN require Next Generation Security monitoring with the help of Native Security Agent for Real-Time Security Monitoring and intelligent SIEM (Security Incident and Event Management) with UEBA (User and Entity Behaviour Analytics) and SOAR (Security Orchestration, Automation, and Response) capabilities).

Point of Attention: Increasing entry points increases the number of attack surfaces in applications and systems.

Further challenges in AN standardization related to security are *Infrastructure security and protection from physical to virtual and application levels, Data protection and User security which includes data encryption.*

Security is considered in all the ISGs & TCs and specific recommendations are developed in ISG SAI that is focused on Security in AI.

© ETSI 2023. All rights reserved.

ISG Securing Artificial Intelligence (ISG SAI)

SAI focuses the potential of AI in terms of enhancing as well as decreasing security risks for AI-based systems.

While the group is addressing issues related to AI and cybersecurity, the focus of existing work is on the following key areas:

- Protecting AI-based systems from cyber-attacks
- Use of AI to create novel attacks
- Use of AI to improve conventional security measures

The work of the group is not specific to certain applications, it treats these aspects in the full life cycle of the AI system: starting from the planning of the system, the acquisition and management of data, training, validation and testing procedures; it considers operation, maintenance and eventually dismission.

ISG SAI has studied the various novel attacks that can be used to target AI models and potential countermeasures.

Some examples:

- poisoning and backdoor attacks for manipulating the data used for training an AI model; countermeasures for prevention and detection include using data from trusted sources, protecting the supply chain and sanitising data.
- adversarial attacks that target the model in operation by using specially crafted inputs to mislead the model; They can be mitigated by expanding the training process (adversarial training), introducing additional modules for detecting attacks and sanitising input data.
- attacks that jeopardise the confidentiality and privacy of the data used to train the model or the model's parameters. They can be dealt using differential privacy and homomorphic encryption; introducing restrictions on the number and type of queries to the model and tailoring the output to queries can also hamper such attacks.

© ETSI 2023. All rights reserved.

Recommendations, Perspectives and Evolutions

Autonomous Networks reached momentum in terms of business interest and standardization results.

Several hundreds of experts, SDOs, Fora and Alliances are deeply involved => the risk of fragmentation is high

IT IS MANDATORY to find coordination inside ETSI ISGs/TCs and to extend knowledge exchange and collaboration among the leading SDOs, Fora and Alliances, being proactive to facilitate recommendations and standard convergence in the whole ecosystem and industry.

Autonomous Networks is one of the most interesting area of use and deployment of Artificial Intelligence and Machine Learning.

Significant perspectives and evolutions on AN are:

- Network Digital Twin (NDT)
- Impact of NDT on AN evolution
- NDT for business Assurance and decision making
- Role of AN in 6G
- AN API marketplace

These subjects open new areas of studies, recommendations, standards and software development attracting resources and contributions from all the ecosystems, including Open Source Communities, Universities and developers.

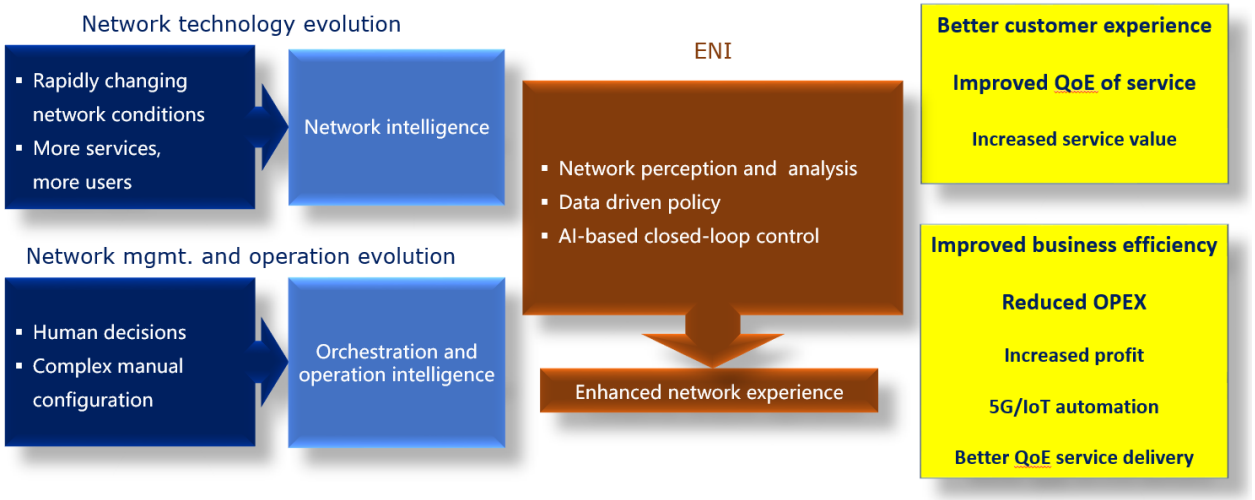
© ETSI 2023. All rights reserved.

ENI (Experiential Networked Intelligence)

Overview from Autonomous Networks perspective

Presented by: Raymond Forbes (ISG ENI Chair)

ENI Vision



ETSI ENI White Papers,
http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp22_ENI_FINAL.pdf
http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp44_ENI_FINAL.pdf

ENI Leadership Team

Role	Name (Organization)
Chair	**Dr. Raymond Forbes** (Huawei)
Vice Chair	**Ms. Haining Wang** (Intel)
Second Vice Chair	**Miss Ziting Zhang** (China Telecommunications)
Technical Architect	**Dr John Strassner** (Futurewei)
Support Officer	**Mrs. Christine Mera** (ETSI)
ENI ISG PoC Review Team	**Raymond Forbes** (Huawei) **Christine Mera** (ETSI Support Officer) **Ultan Mulligan** (ETSI CTI Director) **Bill Wright** (Redhat) **Haining Wang** (Intel) **Yu Zeng** (China Telecom) **Antonio Gamelas** (Portugal Telecom)

The work-program is accessible via Work Item Monitoring - ENI

ENI Scope

- **ETSI ISG ENI in Release 1 (2017–2019):**
  - The ISG ENI has focused on improving the operator experience, adding closed-loop artificial intelligence mechanisms based on context-aware, metadata-driven policies. Enabling quick recognition and incorporation of new and changed knowledge, and hence, make actionable decisions.
  - In particular, ENI has specified a set of use cases, and the functional architecture, for a network supervisory assistant system based on the 'observe-orient-decide-act' control loop model.
  - This model can assist decision-making systems, such as network control and Interact with the domain orchestration systems, to adjust services and resources offered based on changes in user needs, environmental conditions and business goals.
- **Release 1 defined big data-analysis functionality**

- **ETSI ISG ENI in Release 2 (2019–3Q2021):**
  - Definition of AI Categories into levels 0-5 regarding autonomicity.
  - Evaluation criteria for Categorization and methods of measuring.
  - Use of the API broker for non-capable signaling systems.
  - Specification of external reference points, implementation, PoCs, data mechanisms
  - Definition of closed control loops in the real-time network.
- **Core concepts: Network perception analysis, data-driven policy, AI based closed-loop control**

- **ENI Release 3 3Q2021 - 1Q2023:**
  - Revision of the Use Cases & Requirements + Evaluation & Measurement of Categorization + Data Management
    - Priority Use Cases demonstrated in PoCs.
    - Measurement Criteria.
    - Data Handling related with format and flow between FBs.
    - Transformer architecture (now Release 4).
  - Further deployment and specification of the system architecture
    - Interface definitions and information models.
    - Data models and APIs.
    - Handling of Policy Management Model.
    - Handling of Intent-based concept.

Members signed the ENI Member agreement and are ETSI members and Participants signed the ENI Participant agreement but are not ETSI members
https://portal.etsi.org/TBSiteMap/ENI/ListOfENIMembers.aspx

Main concepts: Use Cases

Infrastructure Management
Policy-driven IDC traffic steering
Handling of peak planned occurrences
Energy optimization using AI
Intelligent Optimization for Transmission Network
Energy saving in radio network

Network Operations
Policy-driven IP managed networks
Radio coverage and capacity optimization
Intelligent software rollouts
Intelligent fronthaul management and orchestration
Elastic Resource Management and Orchestration
Application Characteristic based Network Operation
AI enabled network traffic classification
Automatic service and resource design framework for cloud service
Intelligent time synchronization of network
Intelligent Content-Aware Real-Time Gaming Network

Service Orchestration and Management
Context aware VoLTE service experience optimization
Intelligent network slicing management
Intelligent carrier-managed SD-WAN
Intelligent caching based on prediction of content popularity
Service experience optimization of E2E slicing involving both OSS and BSS
Intent-based Cloud Management for VDI service
Intelligent vehicle diversified service fulfillment based on polymorphic network
AI based family broadband network user experience optimization

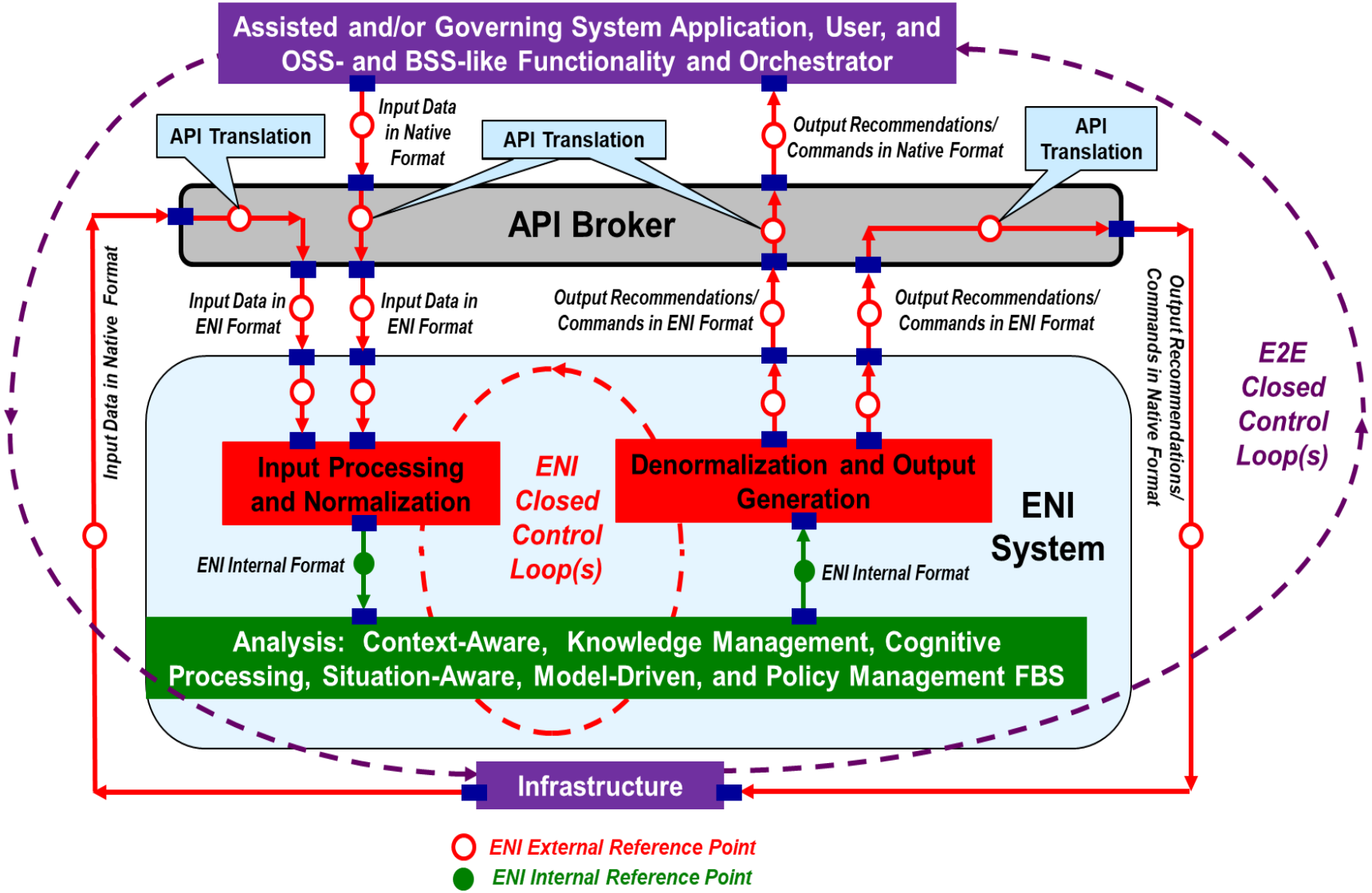
Network Assurance
Network fault identification and prediction
Assurance of Service Requirements
Network Fault Root-cause Analysis and Intelligent Recovery

Network Security
Policy-based network slicing for IoT security
Limiting profit in cyber-attacks

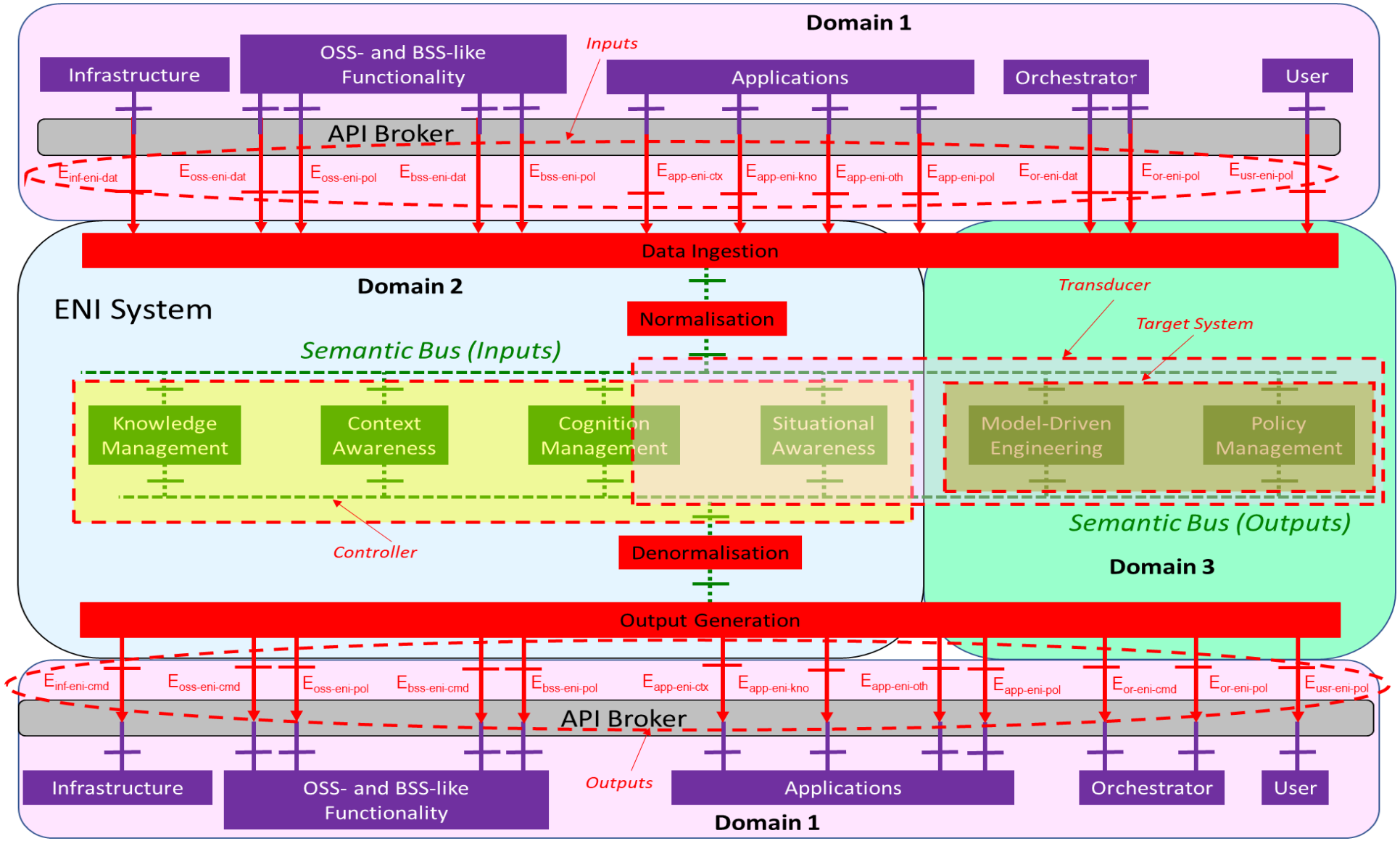
© ETSI 2020

Source: ETSI GS ENI 001 v3.2.1; ENI Use Cases updates in publication

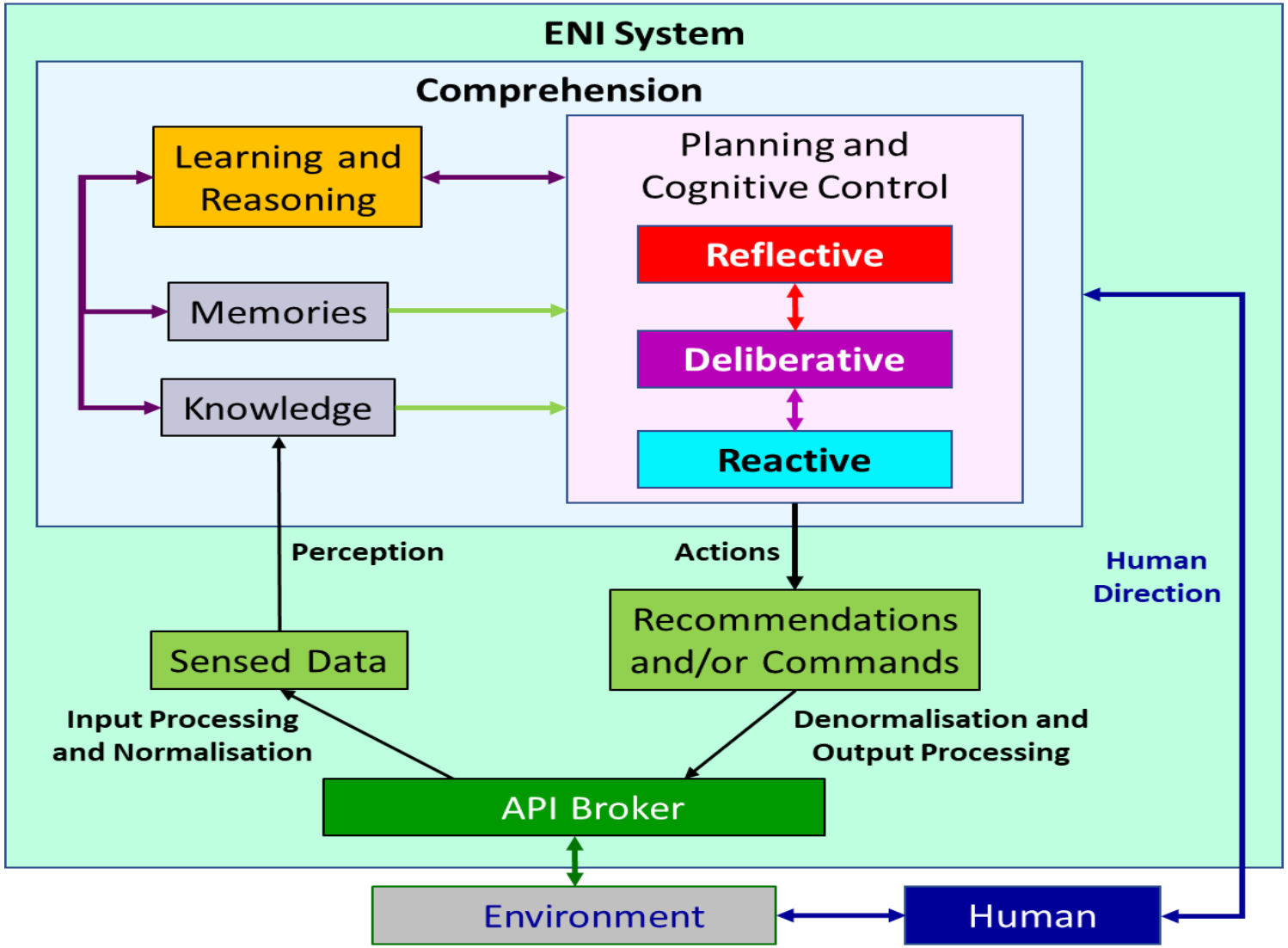
ENI System Architecture Overview



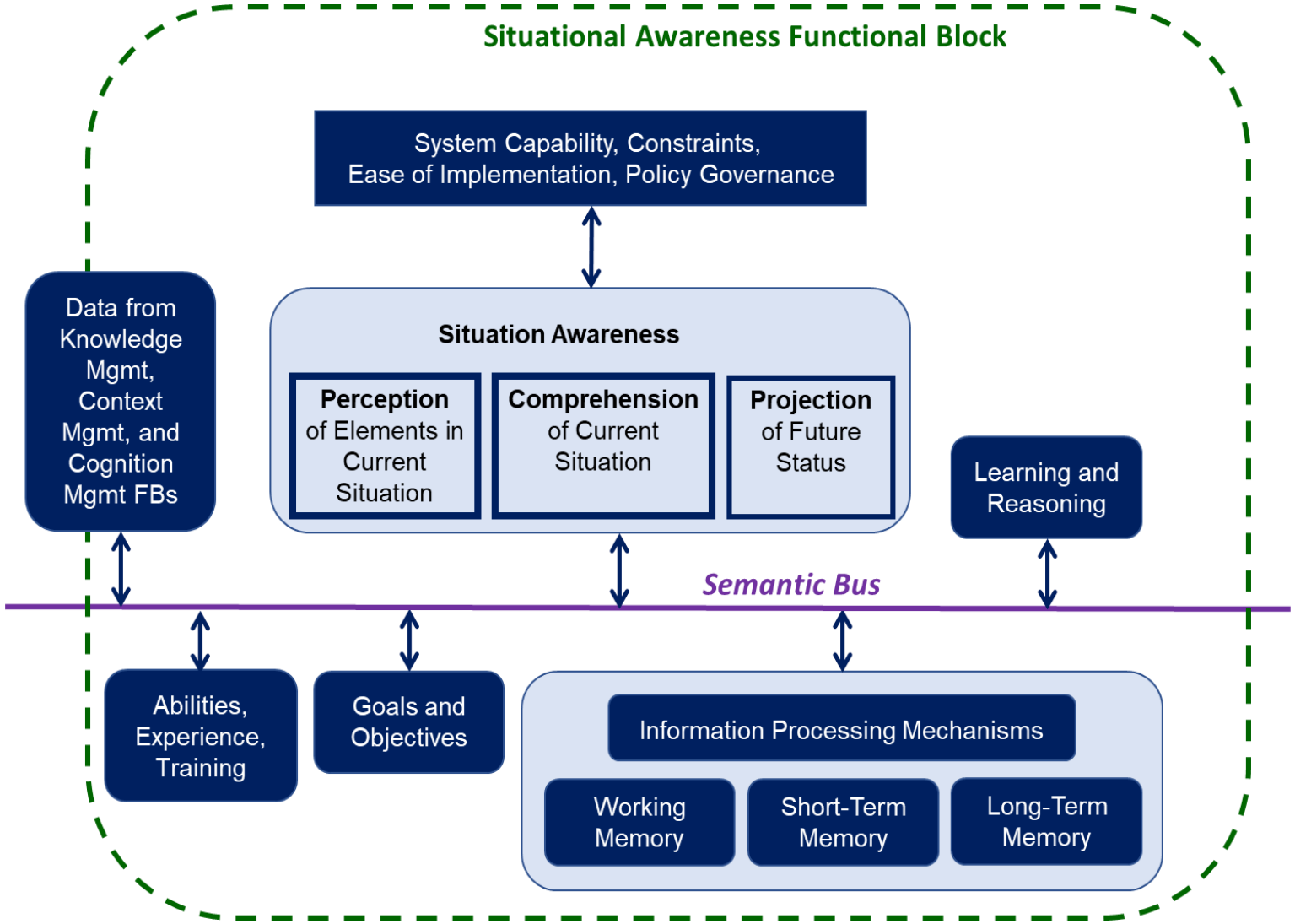
ENI Domains and Control Loops



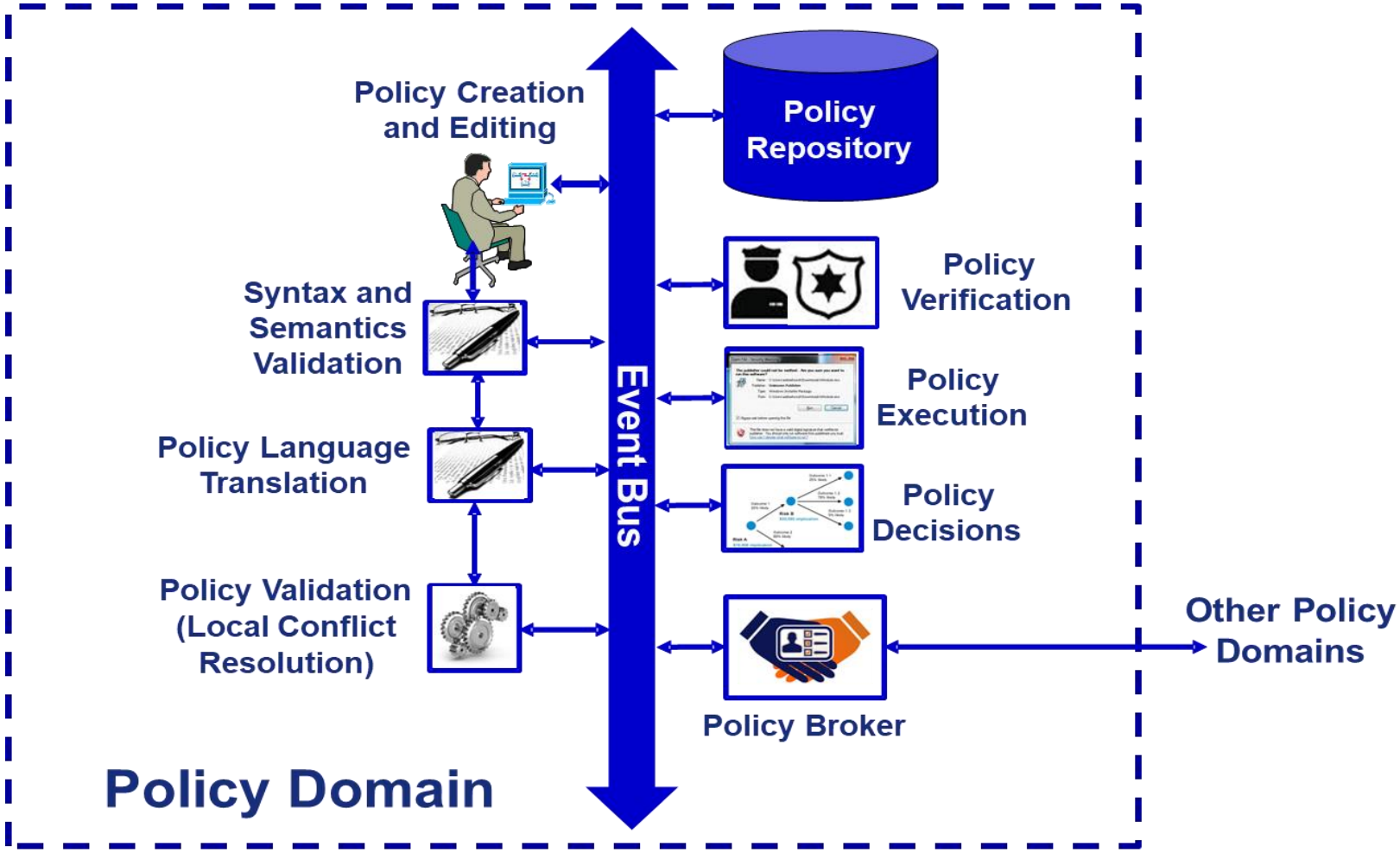
Cognition in ENI



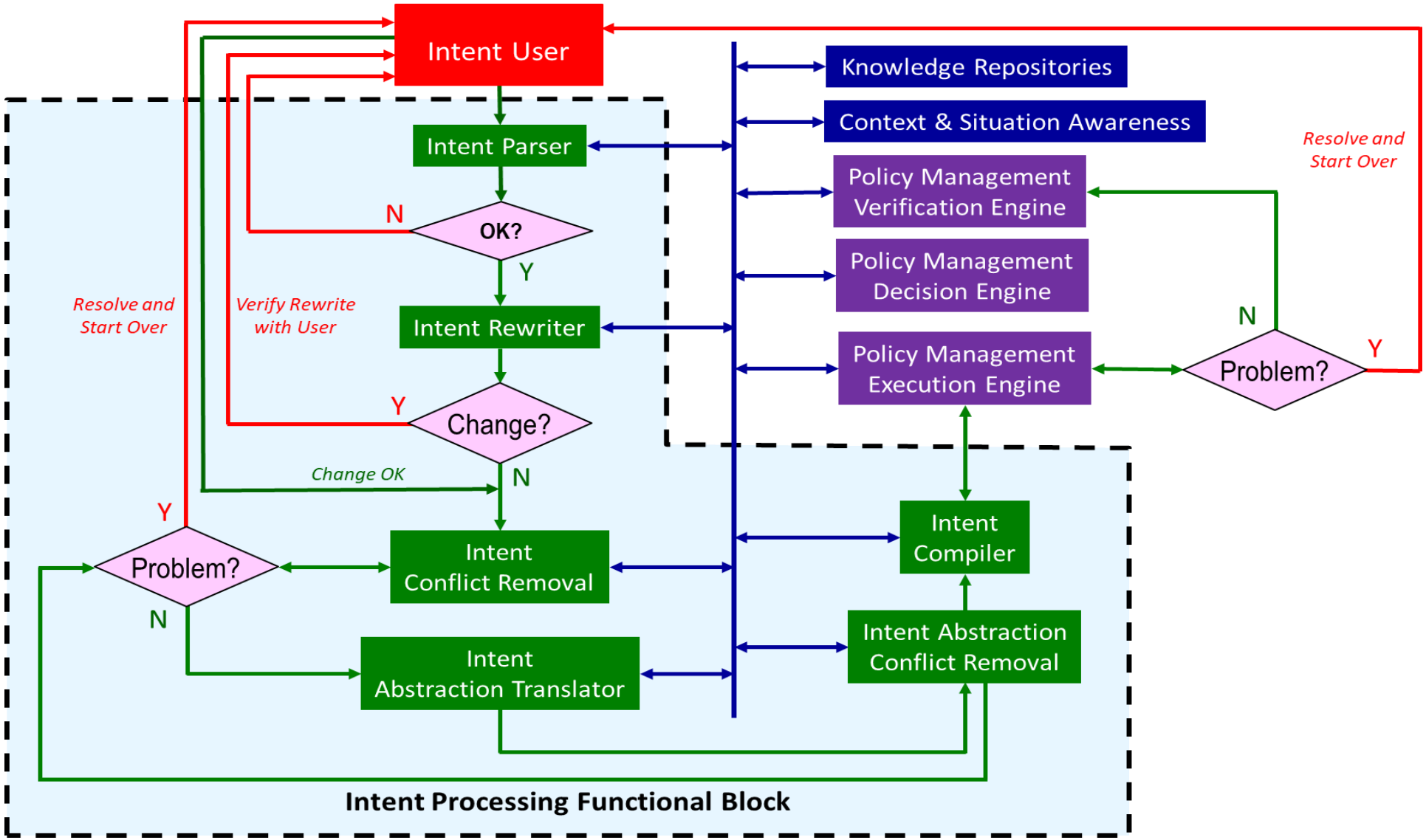
Cognitive Processing in ENI



High Level Policy Architecture



ENI Intent Policy Control



ZSM (Zero Touch Management)

Overview from Autonomous Networks perspective

The ZSM mission

- Define a future-proof, **end-to-end operable framework and solutions**, as well as **key automation technologies** to enable zero-touch automation emerging and future networks and services.
- The ultimate target is to **enable autonomous operations** (self-configuration, self-monitoring, self-healing, self-optimization, self-protection) **empowered with advanced cognitive capabilities** and driven by high-level business policies.
- The ultimate target is to achieve the highest degree of automation (~100%) and **enable fully autonomous network operation**
- Realizing this vision requires to:
  - develop a novel end-to-end architecture framework and enablers designed for self-management, closed-loop automation and optimized for data-driven artificial intelligence solutions
  - demonstrate the viability of the technology
  - facilitate collaboration in the industry to ensure alignment and leverage synergies

© ETSI 2023. All rights reserved.

Industry landscape for network and service automation

Complementary efforts to enable end-to-end automation

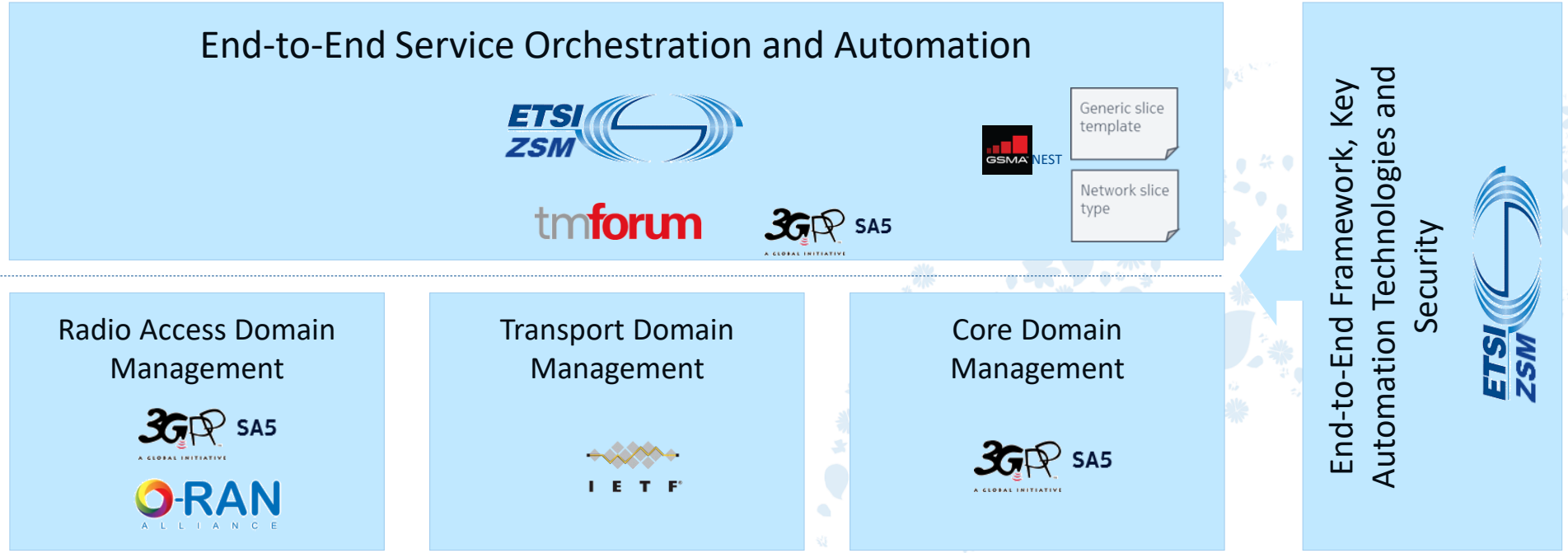
End-to-end service management domain

- Orchestration, SLA enforcement and assurance (incl. closed loop) of E2E services/slices
- Decomposes high-level parameters
- Allocates SLA budget to domains
- Has an abstracted view of the domains' services/sub-slices

Management domains

- Resource orchestration, SLA enforcement and assurance (incl. closed loop) of domain-wide services
- Interprets and translate high-level parameters into domain-level resources
- Decides #V/C-NFs and their placement

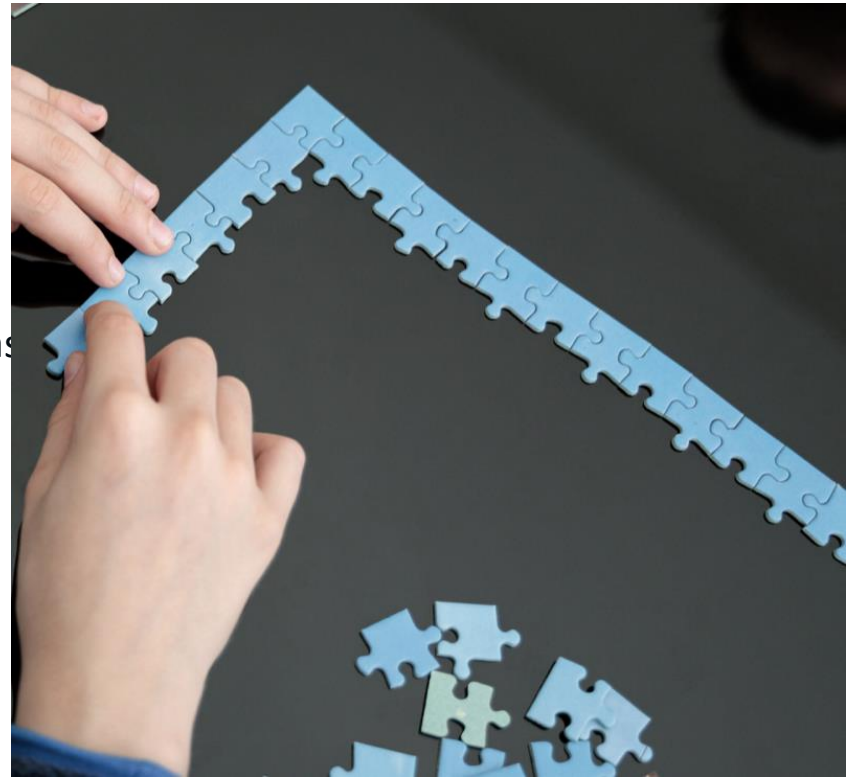
Domain-managed resources



© ETSI 2023. All rights reserved.

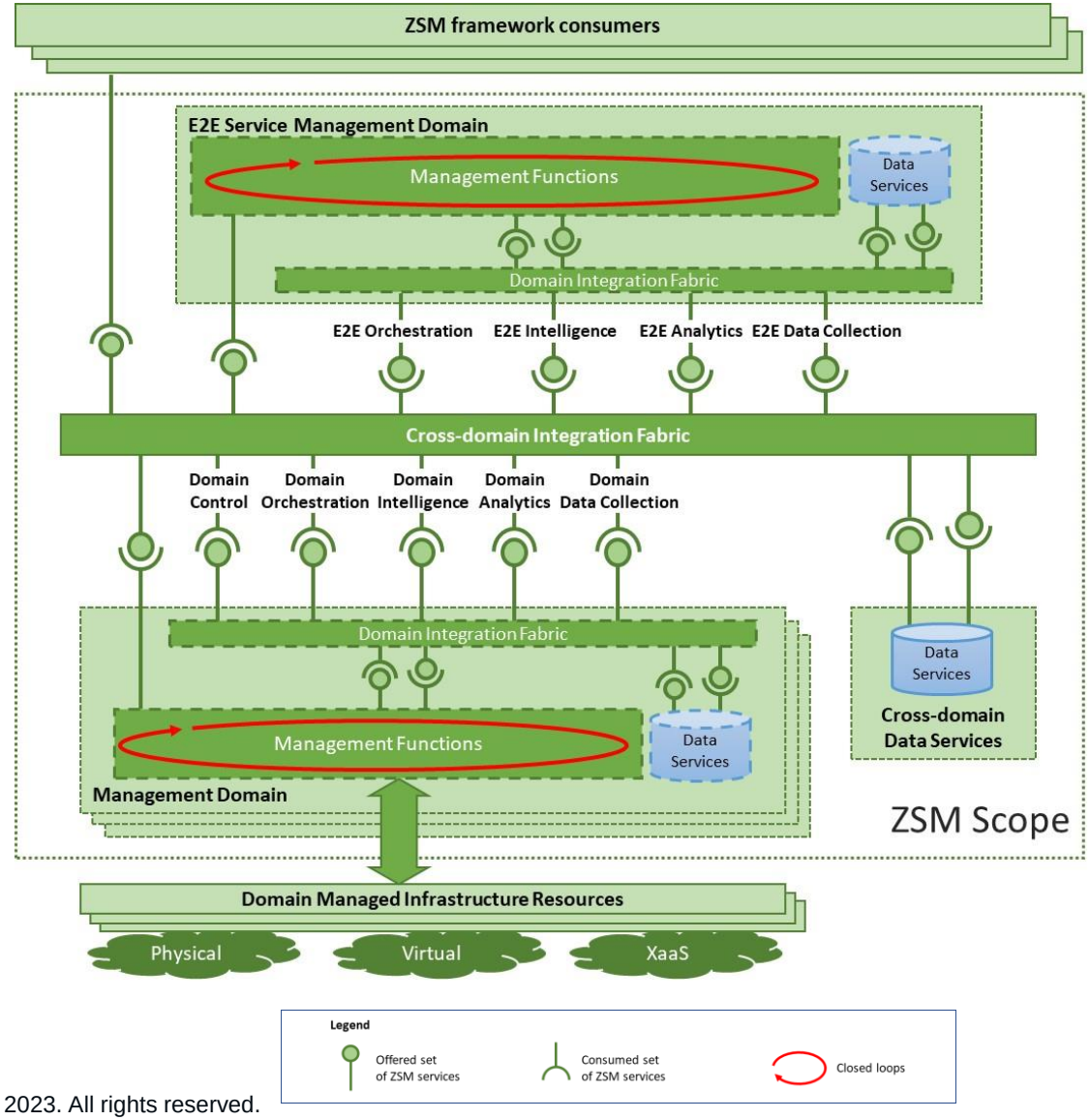
Building the Frame: Architectural Principles

- Modular, flexible, scalable and extensible service-based architecture
- Separation of concerns: network domain management and end-to-end cross-domain service management
  - Resources in multiple domains can be managed separately.
  - Complexity can be abstracted.
- Support of open, model-driven, intent-based interfaces
- Enablement of adaptive closed-loop management automation at various levels as the driver of automaton
  - The automated decision-making mechanisms can be bounded by rules and policies.
- Shared data (stored, streamed) as the lifeblood of automation
  - Support of data services and stateless management functions
- Design for resilience
- Functional abstraction



© ETSI 2023. All rights reserved.

ZSM end-to-end architecture framework (ZSM 002)



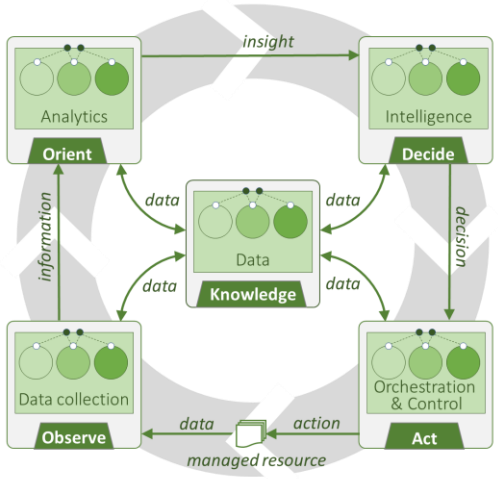
The ZSM framework is designed to enable adaptive, closed-loop automation, allowing:

- Continuous optimization and adaption of network and resource utilization.
- Automated service assurance and fulfilment.

The framework is optimized for data-driven machine learning and artificial intelligence algorithms that can empower the closed-loop operation.

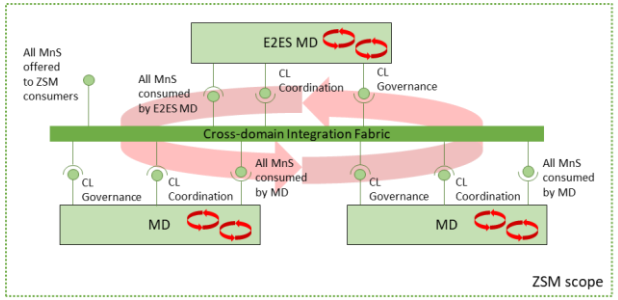
© ETSI 2023. All rights reserved.

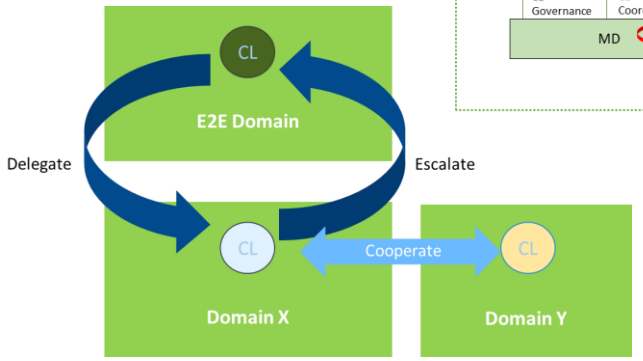
The tools for completing the puzzle
Closed loops (ZSM 009 series)



ZSM enables:

- A **uniform life cycle management** of different closed loops
- Specific Management Services
  - Closed Loop **Governance** services that:
    - Allow the creation, execution and life-cycle management of a closed loop as well as the configuration of related policies and rules to steer the behavior.
    - Support interaction between closed loops and human operators, allowing them to supervise the operation and performance of closed loops.
  - Closed Loop **Coordination** services that:
    - Unified coordination/delegation/escalation between closed loops
- Dynamic management of closed loops
  - Goal change
  - Loop modification



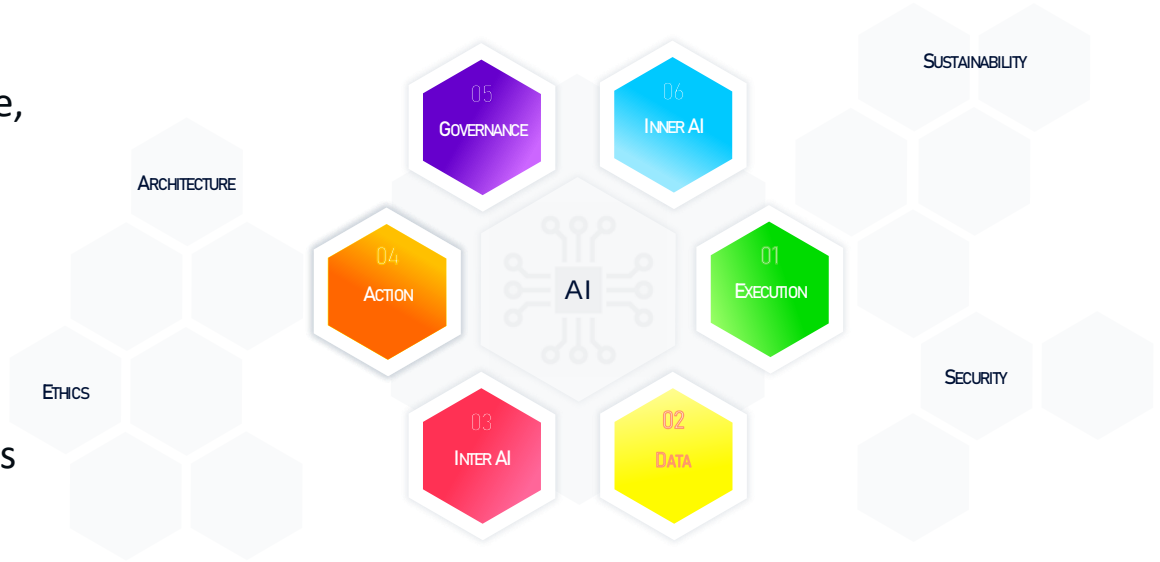


© ETSI 2023. All rights reserved.

The tools for completing the puzzle AI enablers (ZSM 012)

ZSM provides management capabilities to:

- Access to the right data, at the right place and at the right time, while ensuring data integrity and trustworthiness
- Support coordination between multiple, distributed AI applications
- Trigger an action based on the AI output
- Govern and supervise the AI-empowered operations. AI results must be reliable, measurable, interpretable, and accountable.
- Express requirements and constrains for the deployment of AI applications



© ETSI 2023. All rights reserved.

The tools for completing the Puzzle Intent (ZSM 011, ZSM 016)

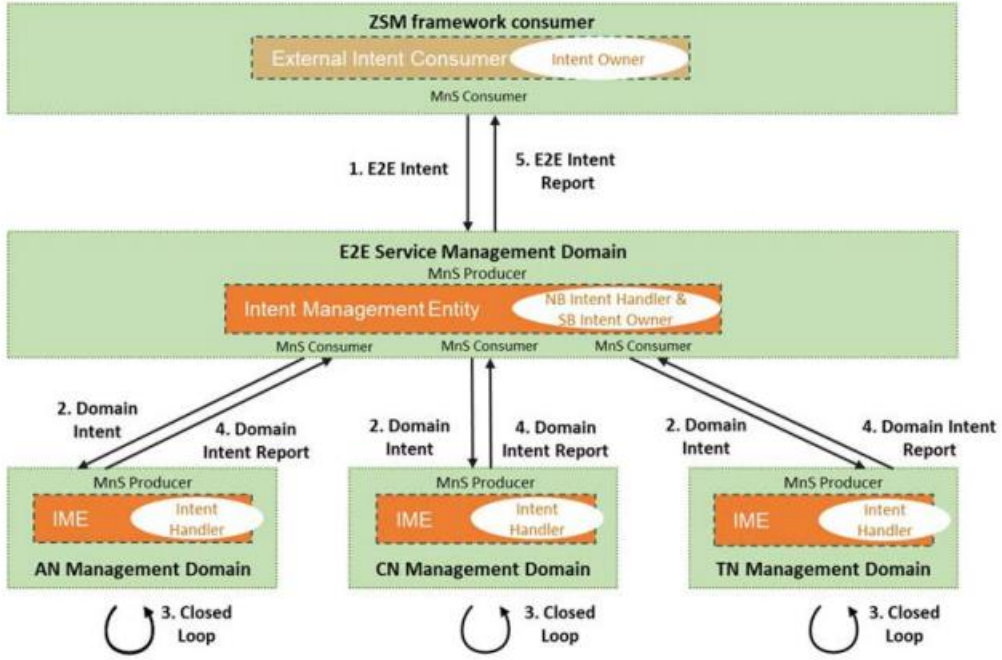
Intents express declaratively all the operational expectations an autonomous management domain needs to fulfill and assure, including requirements, goals, and constraints.

The ZSM intent-driven autonomous networks report focuses on:

- Intent as a key enabler for autonomous networks
- End-to-end aspects
- Conflict handling

ZSM is currently working to specify capabilities to support the combination of closed-loop automation with intents, focusing on:

- Intent governance
- Coordination between closed loops



© ETSI 2023. All rights reserved.

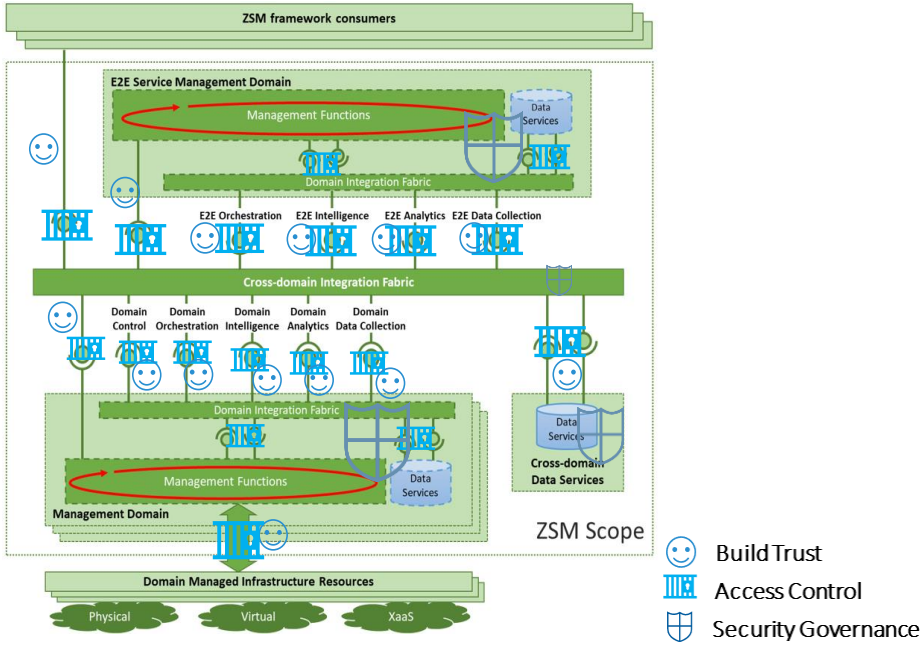
The security dimension (ZSM 010, ZSM 014)

Rationale:

- Threat surface is extensive in the ZSM environment because of the openness of ZSM framework and the nature of emerging technologies (e.g. AI/ML, data lake, cloud native applications)
- Compromising a ZSM system security may adversely impact the business of operator and/or vertical service provider.
- Compliancy with country/region/industry security laws and regulations is an obligation for service providers and their suppliers.

ZSM conducted a comprehensive threat analysis and proposed countermeasures and solutions to high-priority security risks/issues

- Trust, assurance, multi-tenancy and access control, security of AI/ML



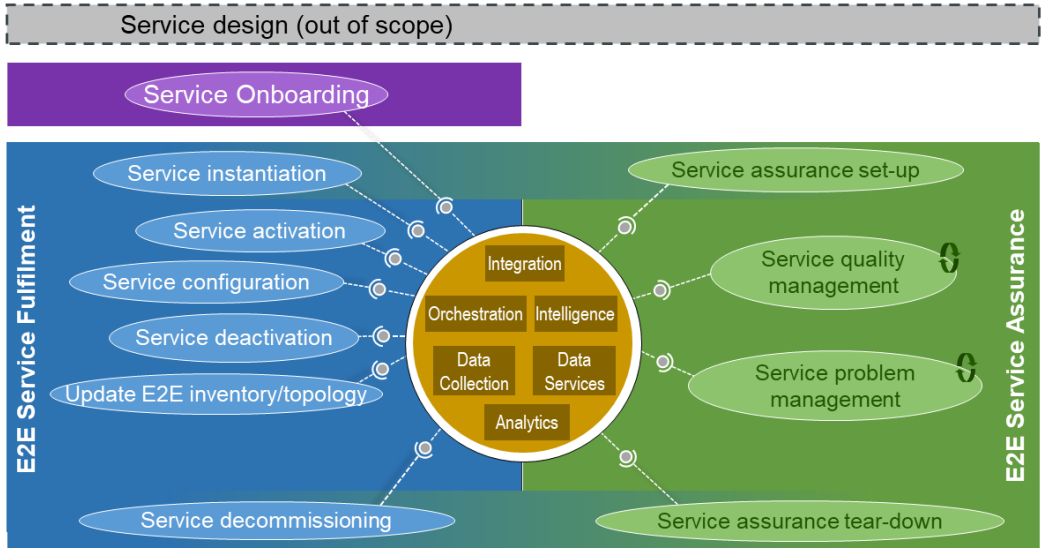
Having native security (e.g. an adaptive secured framework, access control, trustworthiness, security assurance) can help to establish confidence and trust that the automated processes deliver the intended business outcomes.

© ETSI 2023. All rights reserved.

End-to-end service lifecycle management (ZSM 008, ZSM 003)

ZSM defines how to manage the lifecycle of cross-domain and end-to-end (E2E) services. It describes:

- The management processes during the lifecycle of E2E services (service onboarding, fulfillment, and assurance)
- The interaction between the end-to-end service management domain and other management domains.
- End-to-end aspects of network slice management, supporting vertical use cases



Each of the fulfillment and assurance processes is a target for autonomous operation.

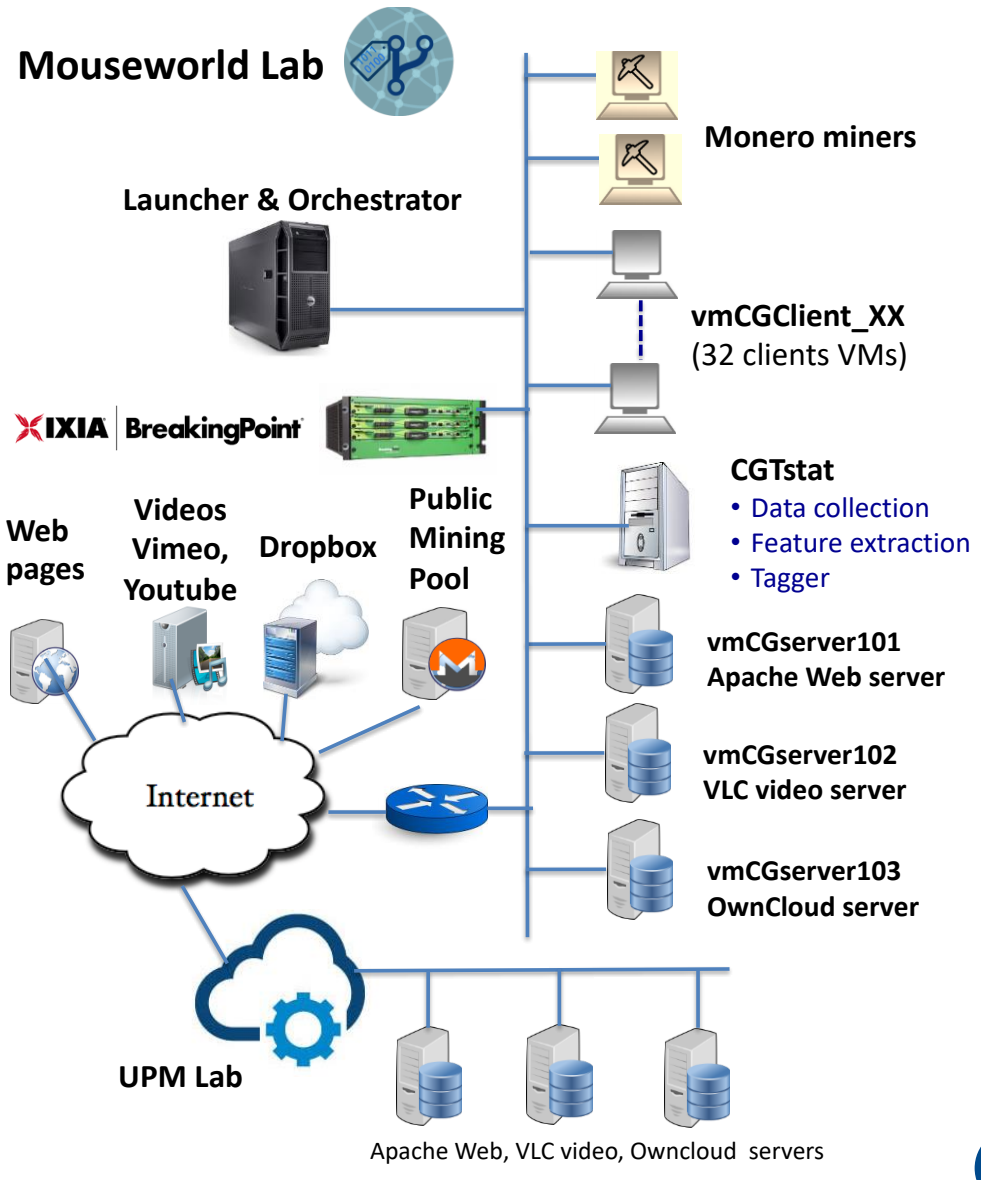
© ETSI 2023. All rights reserved.

Network Digital Twins (ZSM 015)

A Network Digital Twin has the potential to further empower zero-touch network and service automation.

- A virtual replica of a real-world system, allowing to analyze, predict, simulate, diagnose, emulate and test scenarios without adverse impact to the physical world, and recommend or trigger effective actions on the real world
- Identifying risks that might jeopardize normal system operations

The ISG ZSM is studying scenarios that can benefit from Network Digital Twin capabilities and the functionality required to support and utilize it for zero-touch network and service management.

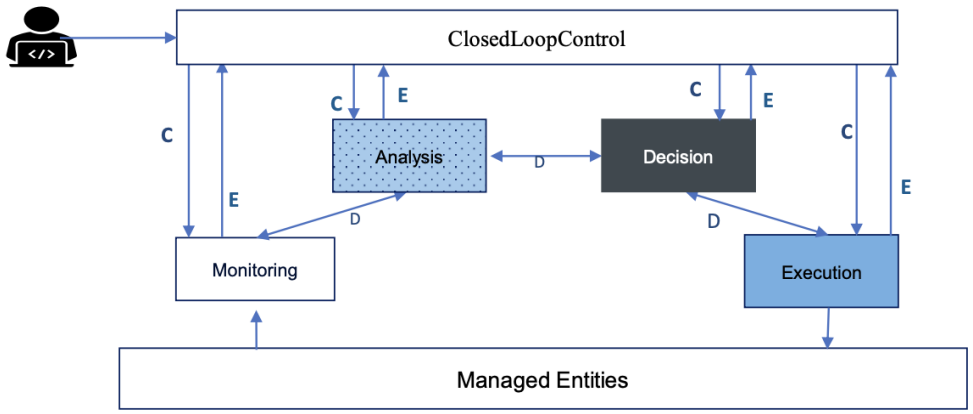


© ETSI 2023. All rights reserved.

And Looking beyond

Concepts for the evolution of closed-loop operations

- Dynamic close loop composition
- Dynamic levels of supervision
- Etc.



© ETSI 2023. All rights reserved.

Let’s reflect on the work status…

	End-to-end architecture and solutions	ZSM key automation technologies
Published Link to specifications/reports	• Requirements based on documented scenarios (GS ZSM001) • Reference architecture (GS ZSM 002) • Cross-domain end-to-end service lifecycle management (GS ZSM 008) • End-to-end management & orchestration of network slicing (GS ZSM 003) • ZSM landsc • Terminolog • Proof of Co	• Means for automation (GR ZSM 005) • Closed-loop automation: enablers (GS ZSM 009-1) • Closed-loop automation: solutions (GS ZSM 009-2) • Intent-driven autonomous networks (GR ZSM011) • AI enablers (GS ZSM012) • spects (GR ZSM 010)
Work in-progress Link to ZSM Open Area		• nation: advance topics (GR ZSM 009-3) • CI/CD automation (GR ZSM013) • Security aspects (GS ZSM014) • Network digital twin (GR ZSM015) • Intent-driven closed loops (GS ZSM 016)

ZSM provides standardized enabling framework and capabilities for Autonomous Networks.

© ETSI 2023. All rights reserved.

The unique value of our specifications/reports…

End-to-end architecture and solutions

Work done in organizations such as 3GPP SA5, NFV, IETF, BBF, ONAP, OSM, Nephio and EMCO, TMF, etc. fits nicely into the ZSM framework and can help enabling the orchestration and automation of end-to-end services.

The ZSM specifications provide guidance to the implementation of management services for achieving automated end-to-end network and service management solutions and architecture.

ZSM key automation technologies

The ZSM key automation technologies can be leveraged across the industry to ensure cross-use cases, cross-domains, cross-planes, interoperable, unified and consistent automation and cognitive operations.

Alignment with the ZSM security capabilities is essential to ensure that the automated processes are secured and deliver the intended business outcomes.

"Collaboration among SDOs is critical to accelerate Telco automation – ETSI ZSM is the glue that holds all of them together from an end to end automaton perspective" (Anil Rao, Analysys Mason)

© ETSI 2023. All rights reserved.

Completing the Puzzle

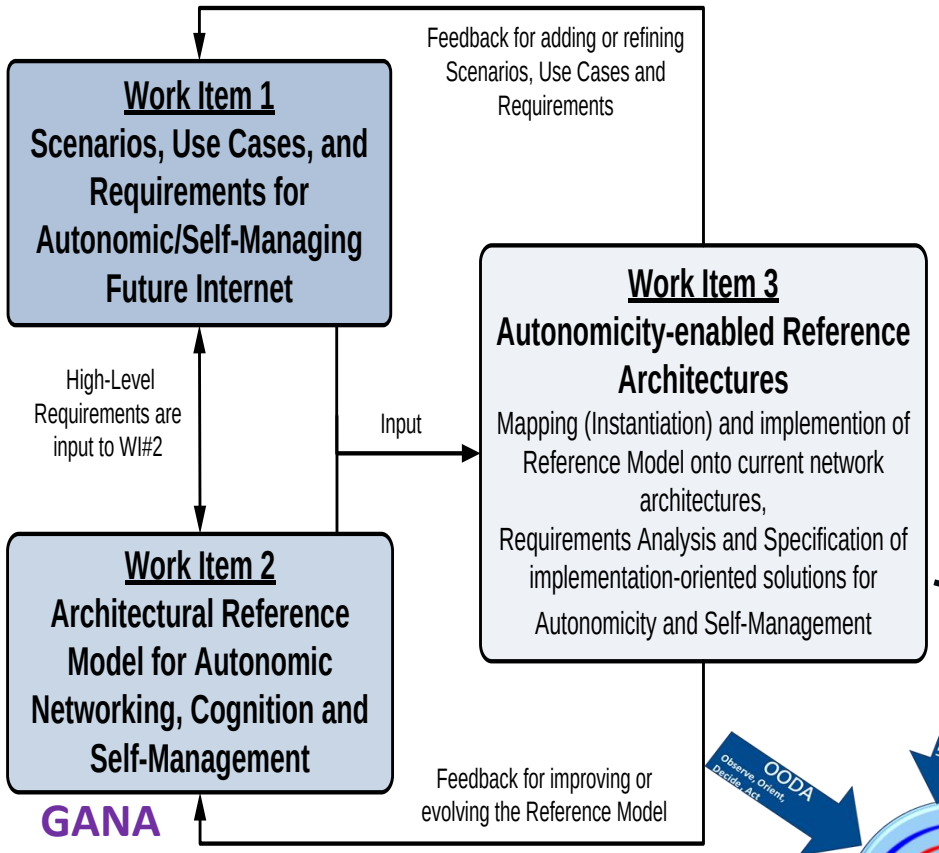
- The automation puzzle is not completed yet
  - But ZSM provides a sound framework ad solutions for addressing it
- The ZSM framework
  - is versatile and built on service-based principles, offering scalability, modularity, extensibility and flexibility.
  - Supports the **transfer of autonomy** from the operator to the network using intent-based interfaces.
  - integrates capabilities for **closed-loop operation and coordination**, in support of the **zero-touch** operational goal.
  - provides means to integrate AI-based functionalities, enabling operational autonomy.
- ZSM specifies key automation capabilities.
- The ISG is working to ensure safeguarding of the ZSM framework and the automation processes
- Alignment and leverage of synergies across the industry is essential to enable the orchestration and automation of end-to-end services, ensure adoption at scale and accelerate time-to-market.

© ETSI 2023. All rights reserved.

AFI (Autonomic Management and Control Intelligence for Self-Managed Fixed & Mobile Integrated Networks)

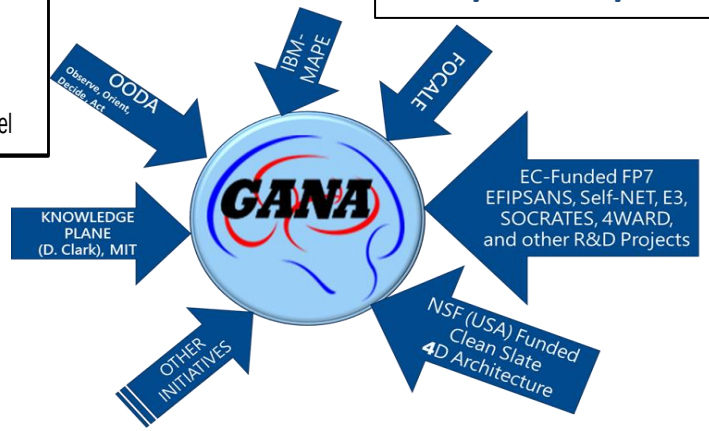
Overview from Autonomous Networks perspective

ETSI AFI in a nutshell



- Scenarios, Use Cases and Requirements for **Autonomic Management & Control (AMC)** for networks and services powered by **Multi-Layer AI Capabilities**
- **Generic Autonomic Networking Architecture (GANA)** Reference Model for cognitive and self-management of networks and services
- **Self-X Features** in Network Elements/Functions (NEs/NFs) and in Management & Control Architectures: ***self-configuration, self-diagnosis, self-repair, self-healing, self-protection, self-awareness, etc***
- **Multi-Layer AMC**: Fast Control-Loops in NEs/NFs & Slow Control-Loops in GANA Knowledge Plane (KP) Platforms
- **GANA instantiations** onto various architecture scenarios (e.g. BBF, 3GPP, IMS, Wireless, ..)
- **Test Methodology and Specifications** for Testing AI algorithms and AI in Test Systems (liaisons with TC MTS, ITU-T SG11, ITU-T SG13)
- Federated Testbeds and Telco Data Space value for AMC; Testing AI models and AI in Test systems; Slicenet; PoC Projects

GANA Multi-Layer Autonomics in Diverse Architectures (3GPP, BBF, ITU-T FN, NGN, Mesh/Ad-hoc/Sensor Networks) and AFI Liaisons with Other Standardisation Groups



© ETSI 2023. All rights reserved.

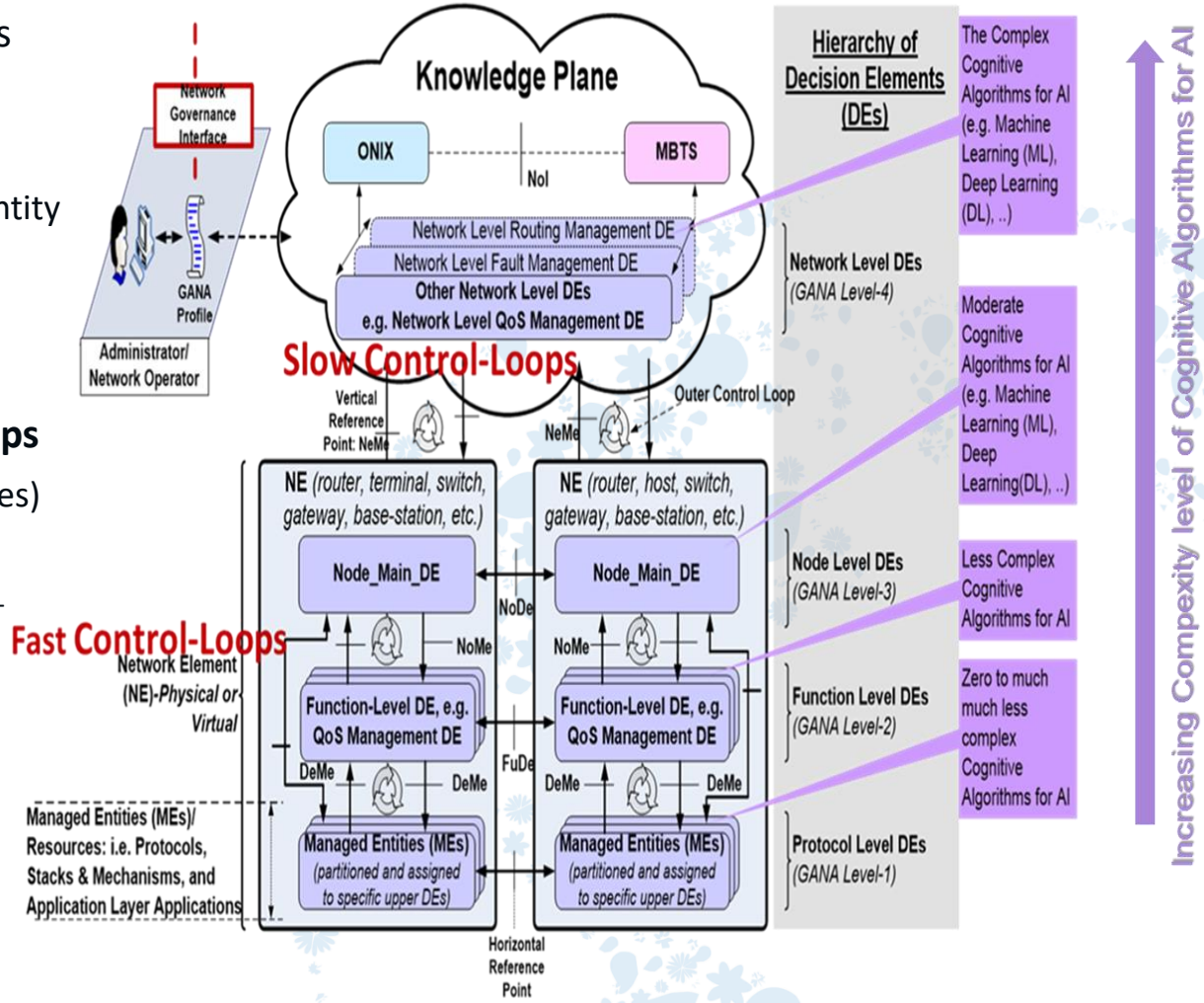
Generic Autonomic Networking Architecture (GANA) Reference Model

ETSI TS 103 195-2

Decision Making Elements (DEs) drive **Self-X properties**

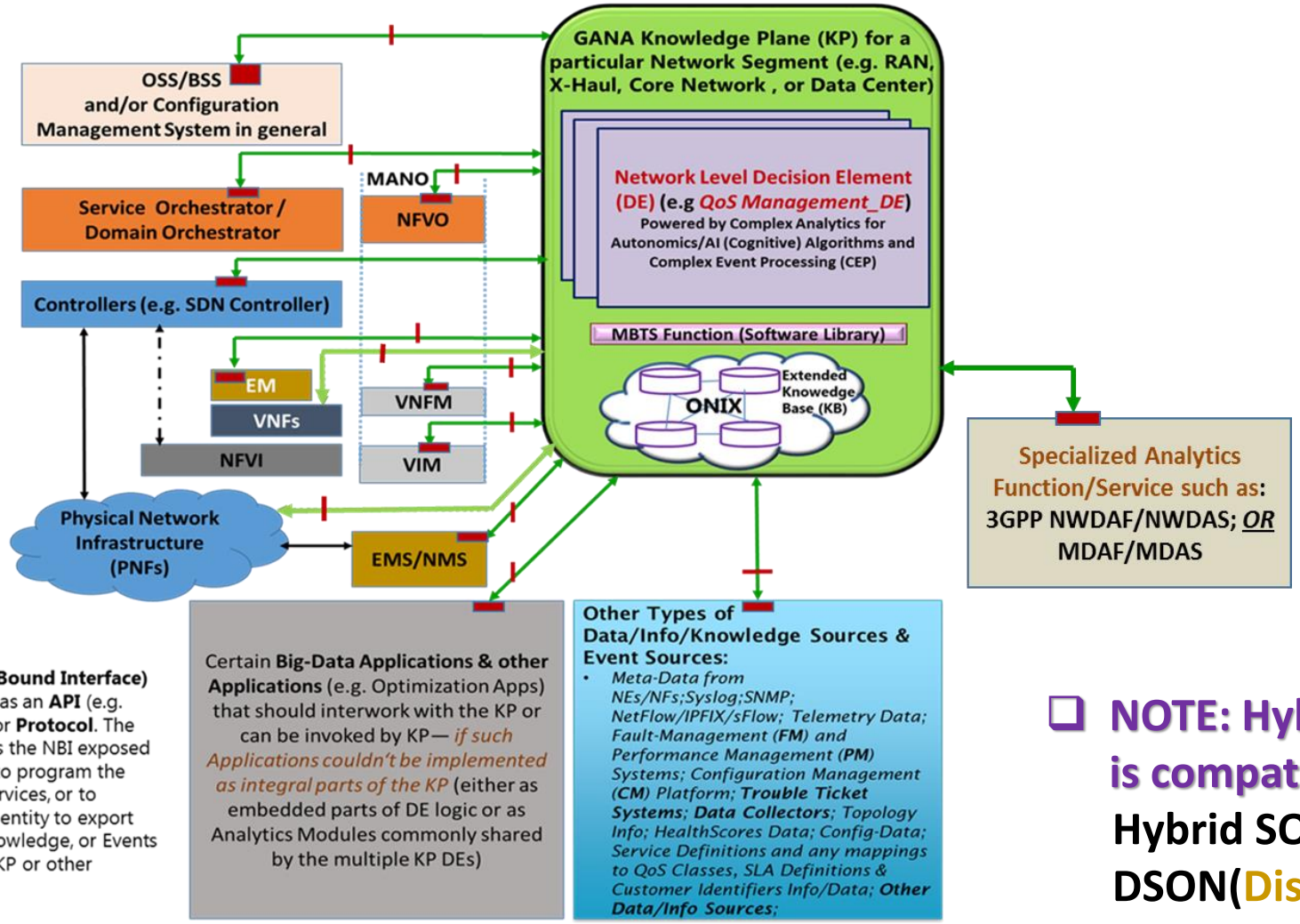
- DE properties designed to cover diverse autonomics uses cases
- Design principles for conflict resolution per design to address stability:
  - Concept of "Ownership" in relationship between DE Managed Entity (ME)
  - Concept of man in the loop to validate and trust decisions

1) **Level of Autonomy/Autonomicity by Hierarchical DEs' Control Loops**
   1) GANA KP DEs (Slow Control-Loops manage and control Autonomic Nodes)
   2) Autonomic Nodes (Fast control loops)
      a) Node-Main DEs : Fault-Management/Security & Resilience/Auto-Discovery &Auto-Configuration
      b) Function Level DEs : Mobility, Forwarding, QoS, Routing, Monitoring, …
      c) Protocol Level DEs : Should be avoided (recommendation)
2) **MBTS** (Model-Based Translation Service)
3) **ONIX** (Overlay Network for Information eXchange):
4) Governance **Framework** (AN is governed with **GANA Profile** (**Intent/Objective, Goals, Policies**)



© ETSI 2023. All rights reserved.

GANA Knowledge Plane(KP) Platform Concept Integration with other Systems in GANA Multi-Layer Autonomics with Multi-Layer AI



ETSI TR 103 747

Remark: The NBI **APIs** indicated should be specified and Standardized if no standards exist, including *KP-to-KP Federation* Reference Points. → ***Implies a Call for Action for Joint efforts by Standards SDOs/Fora***

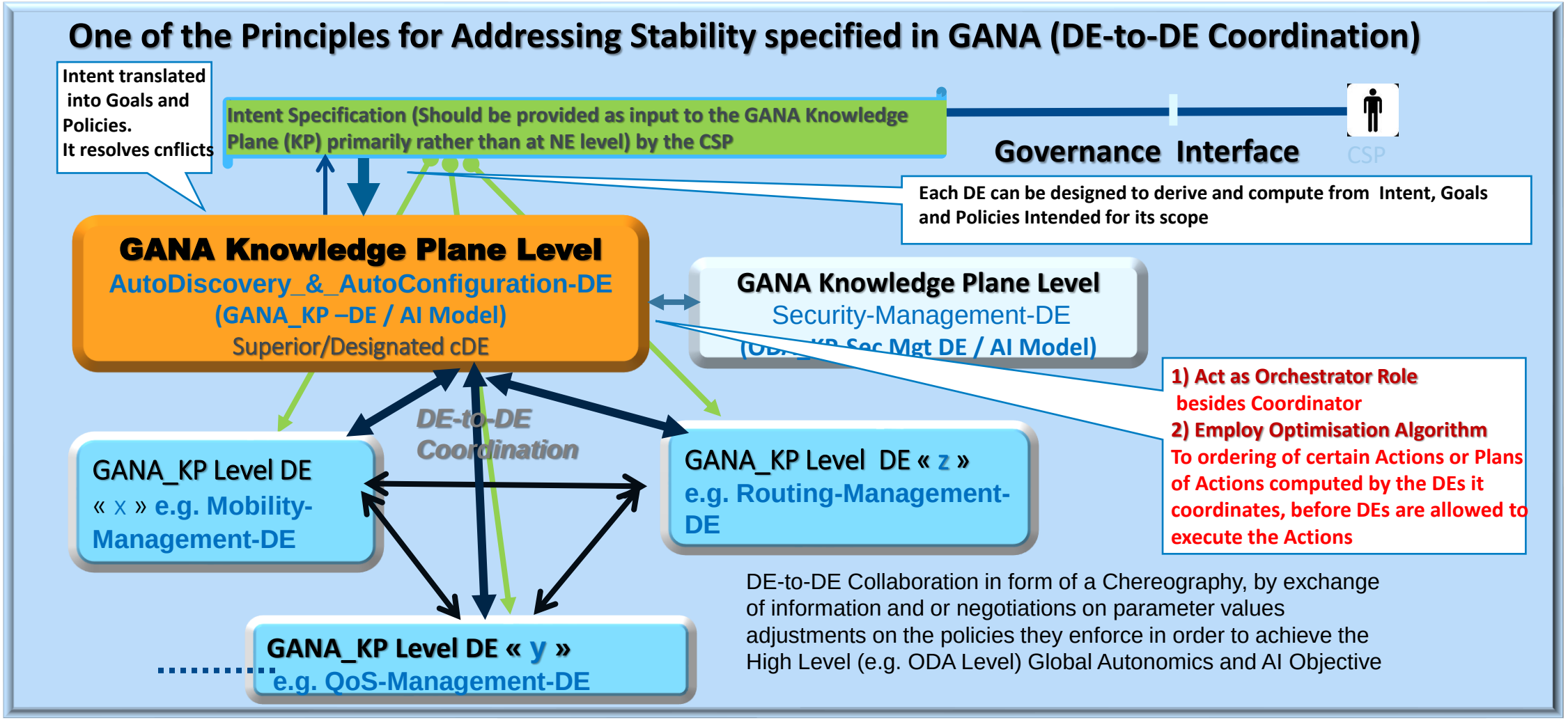
- **NOTE: Hybrid SON Model as specified by NGMN is compatible with GANA**
  Hybrid SON (C-SON(Centralized SON) & DSON(Distributed SON)) are considered as an implementation of the GANA Model for the RAN

Framework for Addressing Stability of Control-Loops and Coordination of Autonomic Functions (e.g. GANA DEs) (1/2)

ETSI GS AFI 002 &
ETSI TS 103 195-2

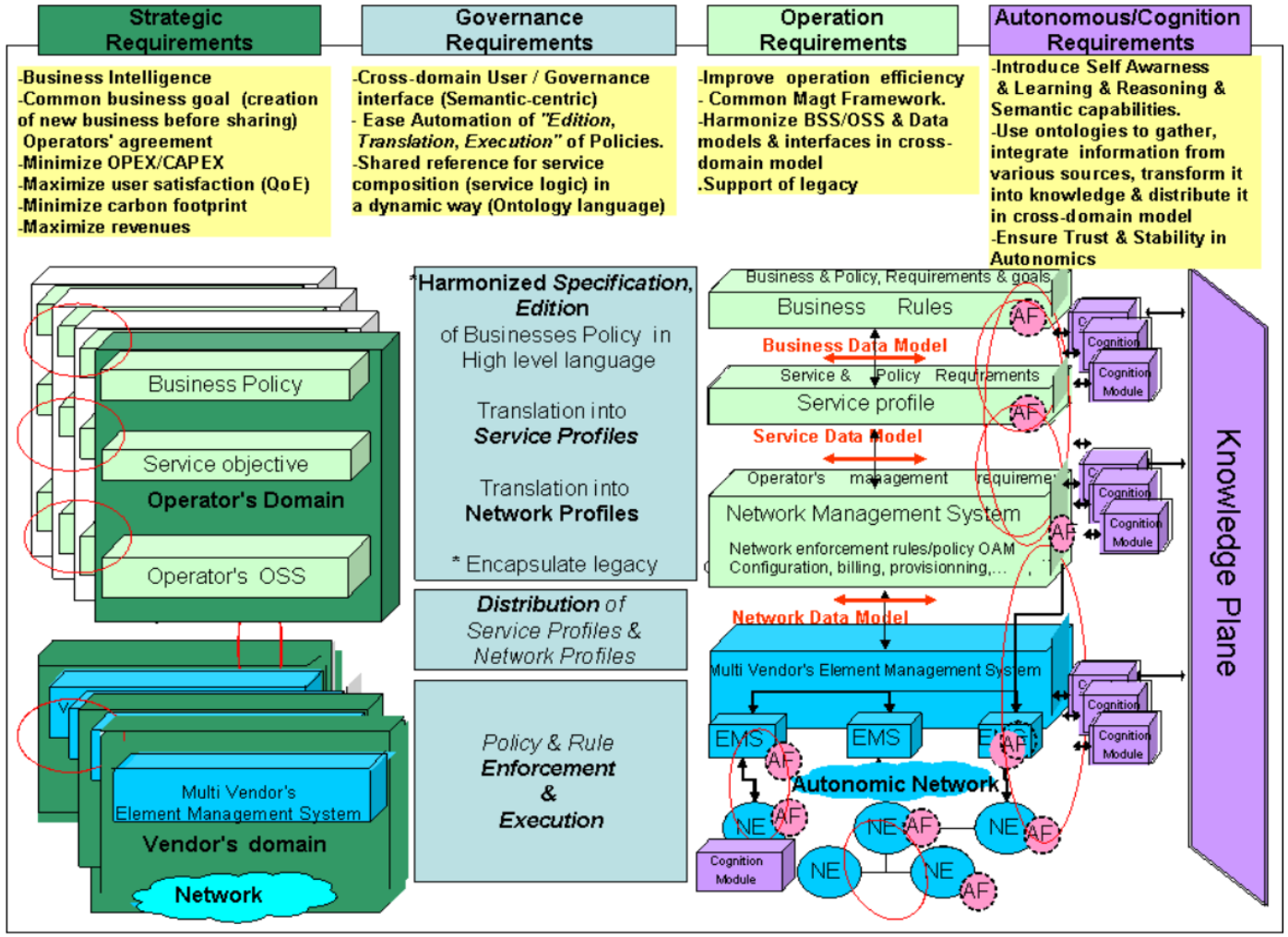
- **Stability Issues in Autonomic Networking (AN)**
- Designing for Stability (Design for Stability Principles)
- Stable Autonomic Behaviors Design through Game Theory - From Theory to Theory
- How to Treat Stability via Analytical Methods? - A Game Theoretic Approach
- How to address stability via Game Theory?
- Addressing Stability in an Architectural Level - From Theory to Practice
- Hierarchy of Control-Loops (DEs)
- Concept of "Ownership" in relationship between Autonomic Function & Managed Entity (ME)
- Separation of "Operating Regions" of Control-Loops
- Model-based Techniques
- Addressing Stability at Runtime
- Autonomic-aware Metrics to Infer and Self-assess Stability by the AN on its own

Framework for Addressing Stability of Control-Loops and Coordination of Autonomic Functions (e.g. GANA DEs) (2/2)



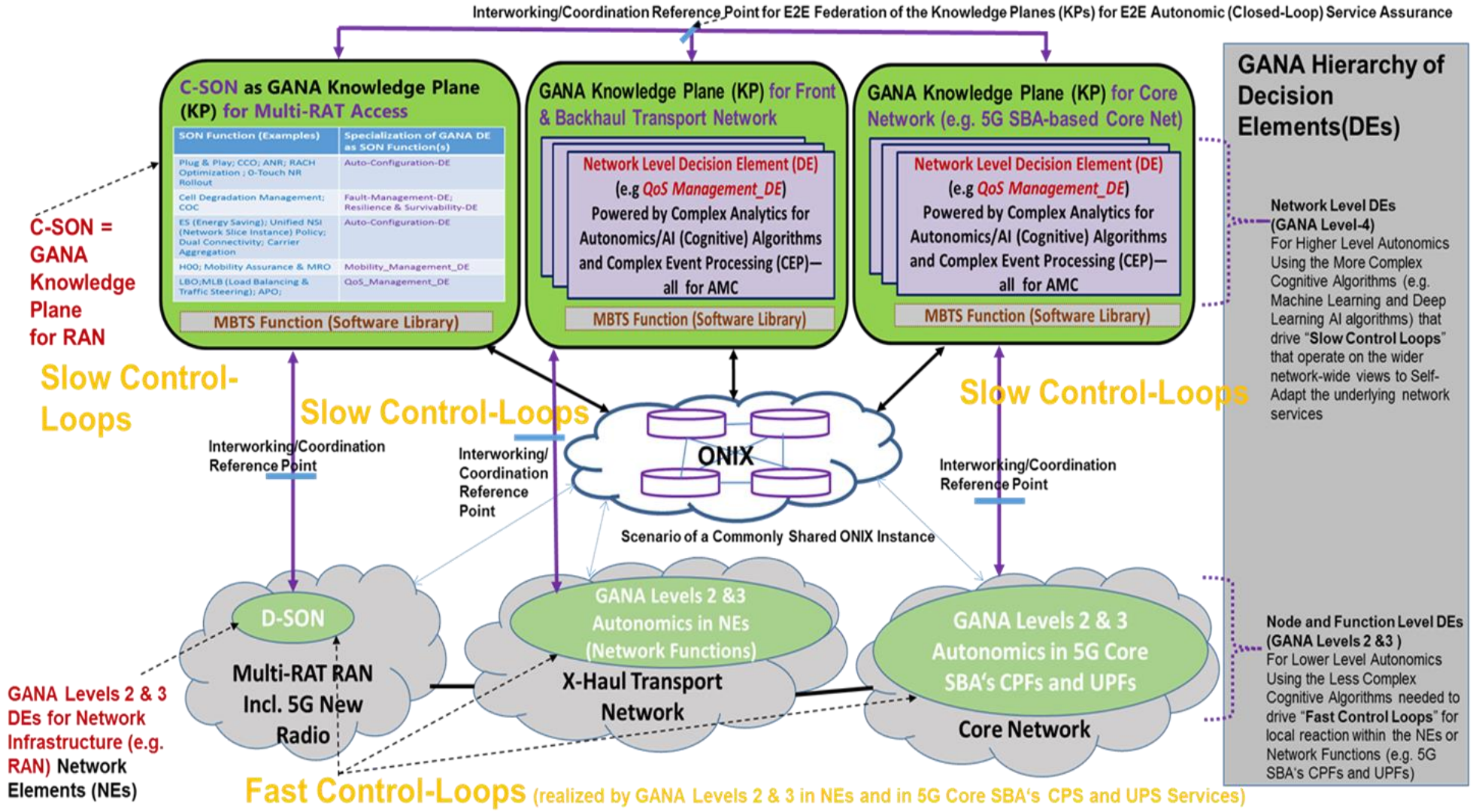
Design for Stability Principles and for **Run-Time Stability Principles** Coordination / Synchronization / Orchestration among DEs

Operator's Policy-based Autonomics Management and Control Framework

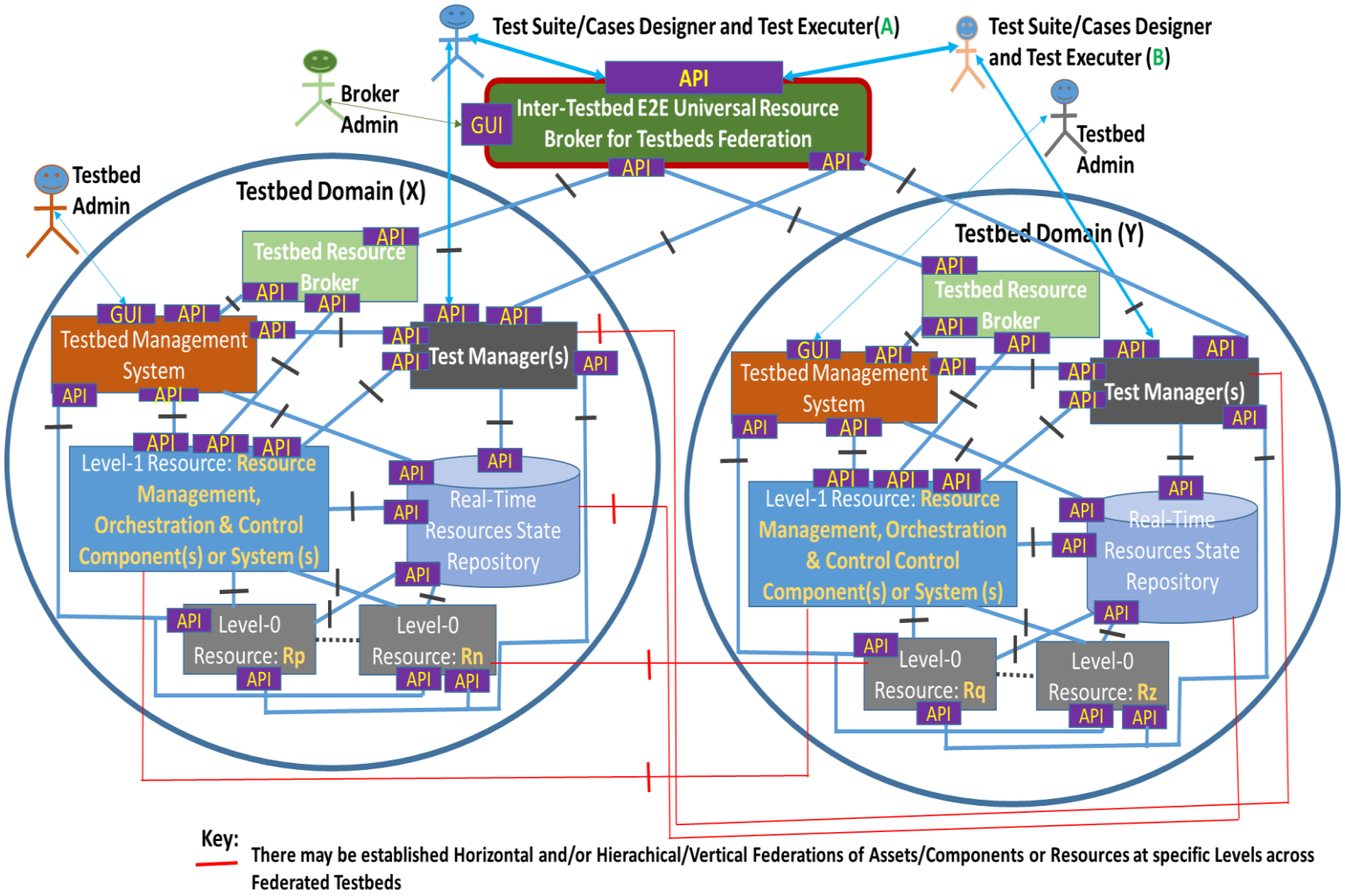


TMForum ODA Intelligence Management adopted ETSI GANA design principles (TMF GB1022)

GANA Knowledge Planes Federations for E2E Service & Security AMC



Testing Framework and Methodology for ANs and associated AI Models for Autonomic Managent & Control (AMC)



AI in Test Systems and Testing AI Models for Closed-Loop Network Automation via a Generic Test Framework

- PoC White paper
- EG Testing Self-Adaptive Networks
- Techniques for Trust and confidence building in ANs

Come and JOIN us within the Joint work Item **ETSI/MTS, ITU-T SG11**

1) Cross-Domain Federation Aspects for ANs, Reference Model for Testbeds Federation: Generic Federated Testbeds Model for ANs
2) Testing AI Models for AMC (**Quality Metrics)**
3) AI in Test Systems

MEC (Multi-access Edge Computing)

Overview from Autonomous Networks perspective

Presented by: Dario Sabella (ISG MEC Chair)

ETSI MEC: Enabling *Edge* through *Standardization*

Foundation for Edge Computing – Fully standardized solution to enable applications in distributed cloud created by ETSI MEC + 3GPP

Watch the new video on MEC

https://www.youtube.com/watch?v=crnPWql-0oo

Application Life Cycle Management

RESTful based APIs for Runtime Application Services

3GPP A GLOBAL INITIATIVE · Wi Fi · broadband forum

ETSI: The Standards People
producing globally applicable standards for ICT-enabled systems

ETSI ISG MEC

ISG: Industry Specification Group
open to all of industry, regardless of ETSI membership and focused on all industry needs

MEC: Multi-access Edge Computing
Cloud Computing at the Edge of the network.

ETSI MEC The Standards People

ETSI NFV The Standards People

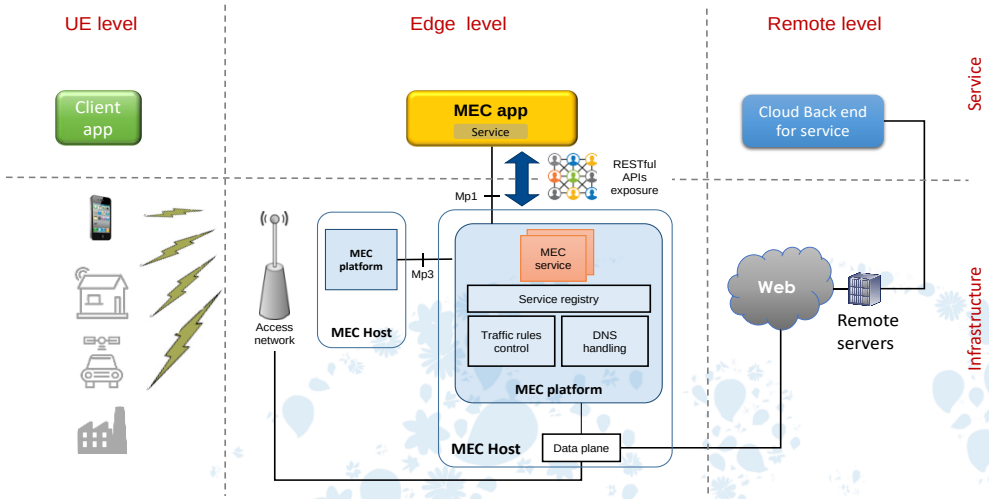
MEC Application Development Community
Interaction & Information Exposure

- **Continuously growing MEC membership:** 124 (updated Dec 2022); e.g. in June 2021 it was 114
- **Diverse ecosystem:** Operators - Technology Providers - IT players - Application developers - Startups - …

Renewed webpage: **ISG MEC Leadership Team, LS officers for Vertical Industries** and **MEC Support Team:** https://portal.etsi.org/TB-SiteMap/MEC/MEC-Leaders-and-Support-Team

ETSI MEC – Foundation for Edge Computing

MEC offers to application developers and content providers cloud-computing capabilities and an IT service environment at the edge of the network



Basic principles:

- *Open standard* → allowing multiple implementations and ensuring interoperability
- MEC exploiting ETSI *NFV framework* and definitions → enabling MEC in NFV deployments
- Alignment with *3GPP* based on fruitful collaboration of common member companies → enabling MEC in 5G
- Access-agnostic nature (as per MEC acronym - Multi-access Edge Computing) → enabling other accesses
- Addressing the needs of a wide ecosystem → enable multiple verticals (e.g. automotive), federations

MEC is focused on *existential* questions of **applications "on the edge"**

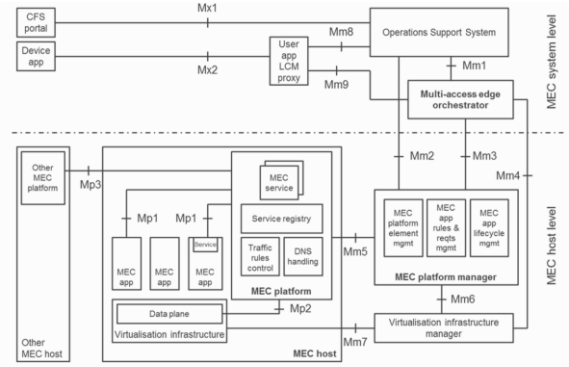
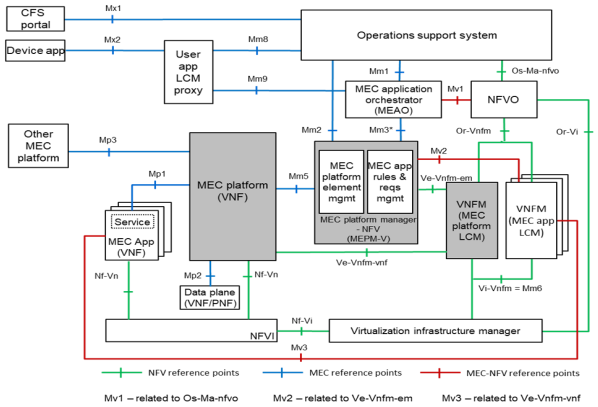
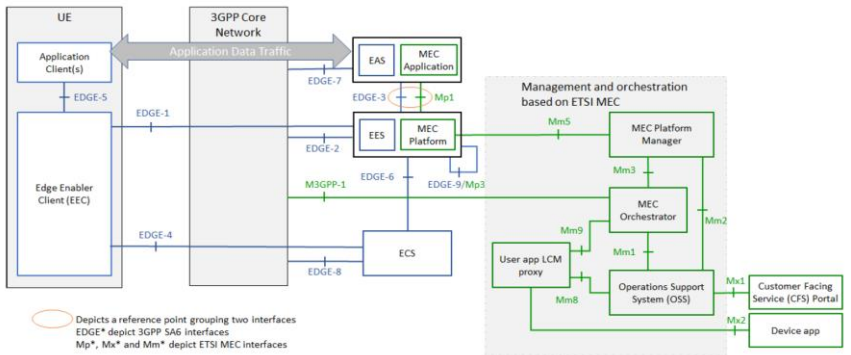


Figure 6-1: Multi-access edge system reference architecture





© ETSI 2023. All rights reserved.

MEC and Management: The Killer Use Case for Automation

MEC deployments present challenging environment

- (large scale: geography) x (small scale: cloud footprint)
- Unmanned/lights out location
- Outside traditional service areas

While supporting “critical infrastructure”

- Telco, public safety, etc.
- “9’s” of availability requirements

Unique requirements and processes

- Minimize need for human presence
- Maximize service time intervals
- Minimize skills required from those on site

In other words

- Get as close as possible to the web-scale maintenance model
- In a very non-web-scale environment

The following **ETSI White Papers** address the MEC deployment aspects:

- *WP#23: Cloud RAN and MEC: A Perfect Pairing*
- *WP#24: MEC Deployments in 4G and Evolution Towards 5G*
- *WP#28: MEC in 5G networks*
- *WP#30: MEC in an Enterprise Setting: A Solution Outline*

All white papers are available in https://portal.etsi.org/TBSiteMap/MEC/MECWhitePapers.aspx

© ETSI 2023. All rights reserved.

MEC use cases and requirements related to Autonomous Networks

Exemplary use cases

- **Optimizing QoE and resource utilization in multi-access network**
  - in presence of multiple access technologies, the overall QoE perceived by the end users as well as utilization of the resources can be optimized with smart selection and combination of the paths used for the user plane: for example, the network paths can be dynamically selected based on knowledge of current conditions in the relevant access networks.
    - These solutions can give the opportunity to jointly optimize the QoE of clients, resource utilization, and fairness among clients by using MEC system and its APIs. Thus, the support for some MEC service APIs might be needed (e.g. RNI API, MTS API, etc.).

- **Security, safety, data analytics**
  - MEC can provide better end-user experience, e.g., reduce down-time for services, improve end-to-end latencies, security and data privacy, introduce intelligent services at the edge, by exploiting the best cloud service deployment for the applications, e.g., edge load balancing, secure messaging across multi-cloud, hybrid-cloud, AI/ML services via distributed cloud, etc.
    - MEC apps might need to store data locally. The data might need to survive the app instance termination. The app performs the required (application-specific) analysis and provides the analysis results to an external entity. In order to do this, the app needs to be able to connect to external apps. Also, the MEC app might need to get location information regarding UEs.

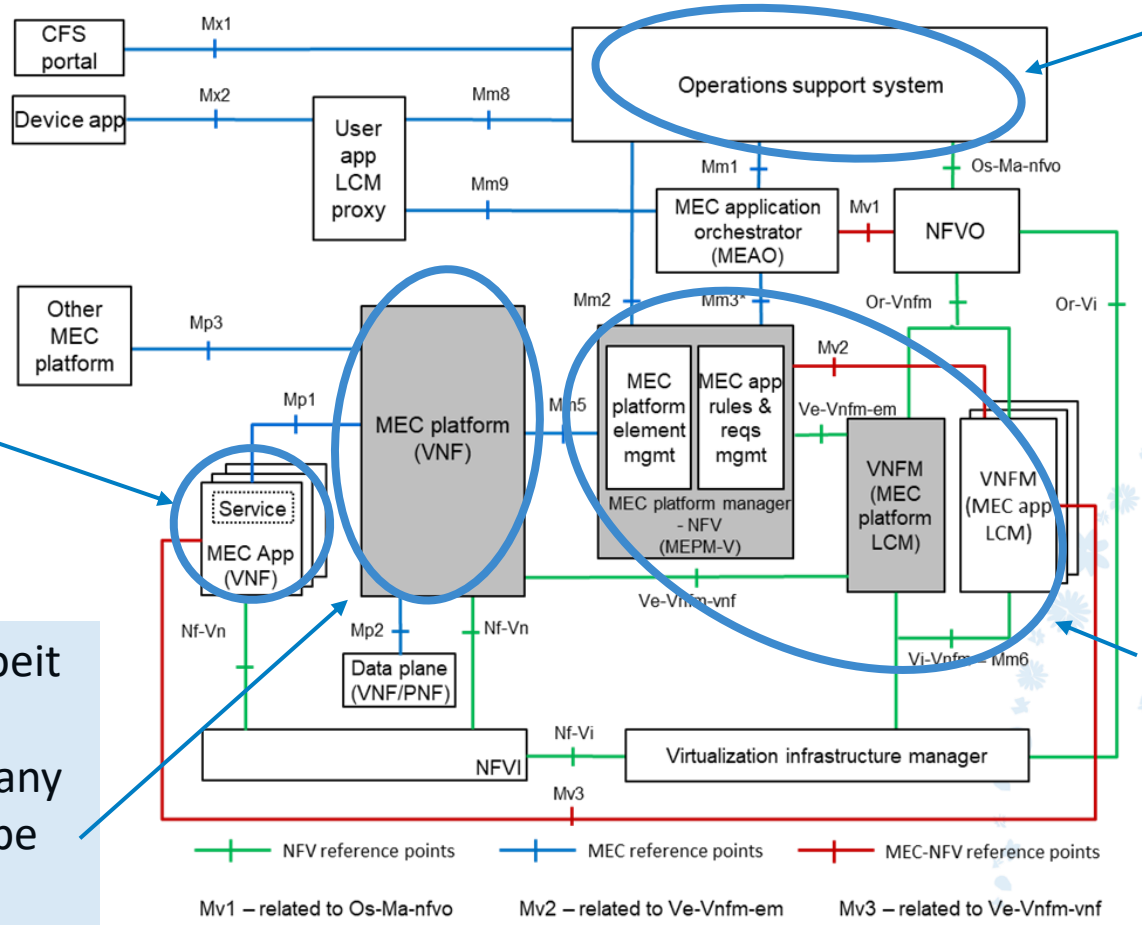
© ETSI 2023. All rights reserved.

Ref. ETSI GS MEC 002 - https://www.etsi.org/deliver/etsi_gs/MEC/001_099/002/03.01.01_60/gs_mec002v030101p.pdf

MEC architecture in NFV environments

MEC Applications can be treated by ETSI NFV system as VNFs (Virtual Network Functions), even if they were not designed as such.

MEC Platform is a VNF, albeit one that requires special handling. For example, in any ETSI MEC system, it must be deployed before any MEC Application.

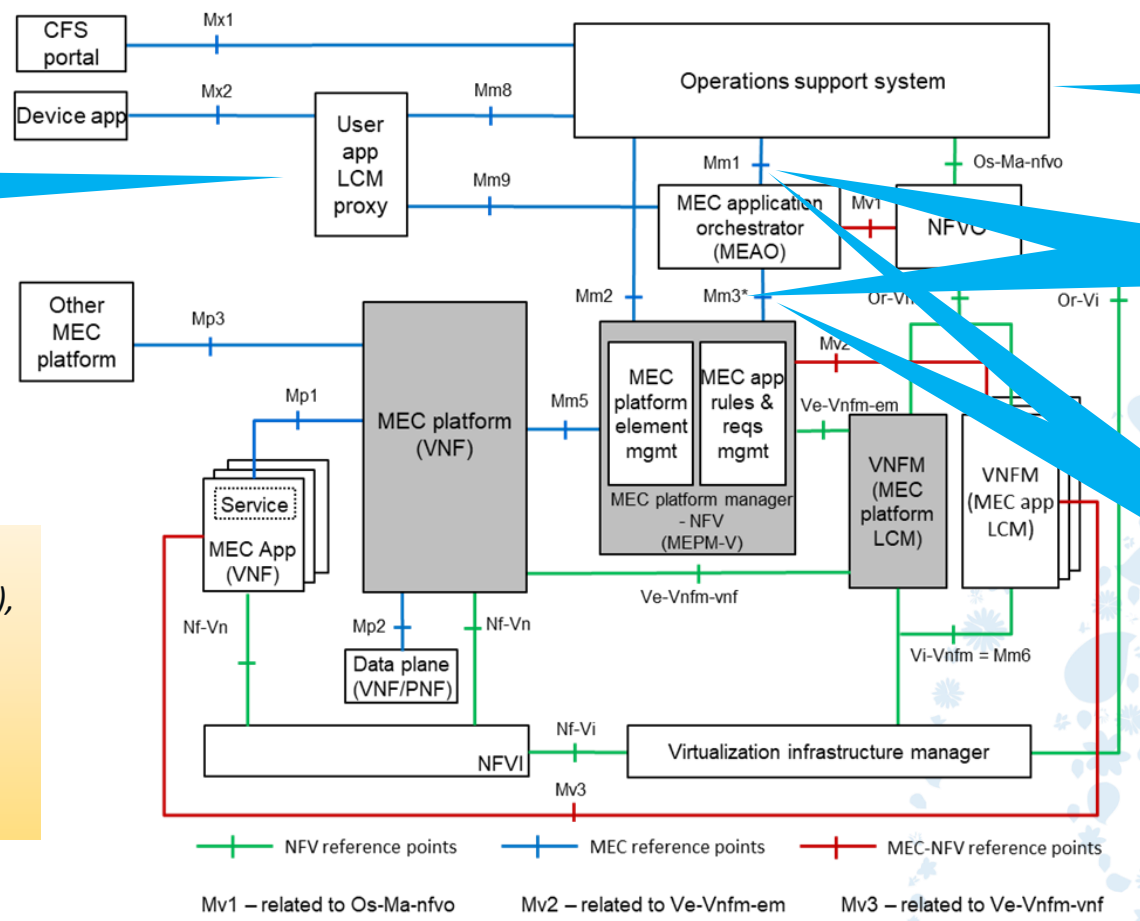


Also the **OSS** (Operations Support System) plays a key role in the MEC system, as it receives requests from outside the MEC system for instantiation/termination/relocation of applications, and decides on the granting of these requests, by properly communicating with the MEC orchestrator.

The **MEC Platform Manager** acts as EM (Element Manager) for MEC Platform, while the LCM (Life Cycle Management) of MEC platforms and MEC applications is delegated to respective VNFMs (VNF Managers).

© ETSI 2023. All rights reserved.

MEC: a key part of ETSI Network Automation Standards



Inter-MEC & MEC-Cloud (MEC 035 Study)

Device-triggered LCM Enablement (MEC 16)

Management of MEP as a VNF (MEC 10-1)

LCM Mgmt of 3rd party Apps (MEC 10-2)

*In the future evolution of the standard (and with the progressive maturity of AN), further normative work in **ETSI ISG MEC** could include aspects that may support end-to-end zero-touch management as defined by ETSI ZSM, and in accordance with ETSI NFV*

ZSM: overall approach → NFV, OSM: managing telco clouds → MEC: managing edge telco clouds

© ETSI 2023. All rights reserved.

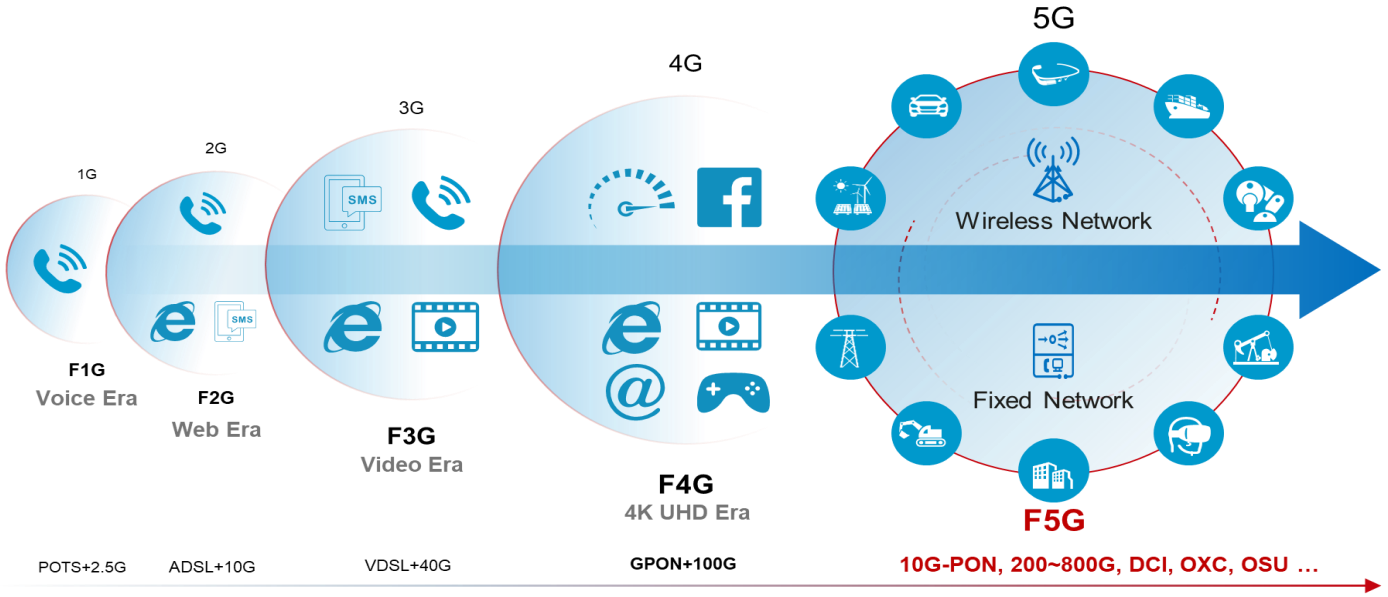
F5G (5th Generation Fixed Networks)

Overview of F5G Autonomous Networks

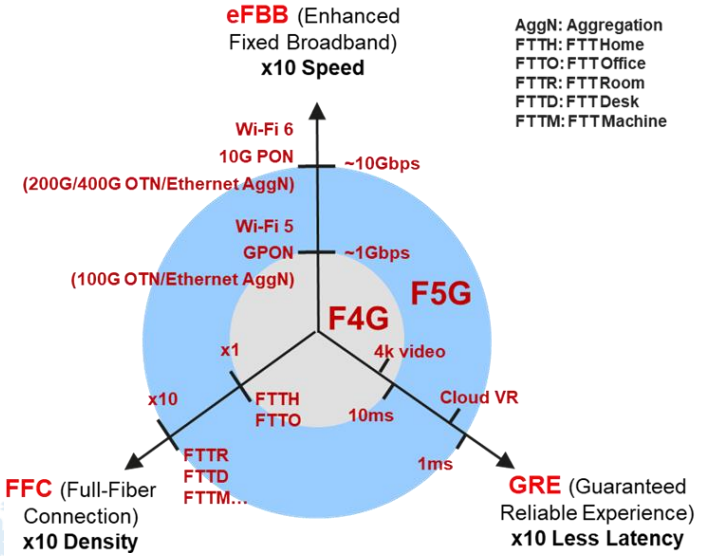
Presented by: Yi Lin

Introduction of F5G and ISG F5G

The Generations of Fixed Networks



Technical Characteristics for F5G



ETSI GR F5G 001: F5G Generation Definition

Fibre connectivity extending from last "mile" to last "meter". F5G helps "last meter" extension for residential, business and verticals

ETSI ISG F5G

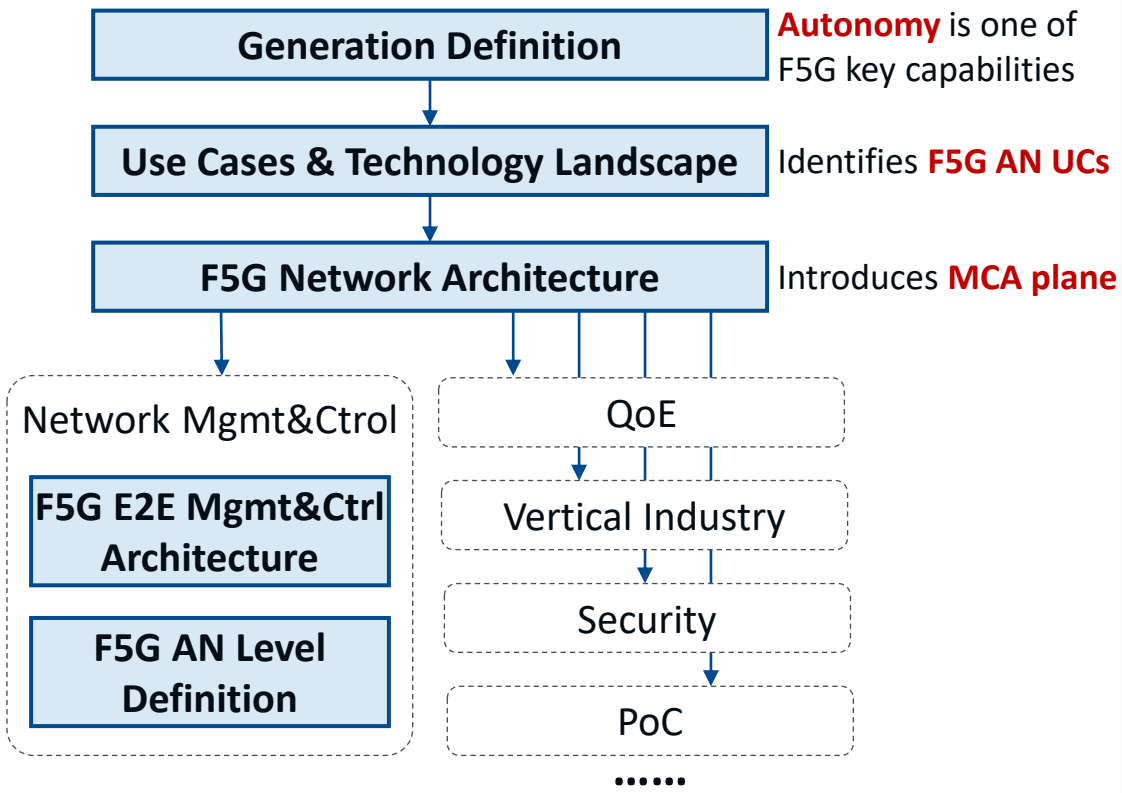
F5G Kickoff (Feb 2020) → Till Now (April 2023)

96	1830	70	22	4	30
Members/participants	Contributions	Liaisons	Work Items	Whitepapers	Industry activities

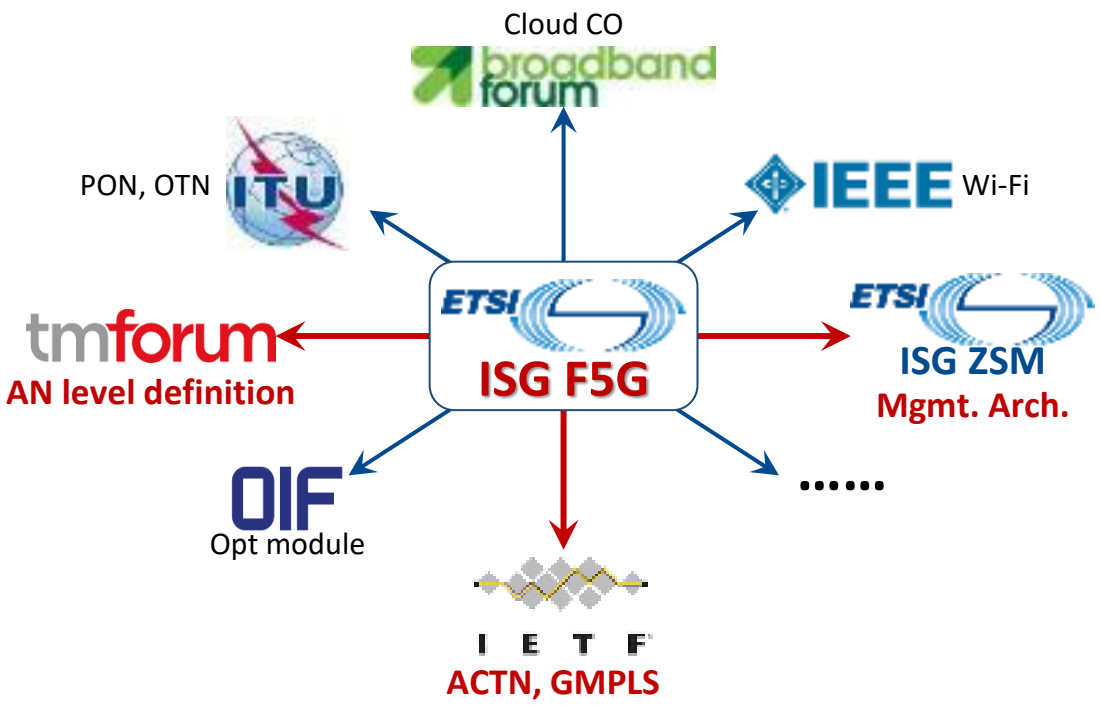
© ETSI 2023. All rights reserved.

Overview of AN @ ISG F5G

Standard Development



SDO Cooperation

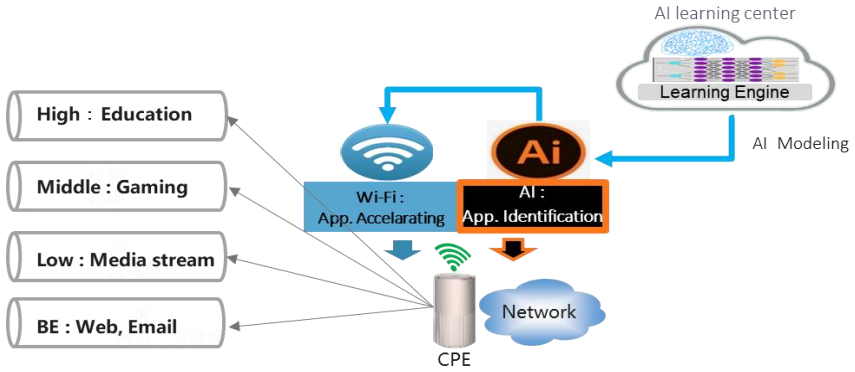


© ETSI 2023. All rights reserved.

F5G Use Cases related to AN

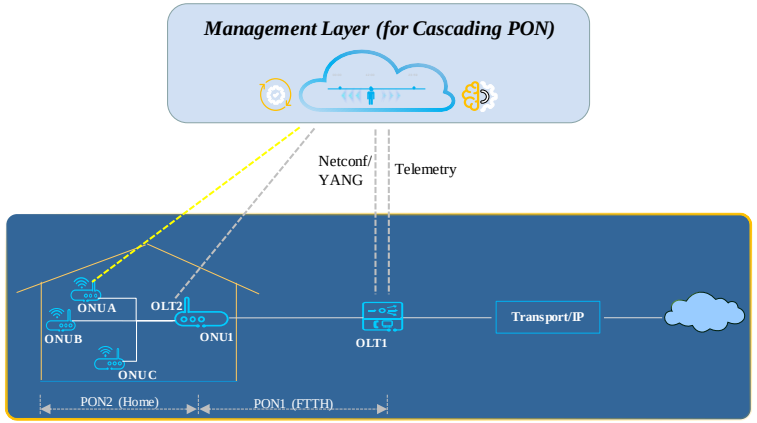
➢ **ISG F5G defines 32 UCs in ETSI GR F5G 008, 5 of which are highly related to Autonomous Network**

UC#10: Scenario based broadband



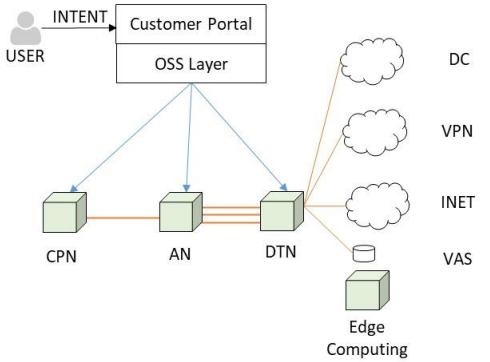
Use AI to learn and distinguish high value broadband applications

UC#11: Enhanced traffic monitoring and network control in Intelligent Access Network



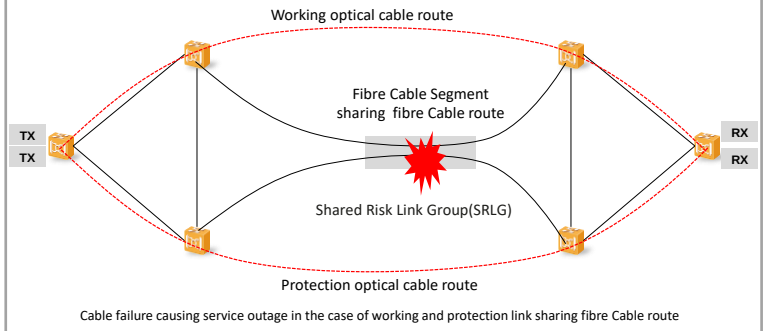
Use ML for traffic monitoring, analysis, prediction and network configuration for FTTR services

UC#29: Orchestration of B2B services in xPON networks



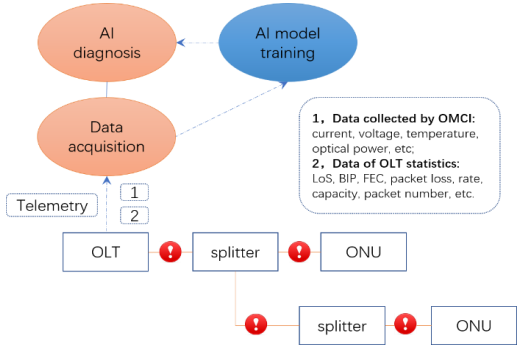
Zero-touch B2B connectivity service provisioning in xPON, with common connectivity service model

UC#31: Intelligent Optical Cable Management



Shared-route fibre identification, and fibre quality monitoring and degradation prediction

UC#32: AI-based PON optical path diagnosis

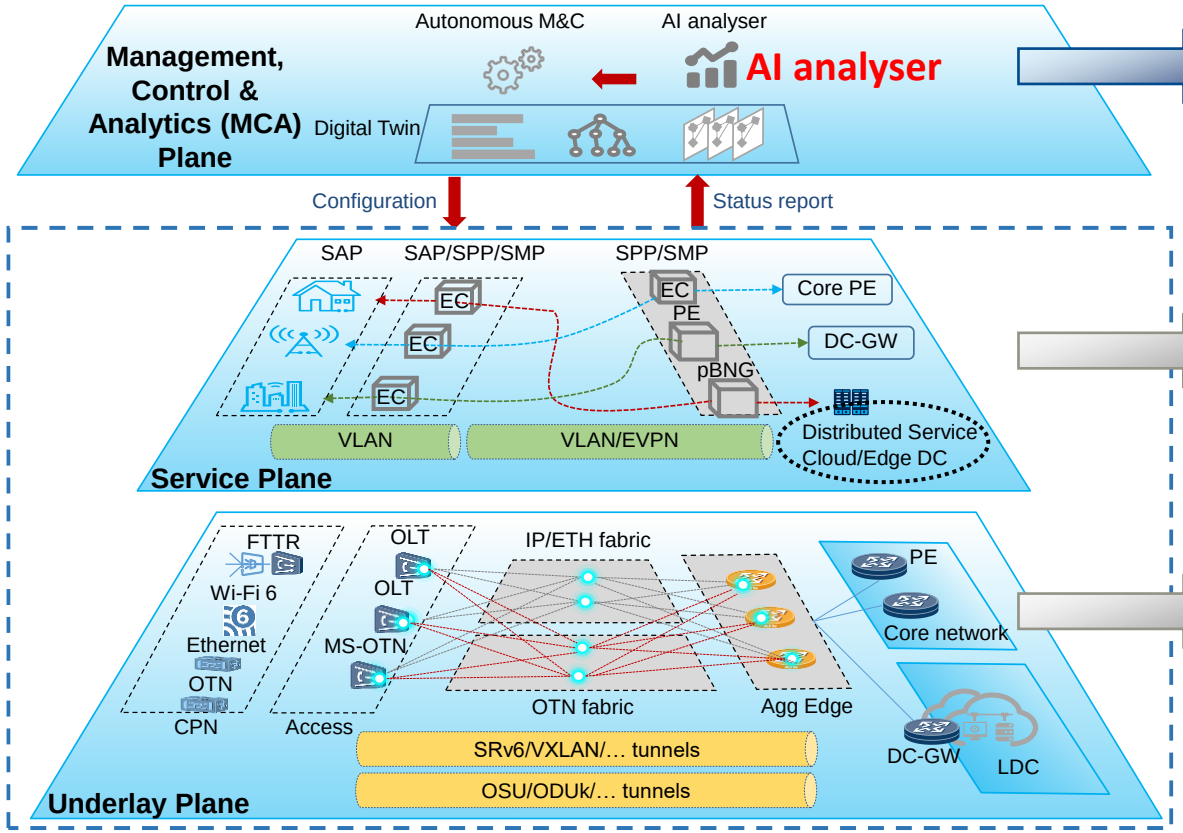


data acquisition, status monitoring and analysis, and fault diagnosis of PON

© ETSI 2023. All rights reserved.

F5G Overall Architecture

F5G network architecture *(ETSI GS F5G 004)*



Management, Control & Analytics (MCA) Plane:

- Introducing **AI analyser** to enable more intelligent operation of fixed networks
- Network data analysis, failure identification, location and prediction, service QoE analysis, …

Service Plane: To allow faster deployment of new services

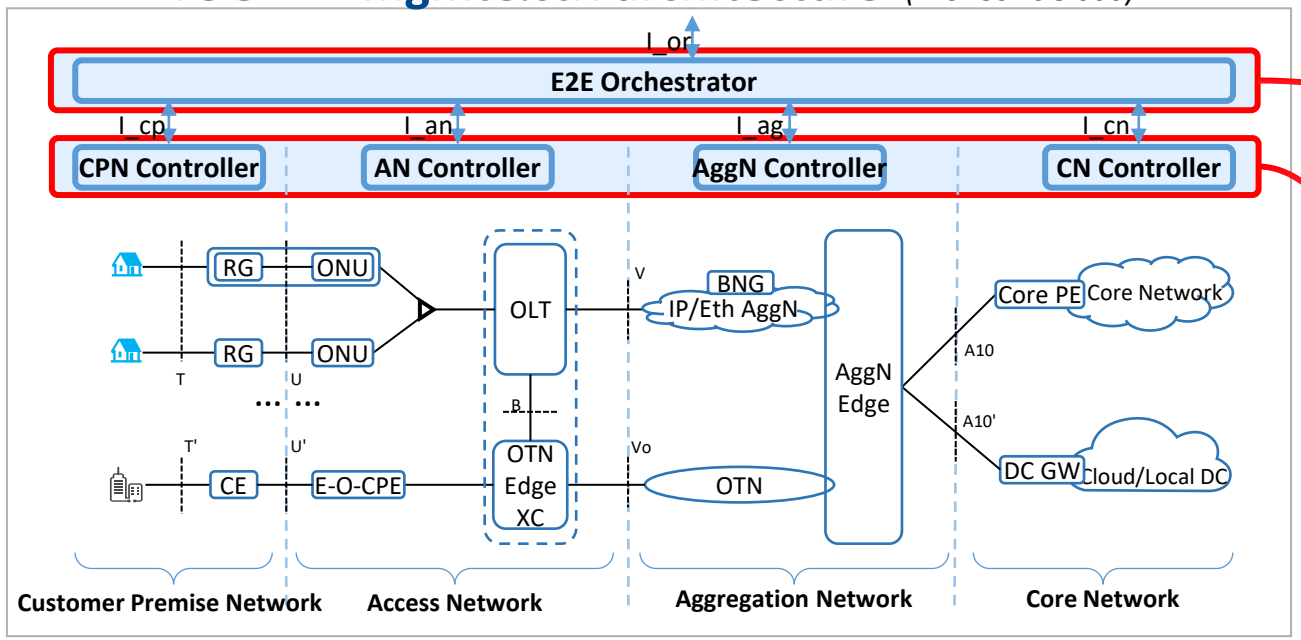
Underlay Plane: OTN and IP/Eth infrastructure

© ETSI 2023. All rights reserved.

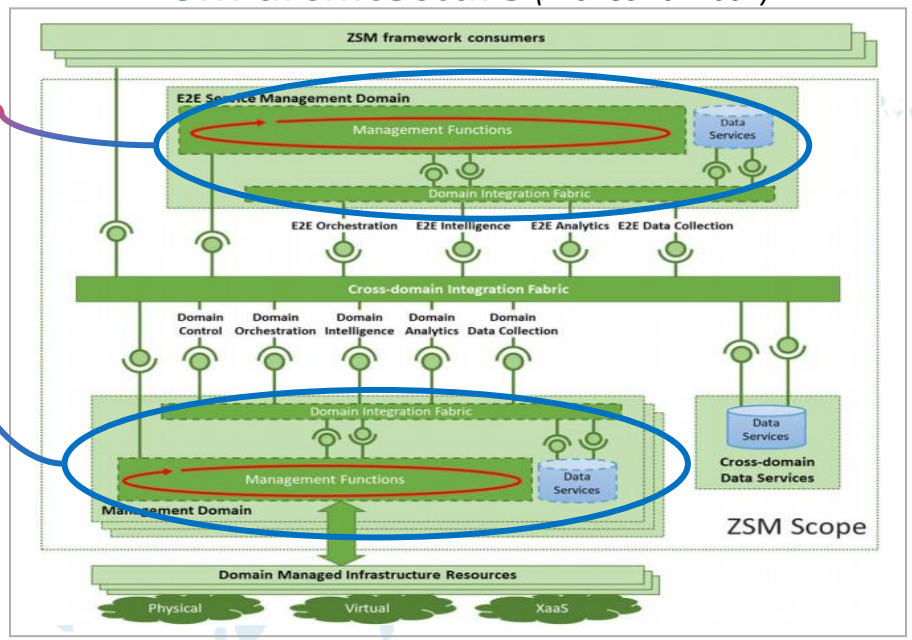
F5G E2E Mgmt&Ctrl Architecture and Key Technologies

ETSI ISG F5G ⟷ **ETSI ISG ZSM**

F5G E2E mgmt&ctrl architecture *(ETSI GS F5G 006)*



ZSM architecture *(ETSI GS ZSM 002)*



- **F5G E2E mgmt&ctrl architecture is an equivalent to an instance of ZSM**
- **Automatic service and resource management:** general processes of F5G service fulfilment and assurance, to enable automatic E2E service and resource life-cycle management
- **APIs and Intent-driven management:** Technical requirements and key parameters of intent-based controller NBIs

© ETSI 2023. All rights reserved.

F5G AN Level Classifications & Evaluations

TM Forum ⟷ **ETSI ISG F5G**

tmforum

Generic Criteria for AN Level Classifications

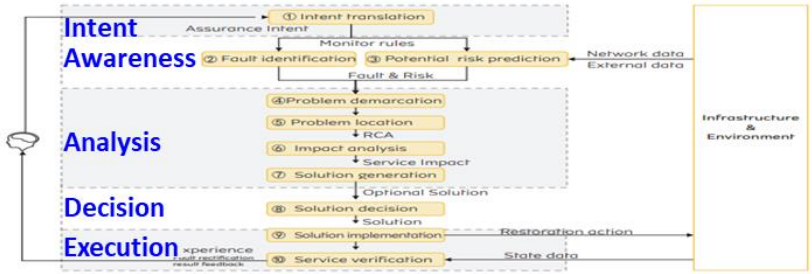
Autonomous Levels	L0: Manual Operation & Maintenance	L1: Assisted Operation & Maintenance	L2: Partial Autonomous Networks	L3: Conditional Autonomous Networks	L4: High Autonomous Networks	L5: Full Autonomous Networks
Execution	P	P/S	S	S	S	S
Awareness	P	P/S	P/S	S	S	S
Analysis	P	P	P/S	P/S	S	S
Decision	P	P	P	P/S	S	S
Intent/Experience	P	P	P	P	P/S	S
Applicability	N/A	Selected Scenarios				All Scenarios

TM Forum IG1230: Autonomous Networks Technical Architecture

TM Forum general AN level framework (IG 1230) will be used as the basis for F5G AN level classification

New WI: F5G AN Level Definition and Evaluation *(DGR F5G 019)*

- To define **F5G workflows** (planning, deployment, fulfilment, maintenance, optimisation & resource mgmt.), and map to generic AN workflow



- To define the **level classification** for each task of each F5G workflow

Workflow	Task	L0	L1	L2	L3	L4	L5
Planning & deployment	Task_1 (intent)						
	Task_2 (Awareness)						
	Task_n (…)						
fulfilment	Tasks ..						
……	Tasks …						

F5G AN Level Classification

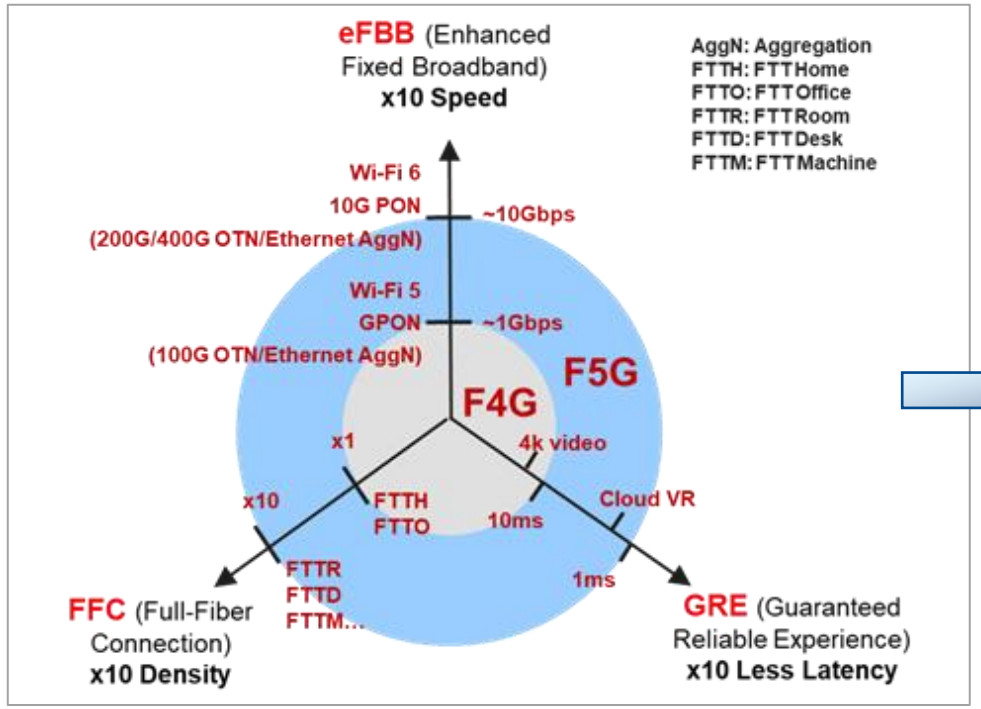
- To define the **evaluation methodology** (e.g., weighted averaging) to evaluate the score of the system, based on the F5G level classification

© ETSI 2023. All rights reserved.

Future Evolution Towards F5G-Advanced and AN Level 4

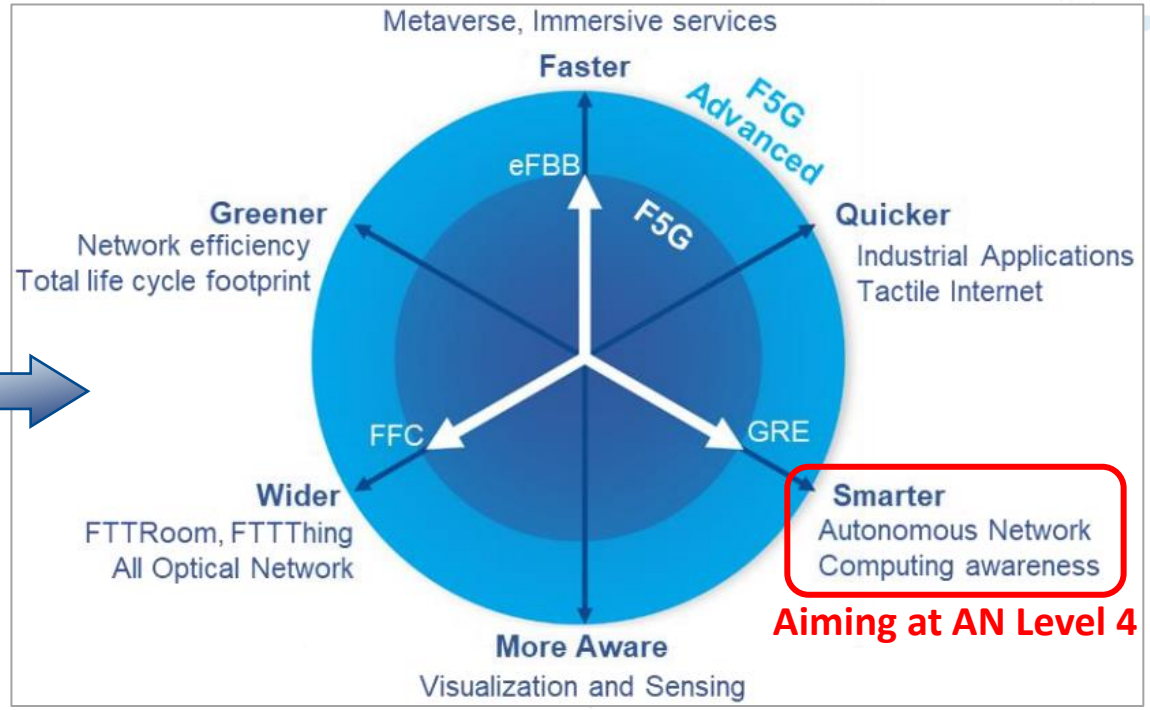
- ISG F5G has started the standardization of F5G-Advanced since 2023
- Aims at reaching AN Level 4 in F5G-Advanced, to achieve the "Smarter"

F5G Features



ETSI GR F5G 001

F5G-Advanced Features



ETSI White Paper No. #50, "Fixed 5th Generation Advanced and Beyond"

© ETSI 2023. All rights reserved.

Thank you for your attention

Follow us on:

© ETSI 2023. All rights reserved.

About MTS

- specification of **requirements** with respect to **efficiency**, **quality** and **testability**
- specification of **standardized tests**, including **formal definition languages**
- requirements for the **test environment**
- methods for **generating**, **executing**, **processing** and **verifying tests**

MTS contribution in OCG AN Whitepaper

OCG AN Whitepaper lists results of **continous coperation** with TC **“Interoperability Testing** (INT)”:

- Development of requirements on testing autonomous systems
- AI is gaining in importance

Work with relevance for Autonomous Network

- ETSI Guide (EG) Approaches ETSI EG 203 341 V1.1.1 on **Testing Self-Adaptive Networks**;
- White Paper No.5 (ETSI 5G PoC):
  AI in **Test Systems**, **Testing AI Models** and ETSI GANA Model's **Cognitive Decision Elements** (DEs)…;
- **Metrics** as Basis for **Test** and **Certifications** for AI Models
- Use Cases to leverage the concept of **Federated Testbeds** for testing Autonomous Networks
- **Evaluation** Methods for **Trust** and **Confidence** in Autonomous Networks
- **Benefits** of **AI** in **test** systems

Example of ongoing work in MTS on „AI“ & „Testing“

Continuous Auditing Based Certification for MLOps (CABC)

Objective:
- Continuous and automated quality assurance of ML models during development and operation

Benefits:
- Proactive identification of potential risks;
- Compliance with quality characteristics;
- Regular analysis of system data;
- Ensuring the implementation of legal and normative requirements.

Source: Fraunhofer Focus: **Industrial Grade Machine Learning for Enterprises** (IML4E); https://iml4e.org/en/iml4e/cabc

Testing Test Methodology and Test Specification for ML-enabled Systems

Objective:
- Define quality attributes
- Describe general conditions of testing
- Describe test objectives and methods

Benefits:
- Unambiguous requirements for certifying trustworthiness
- Statement of test workflow
- Structurisation of testing processes during ML life cycle

Source: ETSI 103 910 V0.0.1 - Testing Test Methodology and Test Specification for AI-enabled Systems

Any further questions?

Contact me:

me@email.com