



ETSI White Paper No. 56

Unlocking Digital Transformation with Autonomous Networks

ETSI perspectives and major achievements

First edition – March 2023

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org



About the 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 Odi (HPE), Luca Pesando (TIM), Benoit Radier (Orange), Dario Sabella (Intel), Nick Sampson (Orange), Nurit Sprecher (Nokia)

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



Contents

About the authors	2
Contents	3
1. Executive Summary	5
2. Autonomous Networks	6
2.1. A View of Autonomous Networks	6
2.2. Autonomous Networks framework and principles	7
2.3. Common enablers	7
3. ETSI activities on Autonomous Networks	9
3.1. ISG Experiential Networked Intelligence (ISG ENI)	9
3.1.1. Purpose of ISG ENI	9
3.1.2. Status of the specifications	9
3.1.3. ENI Cognition Management and Automation of Resource Optimization	10
3.2. ISG Zero touch network and Service Management (ISG ZSM)	12
3.2.1. Use cases	12
3.2.2. ZSM Framework	12
3.3. ISG Network Functions Virtualization (ISG NFV)	17
3.3.1. ISG NFV and the role of AN	17
3.3.2. Use Cases	17
3.3.3. AN in the NFV architectural framework	17
3.3.4. Technical highlights	18
3.3.5. AN Future evolution/ perspectives	20
3.4. TC 'Methods for Testing and Specifications'	20
3.5. TC INT WG AFI (Autonomic Management and Control Intelligence for Self-Managed Fixed & Mobile Integrated Networks)	21
3.5.1. AN in the GANA framework	21
3.5.2. AN Future evolution/ perspective - New industry challenge	25
3.6. ISG "IPv6 Enhanced innovation" (ISG IPE)	26
3.6.1. Overview	26
3.6.2. New industry challenges	27
3.6.3. IPE AN architecture	28
3.6.3. Future Issues	29
3.7. ISG Multi-access Edge Computing (ISG MEC)	29



3.7.1.	Overview from Autonomous Networks perspective	29
3.7.2.	MEC use cases and requirements related to Autonomous Networks	32
3.8.	ISG “5th Generation Fixed Network” (ISG F5G)	33
3.8.1.	Overview	33
3.8.2.	F5G Use Cases related to AN	33
3.8.3.	F5G AN architecture and AN levels	34
3.8.4.	Key technical aspects related to AN	35
3.8.5.	Security	35
3.8.6.	Future evolution towards F5G Advanced	35
3.9.	ISG ‘Securing Artificial Intelligence’ (ISG SAI)	36
3.10.	Further key topics to address	37
3.10.1.	Security and privacy	37
3.10.2.	Testing framework and methodology	38
4.	Mapping of ETSI activities related to AN	40
5.	ICT ecosystem initiatives on AN	42
5.1.	ITU-T	43
5.2.	IETF and IRTF	43
5.3.	TMForum	43
5.4.	NGMN	44
5.5.	3GPP	44
6.	Recommendations	44
6.1.	Joint elaboration of work items in ETSI	44
6.2.	Knowledge Exchange among SDOs	45
6.3.	Perspectives and evolutions on Autonomous Networks	45
7.	Summary	45
8.	References	46
9.	List of Figures	50



1. Executive Summary

Autonomous Networks (AN) are considered one of the most important evolutions in order to enable Digital Transformation, offering new service opportunities and significant cost saving in network operation. It is one of the most attractive environments where to leverage Artificial Intelligence in the Network. By the way they are achieving momentum in Standards and ICT Industry. In this whitepaper, different works on autonomous networks are highlighted, which are implemented by current groups and committees of ETSI. The authors of this white paper represent some of the major companies and are directly involved in the ETSI projects (TC/ISG) related to AN, it is a deliverable of the Operational Co-ordination Group on Autonomous Networks (OCG AN). which monitors and looks to coordinate the ETSI's work on autonomous networks on a continuous basis. The aim is to present the status of AN standardization in ETSI, to point out achieved results, relevant trends and core topics, and to highlight the benefits of autonomous networks. In ETSI Autonomous Networks is not a dedicated ISG/TC but several ISGs/TCs delivered and are currently delivering recommendations and documents on AN, related to the ISG/TC scope, competences, and areas of excellence. That's why OCG decided to deliver this Whitepaper to report and present a comprehensive and synthetic view of AN in ETSI. So that in the current whitepaper, the focus is on Autonomous Networks approaches and associated boundary conditions of the following ETSI committees and groups:

Technical Committees (TCs):

- Methods for Testing and Specification committee (MTS)
- Core Network and Interoperability Testing (INT)

Industry Specification Groups (ISGs):

- Experiential Networked Intelligence (ENI)
- IPv6 Enhanced innovation (IPE)
- Multi-access Edge Computing (MEC)
- Securing Artificial Intelligence (SAI)
- Network Functions Virtualization (NFV)
- Zero touch network & Service Management (ZSM)
- Fifth Generation Fixed Network (F5G)



The contents of the document provide an overview of individual components and architectures for autonomous networks, as well as key metrics and quality criteria for fulfilling the functional requirements. In Chapter 3 a synthesis is reported organized by ISG/TC, outlining the most significant results achieved and in Chapter 4 a table reports progress and focus of the different ISG/TC organized by topics/ activities as follows:

- | | | |
|--|--|---|
| • Architecture / framework | • Self-X properties | • Proof of Concepts |
| • Cognition | • Intent-driven management | • ANs federation and Inter-AN coordination |
| • Analytics and intelligence (including AI topics) | • Policy Control Management Framework(s) | • APIs and data models |
| • Knowledge representation | • AN services, functions and resources Life-cycle management | • Robustness, trustworthiness, traceability |
| • Knowledge management | • Closed control loop automation | • Security/privacy |
| • Governance interface | | • Testing framework and methodology |
| | | • Metrics and KPIs |

A short not exhaustive picture of further standards initiatives on Autonomous Networks is reported to outline the importance of a coordination inside ETSI and with the other Fora to allow information sharing and prevent divergencies in recommendations and standards. Recommendations and future perspectives of Autonomous Networks like Network Digital Twin and Open API marketplace are suggested, as well.

2. Autonomous Networks

2.1. 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, among others, a capability to auto-discover operational information and act on it.

Based on publicly available material (for example [i.1]), an autonomous network can be considered as a network exhibiting the following 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 may vary, ranging from some low levels of automation capabilities to fully matured autonomous capabilities.



An autonomous network may be recursively composed of other autonomous networks, and it is responsible for the necessary interaction with and between them.

2.2. Autonomous Networks framework and principles

There are various models in the industry and the literature of Autonomous Networks. Figure 1 provides an example of a high-level illustration of the capabilities provided by an Autonomous Network connected with external entities via dedicated interfaces. The related enablers are described in 2.3. Common enablers.

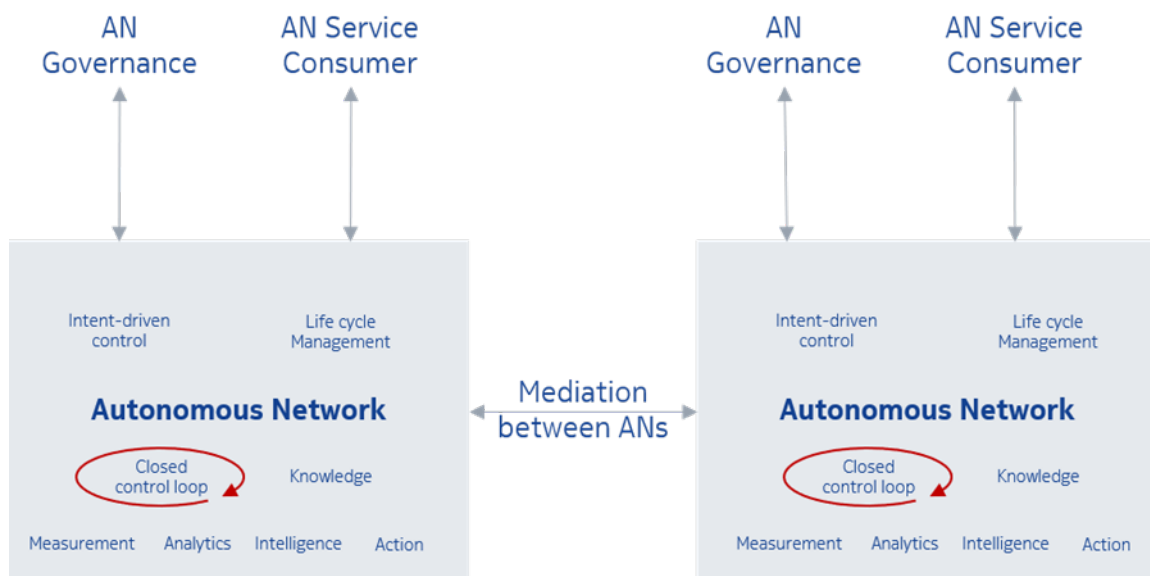


Figure 1: An example of a high-level illustration of Autonomous Networks' enablers and external interfaces

To increase the level of trust, an autonomous network should be reliable, and its automatic actions should be measurable, interpretable, and accountable.

2.3. Common enablers

After reporting some basics on Autonomic Behavior and Cognitive systems, we present here some key enablers of Autonomous Networks.

Enabling Automation and Autonomic Behavior: Autonomics is more than self-configuration, self-healing, self-optimization and self-protection. These benefits also require two key ingredients: self-awareness and self-knowledge. Autonomic systems require cognition, to gather information of the system and analyse, reason, learn and transform it into knowledge which enables change to be recognized in itself and the environment. Knowledge can be subsequently used with respect to its current goals, and the autonomic system can then comprehend how issued commands affect that situation.

Cognitive systems should be used to augment human decision-making and action processes. Cognitive systems are not meant to replace humans, but rather, enhance them. Therefore, for example, the ENI System operates in two distinct modes thanks to context awareness of the system under supervision: statistic, analytic, prediction even recommendation and command could be sent to manage entities. The former enables an Autonomous System to function as an assistant that analyze, interpret, reason, filter sensor information of the system and recommends actions to take. The latter enables an Autonomous System to function as a “super-orchestrator”, governing other management components (e.g.,



orchestrators, management systems, and controllers) and able to monitor and be contextually aware of the system to assure and trust that the system is reaching its goals.

To reach a full degree of autonomy, an autonomous network needs to be capable of solving complex problems under uncertain (sometimes hostile) conditions and adjust/produce effective (re)action plans.

An autonomous network may rely on the following enablers for its operation:

Autonomous Network governance interface: it allows interaction with the autonomous network to transfer the "autonomy-related" goals and expectations that will be under supervision. Furthermore, to enable the reporting of information about the behavior of the Autonomous Network with a proper level of abstraction. The AN Governance interface also supports the interaction with the life cycle management, encompassing the capability to dynamically adapt the level of control of autonomy (e.g., regaining manual control of the Autonomous Network operation in emergency situations).

Intent-based network control: allows the network to automatically validate, translate and interpret the operator's business intents (e.g., expectations and policy) for both network configuration and performance as well as derive and monitor a course of actions (e.g., provisioning) that deliver the desired outcomes.

Closed control loop automation: an autonomous network relies on closed control loops for its base operation. A closed control loop automation is a feedback-driven process. It seeks to reach and preserve a set of objectives without any intervention external to the specific loop. Closed loops (e.g., using the stages Observe, Orient, Decide, Act of the so-called OODA model) allow e.g., self-optimization, improvement of network and resource utilization, and automated service assurance and fulfilment. Several models of closed control loops exist, e.g., adaptive, cognitive, distributed, federated, hierarchical, open, peer. Further details can be found in references provided in section 4.

Closed control loop operation can happen at different levels. Multiple closed control loops can run simultaneously. There should be means for coordination/delegation/escalation between closed control loops as well as ways to steer or adapt their behavior.

Analytics and intelligence: mechanisms used to learn, reason, produce casualty analysis, predict, etc. It may work in uncertainty with epistemic (lack of knowledge) or aleatory (randomness/variability). Analytics uses can learn from collected information, identify patterns, and generate models for various optimization and classification tasks. AI/ML technologies may be used to support of learning (e.g., deep learning) and decision processes.

Knowledge: allows to abstract information from raw data. Semantic reasoning can be applied to derive knowledge and wisdom from the information.

Inter-AN mediation means: allows interaction between Autonomous Networks to support unified and consistent operations across Autonomous Networks. Note that Autonomous Networks interworking support multi-domain and multi-operator related use cases (e.g., network sharing, roaming, network slicing).



3. ETSI activities on Autonomous Networks

ETSI activities on Autonomous Networks refers to several Technical Committees and Study Groups, the following paragraphs report a synthesis of the most significant solutions and results delivered, including project focus and progress, architecture, case studies and future evolutions properly referenced to published/draft documents related to AN topics, grouped thematically. The paragraphs are authored by relevant experts of the TC/ISG, mostly Chairs or Vice-chairs.

3.1. ISG Experiential Networked Intelligence (ISG ENI)

The purpose of the ISG ENI is to define a Cognitive Network Management architecture that improves on the operator experience. Cognition is the process of acquiring and understanding data and information in order to produce new, data, information, and knowledge. A cognitive system is the “thinking part” of an autonomic system. Cognitive processes are used to understand how past behavior, coupled with currently ingested contextual data and information, affect the goals that the ENI System is trying to achieve. The operator experience is improved by adding closed-loop mechanisms (including AI functions) based on context-aware, metadata-driven policies to recognize and incorporate new and changed knowledge, and hence, make actionable decisions more quickly.

For the **ISG ENI**, the most recent work associated with this AN topic may be found in the following published Group Report:

- ETSI GR ENI 004 (V2.2.1): "Experiential Networked Intelligence (ENI); Terminology for Main Concepts in ENI"

3.1.1. Purpose of ISG ENI

The main objectives of ISG ENI are:

- To develop standards for a Cognitive Network Management system. Cognitive behavior is based on a set of closed control loops, which are extensions to the “observe-orient-decide-act” model that include the items „situation awareness“, „learning“, and „reasoning capabilities“.
- To adapt the real-time evolution of user needs, environmental conditions and business goals to determine which services should be offered during a given context.
- To quantify the Operator Experience by introducing metrics and an associated evaluation procedure.
- To provide a telemetry processing framework that uses context and situation awareness to learn and reason about which data should be collected using what types of processing mechanisms to support information collection and measurement about network performance, network resources and services.

3.1.2. Status of the specifications

The ETSI ENI Industry Specification Group was created in Feb 2017. According to the current snapshot, the members represent operators, vendors and research institutes all over the world. Release 3 is working on 11 Work Items, some of which are summarized as follows:

- **GS ENI-001v3.2.1** – Use Cases. Specifies additional use cases and scenarios that are enabled with enhanced experience through the use of network intelligence.
- **GS ENI-002v3.2.1** – Requirements. Specifies requirements for applying intelligence to the network and applications in different scenarios to improve service provisioning and network operation.



- **GS ENI-005v3.1.1** – System Architecture. Continues the development of GS ENI 005 v2.1.1 to:
 - define and specify APIs, Interfaces, and protocols used by ENI based on information and data models.
 - specify the ENI cognition model in detail.
 - enhance the description and specification of the ingestion, normalization, and output generation of data, information, and policies (imperative, declarative, and intent) in greater detail.
 - enhance the description and specification of the control loops used in ENI.
 - enhance the description and specification of policy management used in ENI.
- **GS ENI-019v3.1.1** – Representing, Inferring, and Proving Knowledge in ENI. Specifies the ENI information model. The information model also includes a novel policy model that represents imperative, declarative, and intent policies. Provides two different examples of how to derive technology-specific data models from the ENI information model. It explains how ontologies can be incorporated to augment, enhance, and specify meaning and relationships between modelled entities.
- **GS ENI-030v3.1.1** – Transformer Architecture for Policy Translation. Specifies how a transformer architecture can be used to translate input policies (which can be imperative, declarative, or intent) to ENI Policies for use in cognitive networking and decision making. The transformer-based architecture will be used to parse, understand, and translate text.

3.1.3. ENI Cognition Management and Automation of Resource Optimization

ENI Cognition Principles

The ENI Cognitive Management is based on an innovative cognition model. A cognition model defines how cognitive processes, such as comprehension, action, and prediction, are performed and influence decisions. The ENI cognition model draws heavily on how human cognition is performed. A cognition framework uses multiple diverse processes and technologies, including linguistics, computer science, AI, formal logic, neuroscience, psychology, and philosophy, along with others, to analyze existing knowledge and synthesize new knowledge.

ENI Cognitive Management learns from experience to improve its performance. This includes:

- acquiring new knowledge from instruction or experience
- revising and correcting existing knowledge
- combining existing data and information to infer and deduce new knowledge.

Cognitive Management enables the ENI System to understand normalized ingested data and information, as well as the context that defines how those data were produced; once that understanding is achieved, the Cognition Management then evaluates the meaning of the data and determines if any actions need to be taken to ensure that the goals and objectives of the system are met. This includes improving or optimizing performance, reliability, and/or availability.

Cognition Management is based on an enhanced version of the OODA control loop. Four enhancements to OODA were made. First, OODA was designed to apply to a single decision-maker. ENI's version is designed to accommodate collaborative decision-making. Second, a dedicated planning stage was inserted between the orient and decide cycles. This was done to accommodate situation awareness. Third, learning was inserted to monitor all phases of each control loop. Fourth, policy management is



used to make each function in the ENI cognition loop configurable using a standardized set of commands. This is shown in Figure 2.

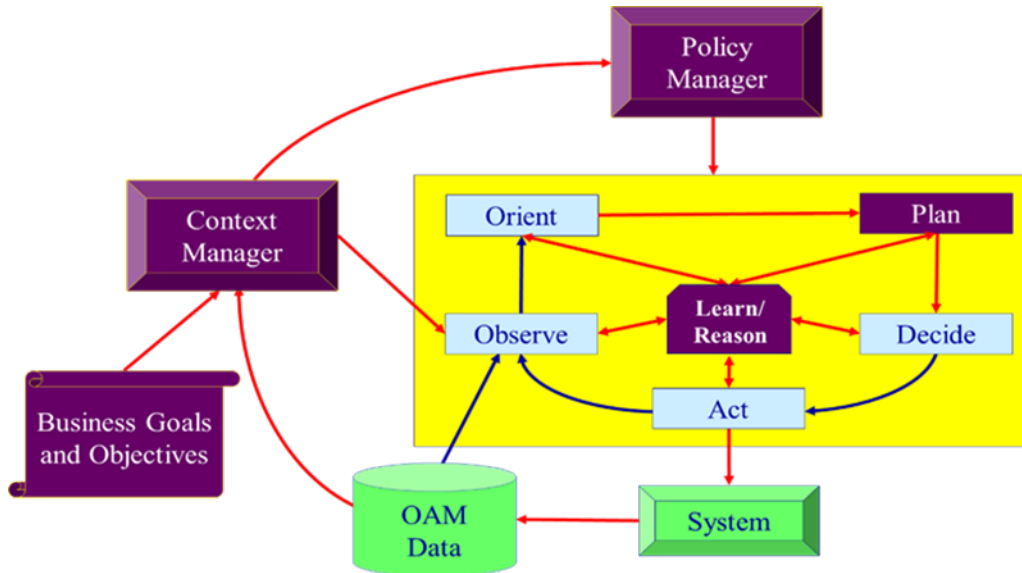


Figure 2: Simplified ENI Cognition Closed Control Loops

The "Observe" part ingests current information from the system being monitored, as well as relevant contextual, situational, and historical information. The "Orient" part analyses, evaluates, and prioritizes information. The "Plan" portion considers different types of responses and their ability to realize system goals. The "Decide" portion defines corrective actions using a model-driven engineering approach; its results are packaged as a set of Policies. These are then sent to the system being managed by the API Broker. Learning and reasoning functions will then compare this and other actions to see if the collected set of actions were the optimal responses that could be taken.

ENI Cognition Management

The Cognition Management mimics some of the processes involved in human decision-making to better comprehend the relevance and meaning of ingested and historical data. Critically, a system that uses cognition shall be able to explain why it acted a certain way in response to stimuli, and more importantly, can learn whether that action was incorrect and, if correct, whether it was optimal.

The Cognition Management uses existing knowledge to validate and generate new knowledge. This means that new knowledge may be added, and in some cases, existing knowledge may be changed. Hence, the ENI System uses a dynamically changing set of repositories (as opposed to other management systems, which typically use repositories that use fixed content).

Enhancing the Operator Experience using ENI Cognitive Management

Operators must manage services provided by the network (e.g., streaming multimedia or call quality) in increasingly complex networking environments. This is exacerbated by new technologies deployed in new applications, including the Internet of Things, 5G, telehealth, Smart Cities, and communications over multiple media. Networks are now a software-driven fusion of virtual and physical networks that may have different Key Performance and Quality Indicators, and even different Service Level Agreements, under different conditions.



3.2. ISG Zero touch network and Service Management (ISG ZSM)

The ETSI ZSM (Zero-touch network and Service Management) group was formed in December 2017 with the goal to define a future-proof, end-to-end operable framework and solutions and key automation technologies to enable agile, efficient, and qualitative management of emerging and future networks and services. The ultimate target is to achieve the highest degree of automation (->100%) and enable fully autonomous network operation. Such autonomous networks will be able to self-manage and self-organize (configuration, healing, assurance, optimization, etc.) without human intervention.

3.2.1. Use cases

In ETSI GS ZSM001, the ISG ZSM examined many business-oriented scenarios and the related automation challenges faced by operators and vertical industries. Subsequently, the team specified the architectural, functional, and operational requirements for end-to-end network and service automation.

3.2.2. ZSM Framework

The ISG ZSM framework developed a novel end-to-end architecture framework and enablers designed for self-management, closed-loop automation and optimized for data-driven artificial intelligence solutions. The ZSM framework (depicted in Figure 3 and specified in ETSI GS ZSM 002) is versatile and built on service-based principles offering scalability, modularity, extensibility, and flexibility. It supports the transfer of autonomy from the operator to the network using intent-based interfaces. The framework provides capabilities to integrate AI-based functionalities and enable closed-loop automation.

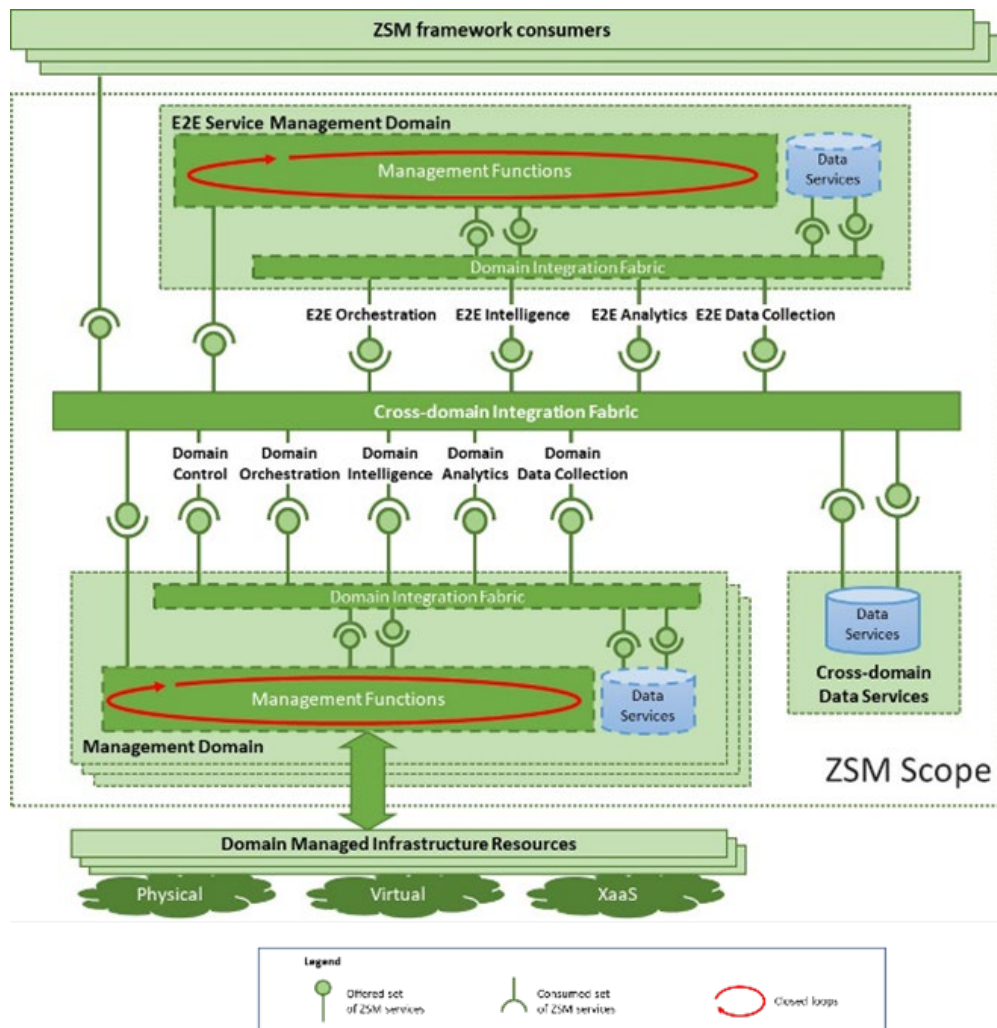


Figure 3: ZSM Framework

The framework supports the separation of management and automation into areas of concern, i.e. management domains (where the scope is delineated, for example, by an administrative or technological boundary, such as Radio Access) and end-to-end cross-domain service management domains. Each management domain is responsible for the fulfillment and assurance processes within its scope. The separation of concerns allows the abstraction of the complexity of the management domains.

The ZSM framework supports open interfaces as well as model-driven service and resource abstraction. The management services, which are exposed by the management domains, are described and specified. The architecture allows operational data to be kept separately from the management applications, enabling rapid and efficient access to current, real-time management data within and across the management domains to support the automation processes.

Closed loop

The ZSM framework is designed to enable adaptive, closed-loop automation – providing a feedback loop (depicted in Figure 4) between data monitoring, data analytics, decision-making and adaptive actions that aim to reach and preserve a set of objectives without external intervention. A closed loop enables the continuous optimization and adaption of network and resource utilization and automated service



assurance and fulfilment. The automated decision-making mechanisms can be bounded by rules and policies. Advanced machine learning and artificial intelligence can empower the closed-loop operation.

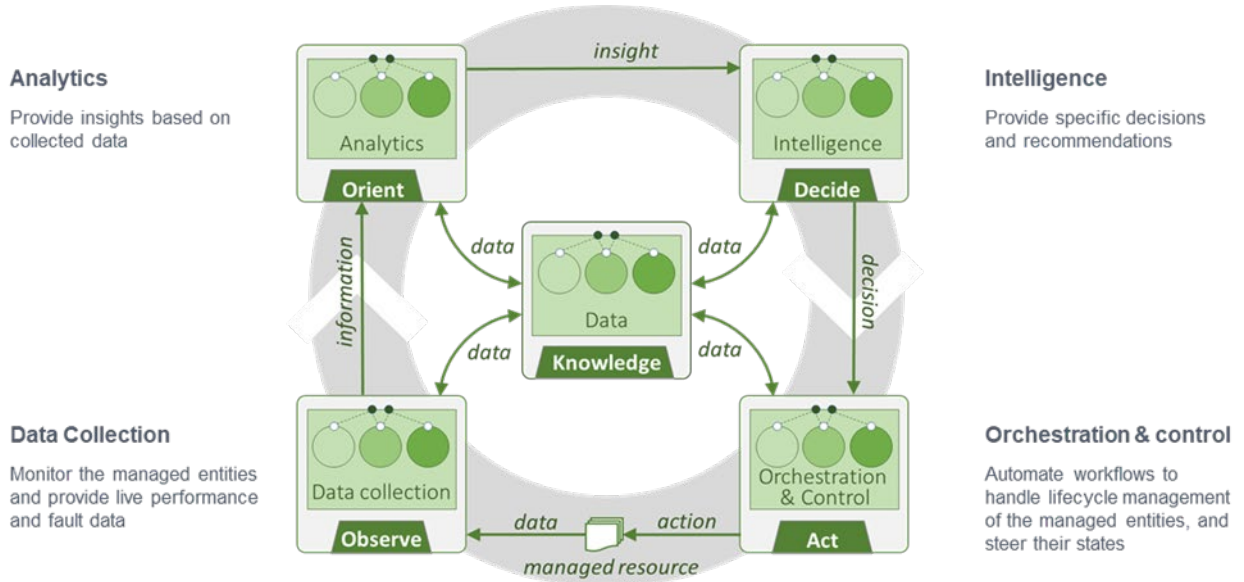


Figure 4: Closed loop example

ETSI GS ZSM009-1 on closed-loop automation enablers specifies “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. The “Governance” services also support interaction between closed loops and external entities, such as human operators, allowing them to supervise the operation and performance of closed loops. As more automation and closed loops are deployed and start to operate safely/efficiently, human trust will increase and the requirement for a level of supervision/visibility will diminish.

In , closed-loop operation can be implemented at the management-domain level. Closed-loop operation can also occur at the end-to-end service-management domain level and can span multiple management domains. Multiple closed loops can run simultaneously.

ETSI GS ZSM 009-1 provides capabilities to support coordination, delegation and escalation between closed loops while ensuring intelligent, consistent and coherent service delivery. Coordination between loops is essential when there is dependency between their operations or when they can adversely interfere with each other. It can also help to improve their operations and fulfill their goals, for example by sharing information produced by the different closed-loop stages.

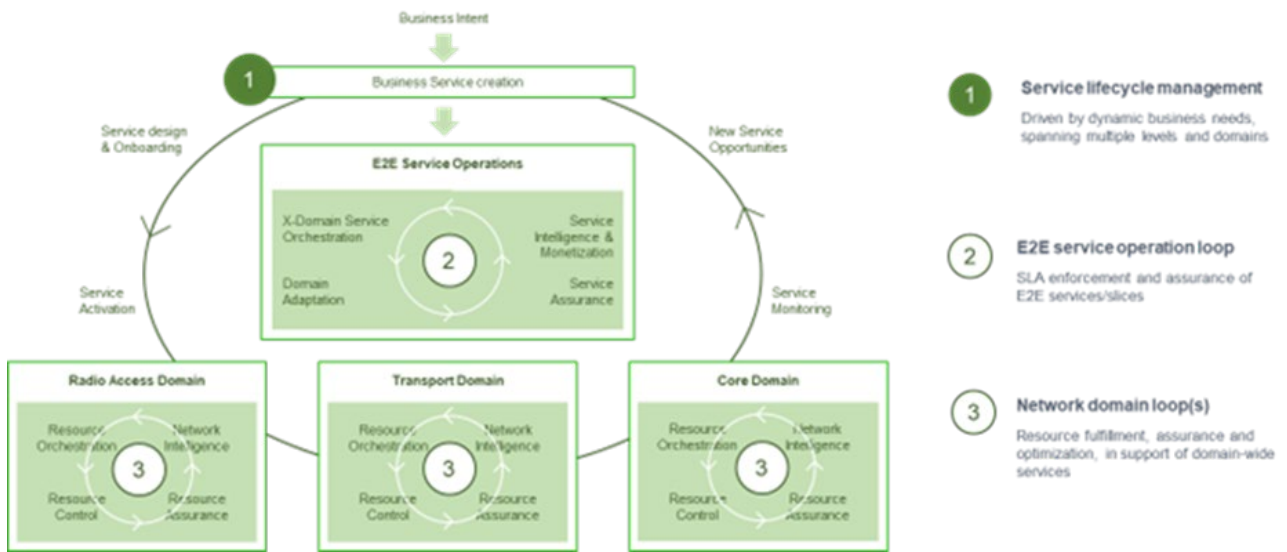


Figure 5: Intelligent, coherent, and interconnected loops across business, service and network management domains

This specification also enables the delegation and escalation of respective goal(s) between superior and subordinate closed loops. A superior closed loop can delegate respective goal(s) to the subordinate closed loop(s), e.g., by setting the policies and/or the intents that allow the subordinate closed loop to act autonomously. A subordinate closed loop can escalate goal(s) to the superior closed loop in a situation, for example, where it is not able to achieve the goal(s) assigned to it. Escalation and delegation support the separation of management and automation into different autonomous areas of concern (end-to-end cross-domain service operations, management domains), where each is responsible for assurance and intelligent automation within its scope.

Intent

The ZSM group has developed a report on intent (ETSI GR ZSM011). Intents express declaratively all the operational expectations an autonomous management domain needs to fulfill and assure, including requirements, goals, and constraints. The report proposes additional management capabilities and services to support intents and their life-cycle management and recommends whether existing intent models and semantics can be leveraged. It also suggests how conflicting intents can be handled. The results from the study will provide the basis for a new normative specification. A report on this is available for approval.

AI enablers

The group focused on specifying additional management capabilities to enable full AI operations within the ZSM framework (ETSI GS ZSM012), ensuring support for deployment diversity. The specification is ready for approval.

These AI enablers include capabilities to:

- access 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, ensuring a consistent and holistic operational view and the means to act on it. AI applications can collaborate in learning different tasks or contribute collectively to solve a common problem;
- trigger an action based on the AI output to support closed-loop automation. Understanding the output is important for correctly applying the decisions/recommendations;



- govern and supervise the AI-empowered operations. AI results must be reliable, measurable, interpretable, and accountable. The AI applications should adhere to applicable laws, regulations, ethical principles and values as well as be robust against adversarial threats and missing or erroneous data;
- express requirements and constraints for the deployment of AI applications.

End-to-end service/slice lifecycle management

ETSI ZSM 008 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) and describes the interactions between E2E service management domain and other management domains. Furthermore, ETSI ZSM 003 focuses on the E2E aspects of network slice management, supporting vertical use cases.

ZSM security

The threat surface in the ZSM environment is extensive, firstly due to the openness of the framework. Protecting the interfaces and the management services within and across the domains is essential to ensure the trustworthiness of the framework.

In addition, the ZSM services can be produced and consumed by new players from diverse domains (e.g., government, vehicle industry, energy, transport, etc.). Each player may require different trust levels according to its own deployment/execution environments, security policies and regulations. This variety demands flexible and adaptive security control.

Furthermore, the ZSM framework leverages emerging technologies, such as AI/ML, data lake, cloud, etc., which introduce new vulnerability to attacks and impose additional security requirements. For example, it is necessary to ensure trustworthiness and shield the AI/ML algorithms from highly sophisticated, creative, and malicious attacks, including abuse, trolls, data poisoning, and model rescue. Moreover, it is critical to protect data, ensuring its integrity, confidentiality, and availability, and to preserve privacy to comply with security laws and regulations. At the same time, the ZSM framework can take advantage of these emerging technologies to increase security management efficiency. For example, using AI/ML-empowered analytics to trigger actions can help to automate security monitoring and a real-time response to incidents.

ETSI ZSM010 presents a comprehensive security study identifying and analyzing potential security threats and assessing the related risk scores and priorities. It proposes mitigation options, countermeasures, and security controls to address the threats and risks to the ZSM framework and solutions. The ZSM group is working to specify requirements and security capabilities (ETSI ZSM014) to support the automatic security assurance of the ZSM framework, management application and services.

ZSM PoCs

ZSM PoCs demonstrate the viability of the technology. The list of current ZSM Proofs of Concepts (PoCs) can be found [here](#).

Network Digital Twin

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



It can also identify risks that could jeopardize the normal operations of the system.

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 GR ZSM015 will outline recommendations of additional capabilities needed in the ZSM framework to support Network Digital Twins.

3.3. ISG Network Functions Virtualization (ISG NFV)

3.3.1. ISG NFV and the role of AN

The ISG NFV develops specifications and reports aimed at simplifying the industry transformation and the development of an open, interoperable, ecosystem enabling software-based deployment and automated lifecycle management of virtualized network functions on independently deployed and operated NFV infrastructure platforms. In this context, automation is key to NFV widespread adoption by the industry. The seminal NFV White Paper published in 2012 highlighted that “NFV will only scale if all management and orchestration of the functions can be automated”. The NFV Management and Orchestration (NFV-MANO) system natively provides a basic form of automation to due to its template-driven nature and a policy-based management framework. Autonomous Network (AN) techniques can be leveraged to provide a higher level of automation to satisfy increasing expectations for operational agility and efficiency.

3.3.2. Use Cases

ETSI GR NFV-IFA 041 , the Group Report on enabling autonomous management in NFV-MANO, identifies three categories of use cases that can benefit from AN techniques: Intent-based Network Service (NS) management, Management Data Analytics (MDA) assisted management and Autonomous container infrastructure management. Use cases in the MDA category include:

- Network service alarm incident analysis
- Network service health analysis
- Network service resource utilization analysis
- Cross administrative domain management data analytics
- Cross management domain data analytics (e.g., between NFV-MANO and other OSS/BSS functions)

Furthermore, ETSI GR NFV-REL 013, the Group Report on cognitive use of operations data for reliability, identifies several use cases to determine the levels of cognition that apply to scenarios such as service availability assurance, root cause analysis and anomaly prediction. In the context of cognitive management, NFV systems can significantly benefit from predictive maintenance to avoid service perturbation or disruption.

3.3.3. AN in the NFV architectural framework

ETSI GR NFV-IFA 041 recommends that the NFV architectural framework be augmented with two new functions: The Intent Management (IM) function and the Management Data Analytics (MDA) function. Figure 6 provides a simplified representation of the integration of these functions in the NFV architectural framework.

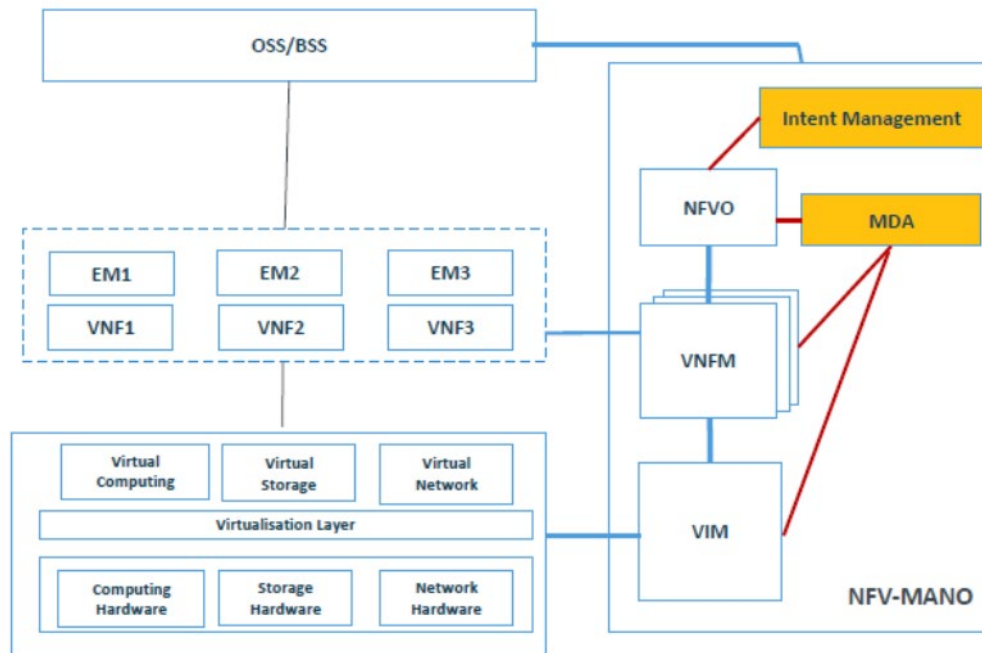


Figure 6: NFV-MANO architectural framework with IM and MDA functions

3.3.4. Technical highlights

Intent Management (IM): IM functions are used for expressing goals and requirements related to management of Network Services. Intent-driven management of network services aims at simplifying information exchange with NFV-MANO consumers (e.g., other OSS/BSS functions). Consumers do not need to have a deep knowledge of NFV-MANO data models, but just communicate their expectations and goals to NFV-MANO in terms of NS functionality and performance metrics. An IM function consumes the interfaces offered by the NFVO, such as NS descriptor management, NS lifecycle management, NS performance management, NS fault management, NS FM and VNF package management.

Main applicable deliverables:

- ETSI GR NFV-IFA 041 “Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Report on enabling autonomous management in NFV-MANO”.
- ETSI GS NFV-IFA 050 “Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Intent Management Service Interface and Intent Information Model Specification”.

Management Data Analytics (MDA): The MDA function leverages Artificial Intelligence (AI) and Machine Learning (ML) techniques. The MDA function is responsible for processing and analyzing management data to provide analytics reports upon requests from a consumer (e.g. an NFV Orchestrator). It brings intelligence and automation to NFV-MANO. The closed-loop decision making capability of NFV-MANO can be improved by communicating with the MDA function, which results in reduced on-demand management operations initiated by the OSS/BSS and increased self-detection and/or self-recovery operations.



Main applicable deliverables:

- ETSI GR NFV-IFA 041 “Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Report on enabling autonomous management in NFV-MANO”.
- ETSI GS NFV-IFA 047 “Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Management data analytics Service Interface and Information Model Specification”.
- ETSI GR NFV-REL 013 “Network Functions Virtualisation (NFV) Release 4; Reliability; Report on cognitive use of operations data for reliability”.

Policy Management: Policy-based management is one of the key enablers for constructing flexible management and orchestration functions in the NFV-MANO architecture. Assisted with policies, NFV-MANO functions can be provided with more automatic characteristics which fit in with the dynamic requirements of resource management and network service orchestration in the virtualized network environment. NFV-MANO policies are mainly applicable to NFV-MANO reference points to assist for corresponding NFV-MANO functions like NS lifecycle management, VNF lifecycle management or resource management. Policy information can be transferred using the policy management interface on all reference points of the NFV-MANO architecture.

Main applicable deliverables:

- ETSI GS NFV-SOL 012 “Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; RESTful protocols specification for the Policy Management Interface”.
- ETSI GR NFV-IFA 042 “Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Report on policy information and data models for NFV-MANO”.
- ETSI GR NFV-IFA 048 “Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Policy Information Model Specification”.

Closed loops: The NFV framework can participate in closed loop automation, for both internal closed loops to NFV-MANO, as well as external closed loops that traverse different management and orchestration layers, including NFV-MANO. For the NFV domain, closed loop automation follows the following main functional, and often circular, steps: monitoring and management data collection (as input), execution of actions (output), and any number of analysis and decision-making steps as needed in between. The closed loop automation logic and processes can involve any element of the NFV architectural framework, as well as the orchestration and management layers above NFV-MANO, or combinations of both. NFV-MANO enables closed loop automation via rule-based auto-scaling and auto-healing, via the new IM and MDA functions augmenting the decision capabilities of the closed loops, as well as by leveraging native capabilities for autonomous container infrastructure management, embedded in the Container Infrastructure Service Management (CISM). This closed loop automation concept in the NFV domain is illustrated in Figure 7.

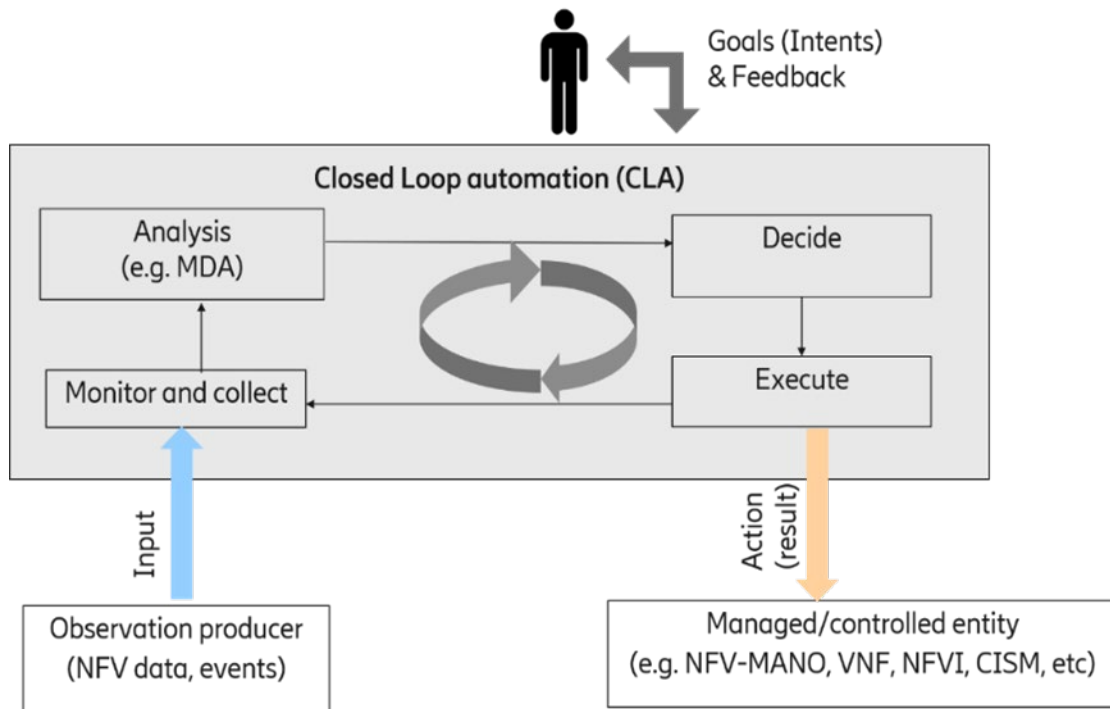


Figure 7: Closed loop automation in the NFV domain

3.3.5. AN Future evolution/ perspectives

In line with its mission to facilitate the development of an open ecosystem for NFV, it is expected that the ISG NFV will develop the specifications of the APIs exposed by the IM and MDA functions (or will profile specifications developed by external organizations) as well as the associated interoperability and conformance testing specifications. Furthermore, delivering the specifications of an operational and secure solution will require addressing the security implications of using AN techniques in the management of virtualized network services.

3.4. TC 'Methods for Testing and Specifications'

In general, the Technical Committee "Methods for Testing and Specification (MTS)" focuses on the evaluation of available methods and techniques for the advanced and/or formal specification of standards with respect to efficiency, quality, and testability. In this context, the working groups of the committee address methods for the specification of standardized tests, including formal definition languages and the definition of proformas. Building on this, the group deals with requirements for the test environment, with operational and procedural aspects as well as with methods for generating, executing, processing, and verifying tests and analyzing the corresponding results.

In cooperation between INT and MTS, requirements have been developed, particularly regarding testing autonomous systems, also with a view to artificial intelligence.



3.5. TC INT WG AFI (Autonomic Management and Control Intelligence for Self-Managed Fixed & Mobile Integrated Networks)

The ETSI TC INT AFI WG initially started as an ISG that succeeded in producing the Generic Autonomic Network Architecture (GANA) framework and scenarios, use cases and requirements for autonomic/self-managing future Internet [INT 11]. The ETSI ISG AFI then transformed from pre-standardization (i.e. an ISG AFI) into a technical committee (i.e. ETSI TC INT AFI) ETSI GANA Framework [INT 9] onto diverse network architectures and associated management and control architectures.

ETSI TC INT AFI provides landscape for Autonomic cognitive Management and Control (AMC):

- GANA Reference model [INT 9];
- Implementation guide for GANA reference model [INT 2] [INT 6];
- GANA instantiations reports onto various reference network architecture and its management and control architectures defined by standardization developing organizations such as 3GPP [INT 3], BBF [INT 12], IEEE [INT 4], ITU-T, NGMN [INT 10];
- Testing and trust reports of AN [INT 10] [INT 8].

3.5.1. AN in the GANA framework

ETSI TC INT AFI has produced the GANA framework [INT 9]; GANA Implementation Guide [INT 2] and instantiation reports [INT 3] [INT 4] onto various types of reference network architectures and their associated Management and Control Architectures.

Figure 1 depicted the GANA framework snapshot of the Multi-Layer Autonomics' cognitive algorithms Management and Control (AMC) architecture and the levels of Decision making Element (DE) (abstractions of self-management functionality). DE 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.

As depicted in GANA Model diagram, Time-scaling and Abstraction Levels for Control-Loops Designs and Implementation are addressed (including how they complement each). GANA provides insights on how “Fast Control-Loops” and “Slow Control-Loops” complement each other.

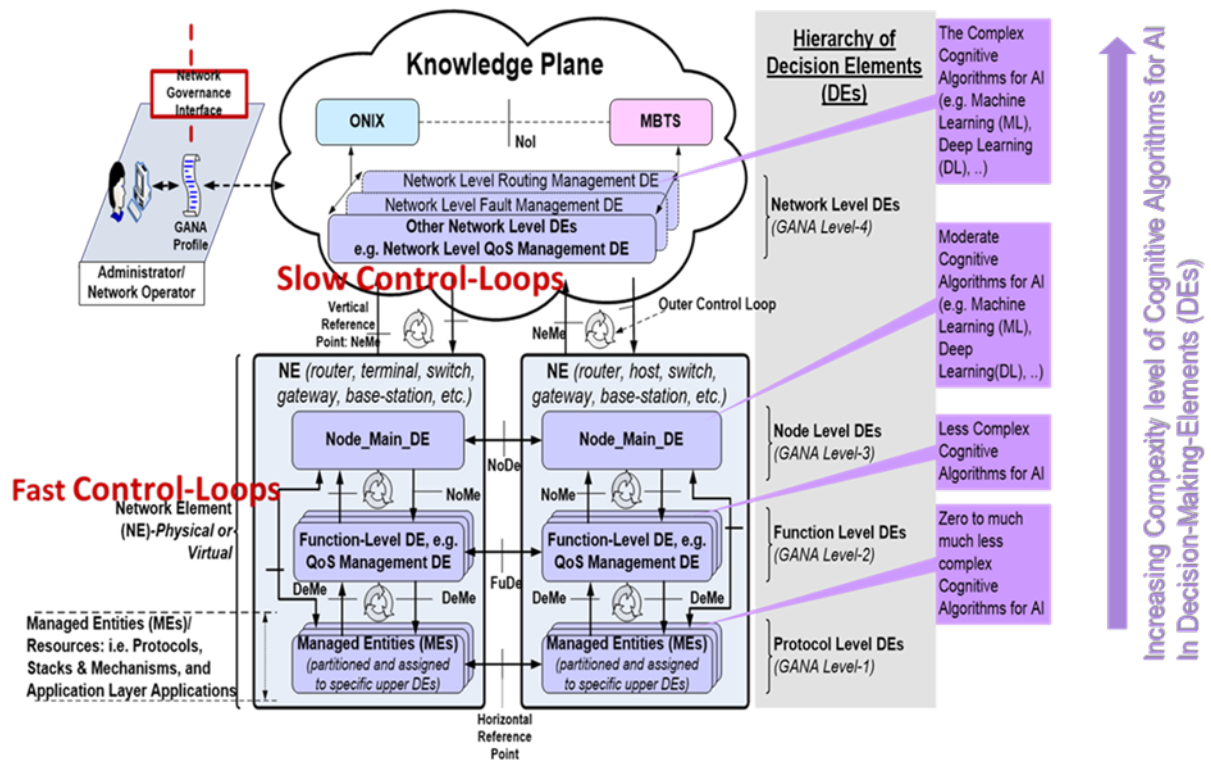


Figure 8: Snapshot of the GANA Reference Model and Autonomics Cognitive Algorithms for Artificial Intelligence (AI), and illustration of the notion of increasingly varying complexity of AI/ML from within a Node Element up into the Knowledge Plane level

The three key Functional Blocks of the GANA Knowledge Plane are summarized below (in reference to Figure 8):

- **Hierarchical GANA Level DEs:** GANA KP and its associated **Network-Level 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 DEs 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 AMC (the "Macro-Level" autonomics).
- **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 could be used to find information from data lake, data warehouse database like a data hub.
- **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. Network-Level 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-manage and control their embedded DEs. 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 to design Network-Level DEs to talk a language that is agnostic to heterogenous vendor specific NEs.

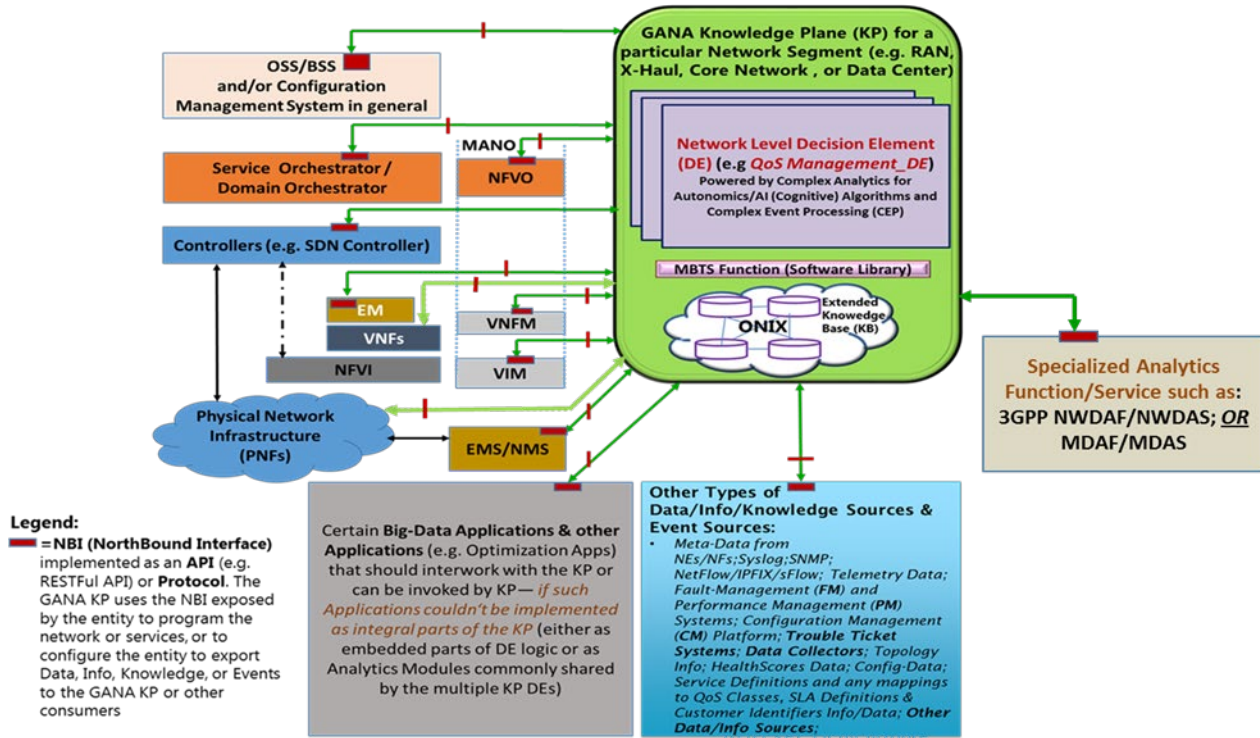


Figure 9: Platform Integration with other Systems

Further elements of GANA framework provided by TC/INT AFI WG:

Policy management Framework by which various inputs and methods can be used to govern the AN as described in [INT 1] and [INT 9] and validated in [INT 6]. As well how legacy management architecture could be govern and upgraded to an autonomic network. A GANA Profile is the composite structure that is meant to encapsulate Goals, Intentions and Policies generated and validated as Conflict-free Policies by Automated Management Tools that can be supplied by the Human Operator. Against this background, new policies can be decided and supplied as input at any point in the network operation to reach network Goals according to network behaviors.

Then addresses the subject of “Dynamic Policies” generated and applied by GANA DEs during their operations, what constitutes the autonomic behavior. The **Policy management** Framework provides Reference points and functions within the GANA Framework to address Stability of Vertical DEs (from business to manage entities) and Horizontal DEs (between different administrative network domains e.g. access, backhaul, core network, backbone) for different self-X properties in the Context of the GANA Architecture for synchronization of actions and policies.

Self-X properties which could be used for different use cases [INT 1] to avoid having one DE designed per Use cases [INT 9] such as those listed below:

- Self / Auto Discovery: this property relates to the ability of an AN to automatically and autonomously discover resources, assets, and services by locating, identifying, and leveraging on them in its ecosystem;



- Self-configuration: this property relates to the autonomic capability of an AN to configure and govern any parameters or settings which relate to functions, services, DEs or assets that make up or relate to the AN;
- Self-healing, Self-repair: this property relates to the capability of AN to fix anomalies after detecting them and to get back to a normal fully operational mode through a process of automated steps;
- Self-awareness: this very important property of ANs relates to cognitive-like awareness regarding several dimensions such as context information, time, SLAs, KPIs, environment (peer networks, entities, performance, load, threats and security, etc.);
- Other Self-X properties defined in the ETSI documents include: Self-monitoring, Self-security (against attack), Self-Generic and control plane, self-forwarding, self-routing, self-mobility and Self-organisation of DEs within the Radio Access Network.

Level of cognition with regards to GANA Multi-Layer Autonomics [INT 9] [INT 1]. The concept involves “Cognitive GANA DEs” and Cognition Modules designs approaches for GANA DEs. The document differentiates between types of GANA DEs that may need to be “Non-cognitive” and those that must be cognitive. In the DEs Hierarchy of the GANA “Decision Plane”, a concept of “degree of cognition” has been defined and the degree of cognition increases up the so-called Decision Plane Hierarchy. Moreover, the **TC INT AFI WG** designed a marketplace for GANA DEs and implications for Stakeholders involved in design, procurement, test and certification of DEs and other stakeholders of the ecosystem [INT 6 WP#5].

Level of Autonomy/Autonicity:

The **TC INT AFI WG** provides degree of Autonomy in association with Maturity Levels for Autonomy that are increasingly attained by an 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. The expectations on an AN 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 AN without direct human involvement in the decision and actions" [INT 10]. In this context, two Dimensions for Autonomics Evolution to maximize the property of being “autonomous” are described [INT 9].

Stability and Coordination of Autonomic Functions (AFs) and their Control-Loops

The issue of Stability of interacting control-loops has been well depicted on the GANA Model. The GANA Framework brings Techniques for Addressing Stability and Coordination of Autonomic Functions (AFs) and their Control-Loops. Techniques include Design for Stability Principles and Run-Time Stability Principles for Coordination, Synchronization, and Orchestration among DEs, i.e. techniques for addressing Stability of Control-Loops and Coordination of Autonomic Functions (e.g. GANA DEs) [INT 6] [INT 9].

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
- Autonomic-aware Metrics to Infer and Self-assess Stability by the AN on its own
- Concept of man in the loop to validate and trust decision



- Stability Issues in Autonomic Networking (AN) by design through Analytical Methods, Game Theory - From Theory to Theory.

3.5.2. AN Future evolution/ perspective - New industry challenge

The behaviors of GANA DEs are called self-* features because humans are relieved from having to perform the traditionally manual management-oriented tasks, and software, i.e. the DEs, automate the tasks and dynamically perform the tasks based on human specified networking goals and policies, context or state changes, and events detected in network nodes as well as the network. A DE should receive as input network goals or governance policies specified by the human operator, and also discover automatically other DEs. The DE requires DE to DE collaboration, and the capabilities of its assigned MEs before the DE starts performing the self-* operations it is designed to perform. Such DE behaviours should be performed by individual DEs embedded in NEs (for self-management that are driven by local reactions within the NE).

Horizontal (distributed) DE-to-DE collaboration: Some DE algorithms may require the collaboration of a DE within an NE with other DEs along an end-to-end (E2E) path in the network, involving hop-by-hop NEs, for a self-* operation (e.g., self-optimization) that may require the collaboration of distributed DEs along a path in the network.

Vertical (Hierarchical) DE-to-DE collaboration: Another possibility is that for actions of an NE, DEs may also need to be synchronised by higher level autonomic behaviours coordinated by upper layer DEs (inside and outside the NE) at the GANA Knowledge Plane (KP) level. Concept of GANA KP enables advanced management & control intelligence at the Element Management (EM), Network Management (NM) and IT System (BSS/OSS) levels by interworking with them or enhancing and evolving the intelligence of the systems at these levels by way of replaceable and (re)-loadable autonomies modules (DEs) that can be loaded at specific abstraction levels of management and control operations [INT 2] [INT 6]. The GANA KP concept is inherited from the GANA KP concept defined in [5] as a pervasive system within the network that builds and maintains high-level models of what the network is supposed to do, in order to provide services and advice to other elements of the network. As illustrated in Figure 9, GANA KP's DEs should be complementarily designed to collaborate with DEs at lower layers of the GANA model.

The ETSI NTECH AFI WG fused a number of leading autonomies efforts/models, including Research Project and SDOs architectures and other models, as a unified GANA reference model for AMC [INT 9]. This subject, on how concepts from the various models are unified and fused together (accommodated) in GANA is discussed in [INT 6].

The following two categories determine the actors or players the GANA model is addressing:

Category 1: Suppliers (vendors) of GANA Functional Blocks (FBs): The suppliers can be further categorized as follows, bearing in mind that DE algorithms, just as in the case with Self Organizing Network algorithms [INT 5 White Paper #1], may not be standardized as they should provide the means for DE vendor differentiation so as to facilitate for DE vendor differentiation (and actually there is a need to promote continuous innovation in autonomies algorithms):

- Independent developers of software components and algorithms for autonomies from the research community (research institutes, universities, etc.);
- ISVs (Independent Software Vendors) e.g., OSS (Operations and Support Systems) vendors ☐
Traditional networking equipment vendors;



- Network operators who may have software development capabilities may develop some DEs on their own and load them into nodes (provided this can be supported by the host platform or operating systems) and/or in the GANA KP Figure 9.

Category 2: Provider of assets required by the developers of GANA FBs Perspectives on such assets are as follows:

- GANA presents a framework to design self X GANA FBs required at various GANA levels of abstraction for self-management functionality. The section on the implementation guide for GANA and [INT 6] discuss the subject of how to implement, step-by-step, autonomies at various levels of abstractions defined by the GANA model and developed within PoCs [INT 5]. The GANA specification and other assets described in the section on the implementation guide for GANA constitute useful input required by developers.
- Developers should perform the steps described in the section on the implementation Guide for the GANA, while interacting with ETSI NTECH AFI WG on implementation guidance and help to close gaps in the autonomies standards and the frameworks.

Joint cooperation within ETSI in the future:

There are ongoing discussions on working together in a Newly Launched Work Item in TC INT on developing, i.a., the “Industry Implementation Framework/Guide on Autonomic/Autonomous IPv6 based 5G Networks: powered by ETSI GANA Multi-Layer Autonomics & Multi-Layer AI-Algorithms and IPv6 Capabilities”. In this context it is envisaged to launch a PoC Program on: “Industry Implementation Framework/Guide on Autonomic/Autonomous IPv6 based 5G Networks: powered by ETSI GANA Multi-Layer Autonomics & Multi-Layer AI-Algorithms and IPv6 Capabilities.

3.6. ISG “IPv6 Enhanced innovation” (ISG IPE)

3.6.1. Overview

ISG IPE¹ is promoting IETF IPv6-based protocols and developing use cases, and guidelines for IPv6 deployment, fulfilling this high-priority industry need.

In the 5G and Cloud era, IPv6 fundamentally solves the problem of global IPv4 address depletion. Emerging businesses, such as automatic driving, industrial automation, immersive services (e.g. VR/AR), Internet of things, etc., need massive, high-quality, and smart connections, which requirements for IPv6 enhanced innovation with enhanced network experience assurance, and network automation & intelligence.

¹ ISG IPE expired January 18th, 2023 - ISG working documents will remain available to the ETSI membership on the ETSI Portal through the closed bodies’ area (archives).

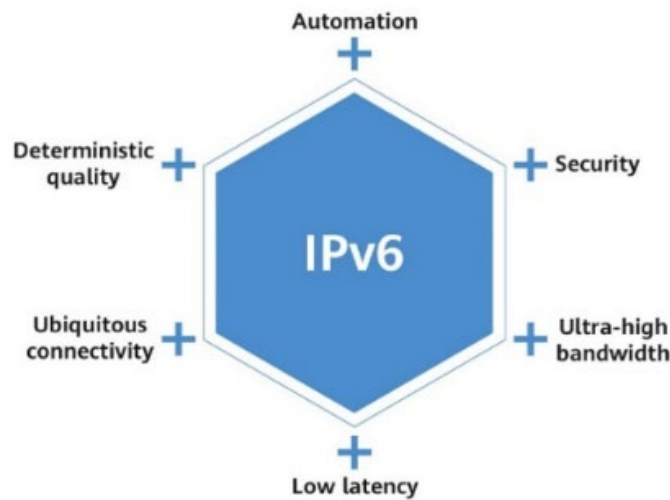


Figure 10: Six key features of IPv6 Enhanced Innovations (from Figure 4 of ETSI GR IPE 001 [1])

Automation is one of the six key features identified by IPE: In a concrete use case, new services make requests to a network to support fast service provisioning and provide faster and more reliable self-healing capabilities to cope with possible network faults in several minutes. The network needs to be able to recover from failures in a short time to reduce the impact on services. Constantly increasing network scale and complexity may not be sustainable without a new level of automation. The possibility provided by IPv6 to have e2e connectivity visibility and management of its entire lifecycle provides a great opportunity to simplify the automation mechanisms and their effectiveness with respect to the IPv4 network with multiple levels of Network Address Translation (NAT) and multiple protocols utilized to complete each connection.

3.6.2. New industry challenges

- Connectivity has major challenges from the emerging scenarios, where the applications are located remotely in respect to the utilizer. In particular, Industrial applications and services of public utility, like „Unmanned Industry“, „Smart Cities“, „Health Care“, and „Autonomous Driving“ to mention some. The automation of the whole connectivity lifecycle (e.g., creation, monitoring and troubleshooting) is of major importance to grant the following requirements: Guaranteed performance: Predictive behavior is necessary to grant service SLA preservation.
- Security: IPv6-related protocols have been defined with security as a high priority, unlike IPv4 which has been patched over time. In addition, Autonomous e2e connection configuration and management avoid human mistakes leading to security problems as well as intentional misconfiguration (man in the middle).
- Agility: coordination between the integrated resource management and operation systems should be implemented to ensure that the setup and configuration of the connections run smoothly without any mismatch. E2E automation is fundamental to offer proper service lifecycle adaptability to end-user needs.



3.6.3. IPE AN architecture

ETSI GR IPE 002 [2] highlight the need for a functional orchestrator to coordinate the controller in different domain of the IP network in order to achieve a fully automated service lifecycle.

This architecture enables the following characteristics to be ensured: performance, security, flexibility, and scalability, matching the paradigm of Cloud computing from the transport side.

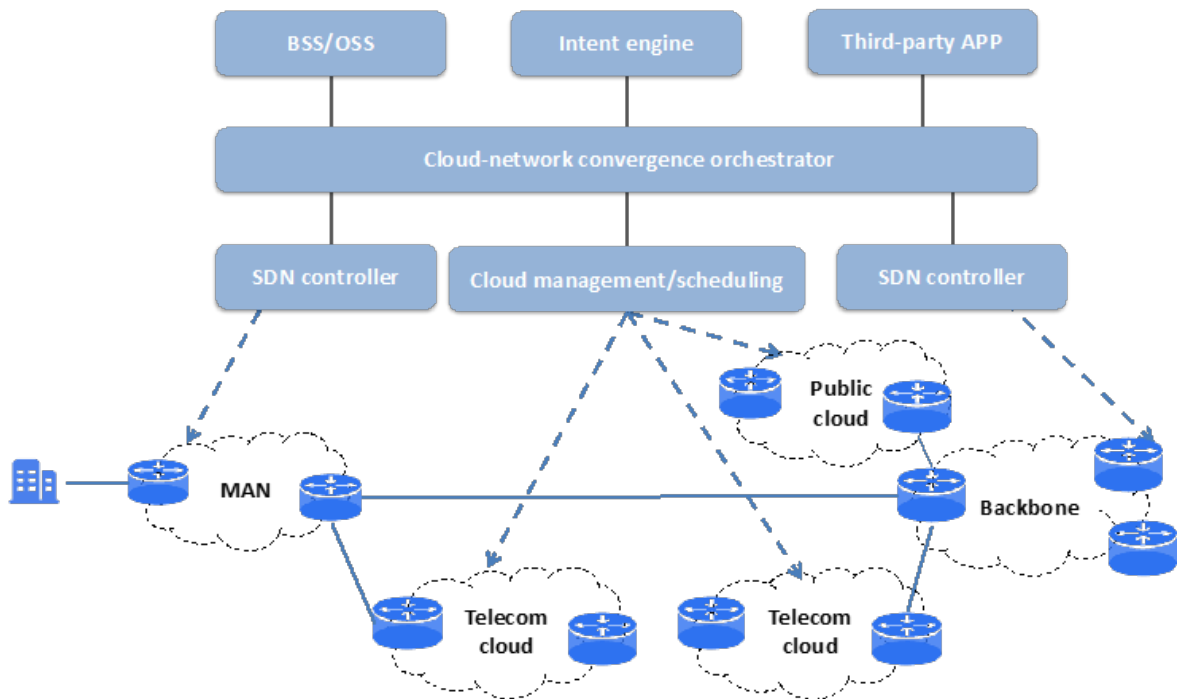


Figure 11: Intent-based architecture of telecom network (from Figure 7 of ETSI GR IPE 002 [2])

To deliver network-Cloud converged products and services, operators need to build a new-generation O&M system. Integrated network-Cloud orchestration is the key to the new-generation O&M system and the basis for one-point service provisioning and end-to-end service guarantee. With this new architecture, operators need to have the network ability of closed-loop automation.

This overall architecture applies to access networks as well as to industrial internet and other connectivity scenarios.

ETSI DGR/IPE-004 [3] analyzes IPv6 based enterprise networking and Industrial Internet. The SDN service architecture allows to manage an enterprise/industrial network and is also essential to connect to Internet, network operators and for the communication between Branches and Head Quarter (HQ) / Data Center (DC).

ETSI DGR/IPE-006 [4] describes IPv6 and Cloud using DataBlockMatrix for Food Supply Chain Tracking and Tracing (FSCTT). Two factors are key to the success of the Food Supply Chain: the large number of IoT devices used to monitor the state of food and manipulate the food storage devices and the Cloud that collects the data and makes predictions.



3.6.3. Future Issues

In principle, Artificial Intelligence may be used as part of a broader network intelligent scheme for the network. The scalability and flexibility of IPv6 simplify the collection of network data for further processing by AI-based systems. With the help of AI, IPv6 networks can offer intelligent application possibilities: in 5G, private line service, home broadband, and other business scenarios, IPv6-based intelligent routing, network fault analysis, root cause analysis, positioning, self-healing and prediction, network resource arrangement and management, IPv6 intelligent security, etc.

Technologies like Segment Routing over IPv6 dataplane (SRv6), combined with per-flow monitoring technologies like In-situ Flow Information Telemetry (IFIT), enable simplifying the e2e connectivity, dramatically reducing the need for multiple protocol utilization. The possibility to have any connectivity with specific key performance indicators collected in real-time summed with the possibility of rerouting and reconfiguring each flow represents the best environment to underpin automation.

IPv6 automation benefits can be applied in multiple scenarios and use cases (e.g., Datacenter, Cloud integration, 5G slicing, Enterprise network, IoT)

Automation of 5G network, as defined by 3GPP, based on SRv6 is described in ETSI GR IPE 005 [5] “5G Transport over IPv6/SRv6”, where the slicing mechanisms of the 5G core find an extension in the transport SRv6 flow towards the application servers.

The PoC entitled is being managed by IPE on “SRv6 based 5G Non-Terrestrial Network to provide services with granted SLA, like V2X communication” this PoC will investigate how SRv6 increases AI-based automation in complex service scenarios.

3.7. ISG Multi-access Edge Computing (ISG MEC)

3.7.1. Overview from Autonomous Networks perspective

The MEC architecture is specified in the ETSI GS MEC 003 specification [Mref2], which is defining also multiple architectural variants. One of them, relevant in the context of the present document, is the MEC-in-NFV reference architecture, reproduced below in Figure 12, as it is clarifying how a MEC system can be deployed in virtualized environments, and its relationship with ETSI NFV (Network Functions Virtualization) framework.

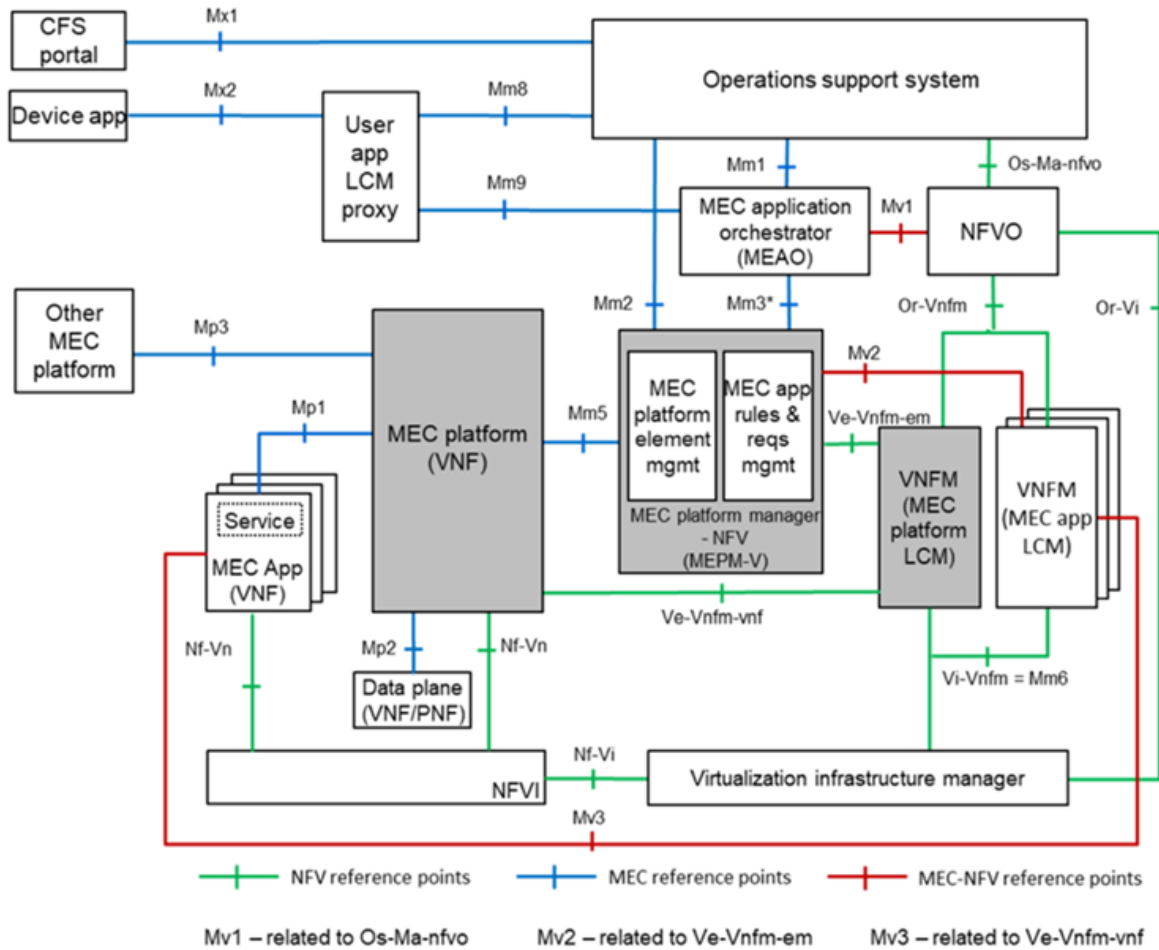


Figure 12: MEC-in-NFV Reference Architecture (ETSI GS MEC 003 [Mref2])

As shown in figure, and described in MEC 003, this architectural variant takes full advantage of the ETSI NFV MANO architecture and demonstrates how the entities defined by ETSI MEC can integrate with it. Specifically, the following key observations can be made:

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

When it comes to Autonomous Networks, ETSI ISG ZSM is expected to take the overall approach from an architectural point of view, while NFV framework is intended to telco cloud management, and finally MEC managing telco edge cloud (see Figure 13).

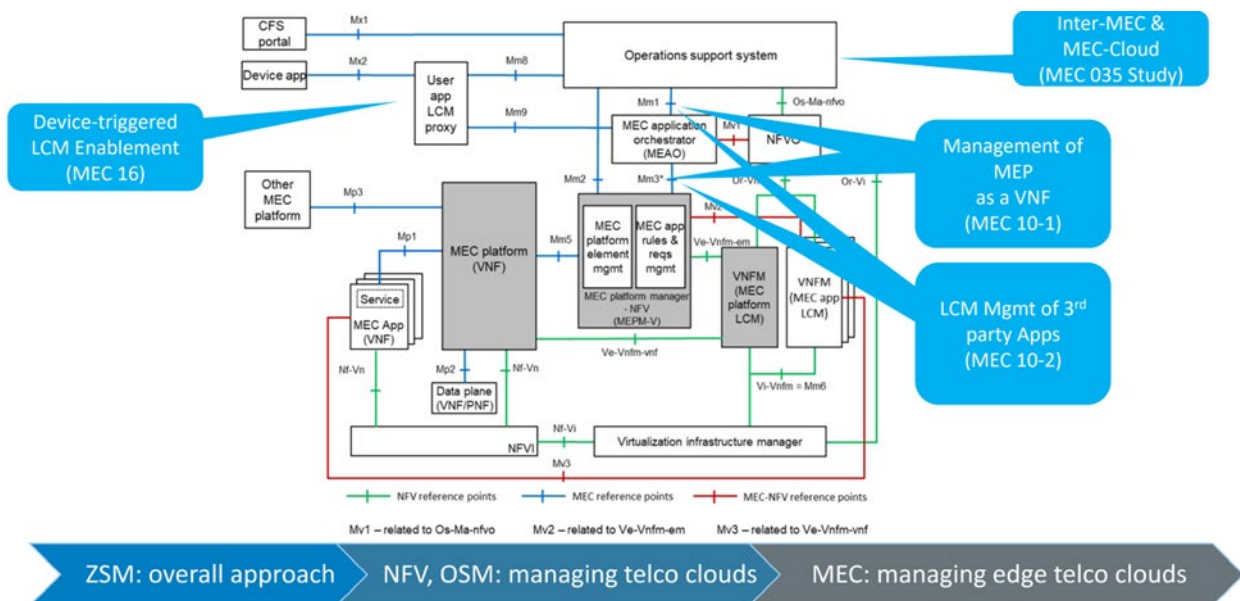


Figure 13: Role of MEC in ETSI standards for Autonomous Networks (ref. ETSI MEC slides [Mref1])

As shown in Figure 13, some MEC specifications are relevant in the context of Autonomous Networks:

- ETSI GS **MEC 016** (Multi-access Edge Computing (MEC) Device application interface). This document contains the API definition for the lifecycle management of user applications over the Mx2 reference point between the device application and the User Application LifeCycle Management Proxy (UALCMP) in the MEC system. Since it covers some important lifecycle management operations (e.g., user application look-up, instantiation and termination), in addition to a mechanism for the exchange of lifecycle management related information between the MEC system and the device application, this specification can be relevant also in the domain of Autonomous Networks [Mref7].
- ETSI GS **MEC 10-1** (MEC Management; Part-1: System, host and platform-vnf management). This document defines the management of the mobile edge system, mobile edge hosts and mobile edge platforms. This includes platform configuration, performance and fault management, application monitoring, remote service configuration and service control, information gathering regarding the platform features, available services, and available virtualized resources. All these aspects are relevant to Autonomous Networks [Mref8].
- ETSI GS **MEC 10-2** (MEC Management; Part-2: Application lifecycle, rules and requirements management). This document is relevant to Autonomous Networks as it provides information flows for lifecycle management of MEC applications, and it describes interfaces over the reference points to support application lifecycle management. It also describes application rules and requirements, application-related events, mobility handling and MEC service availability tracking [Mref9].
- ETSI GR **MEC 035** (MEC; Study on Inter-MEC systems and MEC-Cloud systems coordination). This document studies the applicability of MEC specifications to inter-MEC systems and MEC-Cloud systems coordination that supports, e.g., application instance relocation, synchronization and similar functionalities. Another subject of this study is the enablement and/or enhancement of functionalities for application lifecycle management by third parties (e.g., application developers) [Mref10].



ETSI ISG MEC expects to align with the emerging zero-touch management entities, such as those in the ETSI ZSM End-to-End Service Management domain. Moreover, given the critical importance of automation for actual MEC deployments, we expect Telco's to increasingly focus on such modern evolutions of OSS for their deployments [Mref3].

3.7.2. MEC use cases and requirements related to Autonomous Networks

Among the use cases and requirements specified by ETSI ISG, MEC [Mref4] has described use cases that are providing technical enablers for scenarios that can be relevant to Autonomous Networks, as they help to identify business-oriented and automation-related challenges faced by operators and vertical industries, when running edge computing infrastructures. The relevant use cases in this context are included in the Group Specification MEC 002 [Mref4].

A few examples of use cases that may have an impact on enabling Autonomous Networks are:

- 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 (e.g. RNI API, MTS API, etc.).
- Security, safety, data analytics: - MEC can provide the best end-user experience, e.g., reduce downtime 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 [Mref6].

MEC deployments represent some challenging environments, characterized by the need to manage both aspects at large scale (requirements impacting on geography) and small scale (cloud footprint). To give few examples, MEC has to be managed in such scenarios:

- Unmanned/lights out locations
- Outside traditional service areas

Moreover, managing the telco edge clouds from AN perspective implies the need for MEC to support mechanisms to manage this “critical infrastructure”, both for Telco but also for public safety and related stakeholders, where a set of demanding Service Level Requirements (SLR) are requested:

- a certain number of “9's” in terms of availability/reliability
- Need to minimize human presence, to manage LCM procedures
- Maximize service time intervals
- Minimize skills required from those on site
- Get as close as possible to the web-scale maintenance model
- Doing the above in a very non-web-scale environment



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.

3.8. ISG “5th Generation Fixed Network” (ISG F5G)

3.8.1. Overview

ISG F5G is focusing on the development of standards for the Fifth Generation Fixed Network (F5G), and fostering the evolution to a “fibre to everywhere and everything” ecosystem.

Fiber technologies play an essential role in the fixed network, promoting the evolution of network capacity and capabilities. Till now, such evolution can be mapped to five generations from F1G to F5G. The current F5G has the technical characteristics of enhanced Fixed Broadband (eFBB), Full-Fiber Connection (FFC) and Guaranteed Reliable Experience (GRE). See ETSI GR F5G 001 [1].

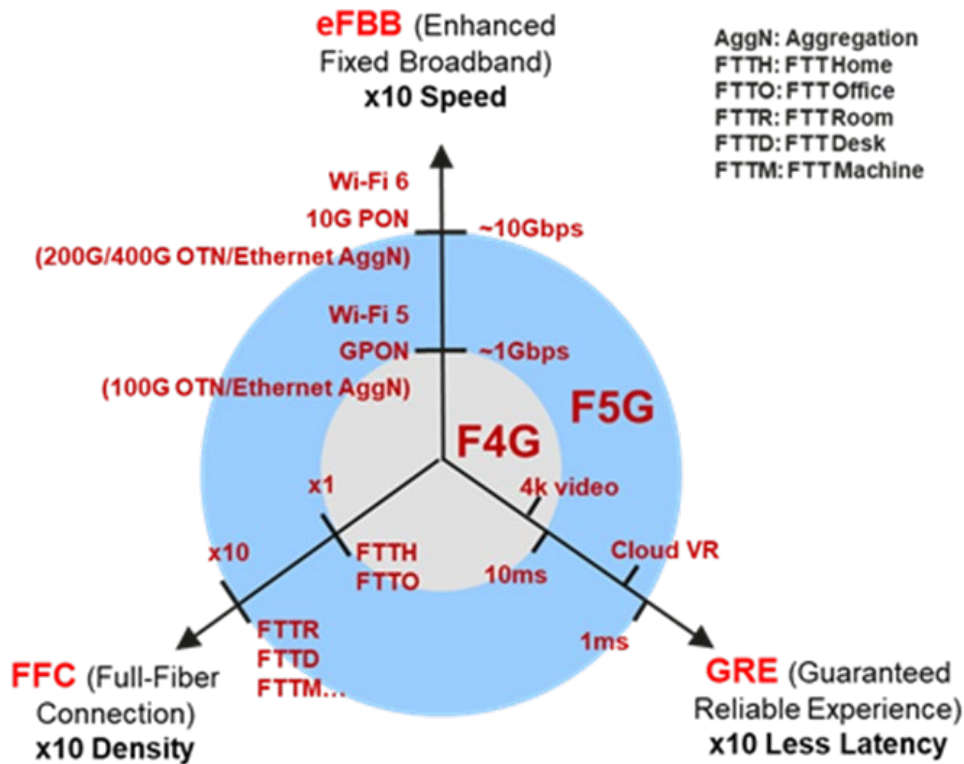


Figure 14: Technical characteristics for F5G (from Figure 5 of ETSI GR F5G 001 [1])

1.

3.8.2. F5G Use Cases related to AN

ETSI GR F5G 008 [2] describes 32 use cases to be enabled by the F5G network, five of which are addressing the aspects of automation and autonomy of the fibre networks:



1. Use case #10: Scenario based broadband. AI technologies are used to learn and distinguish high value broadband applications, which are to be guaranteed.
2. Use case #11: Enhanced traffic monitoring and network control in Intelligent Access Network. Telemetry and machine learning are used to perform traffic monitoring, analysis, prediction and network configuration for the Fibre To The Room (FTTR) services.
3. Use case #29: Orchestration of B2B services in xPON networks. By defining a common connectivity service model (combining Customer Premises Network and Access Network) on the centralized service orchestrator, zero touch B2B connectivity service provisioning in xPON Access Network can be achieved.
4. Use case #31: Intelligent Optical Cable Management. Typical examples are automatic identification of shared-route optical fibres, association of the optical cable with geographic information, and optical fibre quality monitoring and degradation prediction.
5. Use case #32: AI-based PON optical path diagnosis. AI platform is introduced to perform data acquisition, status monitoring and analysis, and fault diagnosis of the PON optical paths.

The technology requirements and standardization gaps of these use cases are specified in ETSI GS F5G 003 [3] and DGS/F5G 0013 [4].

3.8.3. F5G AN architecture and AN levels

ETSI GS F5G 004 [5] defines the F5G network architecture to support the F5G use cases and their requirements. The F5G network architecture introduces a Management, Control and Analytics (MCA) Plane that integrates network automation and autonomy functionalities.

In the MCA Plane, ETSI GS F5G 006 [6] specifies the F5G End-to-End (E2E) management and control architecture, aiming to design an "Autonomous F5G Network" to enable the self-configuration, self-healing, self-optimising and self-evolving of the F5G network.

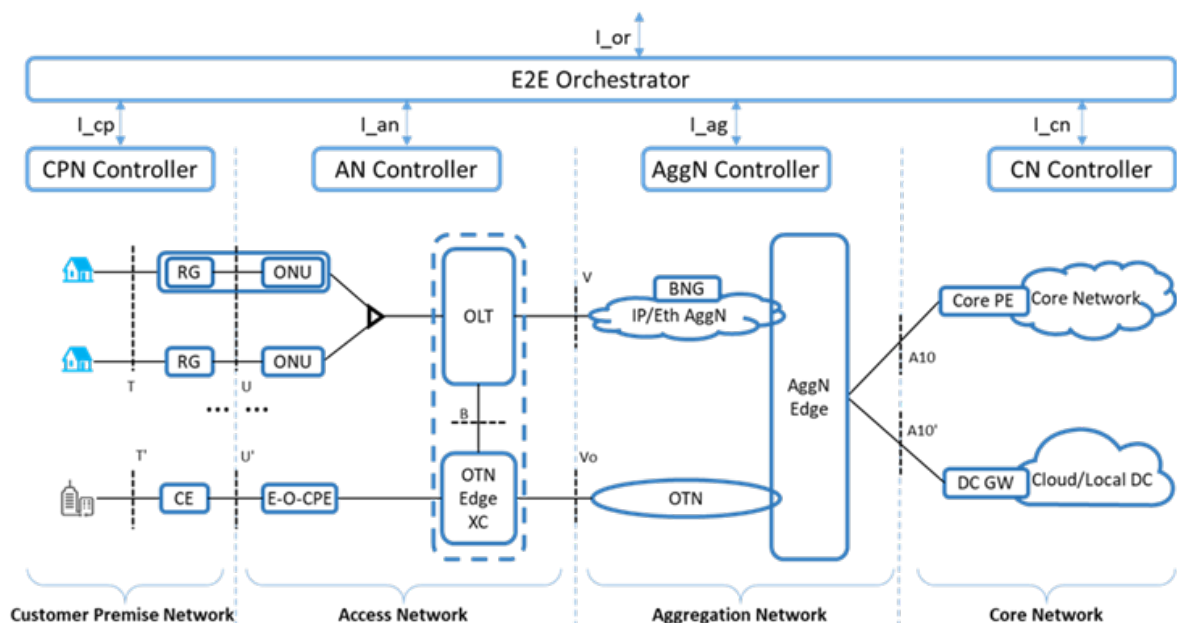




Figure 15: F5G E2E management and control architecture (from Figure 1 of ETSI GS F5G 006 [6])

In this architecture, each F5G domain, including the Customer Premises Network (CPN), the Access Network (AN) and the Aggregation Network (AggN), is considered as an autonomous domain and is managed and controlled by its own domain controller. The E2E Orchestrator interacts with each domain controller to perform the inter-AN coordination.

In addition, ISG F5G has started considering and defining the AN level classification and evaluation of the F5G networks in a newly created WI.

3.8.4. Key technical aspects related to AN

Automatic service and resource management: ETSI GS F5G 006 [6] specifies the general processes of service fulfilment and service assurance in the context of F5G, to enable the automatic E2E service and resource life-cycle management.

APIs and Intent-driven management: ETSI GS F5G 006 [6] specifies the technical requirements and key parameters of the northbound interfaces (NBIs) of the domain controllers and the E2E Orchestrator, and adopts the intent-based management approach on these NBIs.

Analytics and intelligence: In ETSI GS F5G 004 [5], the AI analyser is introduced in the MCA plane of the F5G architecture, to analyse network data, identify, locate and predict network failures, and provide management tools for QoE and analysis tools for network operations.

3.8.5. Security

ISG F5G is considering the security issues that a wider penetration and automation of fibre network and service configuration will introduce. ETSI GR F5G 0010 [x] identifies security threats to F5G and recommends mitigation strategies against them. DGS/F5G 0012 [x] further defines the security countermeasures against security threats to F5G.

3.8.6. Future evolution towards F5G Advanced

As technology continues to evolve, ISG F5G is considering the technologies of the F5G advanced and beyond. In the ETSI White Paper No. #50 [7], the characteristics of the F5G advanced system are categorized as faster, smarter, wider, greener, quicker, and more aware (see Figure 3). Among them, to achieve the “smarter”, the autonomous level of the fibre network needs to be increased to level 4, to improve the user experience and service quality.

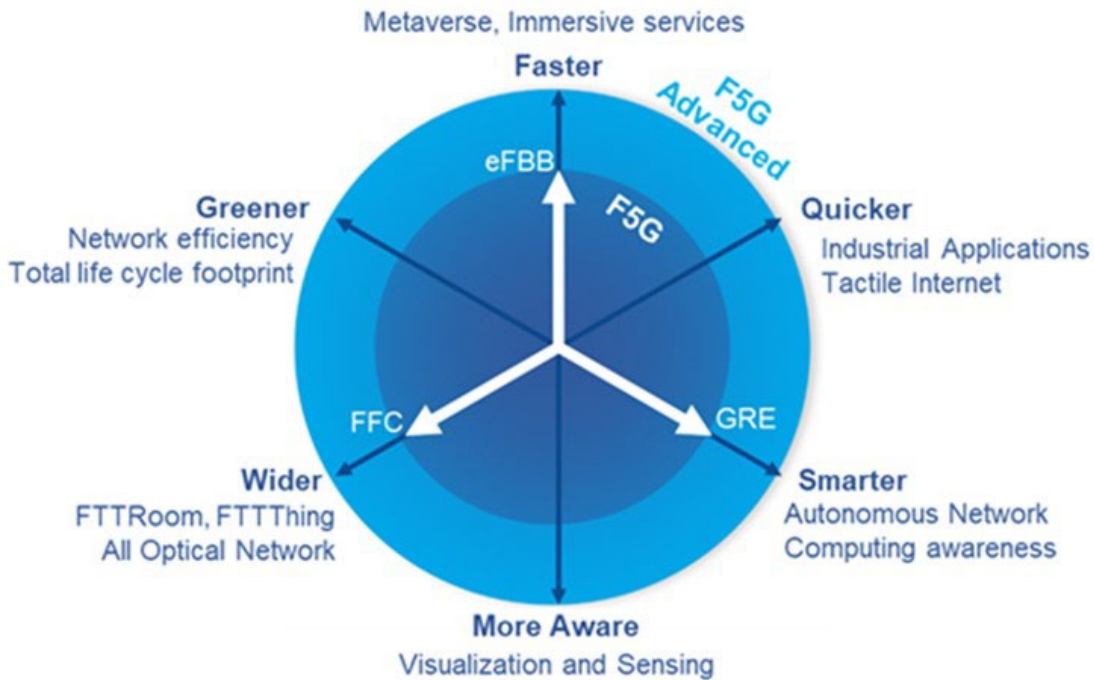


Figure 16: Features of F5G (From Figure 2 of ETSI White Paper No. #50 [7])

3.9. ISG 'Securing Artificial Intelligence' (ISG SAI)

The Industry Specification Group Securing Artificial Intelligence (SAI) discusses 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, but treats these aspects of AI in a general way. So far, the group has focused on the first aspect, i.e., ensuring cybersecurity of AI systems, in particular with respect to novel, AI-specific threats. In so doing, the group considers the whole AI life cycle as different phases in the life cycle give rise to different threats to the AI system. The life cycle starts with the planning of the system and the acquisition and curation of data and continues with training, validation and testing procedures until the AI system is put into operation, maintained and eventually retired.

So far, the group has done work on an overview of threats that AI systems are exposed to in ETSI GR SAI 004 and created a corresponding ontology in ETSI GR SAI 001. It has also produced reports on existing approaches that can be used to mitigate the various threats to AI systems in ETSI GR SAI 005, and on generic measures for improving data quality and protecting the data supply chain in ETSI GR SAI 002. In addition, the group has studied the hardware requirements for supporting a secure operation of AI systems in ETSI GR SAI 006.



3.10. Further key topics to address

3.10.1. Security and privacy

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 for the AI/ML model before moving it to production and then on a regular basis, the model should be evaluated to ensure it provides the desired functionality and is sufficiently robust to changes in input data both natural and (potentially) adversarial. This differs from the security control “Use methods to clean the training dataset from suspicious samples” [ref1]. In general, Autonomous Networks 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 will assistance to enhance the overall Centralized monitoring system of Autonomous Network.

Increasing entry points increases the number of attack surfaces in applications and systems. There are many challenges related to security that need to be considered in future standardization work: Infrastructure security and protection from physical to virtual and application levels, Data protection and User security which includes data encryption - at rest, in transit and in motion [[MEC federation: deployment considerations \(etsi.org\)](#)].

ISG ENI: The specification of this area is expected to be reactivated during Release 3 building on the ISG SAI work.

ISG ZSM has published a comprehensive report on general security aspects related to the ZSM framework and solutions, and potential mitigation in the following Group Report:

- DGS/ZSM-014_SecAspects “Zero-touch network and Service Management (ZSM); ZSM security aspects”

A related normative specification work (ETSI GS ZSM 014) has commenced on June 2021.

ISG NFV While specific work was not yet initiated to address the security aspects for the new AN functions recommended in the ETSI GR NFV-IFA 041, the ISG NFV has a dedicated Expert Group on Security and Lawful Intercept matters, so it is expected that the NFV security aspects can be analysed once the respective AN normative work at stage 2 (IFA specifications) becomes stable.

TC INT AFI WG: There is ongoing work on a standardizable Generic Framework for E2E Federated GANA Knowledge Planes for AI-powered Closed-Loop Self-Adaptive Security Management & Control, Across Multiple 5G Network Slices, Segments, Services and Administrative Domains. The work addresses End-to-End AI-powered Autonomic Security Management & Control Across Multi-Domain 5G Networks [INT 5: WP#6]. Reference Work Item is DTR/INT-00900: https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id=63106

ISG IPE (IPv6 Enhanced Innovation) in ETSI GR IPE 010: “IPE Proof of Concepts Framework” highlighted Security as one of the 6 major evolution dimensions of the IPE. Adoption of updated protocols designed



by IETF according to recent security criteria and increased automation enabled by IPv6 e2e connectivity eliminates human configuration errors, increasing security. Newly created Report ETSI GR IPE 013: “CGA for IPv6 Zero Trust” is focusing on IPv6 Cryptographic Generated Address functionality and the possibility offered to authenticate network host and node increasing security

ISG MEC (Multi-access Edge Computing) published a White Paper titled MEC security (“Status of standards support and future evolutions”) providing an overview of ETSI MEC standards and current support for security, also complemented by a description of other relevant standards in the domain (e.g., ETSI TC CYBER, ETSI ISG NFV, 3GPP SA3) and cybersecurity regulation potentially applicable to edge computing. After this publication, ISG MEC started a work item on MEC Security (DGR/MEC-0041 MECSecurity), with the aim of studying security topics and paradigms that apply to MEC deployments. The study will broadly cover the themes of application and platform security, Zero-Trust Networking, and security requirements for MEC Federations.

ISG F5G is considering the security issues that a wider penetration and automation of fiber network and service configuration will introduce. The following Group Report identifies security threats to F5G and recommends mitigation strategies against them:

- ETSI GR F5G 010 “Fifth Generation Fixed Network (F5G); Security; Threat Vulnerability Risk Analysis and countermeasure recommendations for F5G”

The security countermeasures against security threats to F5G is under development in the document DGS/F5G 0012 ‘F5G Security Framework’.

ISG SAI has done extensive work on the security aspects of AI in ETSI GR SAI 001, 002, 004, 005 and 006 (cf. also section 3.1.7) and is currently working on privacy aspects in ETSI GR SAI 008.

ISG SAI has studied the various novel attacks that can be used to target AI models and potential countermeasures. A prominent example is 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. Another attack type are adversarial attacks that target the model in operation by using specially crafted inputs to mislead the model; adversarial attacks can be mitigated by expanding the training process (adversarial training), introducing additional modules for detecting attacks and sanitising input data. Other attacks jeopardise the confidentiality and privacy of the data used to train the model or the model’s parameters. They can be dealt with by approaches such as 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.

As a general word of caution, it should be noted that so far there is no individual measure that can reliably block any of the attacks listed above, and in particular adaptive attackers that are aware of the defensive measures in place can usually circumvent them with limited effort. Nevertheless, protective measures outlined in ETSI GR SAI 002 and 005 increase the level of security of the respective AI model. In general, various measures should be combined throughout the life cycle for security-critical AI models.

3.10.2. Testing framework and methodology

In the following, perspective work of groups and committees with regard to testing with relevance to autonomous networks is shown. As testing represents a fundamental process from conformity assessment, a broad discussion with relevance for the identification of specifications to be presented in autonomous networks is inevitable. Currently, the particular challenge in formulating requirements for



testing autonomous networks is the parallelized combination of innovations, including software-defined telecommunication units and novel network architectures, which are closely linked to sophisticated systems based on artificial intelligence.

ISG ENI: The activities devoted to this topic is starting to be considered and introductory cooperation work has been carried out with ETSI CTI. The associated WIs that may be needed for this work have not been created yet.

ISG NFV While specific work was not yet initiated to address the testing aspects for the new AN functions recommended in the document Management and Orchestration;

Report on enabling autonomous management in NFV-MANO - ETSI GR NFV-IFA 041, the ISG NFV has a dedicated Working Group on Testing, interoperability and open source (TST WG). It is therefore expected that the interoperability testing specifications and API conformance testing specifications will be enhanced to address AN once the normative specifications will become stable.

TC INT and TC MTS are working on the following work of relevance to Testing ANs:

- ETSI published an ETSI Guide (EG) Approaches for Testing Adaptive Networks - ETSI EG 203 341 V1.1.1 on Testing Self-Adaptive Networks;
- White Paper No.5 of the ETSI 5G PoC (Publicly available): 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: Published and downloadable from here:
https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals;
- Metrics as Basis for Test and Certifications for AI Models: Example of Standardizable Metrics for AI Models for Autonomic Systems are being defined in ETSI TR (yet to be published): Reference Works Item is https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59456 ;
- Reference Work Item on the need for Autonomic Test Systems for Testing ANs:
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59455 ;
- **TC INT and TC MTS** are also working on the following work of relevance to Testing ANs.
 - Use Cases to leverage the concept of Federated Testbeds for testing ANs, and leveraging on the ongoing ICT ETSI Standard on End-to-End AI-powered Autonomic Security Management & Control Across Multi-Domain 5G Networks, (Ref. Nr. DTR/INT-00900):
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=63106 ;
 - Evaluation Methods for Trust and Confidence in ANs; Multi-layer Autonomics/AI and Cross-Domain Federation Aspects for ANs, Reference Model for Testbeds Federation: Generic Federated Testbeds Model for ANs (as joint work between ETSI TC INT AFI and ITU-T SG11);
 - Benefits of artificial intelligence in test systems Artificial Intelligence (AI) in Testing Autonomous Networks (ETSI TR 103 748 V1.1.1 - 2022-06). In terms of content, the document is about which autonomous services in telecommunication networks can be tested by integrating AI-based test systems. For this purpose, the document deals with the question of how tests of autonomous network functions involving several network domains may operate. With an emphasis on autonomy of test systems, the document discusses testing on the basis of AI, including performance testing, security testing and fuzzing, test execution automation,



regression testing and unit testing. For this, the need for test systems that might use AI for testing existing communication networks and services like 5G is described, for example with regard to Software Defined Network (SDN), Network Function Virtualization (NFV) and AMC (Autonomic Management and Control).

ISG IPE: has AN related testing activities in reports ETSI GR IPE 008: “IPv6 Ready Logo: IoT & 6TiSCH” and ETSI GR IPE 016: “Testing/Validation IPv6/SRv6 network”. In line with the PoC framework indicated below, two PoCs started in last plenary IPE#008: ETSI GR IPE 010: “IPE Proof of Concepts Framework”;

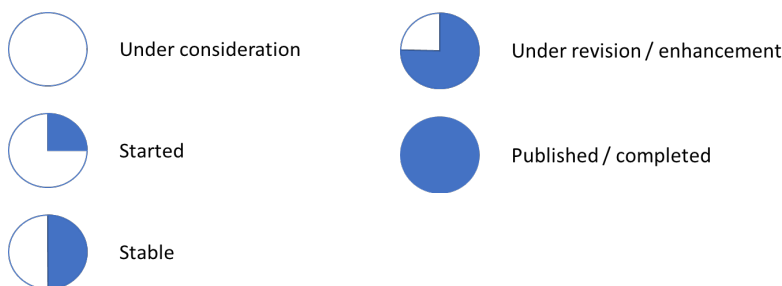
- In particular, PoC “SRv6 based 5G Non-Terrestrial Network to provide services with granted SLA, like V2X communication” this PoC will investigate how SRv6 increases AI-based automation in complex service scenarios.

ISG SAI has been doing work on testing procedures concerning the security aspects of AI models in ETSI GR SAI 003, which includes a great array of test methods that can potentially be used. ETSI GR SAI 003 is currently in the stage of a stable draft and might soon be published.

4. Mapping of ETSI activities related to AN

In Chapter 3 a synthesis of the most significant results achieved in TC and ISG is reported. In order to present the reader a map of ETSI activities and work progress in the table below shows the current ongoing work in the several groups of ETSI, on topics related to Autonomous Networks. The table represents also a way to give a picture of complementarities and potential overlaps, where a dialogue among experts of the different projects is suggested.

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





Note: the “published / completed” status shows that the topic may be subject to further activity (revision or enhancement)



	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/autonomy	●	●	○	◐					
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)	◐	◐	◐	○		◐		◐	

² The initial transmission of the “autonomy-related” goals, rules and constraints can be provided by other means than intent.



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									

5. ICT ecosystem initiatives on AN

Significant effort and relevant initiatives are active across the Industry Ecosystem on Network Automation. This outlines the business interest and technological value of Autonomous Networks across the Industry. Major Standard and Industry Fora (e.g. ETSI, IETF, ITU, TMForum, GSMA, NGMN etc.), Multi-partnership Project for interoperable standards (3GPP) and open-source communities (eg. ONAP etc.) are delivering recommendations, preliminary standards, deliverables and APIs. Industry cooperation and coordination are essential for harmonization, widespread interoperability, and consistent behaviours, across a multi-vendor ecosystem. This cooperation softly started with the M-SDO Autonomous Networks (AN) Table, supported by TMForum. This AN M-SDO Table that includes the main projects on AN across the mentioned Fora and Open Source (ETSI, ITU-T, IETF, GSMA, 3GPP, Linux Foundation...) organized on-line workshops to share results and present ideas, architectures, solutions. Initiatives like this represent a good starting point to improve and launch a stronger coordination, where ETSI can play a significant role. Most of the areas require studies and a coordinated committed in the Industry.

A not exhaustive list of activities on Autonomous Networks in major Fora, beside the ETSI ones, are briefly reported below.



5.1. ITU-T

The Focus Group on Autonomous Networks (AN) (Study Group 13) issued recently two Technical Specifications (TS) from the Questions 13 and 20 for discussion. The documents deal with autonomous components and the assessment of trustworthiness for autonomous networks. In the following is given an overview of both documents:

The TS “Architecture framework for Autonomous Networks” includes

- requirements for an architecture framework for Autonomous Networks;
- a description of components and subsystems in Autonomous Networks;
- a description of interactions between architecture components.

The TS “Trustworthiness evaluation for autonomous networks including IMT-2020 and beyond” describes

- a system for characterizing the trustworthiness of autonomous networks by formulas and metrics;
- the document applies the scheme to the following use cases:
Planning, Deployment, Maintenance, Optimization and Operation of networks.

5.2. IETF and IRTF

The IETF is working on standards for automated network management mainly in the network configuration Working Group (NETCONF), network modeling Working Group (NETMOD), Operations and Management Area Working Group (OPSAWG) in OPS area and also most of protocol specific working groups (e.g., TEAS Working Group) in RTG area. A key to automated network management is the YANG data modeling language used to model configuration and state data manipulated by the Network Configuration Protocol (NETCONF) and RESTCONF which were developed within the IETF. Data modeling-driven management applies the YANG modeling language to formally describe higher-level network services (e.g., L3SM, L2SM, IETF Network Slice) at the service layer, various aspects of a network infrastructure (e.g., L3NM, L2NM, Network Topology, L3 topology), including devices and their subsystems, and relevant protocols at the network layer, technology specific configuration and state at the device layer (e.g., ACL, OSPF).

- [RFC8969] describes a framework for service and network management automation and provide guidance for Network operators and developers on how to use YANG data models at different layers to provide closed-loop control for adaptive and deterministic service creation, delivery, and maintenance and build fully automated YANG system.
- In addition, Research on automated network management in the network management research group (NMRG) of IRTF Results in [RFC9315] on Intent-Based Networking - Concepts and Definitions and [RFC9316] on Intent Classification. NMRG is also starting to work on Digital twin network architecture and Concept [I-D.irtf-nmr-network-digital-twin-arch] which aims at efficient and cost effective data driven network management and accelerate network innovation.

5.3. TMForum

TMForum was one of the first Forum to invest significantly on Autonomous Networks. They started with a AN dedicated workshop at Digital Transformation World (DTW) to present the business value of Autonomous Networks and collect experts for a dedicated project on Autonomous Networks focusing on Technical aspects and Business opportunities. Several documents, workshops and white papers were delivered. According to TMForum view Autonomous Networks is a key enabler of the Digital



Transformation of the new extended Ecosystem, that includes ICT companies, Service Providers, Verticals and R&D players.

The project was extended to a Cluster of AN related projects extending Autonomous Networks to Autonomous Operations and Data Governance. Significant progress and deliverables were done on Architecture Evolution, Intent, Business Opportunities, Use Cases and AN APIs. It is important to outline the significant number and value of Catalysts Projects on Autonomous Networks, presented at DTW events, where companies develop together concepts and software on several innovative use cases. As anticipated the are playing also the role of facilitator of the M-SDO table to share ideas and information among the leading SDO.

5.4. NGMN

NGMN launched recently a Working Group: Network Automation and Autonomy based on AI, with a significant participation of Telco Operators and vendors, the most significant deliverables produced were a Network Operators Survey on Network Automation and a Paper: *Automation and Autonomous system Architecture Framework*.

5.5. 3GPP

In 3GPP, studies and specifications are focussing on topics with relevance for autonomous networks which including autonomous network levels and evaluation, intent driven management, AI/ML-based Services etc. While the TS 23.288 Architecture enhancements for 5G System (5GS) to support network data analytics services is focussing, i.a., on model distribution, transfer, training for various AI capabilities. TS 28.100 „Levels of autonomous network“ states concepts for autonomous networks, its levels as well as autonomous functions inside a 3GPP network. Moreover, the document 3GPP TR 28.910 is discussing the enhancement of generic autonomous network level for network optimization, e.g., by an autonomous network level for RAN energy saving. Furthermore, the report TR 28.909 describes a concept for autonomous network level evaluation. Intent-driven management concept and solution are captured in TS 28.312.

6. Recommendations

The massive activities and deliverables around Autonomous Networks clearly indicate the hype role of AN in Digital Transformation in the extended Ecosystem. This means that Autonomous Networks reached momentum in terms of business interest. Unfortunately there is a potential risk of fragmentation, recommendations and standards not convergence and resource waste. In order to avoid this risk it is mandatory to find coordination inside ETSI TC/ISGs and to extend collaboration and knowledge exchange among leading SDOs/ Fora.

6.1. Joint elaboration of work items in ETSI

Within ETSI, further cooperation between individual groups should be sought, as it has been done in the past, for example, for the joint development of standardization documents. Cooperation enables a reaction to new and changed requirements for own products and services in the course of their production or design. In addition, from the point of view of the actors involved, requirements for products and innovations for conformity assessment processes, especially tests, can be influenced in their own favour in the course of joint cooperation. OCG AN can play a role to facilitate cooperation inside ETSI TC/ISG; the previous internal progress document on Autonomous Networks and the current White paper



started this collaboration process, that can progress with workshops on dedicated items and coordinated meetings.

6.2. Knowledge Exchange among SDOs

In general, cooperation among different organizations should be envisaged and encouraged. This information sharing and knowledge exchange started thanks to the mentioned AN M-SDO Table, promoted by TMForum and the first bilateral meetings between WGs from different SDOs. In particular the ITU-T (SG13), was active in soliciting an exchange of information with ETSI TC/ISGs and TMForum. The exchange can take place, also via presentations in ITU focus groups, after inviting stakeholders from other organizations to ETSI and vice versa.

Being proactive in these initiatives is a way to promote ETSI results on AN, to contribute to the success of Autonomous Networks and to facilitate recommendations and standards convergence in the European Union and worldwide.

6.3. Perspectives and evolutions on Autonomous Networks

Autonomous Networks is for sure one of the most interesting areas of use and deployment of Artificial Intelligence and Machine Learning in Network evolutions, opening business opportunities both in terms of launch of new services and cost optimization. Significant innovation opportunities beside the current work and activities reported in the White paper chapter 3, can be:

1. Network Digital Twin (NDT)
2. Impact of NDT on AN evolution
3. Digital Twin for business Assurance
4. 6G & Autonomous Networks
5. Autonomous Networks API marketplace

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

7. Summary

The transition towards cognitive Autonomous Networks becomes an urgent necessity to unlock the business potential of 5G and beyond. The transition will be gradual, with the ultimate goal to enable service delivery with agility and speed and ensure the economic sustainability of the very diverse set of services offered by Digital Service Providers.

ETSI is playing a leading role in the definition, study, specification, and demonstration of the extensive enabling technologies and aspects related to Autonomous networks. As described in section 3 and 4, various ETSI groups (TBs/ISGs) contribute to the work within their respective scopes. In particular:

- ISG F5G in the scope of fifth generation fixed networks;
- ISG MEC in the scope of multi-access edge computing infrastructure;
- ISG NFV in the scope of the NFV management domain and virtualized infrastructure;



- ISG IPE in the scope of 5G, cloud and industrial Internet, using AI SDN-based IPv6 networks;
- ISG ZSM in the scope of zero-touch end-to-end network and service automation;
- ISG ENI in the scope of experiential networked intelligence enabled by cognitive network management;
- ISG SAI in the scope of Security;
- TC INT AFI WG in the scope of a generic autonomic networking architecture;
- TC MTS in the scope of testing.

These ETSI groups have established fruitful cooperation with internal and/or external organizations as well as with research projects.

The authors of this paper hope that this document would help the ETSI OCG AN to develop a holistic view on Autonomous Networks, show the synergy among the related activities within ETSI, and brand the achieved results in the Standard/ Fora Ecosystem.

Moreover, the information can help to identify opportunities for collaboration between the ETSI groups and leverage synergies and can also help to identify gaps and additional areas where ETSI can play a role in the industry.

8. References

The following referenced documents aims to assist the user with regard to a particular subject area.

Note that the list does not include documents where names/references are explicitly cited in the text above.

- [ETSI White Paper #16](#): GANA - Generic Autonomic Networking Architecture Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services
- [ETSI White Paper #40](#): Autonomous Networks, supporting tomorrow's ICT business
- [ETSI White Paper #46](#): MEC security: Status of standards support and future evolutions Edition 2
- [ETSI White Paper #49](#): MEC federation: deployment considerations [MEC federation: deployment considerations \(etsi.org\)](#)
- [ETSI TS 103 195-2](#): 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
- [INT 1] [ETSI TS 103 194](#): "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet".
- [INT 2] [ETSI TR 103 195-1](#): "Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 1: Business drivers for autonomic networking".



- [INT 3] [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".
- [INT 4] [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".
- [INT 5] ETSI INT PoC [Accepted PoC proposals - INTwiki \(etsi.org\)](#)
- [INT 6] [ETSI white paper 16](#)
- [INT 7] [ETSI EG 203 341](#) "Testing Self Adaptative Networks"
- [INT 8] [ETSI TR 103 748](#) "Artificial intelligence in test systems Artificial Intelligence (AI) in Testing Autonomous Networks"
- [INT 9] [ETSI TS 103 195-2](#) "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
- [INT 10] [ETSI TR 103 747](#): 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
- [INT 11] [ETSI ISG AFI work items](#)
- [INT 12] [ETSI NTECH TR 103 473](#) "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Autonomicity and Self-Management in the Broadband Forum (BBF) Architectures"
- [ETSI GS ENI 001](#) (V3.1.1): "Experiential Networked Intelligence (ENI); ENI use cases"
- [ETSI GS ENI 002](#) (V3.1.1): "Experiential Networked Intelligence (ENI); ENI requirements"
- [ETSI GR ENI 004](#) (V2.2.1): "Experiential Networked Intelligence (ENI); Terminology for Main Concepts in ENI"
- [ETSI GS ENI 005](#) (V2.1.1): "Experiential Networked Intelligence (ENI); System Architecture"
- [ETSI GS ENI 006](#) (V2.1.1): "Experiential Networked Intelligence (ENI); Proof of Concepts Framework"
- [ETSI GR ENI 007](#) (V1.1.1): "Experiential Networked Intelligence (ENI); ENI Definition of Categories for AI Application to Networks"
- [ETSI GR ENI 008](#) (V2.1.1): "Experiential Networked Intelligence (ENI); InTent Aware Network
- [ETSI GR ENI 009](#) (V1.1.1): "Experiential Networked Intelligence (ENI); Data Processing Mechanisms"
- [ETSI GR ENI 010](#) (V1.1.1): "Experiential Networked Intelligence (ENI); Evaluation of categories for AI application to Networks"
- [ETSI GR ENI 013](#) (V1.1.1): "Experiential Networked Intelligence (ENI); ENI Intent Policy Model"
- [ETSI GR ENI 016](#) (V2.1.1): "Functional Concepts for Modular System Operation"
- [ETSI GR ENI 017](#) (V2.1.1): "Overview of Prominent Control Loop Architectures"



- [ETSI GR ENI 018](#) (V2.1.1): "Introduction to Artificial Intelligence Mechanisms for Modular Systems"
- [ETSI GS ENI 019](#) (V3.1.1): "Experiential Networked Intelligence (ENI); Representing, Inferring, and Proving Knowledge in ENI"
- [ETSI GR NFV-IFA 041](#) "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Report on enabling autonomous management in NFV-MANO"
- [ETSI GR NFV-IFA 042](#) "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Report on policy information and data models for NFV-MANO".
- [ETSI GR NFV-REL 013](#) "Network Functions Virtualisation (NFV) Release 4; Reliability; Report on cognitive use of operations data for reliability".
- [ETSI GS NFV-SOL 012](#) "Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; RESTful protocols specification for the Policy Management Interface".
- [ETSI GS NFV 005](#), "Network Functions Virtualisation (NFV);Proofs of Concept; Framework".
- [ETSI GR F5G 001](#) v1.1.1, "Fifth Generation Fixed Network (F5G); F5G Generation Definition Release #1"
- [ETSI GR F5G 002](#) v1.1.1 'Fifth Generation Fixed Network (F5G); F5G Use Cases Release #1'
- [ETSI GS F5G 003](#) v1.1.1 'Fifth Generation Fixed Network (F5G); F5G Technology Landscape'
- [ETSI GS F5G 004](#) v1.1.1, "Fifth Generation Fixed Network (F5G); F5G Network Architecture"
- [ETSI GS F5G 006](#) v1.1.1, "Fifth Generation Fixed Network (F5G); End-to-End Management and Control"
- [ETSI GR F5G 008](#) v1.1.1, "Fifth Generation Fixed Network (F5G); F5G Use Cases Release #2"
- ETSI DGS/F5G 013, "Fifth Generation Fixed Network (F5G); F5G Technology Landscape R2"
- [ETSI GS ZSM 001](#) "Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios"
- [ETSI GS ZSM 002](#) "Zero-touch network and Service Management (ZSM); Reference Architecture"
- [ETSI GS ZSM 003](#) "Zero-touch network and Service Management (ZSM); End-to-end management and orchestration of network slicing'
- [ETSI GR ZSM 005](#) "Zero-touch network and Service Management (ZSM); Means of Automation"
- [ETSI GS ZSM 006](#): "Zero touch network and Service Management (ZSM) Proof of Concept Framework"
- [ETSI GS ZSM 007](#) "Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM"
- [ETSI GS ZSM 008](#) "Zero-touch network and Service Management (ZSM); Cross-domain E2E service lifecycle management"
- [ETSI GS ZSM 009-1](#) "Zero-touch network and Service Management (ZSM); Closed-loop Automation; Part 1: Enablers"



- DGS/ZSM-014_SecAspects “Zero-touch network and Service Management (ZSM); ZSM security aspects”
- [ETSI GR IPE 001](#) “Gap analysis”
- [ETSI GR IPE 002](#) “IPv6 based Data Centers, Network and Cloud Integration”
- [ETSI GR IPE 005](#) “5G Transport over IPv6 and SRv6”
- [ETSI GR IPE 006](#) “IPv6 and Cloud using DataBlockMatrix for Food Supply Chain Tracking”
- [ETSI GR IPE 010](#): “IPE Proof of Concepts Framework”
- [ETSI GS MEC 002](#) “Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements”
- [ETSI GS MEC 003](#) “Multi-access Edge Computing (MEC); Framework and Reference Architecture”
- [\[Mref1\]](#) ETSI MEC overview
- [\[Mref2\]](#) ETSI GS MEC 003, V3.1.1 (2022-03): “Multi-access Edge Computing (MEC); Framework and Reference Architecture”,
- [\[Mref3\]](#) ETSI White Paper #32: Network Transformation: (Orchestration, Network and Service Management Framework), October 2019,
- [\[Mref4\]](#) ETSI GS MEC 002 v2.2.1 (2022-01), “ Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements”,

- [\[Mref7\]](#) GS MEC 016 (Multi-access Edge Computing (MEC) Device application interface)
- [\[Mref8\]](#) GS MEC 10-1 (MEC Management; Part-1: System, host and platform management)
- [\[Mref9\]](#) GS MEC 10-2 (MEC Management; Part-2: Application lifecycle, rules and requirements management)
- [\[Mref10\]](#) GR MEC 035 (MEC; Study on Inter-MEC systems and MEC-Cloud systems coordination)
- [1] [ENISA - Securing Machine Learning Algorithms](#)



9. List of Figures

Figure 1: An example of a high-level illustration of Autonomous Networks’ enablers and external interfaces	7
Figure 2: Simplified ENI Cognition Closed Control Loops	11
Figure 3: ZSM Framework	13
Figure 4: Closed loop example	14
Figure 5: Intelligent, coherent, and interconnected loops across business, service and network management domains	15
Figure 6: NFV-MANO architectural framework with IM and MDA functions	18
Figure 7: Closed loop automation in the NFV domain	20
Figure 8: 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/ML from within a Node Element up into the Knowledge Plane level	22
Figure 9: Platform Integration with other Systems	23
Figure 10: Six key features of IPv6 Enhanced Innovations (from Figure 4 of ETSI GR IPE 001 [1])	27
Figure 11: Intent-based architecture of telecom network (from Figure 7 of ETSI GR IPE 002 [2])	28
Figure 12: MEC-in-NFV Reference Architecture (ETSI GS MEC 003 [Mref2])	30
Figure 13: Role of MEC in ETSI standards for Autonomous Networks (ref. ETSI MEC slides [Mref1])	31
Figure 14: Technical characteristics for F5G (from Figure 5 of ETSI GR F5G 001 [1])	33
Figure 15: F5G E2E management and control architecture (from Figure 1 of ETSI GS F5G 006 [6])	35
Figure 16: Features of F5G (From Figure 2 of ETSI White Paper No. #50 [7])	36





The Standards People

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

This White Paper is issued for information only. It does not constitute an official or agreed position of ETSI, nor of its Members. The views expressed are entirely those of the author(s).

ETSI declines all responsibility for any errors and any loss or damage resulting from use of the contents of this White Paper.

ETSI also declines responsibility for any infringement of any third party's Intellectual Property Rights (IPR), but will be pleased to acknowledge any IPR and correct any infringement of which it is advised.

Copyright Notification

Copying or reproduction in whole is permitted if the copy is complete and unchanged (including this copyright statement).

© ETSI 2018. All rights reserved.

DECT™, PLUGTESTS™, UMTS™, TIPHON™, IMS™, INTEROPOLIS™, FORAPOLIS™, and the TIPHON and ETSI logos are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ and LTE™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM™, the Global System for Mobile communication, is a registered Trade Mark of the GSM Association.

