ETSI White Paper No. 40

Autonomous Networks, supporting tomorrow's ICT business

1st edition – October 2020

ISBN No. 979-10-92620-37-6

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

About the Authors

Contributing Organisations and Authors:

China Telecom: Yannan Bai
China Unicom: Bingming Huang
Futurewei: Dong Sun, John Strassner
Huawei: Luigi Licciardi, Hui Li, Lei Wang, Aldo Artigiani
Intel: Dario Sabella, Haining Wang
Orange: Christian Maitre
Portugal Telecom: Francisco Fontes
Samsung: Yue Wang
Telecom Italia: Luca Pesando, Cecilia Corbi
Cadzow: Scott Cadzow

Editors:

Dong Sun, Cecilia Corbi, Scott Cadzow

Contents

Executive Summary

This White Paper presents how Autonomous Networks can impact the role of telecommunications in assuring the success of the digital transformation of industry by enabling more responsiveness to the verticals in exploiting their business, in terms of operations efficiency and new revenue opportunities that are the Autonomous Networks' basic business objectives. The new revenue opportunities are driven by upgrading the Information and Communications Technology (ICT) ecosystem due to the arrival of business partners such as verticals and solution providers (e.g., communications service providers (CSPs), vendors, integrators and consultants).

The rationale of this White Paper is that Autonomous Networks (AN) are designed to support this transformation. This technology evolution has now reached a point where a revolution is required in the way networks are managed, leading to the introduction of new level of automation and intelligence in the management and provisioning of services and networks. This revolution is termed Autonomous Networks.

In order to gain support, ranging from telecommunications to the extended ecosystem, this White Paper explores the challenges, business value, vision and the framework around Autonomous Networks. We also discuss Autonomous Network Levels along with key components associated with the concept of Autonomous Domain and describe security and privacy capabilities in the evolution of Autonomous Networks. A small number of use cases, in conjunction with Autonomous Network Levels, are described in order to illustrate the value proposition of Autonomous Networks and to highlight the contribution of Standards Development Organisations (SDOs) in driving both the definitions and recommendations associated with Autonomous Networks. We believe that what is needed is a proper perspective in order to deliver reliable standards; and to do so successfully, we must solicit feedback from decision makers and professionals in order to prevent fragmentation in a collaborative environment.

The Autonomous Networks' objective is to provide a wide variety of autonomous "Network/ICT" services, infrastructure and capabilities with "Zero-X" (zero wait, zero touch, zero trouble) experience based on fully automated lifecycle operations of "Self-X" (self-serving, self-fulfilling, self-assuring) to dynamically accommodate and adapt to customer needs and available resources. These services range from more efficient versions of current services to mission-critical services to new disruptive services for support of new business models and innovative user experiences; Autonomous Networks also feature self-evolving telecom network infrastructures.

An Autonomous Network consists of a simplified network architecture, virtualized components, automating agents, intelligent decision engines which present self-dynamic capabilities with the goal to create intelligent business and network operations based on the concept of closed-loop controls.

The key design principles of Autonomous Networks in order to support tomorrow's ICT systems are:

- ***Simplification*:** Componentize the technology into discrete business capabilities to simplify and accelerate the on-boarding of partners.
- ***Automation*:** Create zero touch interactions through closed-loop automation of business and technology operations.
- ***Intelligence*:** Move from pre-programmed to real-time data analysis based on ML and AI.

From a business perspective, Autonomous Networks are composed of Autonomous Domains that serve as the basic entity exposing network resources/functionalities as services/capabilities. The basic operational principals of Autonomous Domains are:

- ***Autonomy:*** each Autonomous Domain can govern its own behaviour in support of business goals.
- ***Abstraction:*** each Autonomous Domain hides the details of domain implementation, operations and the functions of the domain elements from its users.
- ***Collaboration:*** Service Operations direct specific Autonomous Domains to cooperate with each other based on the intent mechanism to fulfil business and customer needs throughout the service's lifecycle

The Autonomous Networks will leverage the technology innovation capabilities offered by 5G, artificial intelligence, virtualization, cloud and edge computing as underlying elements ensuring that the verticals are an integral component of the telecommunications ecosystem.

ETSI is playing and can play a key role in the recommendation for and standardization of Autonomous Networks due to its excellence and worldwide recognition as an SDO in Network standardization. A successful industry-wide adoption of Autonomous Networks requires large consensus in building a common ecosystem. Therefore, we recommend a coordinated effort by leading SDOs, cross industry and vertical organisations, open source alliances and regulatory entities in order to succeed in this digital telecommunication transformation. In some sense, the creation of Autonomous Networks in telecommunications is similar to the advent of autonomous driving vehicles in the automotive Industry.

1 Challenges, Opportunities and Business Value

1.1 Challenges and Opportunities

Over the past few years, business and social activity have become increasingly digital, enabled by computers and telecommunication services. The ad-hoc arrival of innovative technologies, be that in the domain of software defined networking and the virtualization of network functions, or increasing demands for decoupled IT capabilities, such as cloud computing and storage, or major new network technologies, such as 5G, enables and enhances the users of ICT to not only evolve their business but also to develop new ones.

The consequence of this evolution is that the demands placed on networks are increasingly driven by end-users. Whichever type of user is considered, they all require a combination of fast and context-aware network and service configuration, flexible new service generation, dynamic and efficient resource allocation, and ultimately, accountability - as ICT is essential to the operation and development of business. To accommodate these evolving customer needs, the telecom industry has taken the investments in base technology and applied it to rapidly evolving technologies, ranging from discrete networks for voice, video and data to a complex one-stop-shop supporting many forms of traffic simultaneously. The next stage of this evolution, which is taking place now, requires a new form of convergence: from CSPs as providers to CSPs as partners. Thus, technology evolution is forging ahead alongside the business evolution of CSPs as they form active partnerships with the vertical industries that use their ICT capabilities.

Existing networks are made up of a complex set of heterogeneous devices that must be integrated to provide seamless end-to-end services. Until very recently the planning, implementation and management of this mix of services has been a largely manual activity with some automated assistance. In short, no matter the degree of refinement, it is recognized that these services can no longer be managed using such approaches. The new requirements need a transformation supported by the integration of new technologies, such as virtualization, 5G and Artificial Intelligence that together, as well as a new level of automation and intelligence in the management and provisioning of services and networks, provide scalable mechanisms for managing complexity.

1.2 Business Values

The premise of this White Paper is that in a world of user driven services, automation is not an option but rather, a necessity- as the only realistic means of dynamically managing, orchestrating and coordinating the many high volume and complex services across both data and technical domains.

Furthermore, automation prevents isolation and addresses complexity; delivering efficiency and growing revenue. By using AN, customers can benefit from increased network reliability, optimized usage, control, connectivity and customizable services. For example, customers can have access to more flexible usage models (e.g., pay per use, pay per active services, etc.) according to their needs with the required performance and Service Level Agreements (SLAs) that can dynamically scale up and down.

Autonomous Networks are perceived differently, depending on the perspective. Below we describe this phenomenon for Telcos, acting as core providers; business partners, acting as buyers from Telcos; and customers, acting as final users:

- *Telcos* ➔ Features*:* cloudified, reduced complexity, self-repairing, less OSS, Autonomous Domains, reduced OPEX and APIs everywhere.
- *Business Partners* ➔ Characteristics: lower cost, higher reliability, reduced time to market, customer facing APIs and cross-domain orchestration.
- *Customers* ➔ Capabilities*:* X-as-a-Service model, custom services, on-demand, self-service, integration and cloud convergence.

The introduction of cloud-enabled Autonomous Networks capabilities will evolve the Telco Business models from the traditional classic services to the most sophisticated platform business model working with the partners' ecosystem. New services will be introduced: customized network services, on demand services, self-service, edge/cloud convergence, Network-as-a-Service; with significant advantages for the whole Industry in terms of end-to-end service availability and time to market.

When the Autonomous Networks is in place, operators will be able to benefit from *a strong improvement in efficiency*. And for Telcos, the shared innovative services could present *new revenue opportunities* in new markets.

The Autonomous Networks' model of Figure 1 from the GIO report on Autonomous Digital Infrastructure Workshop **Error! Reference source not found.** shows how proper operating model can be developed. The A utonomous Networks' capabilities required by the customer are realized in both the network core and network platform.

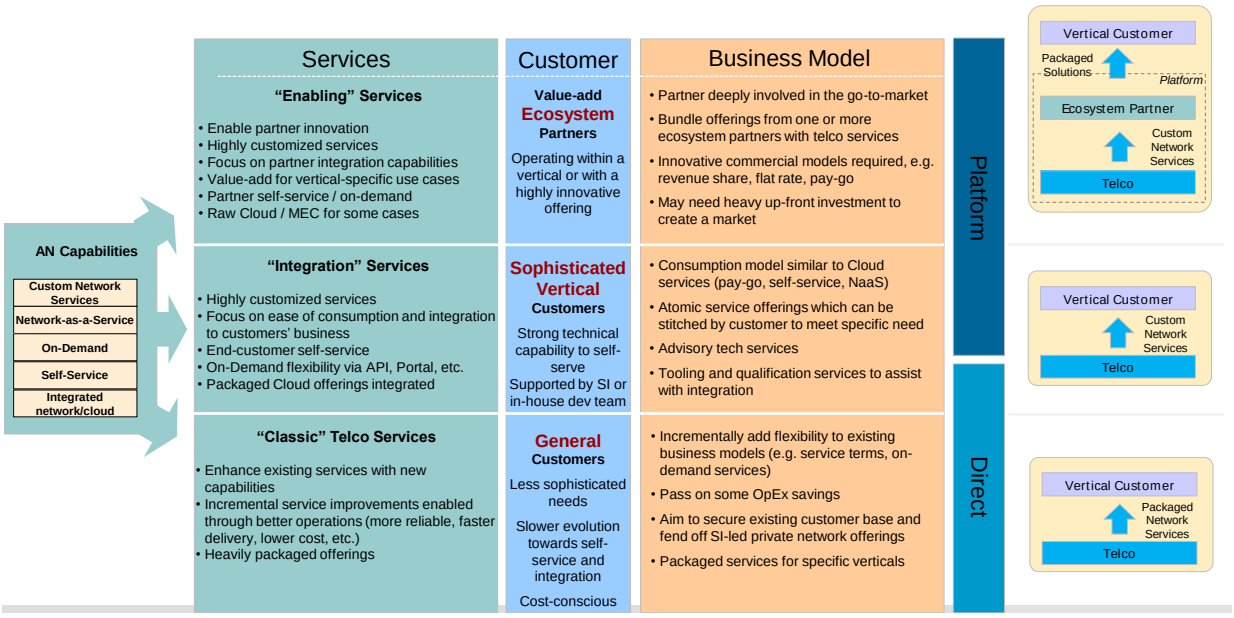

Figure 1: The AN Telco business model

2 Vision and Framework

2.1 Vision

Figure 2 illustrates that the vision of Autonomous Networks (see Autonomous Networks – the network of the future being designed and built today! [1]) is to provide innovative ICT services and capabilities with "Zero-X" experience, like zero wait, zero touch and zero trouble for the users of vertical industries and consumers; offering simplicity and leaving the complexity with the providers.

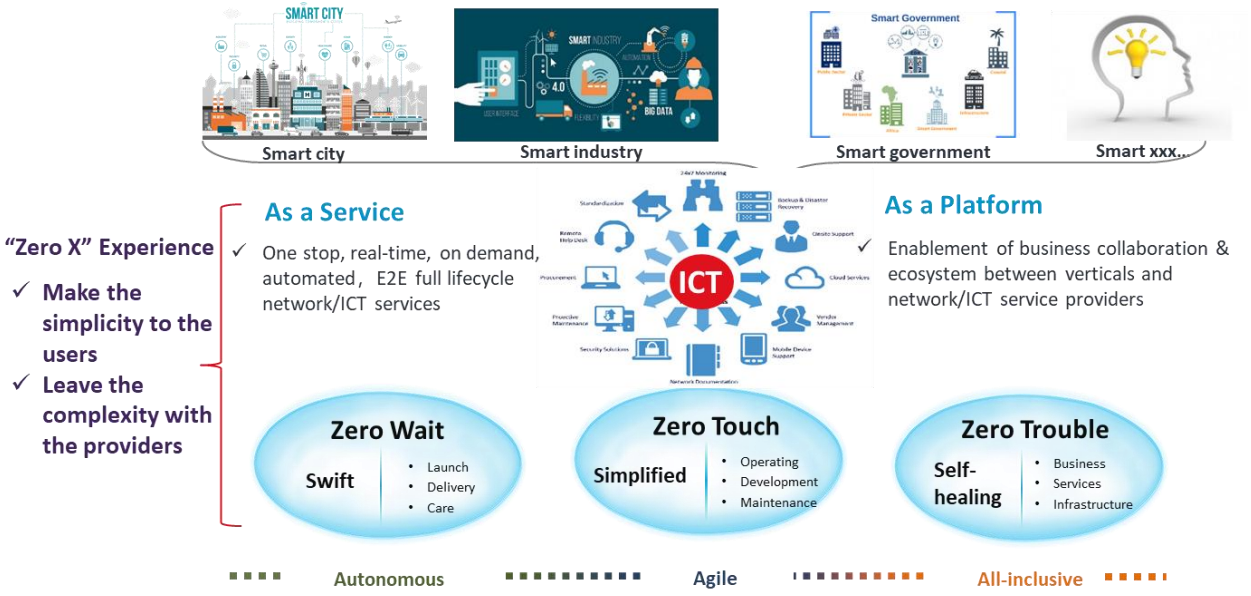

Figure 2: Vision of Autonomous Networks: Upgrading the ICT Industry

The Autonomous Networks, whose initial concept had been described in TM FORUM Whitepaper (2019, May). Autonomous Networks: Empowering Digital Transformation for the Telecoms Industry [2], TM FORUM IG1193 [3], TM FORUM IG1218 [4]) and TMF Whitepaper (2020, October) [5] by the TM Forum, can enable highly automated business and network operations of "Zero-X" experience for innovative services as well as existing services, which can lead to innovative business models – also described in TM FORUM IG1218. [4] by the TM Forum:

- **… *as a Service:*** one stop, real-time, on demand, automated, E2E full lifecycle network/ICT services.
- **… *as a Platform*:** enablement of business collaboration & ecosystem between verticals and network/ICT service providers.

In order to achieve these objectives, it is essential to transform the existing production, business and collaboration models into new ones, as has been described in TM FORUM Whitepaper (2019, May). Autonomous Networks: Empowering Digital Transformation for the Telecoms Industry [2], TM FORUM IG1193 [3] and TM FORUM IG1218 [4] by the TM Forum:

- **Digital partner collaboration ecosystem:** transform from traditional customer-provider-supplier model to form digital partner collaboration ecosystems. This is done to accommodate the customer need of easy-to-use customized and dynamic network/ICT services and capabilities.
- **Collaborative production:** leverage the best-suit solutions using cutting edge technologies through benefit co-sharing.
- **Knowledge-as-a-service:** sharing of operational knowledge and corresponding business benefits through a common platform as an enabling service rather than a cost reducing activity.

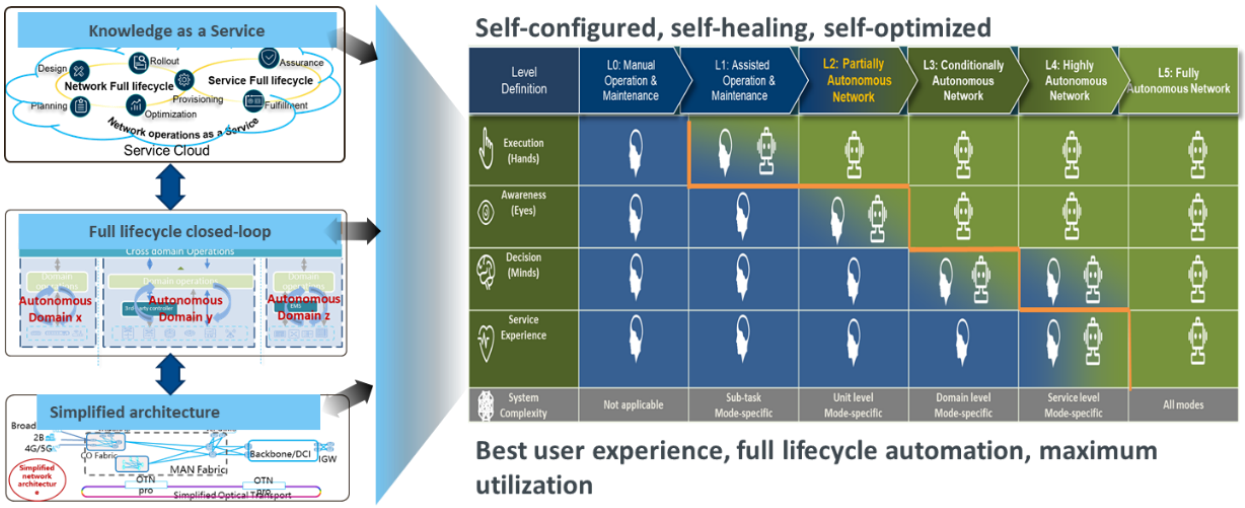

Figure 3: Autonomous Networks Levels: Main thread of Autonomous Networks

The vision and business requirements listed above lead to the need for classification of Autonomous Networks Levels to ensure that digital partners (customers, CSPs and vendors) can interact using the same mechanisms in terms of the automation, service intelligence and capabilities.

In a manner somewhat akin to the levels of automation in cars (see SAE J3016 [6]) there are several autonomous network levels. These levels are described in in TM FORUM Whitepaper (2019, May) [2], TM FORUM IG1193 [3], TM FORUM IG1218 [4]) and are as follows:

Table 1: Autonomous Networks Levels

Level 0 - manual management	The system with assisted monitoring capabilities, and all dynamic tasks are executed manually, which is not viewed as Autonomous Networks.
Level 1 - assisted management	The system runs certain repetitive sub-task based on pre-configured policy to improve the efficiency, which is not viewed as Autonomous Networks.
Level 2 - partial Autonomous Network	The system runs closed-loop O&M for certain business units based on the intelligence of certain external environments.

Level 3 - conditional Autonomous Network	The system furthers with awareness of sensing real-time environmental changes. In certain scenarios, optimizing and adapting itself to the external environment to enable intent-based closed-loop.
Level 4 - high Autonomous Network	The system runs, in a more complicated cross-domain environment, analyzing and making decision based on predictive or active closed-loop of services and customer experience-aware networks.
Level 5 - full Autonomous Network	The system runs closed-loop capabilities across multiple services, multiple domains in the full lifecycle

Note that more example use cases are illustrated in Clause 4.

2.2 Autonomous Networks Framework

The overall framework of Autonomous Networks consists of 3 layers plus 4 closed-loops as defined in Figure 6 of TM FORUM IG1218 [4] and Figure 8 of the Whitepaper [5] by the TM Forum.

-3 layers: Base groups of functions for diverse customer need and Autonomous Networks services:

- **Business operations layer**: supports customer, ecosystem and partner business enablement and operations.
- **Service operations layer** supports network planning, design, rollout, provisioning, assurance and optimization operations across multiple autonomous domains.
- **Resource operations layer** supports automation of network resources and capabilities in each autonomous domain level.

-4 closed-loops: To fulfil the full lifecycle of the inter-layer interaction process.

- **Business closed-loop** enables the interaction between business and service operations layers for business-service lifecycle
- **Service closed-loop** enables the interaction between service and network resource operations layers for service-resource lifecycle
- **Resource closed-loop** enables the interaction of network resource operations in the granularity level of autonomous domains.
- **User closed-loop** enables the interaction across three layers and three closed loops for the E2E full lifecycle of user service.

In order to support the aforementioned full lifecycle of closed-loops, key capabilities of Autonomous networks have been described in TM FORUM IG1218 [4] by the TM Forum and are as follows:

Table 2: Capabilities of AN

Category	Sub-category
Self-serving	**Self-planning/capability delivery** supports the customization (DIY) capabilities of network/ICT service planning, design and deployment.
	Self-ordering supports the online, digitalized and/or one-click ordering capabilities of network/ICT services.
	Self-marketing supports the automated marketing activities for general and/or personalized campaign/promotion.
Self-fulfilling	**Self-organizing** supports the collaboration of business/service/resource intent delivery on demand.
	Self-managing supports the orchestration of business/service/resource intent delivery on demand.
	Self-governing supports the governance of business/service/resource intent delivery on demand.
Self-assuring	**Self-monitoring/reporting** supports the Automated, continuous monitoring and alerting in real time.
	Self-healing supports the recovery of SLA such as performance, availability and security in real time.
	Self-optimizing: supports the optimization of SLA such as performance, availability and security in real time

In a nutshell, Autonomous Networks use a simplified network architecture along with physical and/or virtualized components, intelligent agents and decision engines that provide fully automated “Zero-X” innovative, critical ICT services. These features affect the experiences of users/consumers of vertical industries and support “Self-X” (self-serving, self-fulfilling and self-assuring) capabilities in order to enable digital transformation of both vertical and telecom industries.

3 Key Perspectives of Autonomous Networks

3.1 Autonomous Networks and Autonomous Domains

An Autonomous Network joins a set of one or more Autonomous Domains, thus for the purposes of this paper ANs connect ADs to provide an autonomous network system. The characteristics that ANs and ADs have to exhibit were initially described in in TM FORUM Whitepaper (2019, May) [2], TM FORUM IG1193 [3], TM FORUM IG1218 [4] by the TM Forum and are:

- **Self-governing:** controlling the actions and behaviour of managed entities within an Autonomous Domain.
- **Programmable:** open APIs, along with standardized external reference points, are defined to support interoperability.
- **Explainable:** an Autonomous Domain can describe why a decision was made in terms understandable to humans.
- **Composable:** a function or service can be built from smaller functions or services.
- **Business-driven:** offered services are defined by business rules and goals.
- **Model-driven engineering**: the systematic use of domain models in all stages of the software engineering lifecycle.

From a business perspective, an Autonomous Domain serves as the basic entity for exposing network resources/functionalities as services/capabilities. An Autonomous Domain is a logical building block that defines a boundary of responsibility and authority to fulfil automated intelligent services. Autonomous Domains use one or more closed control loops to support end-to-end automated lifecycle operations.

The basic principles of the operations of Autonomous Domains are:

- **Autonomy:** Each Autonomous Domain is able to govern its behaviour and support business goals.
- **Abstraction:** Each Autonomous Domain hides the details of domain implementation, operations and the functions of the domain elements from its users.
- **Collaboration:** Service operations direct specific Autonomous Domains to cooperate with each other based on the intent mechanism to fulfil business and customer needs throughout the service lifecycle.

3.2 Usage of Autonomous Domains

The Autonomous Domain can be flexibly instantiated for diverse business/service scenarios such as fixed access network, wireless access network, core network, transmission network, VPN and SD-WAN. Each Autonomous Domain may interact with other Autonomous Domains through open interfaces that are managed according to user, business and service demands. This coordinates different transport networks, as well as core networks, to fulfil business and service needs.

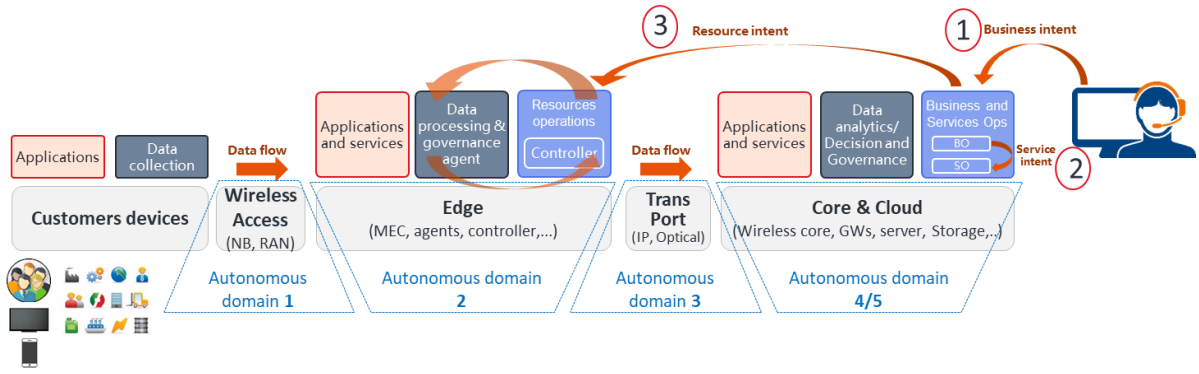

Figure 4: Usage of Autonomous Domains

Figure 4 shows usage of Autonomous Domains to collaboratively ensure that different business needs of Autonomous Networks' services are fulfilled.

The Autonomous Domains function as follows:

- Autonomous domain 1 – ***Access***: This AD supports different types of access like cellular and wireless.
- Autonomous domain 2 – ***Edge***: This AD supports the real-time processing and localization required for connectivity, control, management, orchestration, analytics and applications for AN services.
- Autonomous domain 3 – ***Transport***: This AD supports various transport networks such as IP and Optical; in both separate and integrated modes as well as backbone.
- Autonomous domain 4/5 – AD 4 – ***Core***: This AD supports the core network, along with computing and storage; AD5 – ***Cloud***: This AD supports distributed processing for management and orchestration applications. Physically these two domains could be separate or collocated as required.

The Autonomous Network applies three types of interacting closed-loops to ensure full end-to-end lifecycle operation and management. The detailed process has been described in TM FORUM IG1218 [4] by the TM Forum and is as follows:

1) **Business Closed-Loop:**

   1a) *Business Intent Request:* The user described their "Business Intent" to the "Business Operations (BO)" system that requests AN services.

   1b) *Business Intent Translation:* The BO translates business intent into Service Intentions (SI) such as connectivity, availability, security, quality of service and/or experience; according to the organization's business architecture request to the "Service Operations (SO)" system as SI requests.

2) **Service Closed-Loop:**

   2a) *Service Intent Request:* The SO in AD5 distributes the Service Intent to the SOs in AD4, which then translate the SI into Resource Intent (RI) according to the system architecture of each SO. This results in resource operation management and monitoring commands.

2b) *Service Fulfilment:* The SO will interact with and instruct "Resource Operation (RO)" systems in each Autonomous Domain to deploy all required applications in order to orchestrate, manage and monitor their resources.

3) **Resource Closed-Loop:**

3a) Resource Execution: The RO of each AD manages its resources to meet the needs of each service that it is supporting. It also transfers applicable data to the local PoP (edge) for real-time information processing and decision making.

3b) *Resource Assurance:* Each Autonomous Domain monitors abnormal events such as performance, fault and security attacks; and alerts other affected Autonomous Domains. Affected Autonomous Domains collaborate to plan and implement a solution and inform the BO and SO in AD5 when the solution is implemented, and the problem is resolved. The RO may report to the SO when the events are beyond the management of a single Autonomous Domain Level. In this way, the SO will take responsibility for cross-Autonomous Domain events in real time.

3.3 Key Capabilities

3.3.1 Overview

An Autonomous Network is expected to dynamically adapt to changes in its environment. This dynamic adaptation is built upon three principles that are present in Autonomous Domains: business awareness, self-x capabilities and intent-driven interaction. This forms the basis for two key future features: Knowledge-as-a-Service and explainable decisions. These principles provide dynamic, run-time intelligence to enable business goals and to determine services offered in a given context. Key benefits include:

- A modular and extensible framework that enables support for new technologies, business models and operations.
- The use of business rules to determine the set of resources offered in a specific context.
- The agile, secure and flexible delivery of network services supported by self-governing networks and networked applications.
- Ease of management and operation of infrastructure and services.
- Service adaptation using data-driven intent-based operations.
- An ecosystem that enables digital transformation across many industries.

3.3.2 Business Awareness

An Autonomous Domain enables the goals and rules of an organization to be mapped onto a business architecture; the business architecture is then used to realize a system architecture. This results in a mapping of capabilities and services provided by a business related to the strategies, products and goals of an organization; which is then implemented by an Autonomous Network. The mapping is done using the business, user, service and resource closed-loops described earlier in section 3.2.

The business architecture uses shared knowledge and metadata to determine which business services are needed in a given context; these are translated into goals that one or more Autonomous Domains use to provide enhanced network and service capabilities. The current context defines constraints on the functionality provided by each Autonomous Domain. As a result, end-to-end business services are created using a simplified set of abstractions that defines the network and service capabilities available at that moment to meet those goals.

An Autonomous Domain translates business goals and customer needs into network functions and services that support the end-to-end delivery of services for the business; even when the environment changes. This means Autonomous Domains collaborate to adapt their collective capabilities to maintain contracted services; thus, dynamically providing new services as required. This business awareness is achieved using self-x capabilities, intent-driven interaction and modelled knowledge.

3.3.3 Self-X Capabilities

The governing of behaviour requires network functions and services to be created and/or adapted to meet business needs. The concept of Self-X refers to a set of intelligent functions that collectively ensure the delivery of secure services based on current resource availability.

An Autonomous Domain provides a set of closed-loop systems that manage the resources within it. Each closed-loop system is built upon self-knowledge, which is the ability of an entity to be aware of its own capabilities and the environment effects on those capabilities.

To be clear, self-knowledge provides ***cognition***: the ability to gain knowledge and comprehension. Each closed control loop observes its environment and functionality, orients those observations to the current situation and determines if any goals are threatened. If goals are threatened, then a set of actions are selected to fix the problems and learn from the consequences of those actions. Hence, operations such as configuration and monitoring are largely executed in an automated manner; driven by these cognitive processes. This enables an Autonomous Network to adjust its behaviour when user needs, business goals and environmental conditions change.

Self-X capabilities enable an Autonomous Network to plan new courses of action, set new goals - for itself or for its collaborating Autonomous Domains - and, most importantly, learn from actions that it has taken to become more efficient and effective in the future. More importantly, these can all be done with a minimum of human intervention.

Finally, since an Autonomous Domain has business awareness, it can respond to new business needs and provide corresponding business, network and service capabilities. This includes planning, marketing and similar activities. For example, the Autonomous Domain can be personalized to provide one-click ordering, targeted upsell and other promotional activities.

3.3.4 Intent-Driven Interaction

Policy management is used to provide decisions in a consistent and scalable manner and to ensure that system goals and objectives are met. Formally, the definition is:

> *"A Policy is a set of rules used to manage and control the change and/or maintenance of the state of one or more managed objects."*

Policy can take different forms. Imperative policies are commands that explicitly change the state of a set of targeted entities, while intent policies use a restricted natural language, such as English, to express a set of goals to be accomplished without defining how to implement those goals.

Intent enables the needs of different constituencies to be accommodated by tailoring its language grammar to concepts and terminology familiar to each constituency. This enables business goals to be translated into terms that an application developer or a network administrator could use and vice-versa. For example, a business user can create an intent to maximize revenue; this can be translated to SLAs and class-of-service markings for different applications and for different users.

Intent can be viewed as invariant, so that as the environment changes, the resources are dynamically optimized in all affected Autonomous Domains to ensure that the goals of the intent are maintained. In the above example, if significantly more users at a lower level of service start using applications, then the original intent still holds; each affected Autonomous Domain invokes a utility function to determine the optimal mix of users at different service levels in order to maximize revenue. More importantly, as business needs change, the intent can be adjusted. In the above example, if the intent is altered to maximize a different feature, such as user cost, then the resources in each Autonomous Domain are automatically adjusted to meet that intent.

Thus, intent simplifies the definition of goals and services for different users and hides their implementation complexity.

There are two types of intent-driven interaction: (1) human-machine interaction and (2) resource closed-loop interaction. The first relies on humans *selectively guiding and providing goals* to different types of machine learning systems. The second refers to the intelligent distribution of intent to the affected Autonomous Domains. Each Autonomous Domain interacts with other Autonomous Domains as necessary in order to collaboratively provide an end-to-end service.

Intent interaction may be provided by dedicated external reference points and APIs, as well as other means that abstract the functionality of an Autonomous Domain. This creates the abstraction of a single, simplified network - even though it is made up of different domain-based capabilities.

3.3.5 Future Features

1) Knowledge-as-a-Service

The scaling of resource and service operations requires retrieving knowledge from each applicable Autonomous Domain for a given context. Each Autonomous Domain has different users with different needs, defined by different concepts and vocabularies. The integration of the needs of these different constituencies and their associated knowledge, create different viewpoints that define the business and system architectures. A viewpoint is a set of abstractions that enables a set of users to view what is relevant to their tasks and ignore what is not. Knowledge-as-a-Service (KaaS), delivers knowledge from a viewpoint to a set of users as needed.

Knowledge takes many forms; two important ones are: (1) facts derived from information processing that have to do with system state, and (2) inferences derived from reasoning algorithms and logic that reflect changes to the current state. The commonality of state between the two types of knowledge enables both to be contextualized and reused in similar situations at a later time. The knowledge repositories are shared between Autonomous Domains and are updated in a consensual manner to reflect new knowledge learned.

The modelling of knowledge from different viewpoints enable KaaS to be customized for different consumers. For example, knowledge obtained by telemetry processing in the Autonomous Network can

be harvested and refined by each participating Autonomous Domain; which correlates the information ingested to build higher-level domain knowledge. These insights, such as discovery of trends in user activities or predicting when to offer different services, can then be used to better manage resource assignment and utilization.

Autonomous Domains use KaaS in different ways. For example, KaaS can be used to support intelligent and adaptive resources management to protect system goals and contracted services; both within and across Autonomous Domains. KaaS may also be offered as a platform feature of Autonomous Networks, which would enable a group of stakeholders to flexibly produce and consume knowledge as a commercial service.

2) Explainable Decisions in Autonomous Networks

An Autonomous Network is not a "black box" that prevents its users from understanding why it made the decisions that it did. The inherent complexity in the architecture and algorithm itself give rise to questions, such as "*how did the machine come to that conclusion"* and *"why did the machine choose that approach".* This is especially important for failure analysis, legal and privacy concerns. Most deep learning algorithms exacerbate this problem, since their ability to create probabilistic associations between an input and a desired output is very difficult for humans to predict - let alone understand or visualize. In addition, if a solution operates as a "black box" and its decisions cannot be understood by a human, then that solution can cause trust issues.

In contrast, an Autonomous Network provides both an understanding of how the deployed algorithms work; as well as explanations for why a set of related decisions were made. Explanations in support of decisions made by an AI solution are crucial in many applications, including autonomous vehicles, medicine and financial applications. This has resulted in a field of study called eXplainable Artificial Intelligence (XAI), whose goal is to ensure that humans are able to understand why a machine makes its decisions without knowing the details of the structure of the model or how it processes data internally.

3.4 Autonomous Networks Implications

3.4.1 Simplified Networks

Autonomous Networks provide a set of powerful resource and service abstractions that enable the associated network infrastructure, usage of operations and associated supporting functions and applications to be simplified.

This takes different forms, depending on the type of business-driven services that are being supported:

- The "simplified networks" aim at the simplicity of the usage of network capabilities and services through the intelligent automated closed-loop operations, which will conceal the complexity of the network technologies, implementation and integration to the users of network capabilities/services.
- The scope of the simplified network usage should include both Network (CT) and business operations (IT) perspectives, i.e. a simplified ICT infrastructure usage.
- This simplification approach does not prevent using innovative technologies like 5G, AI, big data, Edge, Cloud or IoT. Rather, from a user's perspective, these technologies will improve and simplify network/service operations.

- The simplification may also result in less architectural layers, transit hops and/or a reduced number of protocols and/or more automated management and monitoring. Another example is the increased reusability, integration and composability of network functions and services that serve as "building blocks" to create more powerful network functions and services.

3.4.2 Network Differentiation

Autonomous Networks differ from traditional networks in several key areas such as operation, maintenance and decision-making. When an Autonomous Network is deployed, the following statements will become apparent:

- "We will observe a move from manual operation to automated execution".
    - Traditional manual operations will be replaced with the automated processes of an Autonomous Network. The network operational model will change from human-in-the-loop (i.e., manual intervention is required in the runtime execution of an operation, such as configuration) to humans *selectively guiding and providing goals* for AI systems. This enables human resources to be better utilize and allocated to tasks that need them. The Autonomous Network assists humans by providing smaller amounts of relevant information based on the viewpoint of the human. Humans design using models, policies and other abstractions. KaaS ensures that the right knowledge is shared by users that need that knowledge, further supporting automation.
- **"**Maintenance is no longer passive; driven by complaints".
    - An Autonomous Network provides proactive maintenance that can be predicted, significantly reducing the human workload and transforming it into more of a monitoring and fine-tuning role. This greatly enhances network exception identification and analysis capabilities and continuously improves network running quality and service experience.
- "Expert decision-making will morph into machine-based decision-making and learning".
    - Traditional management operations that rely on expert experience will be replaced by explainable machine-based decisions that enable humans to comprehend why the machine recommended certain course of action. As trust between humans and Autonomous Networks grows, more and more of these decisions will be automated, with the machine always notifying the human that it made a decision. This enhances the system's capability to cope with complex and uncertain issues, greatly improving the response speed, resource and energy efficiency of network services; thus enabling humans to concentrate on more specialized tasks.
- "Open-loop management will move to data-driven, committable closed-loop autonomy of service experiences".
    - Traditionally, network planning, construction, maintenance and optimization are independent of each other. Upstream and downstream data is transferred through processes and manual operations, without sharing information and the intelligence learned from operations to improve the user experience and simplify network operations. An Autonomous Network will use shared knowledge and distribute that knowledge as a service. The construction, maintenance and optimization phases of network services will be automated through enhanced business awareness - like mapping an organisations business architecture to a system architecture - resulting in leveraging the capabilities and

services provided by a business to determine the functionality of an Autonomous Network.

- “Improved efficiency and reduced cost make the entire solution more flexible and agile”.
    - There will be significantly more connections, resources and services in future networks such as IoT and 5G. This drastically increases the complexity and cost of integration. Autonomous Domains and Networks enable operators to focus on the overall business objectives and health of the network - instead of manual management issues. This is achieved using model-driven engineering and KaaS.

3.5 Security and privacy

The core principles of security and privacy in Autonomous Networks are the following:

- Security provisions are core and cannot be removed or disabled (i.e., security is always on).
- Only data that has proof of provenance should be acted upon and policies determining how that proof is obtained should be open to scrutiny.
- Security provisions are married to hard anchors for the Autonomous Network's assurance of the Confidentiality, Integrity and Availability (CIA) paradigm.
- As stakeholders introduce new business logic, appropriate steps should be taken to assure that both logic and the identifying characteristics of data are protected and treated with appropriate privacy oversight.

In general, security provision in Autonomous Networks demands that countermeasures be present to avoid the risks of attack on integrity and availability of the network. Similarly, with respect to privacy, the measures taken should be justified by an impact assessment in order to identity risks in exposing attributes of confidentiality to data, and personally identifiable data - including those belonging to legal entities such as a business stakeholders.

Unlike manual systems, where that the impact of an attack is always the same, in an Autonomous Network system, the degree of connectivity and the number of affected systems makes an attack much more unpredictable. The dynamic nature of Autonomous Networks may amplify the impact of the attack as it progresses through different levels of autonomy.

Therefore, we anticipate that a much more agile security regime, similar to virtualized networks may be necessary, where each instance of a service is both uniquely identifiable and authorized while anchored to a trusted component of the wider underlying system.

In this respect, we expect that Autonomous Networks will build on the security principles that apply to networks composed of virtual devices and services; such as the principles described in ETSI ISG NFV that are built on the output of ETSI TC CYBER. Additionally, the work of ISG SAI will be taken into account wherever the nature of the deployed artificial intelligence could impact the security and functional nature of Autonomous Networks.

The core concern of AN as regards to security is that as the degree of autonomy increases from L0 to L5 the level of attacker knowledge changes, particularly in the context of insider attack wherein the Autonomous Network attacks itself. This will require a more intensive role of monitoring for adverse behaviour but that has to be balanced as every new application is at risk of being ranked as an adversary.

A policy-based security engine, with applicable policies for each business application and coordinated across all applications by means of a per-loop security orchestrator will be explored as the basis of an Autonomous Network security engine.

This may require use of technologies such as Functional Cryptography, such as attribute based cryptography and homomorphic encryption and Permissioned Ledger Technology in order to ensure the use of non-repudiation functions; acting across various control loops that are central to Autonomous Networks.

The security and privacy protection technologies applied to Autonomous Networks will therefore be designed as "by default, always on" capabilities - taking advantage of well understood security mechanisms to maximize the assurances of each of the CIA paradigm for each stakeholder of an Autonomous Network.

4 Use cases

The exemplary use cases presented in this section, provide an insight into the advantages of using Anonymous Networks. Four complementary scopes are illustrated: general transport networks, slicing extensions in 5G and fifth generation of fixed (F5G) and wireless networks. In each use case, we discus both the scenarios and possible different levels of automation.

4.1 End-to-end lifecycle of Autonomous Transport Network

Transport Network automation is a fundamental use case for both verticals and Telcos, by addressing by addressing business goals such as dynamic setup, quality and quantity.

The central control plane enables the collection and dissemination of all the relevant information at one junction, with local filtering and aggregation. This makes it possible for AI to play a relevant role, having all this aggregate information available for analysis.

The presence of a Digital Twin mechanism enables the management of the E2E Transport Services across the whole Transport Network (e.g., Fronthaul, Backhaul and Backbone), gathering the network behaviour data, such as topology, configuration and routing, and correlating them based on time and space.

Using AI to continuously analysing metrics from IFIT, predictive SLO breach can prevent service degradation proactively by adjusting connectivity paths and resources assignment with SRv6 technology.

This enables the creation of a multi-dimensional Transport Autonomous Domain “Visualization and Reporting”, enhancing all phases of the network lifecycle management.

In the following table, we consider Transport Network underpinning 5G lifecycle management for both infrastructure and service management. Only autonomy levels 2 to 4 are considered, due to the fact that either current technologies already have those functionalities, or they will become available in the foreseeable future.

Table 3: Autonomy of Transport Network 5G lifecycle management

Full lifecycle	Level 2		Level 3		Level 4	
	Key Features	Key Capabilities	Key Features	Key Capabilities	Key Features	Key Capabilities
Network Planning	Offline semi-automated planning	New access rings, new areas (aggregation rings), new bearer networks and 5G edge cloud manual offline design with automated consistency check	On -line Automated Planning Based on Simulation	New access rings, new bearer networks and 5G edge cloud planning based on Digital Twin (DT) capacity simulation and robustness analysis	Automated planning based on prediction	New access rings, new bearer networks and 5G edge cloud planning based on evolution forecast and service planning requirements
Network Deployment	Automated device management and manual remote software commissioning	Commissioning devices connected on the access ring, regional, or edge cloud with compatibility check	Devices automatically go online without manual software commissioning.	Bringing devices on the access ring, regional, or edge cloud online with automated configuration change and automated acceptance test execution	Devices automatically go online without manual software commissioning.	Bringing devices on the access ring, regional, or edge cloud online. Configuration related acceptance error automatically corrected
Service provisioning	Automated network provisioning	VPN, tunnel and single-station service provisioning based on network model and template, with expert review and confirmation	Service-driven automation	1. 5G bearer: VPN service provisioning, intelligent clock provisioning and slicing service automated provisioning with service simulation and verification before implementation 2. 5G edge cloud: interconnection between the edge cloud and central cloud, interconnection between edge clouds and collaboration between the edge cloud and bearer network	Intent-driven automation	Intent driven service management (e.g., new VPN site addition, new 5G MEC applications and 5G B2B access). System perform in advance the simulation of Service Deployment verifying the impact on the existing services and resources by means of DT
Network change	Tool-assisted network change	service migration (CPE relocation), topology change (ring addition or deletion, single-homing to dual-homing), capacity expansion and replacement (NEs, boards and links), and version and patch change. Manual acceptance and commissioning, automated rollback	Automated network change	service migration (base station port migration), topology change (ring addition or deletion, single-homing to dual-homing), capacity expansion and replacement (NEs, boards and links), and version and patch change. Service driven telemetry with automated choice of relevant indicators	Automated network change	Automatically perform smooth evolution, ring to tree, service migration, topology change, capacity expansion and replacement and version and patch change according to observed and forecasted traffic/service evolution
Network Maintenance	NE-level monitoring and troubleshooting	1. Network-level visibility 2. NE-level monitoring and troubleshooting 3. Manual monitor of alarm and performance 4. Manual recovery from fault conditions	Service- and network-level monitoring and troubleshooting	1. Visualization: service visualization (service overview and single service) and network visualization (NEs, topologies, protocols, tunnels and slices) 2. Service and network exception identification and troubleshooting 3. Automated recommendation of fault remediation actions 4. Interaction with operator's Technical Expert to grow knowledge base	Monitoring and troubleshooting based on prediction	1. Visualization: service visualization (service overview and single service) and network visualization (NEs, topologies, protocols, tunnels and slices) 2. Service and network exception identification and fault self-healing 3. Fault prediction for both Hardware and Software faults (e.g., memory leak, process hanging)

Network Optimization	Manual optimization	1. Tunnel-level optimization 2. No dynamic adaptation and overflow avoidance, possible packet loss	Policy-based, manual decision-making and automated optimization	Network optimization (such as link usage balancing) and service optimization (SLA assurance such as bandwidth and latency)	Automated optimization based on service intents	1. Forecast-based optimization 2. System simulation and automated decision-making

4.2 End-to-end Automation of F5G Networks

The fifth generation of fixed networks or F5G, which evolves from today's fixed network and largely extends the optical fibres towards the end users, provides new high-quality services for homes, businesses and vertical industries. Typical use cases for F5G include cloud VR, cloud desktop, cloud enterprise, online gaming, online education, online medicine, smart home, smart factory and smart city.

The key enabler of F5G automation and autonomy is end-to-end management and control system. It makes optimized use of ultra-high bandwidth resources while efficiently managing massive and dense communication networks in order to improve the experience of both operators and end users.

As the aforementioned management and control system evolves towards higher levels of automation and autonomy, it will be able to sense real-time environmental changes, learn, make intelligent analysis and provide advice to network operators or customers on decision-making, optimization and adjustment of the F5G network.

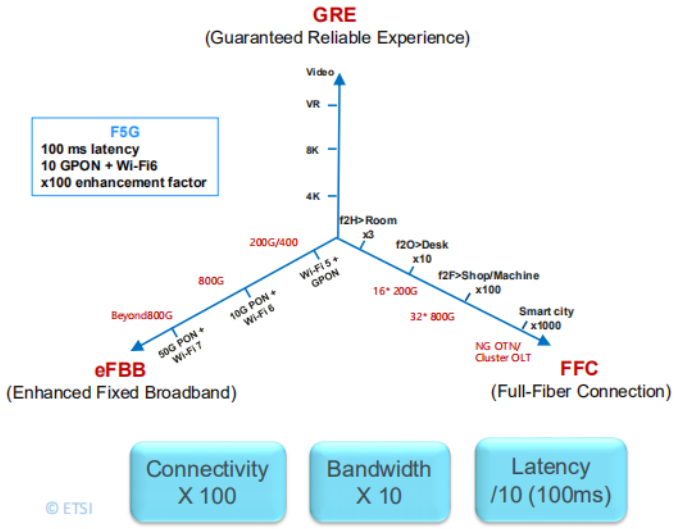

Figure 5: F5G networks

4.2.1 Network Resource Automation and Orchestration

1) Scenario Definition and Description

In F5G, most services need to pass through multiple network segments; from servers to user terminals, such as the Backbone, Metro, Access and Customer Premises Networks (CPN). This requires unified management, operation and maintenance of optical transport, IP, access and CPN network segments, to enable fast automated service provisioning, real-time and online service ordering, and end-to-end Quality of Service (QoS) and Quality of Experience (QoE) assurance.

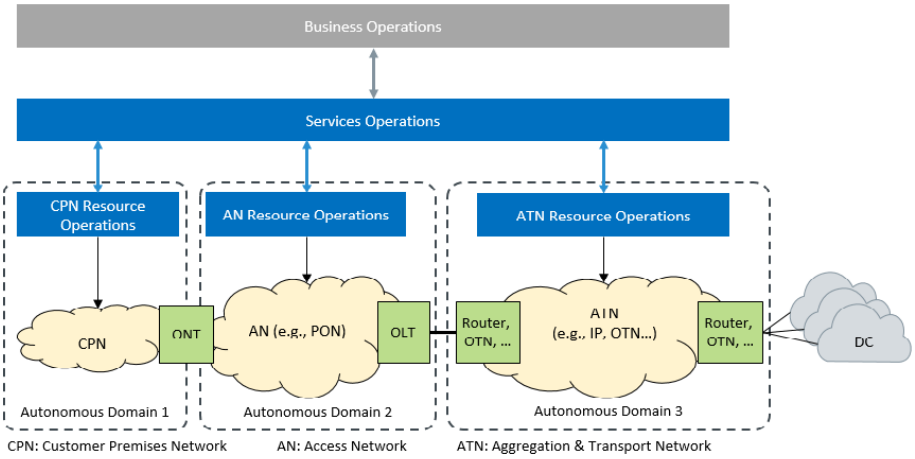

Figure 6: Network Resource Automation and Orchestration

To achieve this, an automated management and control system, like a SDN, will be introduced into each network segment of F5G to form the Autonomous Domain. On top of them, an end-to-end orchestrator is used for the network resource optimization, service provision, fulfilment and global operation. The APIs between SDN controllers and end-to-end orchestrator will be specified to enable these features.

2) Autonomous Networks Levels

Level 1: Each domain segment of CPN, Access Network and Metro Network is controlled by an assisted management system. There are no automated end-to-end orchestration functions.

Level 2: The end-to-end orchestrator is introduced to perform end-to-end network resource configuration and service provisioning, which is based on pre-defined rules.

Level 3: The capabilities of intelligent analysis is introduced into the controllers and orchestrator, to enable the end-to-end closed-loop automation, such as network status monitoring and visualization, and alarms for root cause analysis.

4.2.2 Service Assurance

1) Scenario Definition and Description

Service provisioning with assured extreme experience limits is one of the core features of F5G. For example, UHD video, VR and cloud gaming require high bandwidth, low latency and near lossless

communication; while high-quality private line services require high and flexible bandwidth, millisecond level latency and high reliability to commit SLA of the business users.

In F5G, hardware technologies continue to evolve, providing networks with larger and more flexible bandwidth, lower latency and near zero packet loss. These are the cases for Wi-Fi 6 with lower air interface latency, 10/50G Passive Optical Networks (PON) and next generation of Optical Transport Networks (OTN) with support for flexible bandwidth granularity of connections.

Meanwhile, the software technologies continue improving, supporting the quality required by F5G applications; such as awareness of the service type and service quality requirements; and support for automated resource allocation. Such systems also support continuous monitoring and optimization on the qualities of the service to ensure the users' experiences.

Artificial Intelligence (AI) and Machine Learning (ML) are the key technologies for intelligent service provisioning and assurance. Embedded AI/ML capabilities are needed in many areas an automated multi-service network. With AI/ML, the data transportation models of different application services can be learned so that different kinds of applications can be distinguished automatically, without touching the inner content - thus protecting user privacy. At the same time, the network status can be continuously collected and analysed, in order to detect potential service disruption risks in real time, and to provide input on network resource adjustments in a timely manner.

2) Autonomous Networks Levels

Level 1: Manual service provisioning by assisted management system.

Level 2: Automated configuration for service provisioning.

Level 3: Automated distinction between different kinds of service: intelligently analysing the QoE of the service and adjusting the service if the service is degraded.

Level 4: Proactive QoE assurance: proactively adjust the service, based on the changing trends of the network circumstances, before QoE degradation.

4.2.3 Automated Network Operation and Maintenance

1) Scenario Definition and Description

The F5G will not only improve the QoE of the application services for the users, but also improve the experience on network operation and maintenance. In F5G, the network health status and resources need to be monitored and managed in real time automatically. When network failure or degradation occur, they will be diagnosed, isolated and fixed in real time automatically.

As a typical example, in a PON and OTN network, fibre is the most important media for data transmission. The failure of fibre will adversely impact the network. Therefore, the closed-loop control of fibre failure prediction, allocation and recovery is very useful for F5G to improve the operator's experience on network operation and maintenance.

With AI/ML technologies, physical parameters of the fibre can be collected and analysed to predict the fibre failure based on pre-trained models. Once a failure is predicted, suggestions can be provided on how

to recover from the failure. And when real failure happens, the AI/ML functions can help in allocation of the failure based on models learned from alarm heuristics and related information.

2) Autonomous Networks Levels

Level 1: Assistance tools are used to simplify the manual maintenance of the network.

Level 2: Alarm information will be automatically collected and analysed, and decisions on how to recover from failure need to be made by humans.

Level 3: The network status will be monitored, and the network failure or degradation will be diagnosed, isolated and fixed automatically after it occurs.

Level 4: Proactive operation: Based on the in-depth monitoring and trend analysis on the network status, the sub-health status of each components of the network will be identified and the faults will be predicted and rectified before they occur.

4.3 Autonomous Scenarios in Wireless Network

The autonomous level of a wireless network, including the wireless access network and the core network, can be evaluated by its capability, architecture and multiple scenario coverage. AI-enabled automation includes intent translation, state awareness, big data analysis, intelligent decision-making, programmable workflow and automated execution.

Hierarchical autonomous architecture provides different levels of network autonomy: network elements layer usually implies high real-time closed-loop operations; single-domain network layer usually implies low real-time closed-loop operations; cross-domain network layer implies cross-domain orchestration; and business automation generally indicates an agile and customer centric implementation.

4.3.1 Wireless network Coverage Optimization and Assurance

1) Scenario Definition and Description

Wireless networks are geographically distributed, and activity varies significantly in different places and at different times of day. This makes the wireless network quite dynamic and complex. That complexity is further increased by the diversity of services and device performance, and by the mobility of users. Coverage is critical for good user experience; however, coverage assurance and optimization are complex. For example, massive multiple input multiple output (MIMO) is a key technology deployed in wireless networks to deliver higher capacity and better coverage. However, there are technical roadblocks to efficiently tune massive MIMO using automated data collection and decision. Using AI technology, which allows a learning and iterative mechanism to select the MIMO pattern and predict user traffic, is one potential way to improve the wireless network coverage optimization.

2) Autonomous Networks levels

Level 1: system assists humans to improve the efficiency for coverage optimization action execution and coverage performance awareness.

Level 2: system additionally analyses the coverage performance and identify coverage issues based on the coverage issue rules specified by humans.

Level 3: system additionally analyses the coverage optimization solution and determines the coverage adjustment needed to be executed based on coverage requirements and/or optimization policies specified by humans.

Level 4: system additionally determines and updates coverage optimization policies and the coverage requirements dynamically, based on service assurance intent.

4.3.2 Wireless Network Energy Saving

1) Scenario Definition and Description

As operators' wireless network energy consumption keeps increasing, reducing the energy use of the main equipment is key to a successful strategy. However, reducing power consumption faces many challenges. For one, the networks' traffic volume varies greatly during peak and off-peak hours. When the equipment runs, the power consumption is not dynamically adjusted based on the traffic volume; and as a result, resources are wasted.

While the capability of "zero bits, zero watts" needs to be constructed, in a typical network, the features of different scenarios vary greatly. Automatically identifying different scenarios and formulating appropriate policies becomes key to saving energy.

2) Autonomous Networks Levels

Level 1: Tool assisted execution and awareness.

Level 2: Execution and awareness automation based on human defined rules.

Level 3: Energy-saving closed-loop: Based on the analysis of traffic trends, self-adaptive generation of energy-saving strategies and closed-loop KPI feedback.

Level 4: Real-time adjustment of energy-saving strategies based on traffic prediction. Through integration with third-party space-time platforms, the operator can also add predictive perception of traffic changes, smooth out the user experience and maximize energy-saving.

4.4 Intelligent Network Slicing

4.4.1 Intelligent Slice Lifecycle Management in Core network

1) Scenario Definition and Description

Support for network slicing has gathered special attention in 5G technologies. By using logical private networks to serve vertical industries, network slicing can provide on-demand customization, real-time deployment, dynamic assurance, and security isolation capabilities for slice users. However, compared with traditional networks, the flexibility offered by network slicing also brings management, operation and maintenance complexity. For example, a dedicated management Network Element (NE) needs to be introduced to implement full-lifecycle management of slice instantiation. Additionally, a multi-dimensional management of hardware, resources, slice deployment and applications is required. The need for network slicing can be customized based on users' service requirements – as in in terms of SLA and the envisaged service innovation by verticals and operators requires intelligent operation of network slicing.

2) Autonomous Networks levels

Level 1: The tool assists users in slice subscription, deployment adjustment, SLA monitoring and locating faults. Most operations depend on manual analysis and expert human experience.

Level 2: The system can automatically analyse slice running data and resource configuration information. Based on the analysis, experts can customize some rules to trigger the system to automatically complete slice adjustment.

Level 3: The system can additionally analyse the slice dynamic adjustment solution, determine the optimal solution by humans, based on the SLA requirements of industry slice tenants - and then experts determine whether to automatically implement the solution.

Level 4: The system can additionally determine whether to dynamically adjust slice policies based on the SLA requirements and running data of industry slice tenants. In addition, the system optimizes the original dynamic slice adjustment policy based on the slice running status and SLA after the policy is implemented.

4.4.2 Intelligent Slice Lifecycle Management in the Transport Network

In order to meet the expectations, set by different services over the 5G transport network, while maintaining the benefits of using IP/MPLS, the concept of transport network slice is introduced. A transport network slice contains the whole or part of the underlying transport network, enabling slicing technologies on demand on selected devices as a means to achieving target performance requirements.

From the technical point of view, management of network slicing is not only required to satisfy differentiated SLAs and isolation requirements for various services, such as those during the creation stage; it is also required to provide high efficiency in terms of real-time monitoring, analysis, and self-optimization. These requirements cannot be properly achieved in current network management systems, which rely on manual operation and static configuration.

To that end, the architecture and key technological innovations are critical for network slicing operations. The new technical challenges for network management turns AI into a competitive option for handling different types of complex network slicing scenarios, especially those in which deterministic results cannot be easily derived from analysis or control.

1) Proof of Concept

The first Proof of Concept (PoC) of ETSI ISG ENI (see ETSI GS ENI 001 V2.1.1 (2019-09) [14]) successfully demonstrated the use of AI and intent based interface to improve the autonomy of transport network slicing system.

The Transport Network Slice Manager (TNSM) manages and monitors the transport network slice instances. Its user interface simplifies input by offering intent-based templates specifying device's roles and performance requirements for different scenarios. TNSM converts the intent-based request into detailed request with unified format. During the conversion, parameters will be supplemented according to the build-in relationship between the selected template and the unified format of slice creation requirement. Then the TNSM calculates the optimal result including topology and resources and creates a slice in the underlying network accordingly.

The traffic throughput data of a transport network slice instance is collected from the TNSM and sent to the AI based predictor, which infers prediction results of traffic throughput during the upcoming time periods and then delivers it to the intelligent policy generator.

The intelligent policy generator decides whether the transport network slice instance should be scaled up or down, as well as the bandwidth adjustment policy, and sends the intelligent policy to the TNSM when necessary. The TNSM automatically executes the received scale up or down policy by reconfiguring the port bandwidth of the transport network nodes.

2) Autonomous Networks levels

Level 1: The system assists humans to create, modify and terminate a transport network slice by manual configuration.

Level 2: The system can automatically create, modify and terminate a transport network slice based on scripts, pre-configured triggers and awareness of network data.

Level 3: The system can automatically create, modify and terminate a transport network slice based on collected user intents. And it can also provide suggested optimization options based on comprehensive analysis of network data.

Level 4: The system can make prediction based on learned knowledge about the network and suggest the optimal option for transport network management and operation considering human intents.

5 Cross Industry Organisation Ecosystem

5.1 Overview

The arrival of verticals and new organisations, such as industry and cross-verticals alliances, and open source Communities, transformed the traditional ecosystem into an extended one, as described in the figure below. Note that Autonomous Networks are going to progress in this new ecosystem in order to exploit their full deployment.

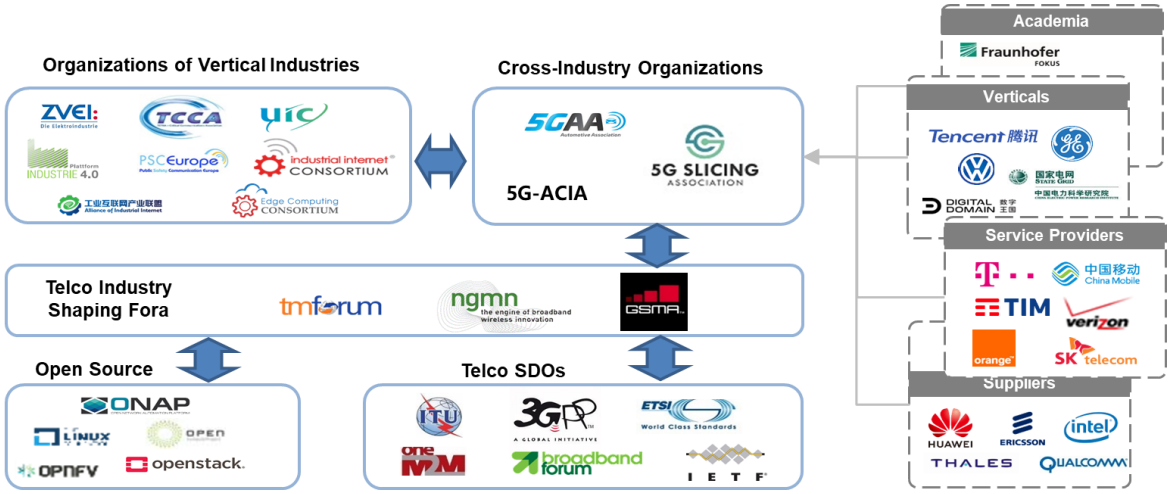

Figure 7: Ecosystem landscape

An overview of the principal actors in the ecosystem follows.

5.2 TM Forum

The TM Forum was one of the first organizations that recognized the strong value of Autonomous Networks in terms of business of Digital Transformation.

In May 2019 a successful workshop was organized in Nice DTW 2019, where a TMF white paper, titled “Autonomous Networks: Empowering Digital Transformation For the Telecoms Industry” [2] was presented by leading CSPs and vendors, touting the savings that AN can bring in operational cost and resource usage. The activity was followed successfully with a dedicated project “Autonomous Network Project”, with webinars, workshops and presentations at major TMF events.

Currently, the main work items are being developed:

- User stories/use cases
- Vision & roadmap
- Business requirements and architecture
- Technical architecture

Two official documents have also been published where basic concept, vision, framework, autonomous network levels, user stories category, business requirements, architecture and capabilities, as well as use cases for Autonomous Networks, have been specified in TM FORUM IG1193 [3], TM FORUM IG1218 [4]).

The TMF activities also addressed some significant use cases and exploited the impact of AN in the new Open Digital Framework (ODF) as well as Open Digital Architecture (ODA).

Some of the use cases are going to be implemented in a few Catalysts - preliminary Proof of Concepts where CSPs, vendors and technology providers develop interoperable software to be showed at next DTW 2020 in Copenhagen. The major focus, due to the know-how of companies and experts involved, will be IT and the upper management and business layers.

The TMF also developed significant experience in Open APIs development: in the case, the TMF develops APIs of interest in AN perspective to evaluate the opportunity of usage, and hopefully, also the opportunity to commit APIs development according to recommendations and specifications done by ETSI.

5.3 GSMA

The GSMA developed a major study and launched a significant initiative on the role of automation, supported by AI, regarding network evolution.

At Shanghai MWC, June 2019, a Workshop supported by a White Paper (see GSMA Whitepaper. (2019, Oct), AI in Network Use Cases in China [7][6]) was successfully organized, where the business and market value was outlined by reporting the viewpoints of leading Chinese CSPs, vendors and verticals, including OTTs. The launch of a new project (now limited to the Greater China Region) on Automation in network evolution was also announced. The exploitation of business value for some leading verticals represents a key attribute and is viewed as a leading driver in the evolution of Autonomous Networks.

5.4 3GPP

In August 2019, 3GPP SA WG5 initiated the ”Study on concept, requirements and solutions for levels of autonomous network” (see 3GPP Rel-16 TR28.810 [8]).

The study provides concepts, evaluation dimensions, definitions, workflow in typical scenarios and detailed classification description of Autonomous Networks. In Jun 2020, a Rel-17 WID on autonomous network levels was approved to continue the standardization work. The main objective is to develop the concept and architecture of automatic network, classification of autonomous networks levels and combine the classification with the existing automation capabilities.

3GPP SA WG5 also carries out a series of automation related standardization projects covering planning, deployment, maintenance and optimization phases of the entire mobile network life cycle. Rel-17 work items include intent driven management services for mobile network, management services for communication service assurance, and studies on enhancement of management data analytics, energy efficiency on 5G and Self-Organizing Networks (SON) for 5G networks, just to name a few.

3GPP SA WG2 and 3GPP RAN WG3 also initiated research on supporting automatic network intelligence. 3GPP RAN WG3 started the discussion on RAN-centric Data Collection and Utilization in Rel-16 (3GPP TR 37.816 [9]). The objective is to study the wireless data collection and application; oriented toward network automation and intelligence, such as SON (e.g. ANR) and RRM enhancement.

3GPP SA WG2 started discussions on enablers for Network Automation for 5G in Rel-16 (3GPP TR 23.791 [10]). The objective is to introduce the NetWork Data Analytics (NWDA) function on 5G Core (5GC) to analyse data on the signalling plane.

5.5 LFN ONAP

Linux Foundation is one of the most important open source communities, now with more than 1300 members and 30,000 developers contributing code.

Linux Foundation Networking (LFN) is an umbrella organisation to harmonize existing initiatives and to provide building blocks for network infrastructure and services. The Open Network Automation Platform (ONAP) project (see LFN ONAP (2020), ONAP specifications [11]) officially launched in February 2017 and is the largest open source networking project that exists today in the industry. It provides an open-source network automation platform for real-time, policy-driven orchestration and automation of physical and virtual network functions.

ONAP's 6th Release (Frankfurt Release) was delivered in June 2020 and it is continuously evolving and enhancing the platform to satisfy service providers requirements and use cases; such as Cloud Native application orchestration, 5G Network Slicing, security, edge and O-RAN orchestration. The Frankfurt Release is the result of a collaborative community consisting of 31 sub-projects, 35 Organisations and more than 400 developers.

According to the community vision, a key component of an Autonomous Network is the ability to perform service and resource orchestration to deliver whole automation across different autonomous domains, across complete service and resource lifecycles; making use of analytics and data-driven machine learning and artificial intelligence algorithms. The "CLAMP module" used for Service Operations has been created for designing and managing control loops in an automated way.

ONAP and other LFN projects such as CCNT, OPNFV and OVP, with their reference Implementations can complement the efforts of the main SDOs in the AN standardization landscape.

5.6 ITU-T

The ITU is addressing aspects of network automation in the Focus Group (FG) ML5G and in the parent Study Group SG13, in particular in question 20, that has so far produced four recommendations focusing on application of machine learning to networking in the Y.317x series and is working on the technical reports produced by the FG to transform them into recommendations or framework documents.

Currently, the most relevant concepts are the identified use cases addressing Autonomous Networks scenarios, like the "ML-based end-to-end network management". This use case focuses in the root cause analysis in a network divided into different domains, each, currently being overlooked by a different human operator.

- **ITU-T SG13** has recently held a joint workshop with ETSI ISG ENI in order to share their vision, and the fundamental concepts to avoid misalignments and divergence of the specifications produced by the two groups.
- **ITU-T, FG-ML5G** (Focus Group on Machine Learning for Future Networks including 5G) was established in November 2017, with the main objective of producing draft technical reports and specifications for machine learning (ML) for future networks, including interfaces, network architectures, protocols, algorithms and data formats. As stated in the group's Terms of

Reference (ToR), “new ML methods for big data analytics in communication networks can extract relevant information from the network data while taking into account limited communication resources, and then leverage this knowledge for autonomic network control and management as well as service provisioning” (see ITU-T recommendations (2020), https://www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=13 [12]).

The objective of the Focus Group is to conduct an analysis of ML for future networks in order to identify relevant gaps and issues in standardization activities related to this topic.

5.7 ETSI

Some key technologies, solutions and standards under study and development in ETSI can significantly contribute to the evolution of Autonomous Networks. Given the scale, heterogeneity and complexity of emerging networks, management solutions need to be highly automated and extremely “intelligent”, in the sense of a “machine intelligence”, able to collect large amounts of relevant data, process it and act on it in an automated fashion.

For this reason, and in order to provide a harmonized view of the ETSI activities in this field, recently a White Paper (see ETSI White Paper 32: Network Transformation [13]) was published to give an insight into Network Transformation challenges, written by the Chairmen of ISGs ENI, MEC, NFV and ZSM. Specifically, the authors address the common framework for the management of virtualized network environments, as defined by ETSI ISG NFV, and extend it to the distributed edge with public-cloud aspects by ETSI ISG MEC. They discuss how ETSI ISG ENI solutions can be deployed within or across network domains in order to optimize the processing of data, extract knowledge, and thus enable decision-making. Finally, they demonstrate how the work of ETSI ISG ZSM is bringing all these and other technologies together into a single automated management framework.

The following text highlights the main topics addressed by ETSI’s groups towards Autonomous Networks.

- **ENI** (Experiential Networked Intelligence) Industry Specification Group (ENI ISG) is defining a cognitive network management architecture to adjust offered services based on user needs, environmental conditions and business goals. Therefore, 5G networks will benefit from automated service provisioning, operation, and assurance. The use of Artificial Intelligence techniques in the network will solve problems of future network deployment and operation. ENI focuses on improving the operator experience, using closed-loop AI mechanisms and metadata-driven policies to recognize and incorporate new knowledge. This model gives recommendations to decision-making systems.

  ENI has published version 1 of the “System Architecture” (see ETSI GS ENI 005 V1.1.1 [14]), Context Aware Policy Management and Categorization. Version 2 of the “Use cases, Requirements” (see ETSI GS ENI 001 V2.1.1 [15]) includes a Terminology and a Proof of Concept (PoC) Framework. ENI has launched a continuing Proof of Concept demonstrating its work. Published deliverables are listed in ETSI ENI (2019), Specifications (https://docbox.etsi.org/ISG/ENI/Open/ [16]).

- **MEC** (Multiaccess Edge Computing) is defining an architecture fully inspired and based on the ETSI NFV framework (see ETSI MEC (2020), Specifications, https://docbox.etsi.org/ISG/MEC/Open/ [17]) and the published standard demonstrated how ETSI MEC defined entities integrate with NFV. The Operations Support System (OSS) is a traditional management node included for completeness of the reference architecture, but ETSI ISG MEC does not specify anything about it. However, as a service-based approach to management is developed by ETSI ISG ZSM and other organisations, ETSI ISG MEC expects to align with the emerging zero-touch management entities, such as those in the ETSI ISG

ZSM End-to-End Service Management Domain and update the reference architecture accordingly. Moreover, given the critical importance of automation for actual MEC deployments, we expect Telco's to increasingly look to such modern evolutions of OSS for their deployments.

- **ISG NFV** (Network Function Virtualization) is the home of the Industry Specification Group for NFV. The ISG develops specifications for the key system interfaces and data models to enable interoperability in an open ecosystem and provides guidance - including best practices. ISG NFV deliverables (see ETSI NFV. (2020). Specifications, https://docbox.etsi.org/ISG/NFV/Open/ [18]), such as AN should refer to NFV Release 4 under development; which includes the enablers for autonomous methodology in NFV management and orchestration.

  We should also mention the work of the ETSI OSM that is delivering an open source Management and Orchestration stack aligned with ETSI NFV Information Models, to address commercial NFV deployments.

- **ISG SAI** (Securing Artificial Intelligence)**, Security Group of NFV** and **TC CYBER** deal with security and privacy protecting activity in the ISG. As noted in clause 4.2, Autonomous Networks present several challenges to security and privacy. However, it is similarly clear that a number of ETSI groups are already providing the framework for resolving these issues. Of particular interest is the work of the Industry Specification Group on Securing Artificial Intelligence (ISG SAI) (see https://docbox.etsi.org/ISG/SAI/Open/ [19]), the activity of TC CYBER and the work in the security group of ISG NFV. With the goal of AN deployed at the higher levels of autonomy - where AI and ML will be key to the operations - the SAI and its partnership with TC CYBER will incorporate their existing works in order to address specific aspects of the role of AI in AN:

  - Securing AI from attack: this will address protection of the AI component t of the AN system.
  - Mitigating against malicious AI: this will address the concerns where a malicious AI is used to improve and enhance conventional attack vectors or create new ones against the AN system.
  - Using AI to enhance security measures: this activity is aimed at protecting the AN systems against attack using AI as part of the 'solution' either uniquely or in parallel to improve and enhance more conventional countermeasures.

  Supporting these goal in ISG SAI is the work in TC CYBER, together with closely related work in ISG NFV SEC that will be transposed to the AN environment. This includes the core "secure by default" paradigm and the issues surrounding security of the orchestrator element of the NFV which will be key in the deployment of AN. The ETSI ISG SAI develops the technical knowledge that acts as a baseline in ensuring that artificial intelligence is secure. Stakeholders impacted by the activity of ETSI's group include end users, manufacturers, operators and governments.

- **ISG ZSM** (Zero-touch Network and Service Management) was established in 2017 and is defining a standard architecture framework to enable Autonomous Networks capable of self-configuration, self-monitoring, self-healing and self-optimization without further human intervention. The ultimate automation target of the ISG activities is to enable large autonomous networks which will be driven by high-level policies and rules. For this reason, ISG ZSM is an excellent group to collaborate with for creating the entire AN framework. In particular, the ZSM Architecture (see ETSI GS ZSM 002 V1.1.1 [20]) deliverable that defines an end-to-end automated network and service management architecture; and ZSM on Automation (see ETSI GS ZSM 005 V1.1.1 [21]) that describes several approaches aimed at achieving automation, are relevant publications to be considered in the definition of AN specifications. ISG ZSM deliverables are available at ETSI ZSM. (2020). Specifications (see https://docbox.etsi.org/ISG/ZSM/Open/ [22]).

- **ISG F5G** (Fifth Generation Fixed Network) aims at studying the evolution of the fixed network needed to match and further enhance the benefits that 5G has brought to mobile networks in particular and to communications in general. Thus, defining improvements with respect to previous solutions and describing the new characteristics of what represents the 5th generation fixed network. Network evolution in the end-to-end fixed area also needs to accommodate the maximum possible degree of autonomy by using AI and virtualization.

  ISG F5G's starting point is the identification of the overall characteristics of the 5th generation fixed network and the exploration of relevant scenarios and related use cases for home, business and multiple vertical industries. This will allow for a gap analysis to identify both enhancements to existing standards and development of new specifications where required by further outlining the complete F5G technology landscape. With the ambition to Fibre to Everything, ISG F5G also addresses some aspects of the new ODN technologies such as XG(S)-PON and Wi-Fi 6 enhancements, control plane and user plane separation, smart energy efficiency, end-to-end full stack slicing, autonomous operation and management, synergy between Transport and Access Networks and adaption of Transport Network.

5.8 Takeaways

Figure 8 below shows a simplified mapping of ETSI contributions for the evolution of Autonomous Networks, as presented at GIO workshop on Autonomous Digital Infrastructure [23}.

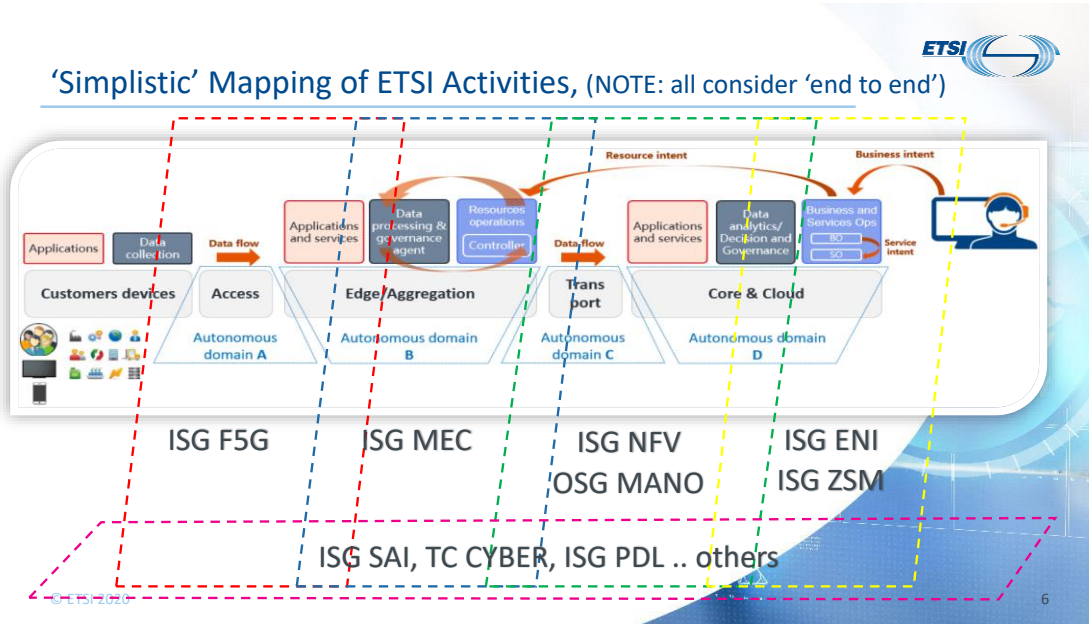

Figure 8: ETSI activities mapping

It is recommended that we form a synergistic and coordinated activity, first inside ETSI and later extended to other forums, starting with the most relevant ones already active in the AN field. A significant common effort is required to work together to facilitate the adoption of common standards what avoiding market fragmentation.

Naturally, in this case, the most important Telco open source communities, like LFN ONAP can contribute in a complementary way to provide reference implementations with quick introduction of new requirements and capabilities, improving interoperability while reducing of vendor lock-in.

For this reason, these important AN stakeholders should collaborate in order to synchronize the initiatives already underway and to promote the engagement and the support of other best-in-class organisations still not active, in particular verticals associations. Similarly, the Cross-SDO environment GIO (Global Initiative Organisation) can also facilitate the coordination and synchronization among SDOs and vertical associations through workshops and round tables.

6 Conclusions and Proposed Actions

The business value of Autonomous Networks is significant to the digital transformation of ICT industry as well as other vertical industries, such as smart city, smart manufactures etc. For example, the fifth generation of mobile communication systems provides a disruptive leap forward in the telecom industry. But unlike previous generations, it won't be mostly about more bandwidth. CAPEX, OPEX and revenue constrained SPs are poised to reinvent themselves and evolve towards a real Digital Transformation, exposing their assets via Open APIs to provision and monetize innovative services with flexibility and reduced time to market.

However, the development toward a fully Autonomous Networks is a long-term goal and requires tremendous effort with step-by-step evolution; forcing the entire industry to have a common understanding and consensus on:

- Definition of Autonomous Networks concept, framework, Autonomous Networks Levels and key capabilities.
- Development of key mechanisms, interfaces and corresponding metrics to measure the maturity of Autonomous Networks Levels.
- Demonstration of valuable use case scenarios and best practices across the industries among CSPs, solution providers and customers.

Standardization plays a significant role in terms of interoperability, feasibility and industrial deployment. Some SDOs already launched dedicated projects or produced important deliverables to support the evolution and deployment of Autonomous Networks. ETSI is already playing a role with many ISGs contributing to AN and plans to increasingly invest in the Autonomous Networks challenge. Single SDO's effort is not enough and a collaborative environment among the leading stakeholders in the new extended ecosystem is meant to address, in their respective area of expertise, the Autonomous Networks evolution.

Therefore, we propose the creation of a sort of "Engagement Roadmap Plan", where Standard Organisations can collaborate to produce complementary specifications and open source projects can target the implementation of the software building blocks and reference implementations based on such architectural specifications.

References

[1] D. Sun, C. Maître (2019, November), Autonomous Networks – the network of the future being designed and built today!, TM Forum Digital Transformation Asia Conference, Kuala Lumper.

[2] TM FORUM Whitepaper (2019, May), Autonomous Networks: Empowering Digital Transformation for the Telecoms Industry.

[3] TM FORUM IG1193 (2019, October), Cross-Industry Autonomous Networks – Vision and Roadmap v1.0.

[4] TM FORUM IG1218 (2020, July), Autonomous Networks Business Requirements & Architecture.

[5] TM FORUM Whitepaper (2020, October), Autonomous Networks: Empowering Digital Transformation for Smart Societies and Industries.

[6] SAE J3016 (2019).

[7] GSMA Whitepaper (2019, Oct), AI in Network Use Cases in China.

[8] 3GPP Rel-16 TR28.810 (2019): Study on concept, requirements and solutions for levels of autonomous network.

[9] 3GPP Rel-16 TR37.816: Study on RAN-centric data collection and utilization.

[10] 3GPP Rel-16 TR23.791: Study of enablers for Network Automation for 5G. Status: Under change control.

[11] LFN ONAP (2020): ONAP specifications, https://www.onap.org/ .

[12] ITU-T recommendations - https://www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=13 (2020).

[13] ETSI White Paper (2019): ETSI White Paper 32: Network Transformation.

[14] ETSI GS ENI 005 V1.1.1 (2019-09) - Architecture.

[15] ETSI GS ENI 001 V2.1.1 (2019-09) - Use Cases.

[16] ETSI ENI (2019): Specifications, https://docbox.etsi.org/ISG/ENI/Open/ .

[17] ETSI MEC (2020): Specifications, https://docbox.etsi.org/ISG/MEC/Open/ .

[18] ETSI NFV (2020): Specifications, https://docbox.etsi.org/ISG/NFV/Open/ .

[19] ETSI SAI (2020): Specifications, https://docbox.etsi.org/ISG/SAI/Open/ .

[20] ETSI GS ZSM 002 V1.1.1 (2019-08) - Reference Architecture.

[21] ETSI GS ZSM 005 V1.1.1 (2020-05) - Means of Automation.

[22] ETSI ZSM (2020): Specifications, https://docbox.etsi.org/ISG/ZSM/Open/ .

[23] Licciardi, L. (2020, July): GIO report on Autonomous Digital Infrastructure Workshop.

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