# TM Forum Exploratory Report

# Cross-Industry Autonomous Networks – Vision and Roadmap

**IG1193**

**Team Approved Date: 04/Oct/2019**

| | |
|---|---|
| Release Status: Pre-production | Approval Status: Member Evaluated |
| Version 1.0.1 | IPR Mode: RAND |

# Notice



Direct inquiries to the TM Forum office:

4 Century Drive, Suite 100

Parsippany, NJ 07054 USA

Tel No. +1 973 944 5100

Fax No.  +1 973 998 7916

TM Forum Web Page: www.TM Forum.org

# Table of Contents

# List of Figures

# Executive Summary

This document shares the vision and roadmap of autonomous networks, including the motivation, vision, requirements and principles, new ecosystem, collaboration and business models, overarching framework and autonomous levels, roadmap and industry collaboration.

This document serves as the general guideline for pertinent work streams and work items, including user stories and use cases, business requirements/metrics and architecture, technical architecture and interface/APIs specs, PoCs/catalyst projects, testing and verification, as well as industry collaboration. Moreover, it provides the baseline for the marketing plan, campaign, social events and public white paper on behalf of the TM Forum and member companies.

Similar to the automobile industry, the telecom industry can offer one-stop shop, network/ICT services based on the automation levels of service lifecycle operations in addition to the traditional SLAs e.g. availability, bandwidth & QoS, which will significantly facilitate the digital transformation of various industries (e.g. smart city, smart manufacturer, smart healthcare) and digital life of consumers.

In order to reach this goal, the telecom industry (including CSPs, suppliers, consultants and integrators) and other vertical industries should collaborate and formulate a new partner ecosystem model from current Customer-SP-supplier models that will lead to the on demand, real-time, customized business relationships associated with a Platform Ecosystem. Accordingly, the partners within telecom industry - CSPs, suppliers, consultants and integrators also need to transform their relationships to a collaborative production model that can enable the automated network/ICT services to other verticals and consumers, as well as internal operations efficiency.

Therefore, it is essential to develop a framework for autonomous networks and define the autonomous levels at cross-industry level from the aforementioned partner ecosystem and collaborative production model perspective, which the development follows the principles of user centric, business driven and top-down, similar to the categorization of autonomous vehicles by SAE for easy understanding and consensus.

In a nutshell, the framework of autonomous networks consists of “3-layer, 4-closed-loop”, i.e. business operations layer, network operations layer and network resource layers, and network resource closed loop, network operations closed loop, business operations closed loop and more importantly cross layer closed loop from a user perspective. In order to fulfil the above closed loops, the key mechanisms are:

a) reducing complexity by simplifying the network architecture;
b) autonomous domains for network resource closed loop;
c) cross-autonomous-domain collaboration for network operations closed loop;
d) business ecosystem and collaboration enablement for business operations closed loop.

This will be a long-term project that requires the collaboration internally with the AI, digital ecosystem, and IT/network transformation programs of the TM Forum, as well as collaboration with cross industry organizations such as GSMA, ETSI, 3GPP, Open sources (e.g. Linux foundation), and other verticals e.g. IIC, industry 4.0, 5GAA and GIO.

This work was kicked off by a workshop entitled “Autonomous networks – building the network of the future” in May 2019 during DTW, Nice; and then followed up with a workshop in July in London, which discussed the overall work plan and roadmap as summarized in this document.

It is expected that several workshops and marketing events will be held in September (Dallas), November (Kuala Lumpur), February (Lisbon) and June (DTW - Copenhagen). The outputs include the umbrella white paper, vision & roadmap, user stories & use cases, business requirements/metrics/ architecture, technical architecture, interface & API specs, catalyst projects, eventually testing &verification program of autonomous levels and capabilities.

# 1. Introduction

In every industry we are seeing varying degrees of digital transformation, from the launch of 5G in the telecommunications industry to the development of prototype autonomous vehicles, the creation of smart services within cities, the trialing of smart health services, the drive for industrial automation to support smart manufacturing, to the exploitation of low latency and high bandwidth for cloud based gaming services. These are all just examples of the opportunities being discussed for telecommunications companies to play this leading Digital Service Enabler (DSE) role in the transformation of 21st century life.

With service providers in every industry striving to transform their production process and management operations into a more agile, flexible and collaborative mode by taking advantage of emerging digital technologies, it is obvious, to all but the casual observer, that the need for automation and intelligence across all domains is pivotal to fully enable and execute a digital transformation. The foundation of enabling automation and intelligence in every industry is how to provide easy-to-use, automated and quick responsive information processing capabilities AKA fully automated intelligent ICT services that includes connectivity service but also beyond-connectivity services from e2e perspectives, i.e. end-to-end closed loop of information/data collection, distribution, analysis, decision and operations in the context of the production and services of SPs.

This is especially true in the world of telecom industry which up until now have been trapped with outdated thinking associated with elongated and protracted negotiations around standards that have followed a very “waterfall” type approach to their development. Networks made up of bespoke elements with fragmented elements and intricate interfaces have complicated the construction and operations, constrained innovation and stifled transformation.

Finally, we are seeing the thinking from the world of software start to gain traction amongst progressive thinking network architects and engineers. As network components are developed using agile, DevSecOps techniques coupled with technological advances in computing infrastructure, especially in the domain of virtualized storage and computing processors, and replication of standardized components to enable much higher levels of scalability and availability than was economically possible with dedicated hardware and infrastructure, it is now possible to design, build and run virtualized software defined networks components with the speed, security, reliability and availability previously associated with bespoke, vendor specific, network elements. As the network elements become software enabled and virtualized, it is essential that the components that deliver these network services are grouped as autonomous domains to enable fully automated closed loop of the management and control of the elements. To achieve this the network services must be abstracted into a set of common services that represent the business capabilities that they deliver, and these capabilities need to be encapsulated and exposed at the autonomous domain level and be interacted across the autonomous domains through operations and management applications via a set of industry agreed API’s and microservices. These services then need to be able to be instantiated, updated, started, modified and stopped, fully automatically and in real time where appropriate. This implies an unprecedented level of network automation that is theoretically possible, but absolutely essential, if service providers are going to remain relevant in today’s digital world.

As industries transform as a result of digitalization then to deliver the flexible production and personalized customer experience that wants an always on, never failing, instantly responsive network/ICT services it will be necessary to take advantage of emerging technologies such as AI, big data, cloudification and virtualization to provide fully automated, self-healing and self-

optimizing network/ICT infrastructure capabilities which operate right across the stack from resource management, service operations, customer experience, service maintenance and service enablement.

Through the launch of autonomous networks, the CSPs can provide automated intelligent network services evolving towards autonomous ICT services eventually and will incubate new collaboration model and production model for upgrading the telecom industry market structure as well as customer experience. The autonomous networks are characterized by properties such as self-configuring, self-healing, self-optimizing, self-evolving and delivering an infrastructure that has the abilities of zero-wait, zero-trouble, zero-touch service offering and operations from the user perspective.

The Open Digital Architecture (ODA) has identified two key opportunities for CSP's where Autonomous Networks play a critical role:

1. **Digital Operations Efficiency:** Evolution of networks towards dynamic, software and virtualized solutions leads to increased scale and velocity of network change. Operational efficiency can only be maintained through automation where Autonomous Networks capabilities handle routine events.
2. **Digital Service Enablement:** Opportunities are emerging for CSPs through partnering and platform business models where they provide trusted enablers to Vertical Industry Customers. One enabler is easy to use and modify Networks as a Service. Autonomous networks facilitate customer self-service for scaling and dynamic re-configuration of NaaS whilst handling the complexities of dynamic networks invisibly e.g. virtualization, closed control loops, policy, etc.

For service providers to be successful with their AI and automation strategies, they need to come together with the wider industry ecosystem to build a common understanding of autonomous networks.

# 2. Intended Audience

As we have indicated in the introduction it is essential that the design and development of autonomous networks is not perceived to be confined to the telecommunications industry, but they must be developed to support a much wider cross industry ecosystem that enables telecommunications service providers to participate in, and actively support, the digital transformation of many different industries.

This paper is targeted at decision makers across all industries undergoing digital transformations, as well as being of particular relevance to CIO's, CTO's together with their architects and designers from both IT and networks backgrounds as we are seeing the consolidation of software thinking across the worlds of IT systems and networks.

This document will also position the TM forums work on autonomous networks in relation to other standards organizations so that it is unambiguous as to the role that each organization will play in the development of the solutions going forward.

# 3. Autonomous Networks Vision

The following section lays out the vision for how we will build and manage Autonomous Networks over the coming years. It will paint a vision of what will be necessary and achievable within approximately 3 years to address the challenges and opportunities that ultra-reliable, low latency, high-bandwidth, automated fixed-mobile converged communications services offer to both individuals and organizations to generate and augment, new or additional, value-added revenue streams that depend upon and exploit this technological advancement.

## 3.1. Objective

The plan for this work on Autonomous Networks is to support a set of innovative network services that enable the digitalization of vertical industries e.g. smart city, smart manufacture and self-driving cars, as well as the digital life of consumers through fully automated intelligent business and networks operations of ICT/network services by taking advantage of artificial intelligence, big data, cloud computing, IoT and 5G etc. cutting technologies, which requires the new collaborative production model, new knowledge-as-a-service operations model and new simplified network architecture, as well as new digital partner collaboration and ecosystem model.

## 3.2. Definition of autonomous networks

**Autonomous networks** aim to provide fully automated zero wait, zero touch, zero trouble innovative network/ICT services for vertical industries users and consumers, and support self-configuration, self-healing, self-optimizing and self-evolving telecom network infrastructures for telecom internal users: planner, service/marketing, operations and management. The Autonomous Networks comprises simplified network architecture/autonomous domains and automated intelligent business/network operations for the closed-loop of digital business, which offer the best-possible user experience, full lifecycle operations automation/autonomy and maximum resource utilization.

In order to measure the maturity and capabilities of autonomous networks, it is necessary to define a common consensus of autonomous levels.

## 3.3. Levels of autonomous networks

The purpose of autonomous networks levels:

- Define the concept of autonomous networks
- Identify six levels from “no automation” to “full autonomy”
- Base definitions and levels on functional aspects of technology
- Describe categorical distinctions for a stepwise progression through the levels

- Educate a wider community by clarifying for each level what role (if any) operators have in performing the dynamic network operations task while a network automation system is engaged

| Level Definition | L0: Manual Operation & Maintenance | L1: Assisted Operation & Maintenance | L2: Partial Autonomous Network | L3: Conditional Autonomous Network | L4: High Autonomous Network | L5: Full Autonomous Network |
|---|---|---|---|---|---|---|
| **Execution** | **P** | **P\S** | **S** | **S** | **S** | **S** |
| **Awareness** | **P** | **P** | **P\S** | **S** | **S** | **S** |
| **Analysis** | **P** | **P** | **P** | **P\S** | **S** | **S** |
| **Decision** | **P** | **P** | **P** | **P\S** | **S** | **S** |
| **Intent/Experience** | **P** | **P** | **P** | **P** | **P\S** | **S** |
| **Applicability** | N/A | Select scenarios | | | | All scenarios |

**Figure 1. Levels of autonomous networks**

**P**: Personnel, **S**: Systems

- **Level 0 - manual management:** The system delivers assisted monitoring capabilities, which means all dynamic tasks have to be executed manually.
- **Level 1 - assisted management:** The system executes a certain repetitive sub-task based on pre-configured to increase execution efficiency.
- **Level 2 - partial autonomous network:** The system enables closed-loop O&M for certain units based on AI model under certain external environments.
- **Level 3 - conditional autonomous network:** Building on L2 capabilities, the system with awareness can sense real-time environmental changes, and in certain network domains, optimize and adjust itself to the external environment to enable intent-based closed-loop management.
- **Level 4 - high autonomous network:** Building on L3 capabilities, the system enables, in a more complicated cross-domain environment, analyze and make decision based on predictive or active closed-loop management of service and customer experience-driven networks.
- **Level 5 - full autonomous network:** This level is the goal for telecom network evolution. The system possesses closed-loop automation capabilities across multiple services, multiple domains, and the entire lifecycle, achieving autonomous networks.

The lower levels can be applied now and deliver immediate cost and agility benefits in certain scenarios. An operator can then evolve to the higher levels, gaining additional benefits and addressing a wider range of scenarios.

It is a long-term objective with step-by-step processes, from providing an alternative to repetitive execution actions, to observing and monitoring the network environment and network device status, making decisions based on multiple factors and policies, and providing effective perception of end-user experience. The system capability also starts from some service scenarios and covers all service scenarios.

This transformation will take several years, so we are following an evolutionary process of gradually introducing automation into different domains to bring immediate value.

## 3.4. New Ecosystem and business models

The ultimate goal of autonomous networks is to upgrade the telecom market structure with simplified, automated and intelligent ICT/network services that will enable the digitalization of various industries and consumers. In order to achieve this objective, it is essential to transform the existing production, business and collaboration models to some new models:

- Digital partner collaboration and ecosystem model: all partners will collaborate to form partner ecosystem for offering on demand, personalized and real time services and capabilities to the customers, which is different from traditional customer-provider-supplier model, AKA everything as a service.
- Collaborative production model: in order to achieve new partner ecosystem, a collaborative production model is pivotal to leverage the best-suit solutions using best breed technologies through win-win benefit sharing collaboration.
- Knowledge-as-a-service operations model: in order to enable collaborative production, the operations knowledge should be shared and monetized through a common platform as an enabling service rather than cost reduction vehicle.

In a nutshell, the basic characteristics of autonomous networks:

- Simplicity: simplified network architecture with fewer layers, less hops and more integrated solutions
- Autonomation: highly automated inclusive closed loop of network operations
- Intelligence: Intent driven full lifecycle of business operations
- Collaboration: enablement of easy-to-use and ecosystem of automated network/ICT services

# 4. Autonomous Networks Principles

As we look at autonomous networks, we're not only talking about an evolution of the legacy network where we try to incrementally fix some broken things, we're mainly talking about a revolution within the intelligent automated network space. We are looking at how, using modern software enabled technology, we can radically transform how network services are managed and delivered.

The concept of Autonomous Networks is of a network that provides the service lifecycle on demand with minimal or no human intervention. The network can configure, monitor, maintain and repair itself independently. By making use of emerging technologies such as cloud computing i.e. essentially unlimited parallel computing processor resources and effectively infinite storage, together with on-demand bandwidth that provides dynamic connectivity, utilizing big data solutions to gather and analyze data from the ubiquitous array of network sensors for better pattern matching of potential service interrupting instances, and rules, model and intent driven software decision engines that learn (via analytics and rules, machine learning or eventually the intent by artificial intelligence) how to maintain service and repair resources in the event of some form of service or resource failure the concept of a fully autonomous network is becoming a reality.

Telecommunication networks are complex and with the transition to cloud, the virtualization of network functions on the arrival of software defined networking what we are seeing is an increase in the amount of complexity which in turn leads to difficulties in the development of products particularly those which are dependent upon network elements or network functions. It is imperative that we find a way of abstracting the complexity of the network to make the management all for the network services and therefore the agility and speed of the development of network-based products simpler and faster.

As the “Internet of Things” grow then we quickly reach the scenario where most aspects of network service management must be zero-touch because of the number of devices within the network generating events there is an exponential increase in the volume they might have or volume of data being generated and hence manual processes and activities to support the volume and velocity of required change is no longer possible.

If we look at a network servicing 10,000,000 endpoints with say 10,000 nodes, then over the next few years it's perfectly feasible that we could see these numbers increasing by up to a factor of five. In terms of incidents per hour this would lead to an estimated 25-times increase from approximately 400 incidents per hour to as many as 10,000 incidents per hour. With this volume of transactions, it would clearly be impossible to handle them manually.

As we look at autonomous networks, we are less concerned about the technology of the network but what we're looking at is some critical ingredients that are going to simplify the management and operations of the network. Open standards are an essential element of any network transformation, together with the appropriate virtualization and normalization of the network and its components which will enable flexibility, agility and simplicity we're looking at demarcating and grouping the current network elements into autonomous domains and encapsulating the complexity of the network within the various autonomous domain. Each of the autonomous domains will contain a closed loop of the infrastructure of both physical and virtual network elements that support appropriate telemetry that enables the monitoring and management of the network elements. To move towards an autonomous network, it is essential that we can expose a set of autonomous domain-based services that are easy to consume. It is also important that any of the autonomous domains can be managed by an external software controller thereby enabling the cross-domain automation.

The programmable infrastructure of physical and virtual network resources will produce significant amounts of data that can be used to determine trends from events and traffic patterns that can be learnt, and can be used to determine vulnerabilities or failures within the network as they happen, or better still in advance of them happening so that proactive actions can be taken to eliminate service or customer impacting events.

We want to ensure that the business capabilities that are exposed from the autonomous domains are vendor agnostic and provide an abstracted set of services that simplify the network architecture and therefore simplify the management of the network going forward.

We're bringing computer science and software design thinking to the design of networks to revolutionize the management of networks.

The impending arrival of autonomous networks is essential to transform the economics (efficiency, timeline and cost) of managing networks from where we are today, which is essential, given the increasing complexity in networks and network technology with the advent of SDN, NfV and 5G.

The rationale of autonomous networks is to make the simplicity to the end users and leave the complexity within the providers, which requires zero-wait service launch, delivery and care, zero-touch operations and maintenance, zero-trouble infrastructure for new business models:

- Autonomous network as a service: provide one stop, real-time, automated, on demand and customized full lifecycle network/ICT services
- Autonomous network as a platform: enable business collaboration & ecosystem between vertical industries and network/ICT services

Meanwhile, the autonomous networks can also provide the automation and intelligence of operations for the efficiency of existing and innovative services.

In order to achieve these objectives, some new approaches such as design-thinking and DevOps will be employed besides traditional static design and pipeline approaches.

# 5. Overview of Autonomous Networks Framework

The following section outlines the architectural framework necessary to deliver autonomous networks.

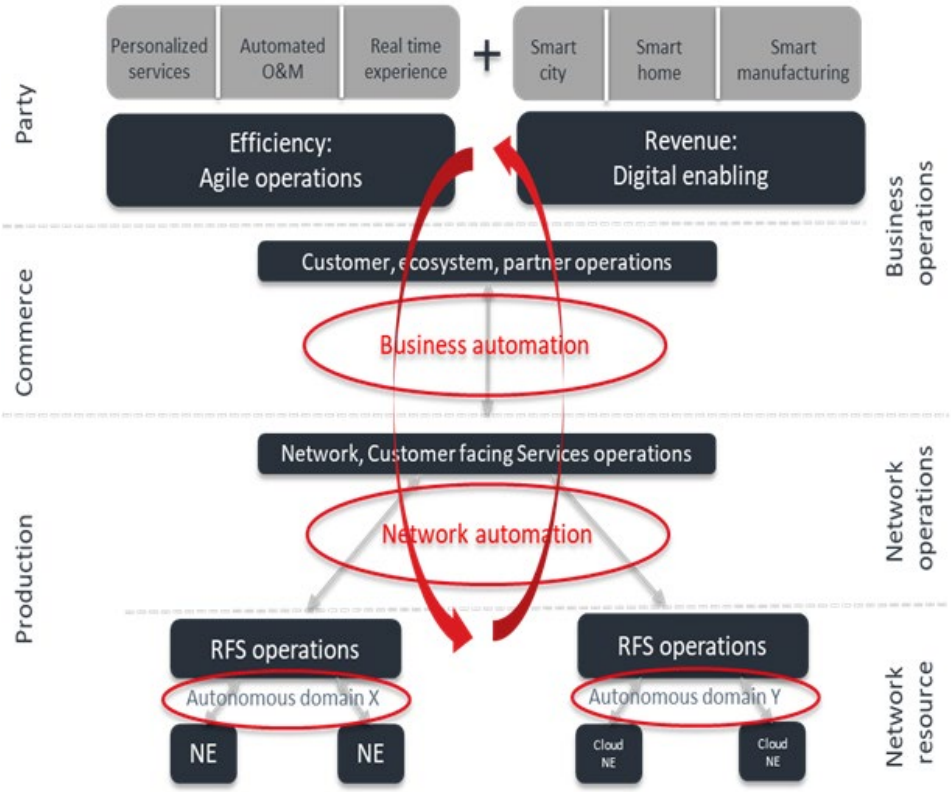



**Figure 2. Overarching framework: 3-layer + 4-closed-loop**

The overarching framework of autonomous networks is 3-layer + 4-closed-loop:

a) 3-layers: represent a group of common capabilities and business logics that can be utilized to support all scenarios, as well as business relationships between the groups of atomic capabilities.

- **Network resources layer** mainly provides the capabilities and business logics of network resources and automation in each autonomous domain level
- **Network operations layer**: mainly provides the capabilities and business logics of network planning, design, roll-out, provisioning, assurance and optimization operations across multiple autonomous domains
- **Business operations layer**: mainly provide the capabilities and business logics of customer, ecosystem and partner business enabling and operations for autonomous networks services

b) 4-closed-loops: represent the execution/fulfilment of the full lifecycle of the operations that can use the select capabilities of above layers upon corresponding business process.
   - **Network resource closed loop**: the network needs to be upgraded from fragmented, siloed network element level integration towards a closed loop of network autonomous domain based on an extremely simplified network architecture, which lay the foundation for the closed loop of network operations and collaborative production by means of cross autonomous domain collaboration
   - **Network operations closed loop**: the operations need to be upgraded from legacy customized project-centric approach to a data/knowledge driven platform based on full lifecycle operations automation. The most important part is a mindset change from a "build-and-operate" to a "design with operate", and the recognition of the value of operations knowledge as a service (KaaS). KaaS is about delivering the right knowledge to the right person in the right context at the right time via desktop, laptop or any mobile device. Operations automation sits at the core of production efficiency and business agility
   - **Business operations closed loop**: the operations needs to be upgraded from isolated business to on demand, automated business collaboration and ecosystem, which enables the closed loop for customer/business/ ecosystem operations, normally requiring collaboration across multiple service providers globally
   - **Cross layer user service closed loop**: leveraging the above three layers' and three closed loop processes to support the user service fulfilment. The interactions across the different layers should be based on simple, abstract API interfaces.

## 5.1. Closed loops

With Autonomous Networks we see clearly the need for closed loops. In the past these control loops were largely confined to a single domain (e.g. the business layer or the network layer), however to deliver the level of automation required to manage the networks of the future it will be necessary for the automatic closed loops to cross domains as indicated by the red ovals in the Figure 2, in addition to the closed loop of each single autonomous domain.

In these scenarios for example an incident in the network will impact a service, that service could potentially have an impact on customers' SLA, so the system will have to automatically determine if, based on the customers contract if an action must be taken. That action, determined by the SLA in the customer domain, may require a change to a service or resource in the production domain to ensure that the digital service provider continues to meet the contracted SLA. If this needs to happen during the use of, or consumption of, the service then it is likely that the change will need to be made in real time. If that is the case then the application of the change needs to be controlled automatically, without the need for human interaction, and flowing a set of pre-determined rules (possibly machine learned) or the system makes a decision on the next action (AI enabled). To facilitate this sort of control on the network from the customer SLA will require a set of network services that can be easily activated through a set of consistent, pre-agreed, industry standard interfaces (Open APIs).

## 5.2. Autonomous domains

Autonomous domains are the business disposition of network functions that is able to fulfil the closed loop automation of the lifecycle of specific network operations. In other words, they are the instantiations of network resource closed loops performing the automatic management of the network resources and capabilities. The autonomous domains demarcate the network into a set of cooperating domains upon the business logic of each CSP. Proposed examples of autonomous domains include the closed loops of access, metro backbone, core, edge, customer network from transport perspective, or SD-WAN, VoLTE, CDN etc. from service perspective.

The basic characteristics of autonomous domains include:

- Each of autonomous domains exposes a set of services via Open APIs for those autonomous capabilities to be employed by upper level users.
- Each of autonomous domain maintains a catalog of services for the domain, together with an inventory of service and resource instances that it knows about and is responsible for.
- A set of autonomous domains must be identified and agreed that represent logical areas of the network that specific elements must reside within. As a rule, a network element should be in one, and only one, autonomous domain.

To date these have been identified as the following architectural functions or services of autonomous domains:

1. identify an industry agreed set of autonomous domains that represent networks of the future
2. define a set of (vendor agnostic) network elements (or functions) within the various autonomous domains. These network elements or functions can be either physical or virtual components, and will expose a set of standard resource services at the domain level instead of element or function level
3. the ability to decouple one domain from another and expose a set of domain-based services via Open APIs to upper layer or other domains
4. the ability for a network element to configure itself and expose its characteristics to upper layer or other domains to allow it to be externally controlled
5. the ability to combine a set of network elements to build or deliver a higher-level network service,
6. the ability to deliver a service using a combination of flexible network services and resources that can be automatically orchestrated, configured, monitored and repaired using the same or similar network services and resources,
7. the ability to specify a set of rules at the business level (e.g. Service level availability, service level guarantee based on response times, repair times etc.) that can be automatically monitored and effected across all domains of the architecture, from here on referred to as closed control loops
8. the opportunity to model the exposure of network capabilities as a set of platform services to enable higher level business services to utilize network services

## 5.3. Loosely coupled Autonomous Domains

To maintain the simplicity, flexibility and agility of the architecture it is essential that we design the autonomous domains to be loosely coupled. This implies that we will expose an agreed set of services out of each domain, using an industry agreed format to expose the services and capabilities (suggestion is that we use TM Forum Open APIs to facilitate this).

## 5.4. Self-configuring and self-optimizing network elements

Where a network element is physically deployed impacts its characteristics, for example, by deploying a network element in an "edge cloud" which by definition is closer to the customer will reduce the latency of the function being invoked or delivered by the network element. For response time critical functions this is a very important capability that will need to be catered for within our architecture to support functions such as facial recognition for security services. When the network element is deployed, those characteristics that are dependent upon the physical infrastructure must run a self-test and expose the results as part of the configuration of the network element. For example, this could involve pinging the end point of the network and measuring the response time to determine the latency characteristics. This self-configuration of the network element could also include the optimization of the network element.

## 5.5. Combining network elements to deliver higher level services (RFS or CFS)

With the reusable components of the network it will be possible to combine elements or link elements together to build higher level services. In simple terms, and only by way of example, it should be possible to combine a firewall with an access service to build a secure access service, or model an access service using two physical, and different, access types together with a control switch that selects which access service to use, and it will be possible to build a resilient access service.

## 5.6. Orchestration and control of network elements

A key component of an Autonomous Network is the ability to use service and resource orchestration to deliver automation around service and network management. Orchestration is not limited to just the fulfilment process but across the complete service and resource lifecycle. We are therefore designing orchestration to automate network planning (proactive and reactive), customer order fulfilment and during the assurance process to support self-

healing and self-optimizing (including new on-demand capacity to support scaling of the network. With the abstraction and decomposition of the network into a set of cooperating autonomous domains, means that we need the ability to construct higher level network services from the base services offered by autonomous domains. This is a common approach in software enabled product and service modelling and is the key to being able to build a set of reusable components that deliver the required business functionality of the network being modelled in this way.

To enable this sort of functionality a series of orchestration capabilities will be utilized across the architecture within and across different autonomous domains. This lower level resource focused orchestration will be used to control and manage the lower level resources (both physical and virtual) within autonomous domains utilizing analytics, machine learning and eventually artificial intelligence (AI) algorithms. Where the resources are virtual, this objective is for these orchestration functions to be fully automatic.

## 5.7. Autonomous Networks exposed as services

A **Network Element** is an architectural concept that represents telecommunication equipment (or groups/parts of telecommunication equipment) and supports equipment or any item or groups of items considered as belonging to the telecommunications environment that performs network element functions. A Network Element communicates with an operations system for the purpose of being monitored and/or controlled. (Source: ITU-T M.3010 *Principles for a telecommunications management network)*

To enable the automated management of the network, the basic building blocks of the network, the network elements, must be capable of being grouped as autonomous domains and managed by a domain orchestration for the closed loop of basic network services. Getting the right level of abstraction within the network as autonomous domains will greatly simplify this task. Suggested “atomic” network elements might include firewalls, routers, edge servers, load balancers, switches, etc.

## 5.8. Autonomous Networks exposed as a platform

When we have our network modelled as a set of reusable components that are controlled and managed automatically moves us closer to the objective of having our network available as a platform service within the context of a wider digital ecosystem. Characteristics such as:

- Plug and play capability
- Flexible and agile
- Low operational costs
- Scalable
- Secure by design
- Easy on-boarding of new participants into the ecosystem

With these characteristics we envisage the network delivering digital enabling capabilities e.g. business collaboration, on-boarding, service development & launch, customer experience management etc.

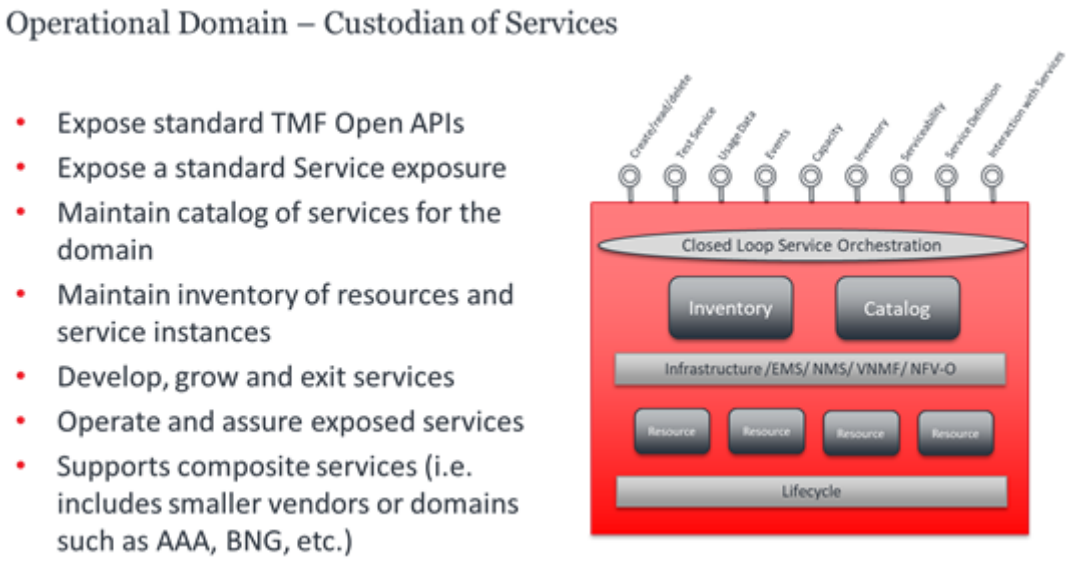



**Figure 3. Operational Autonomous Domain Management**

# 6. Autonomous Networks Roadmap

The roadmap will focus on next 2-3 year timeframe as a closed loop, and then reiterate the cycle periodically. The basic methods to realize the autonomous networks: user centric, business driven, top-to-down, quick reiterative:

- **User centric**: follow the full lifecycle of network/ICT services required by the end users (vertical industries and consumers) to develop user stories and use cases
- **Business driven**: distil business requirements and business metrics, and define business architecture - focus on business relationship, process and cross layer interaction from categorized user stories and use cases
- **Top-down**: use autonomous levels as the main thread, from overall framework to each of business/operations/network closed loops
- **Quick-reiterative**: illustrate the application scenario, reference solutions and catalyst project of autonomous networks per select use cases, and feedback to business requirements and architectures

## 6.1. Roadmap stages

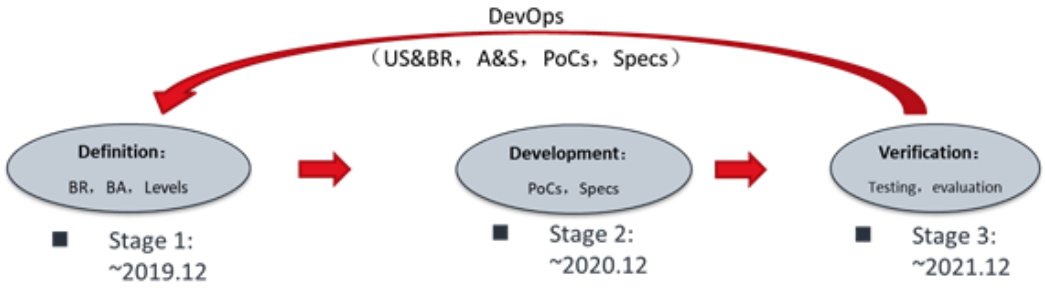



**Figure 4. Roadmap stages**

**Stage 1** (~2019.12): **Define overall requirements & high-level framework**

- User stories, business requirements & metrics, business architecture, automation levels

-Select and launch PoCs

-Collaboration with other IDOs & verticals

**Stage 2** (~2020.12): **Develop detailed specs**

- Technical architecture, data modelling, interfaces & Open APIs, measurement& metrics

- Catalyst projects showcases (2020.06, DTW)

**Stage 3** (~2021.12): **Establish testing and verification**

-Establish Open Digital Labs for showcases, testing and verification

-Start autonomous level verification

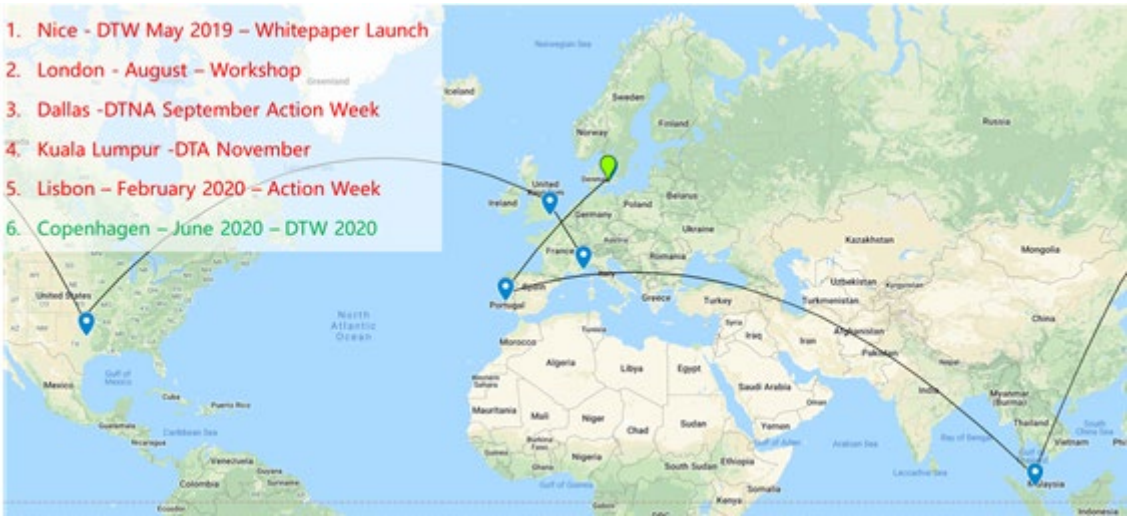
#### 6.1.1. Autonomous network services for user stories

In order to identify the key business requirements, business metrics and technical capabilities for deriving the main metrics and measurement of autonomous network levels, it is sensible to generalize E2E business lifecycle of certain common autonomous networks services. The following matrix is used to categorize autonomous networks services in support of various user stories for vertical industries and telecom industry:

| | Business growth<br><br>(Vertical industries, e.g. smart city, smart manufacture, self-driving car) | Operations efficiency<br><br>(Telecom industry, e.g. network planning, design, fulfilment, assurance) |
|---|---|---|
| Existing | 1. Automated network services e.g. VPN, SD-WAN, 5G slicing | 1. Pipeline operations automation e.g. predefined services and operations |
| Innovative | 2. Automated ICT services e.g. network + cloud + edge<br><br>3. Automated digital enabling services e.g. ICT services + platforms (operations, collaboration) | 2. Flexible agile operations e.g. platform based, dynamic process, flexible production |

## 6.2. Details on early steps

Workshops in next 12 months:




Remark: other workshops may be added upon the progress.

Key deliverables & milestones:

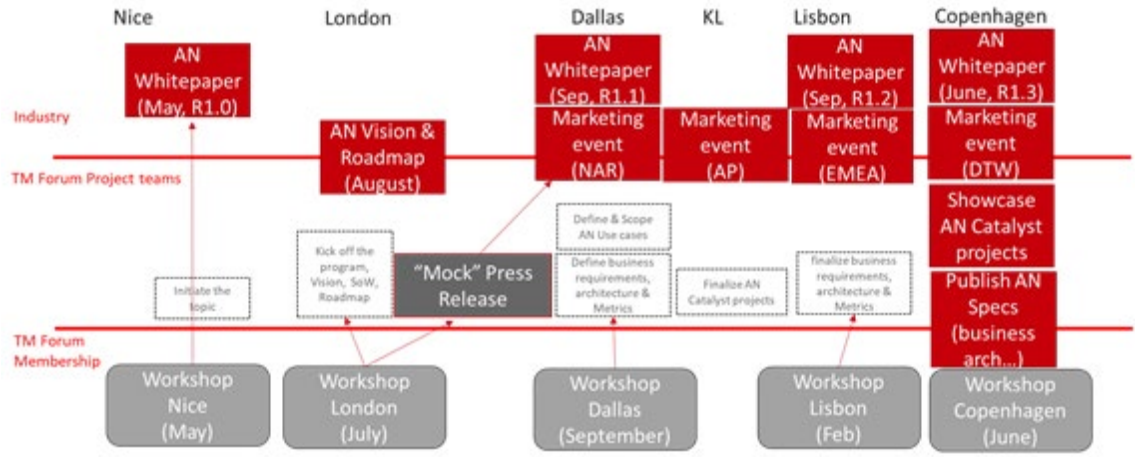



**Figure 5. Key deliverables & milestones**

Key work streams/work items:

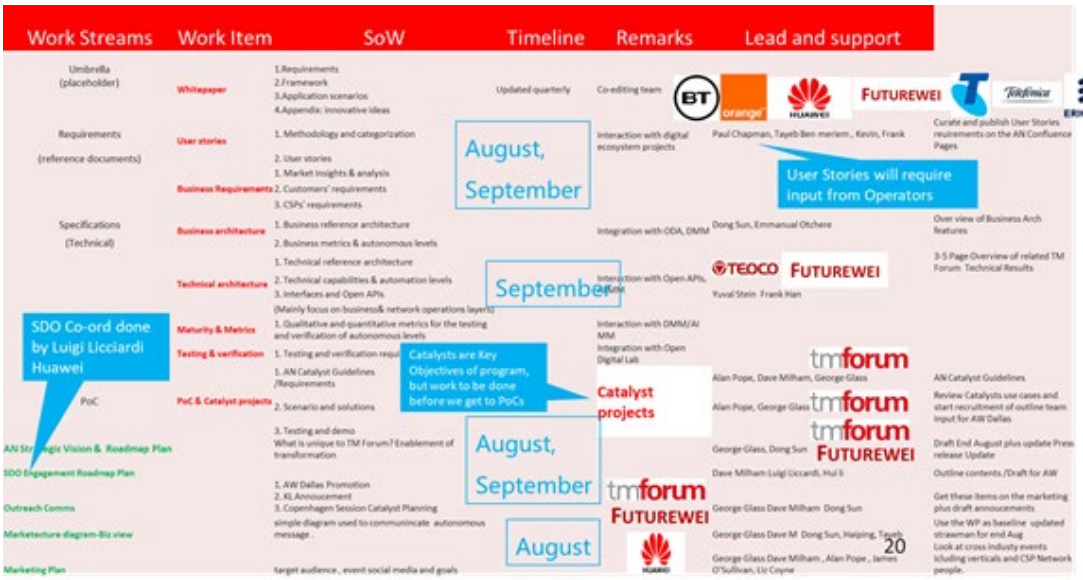



**Figure 6. Key work steams & work items**

# 7. Industry action

## 7.1. Engaging with other industry organizations

TMF will look at from user perspectives (verticals and consumers), define business requirements and business architecture and collaborate with other IDOs/SDOs/OSOs and other industry organizations to reach a consensus, including:

- to evangelize new collaborative production models through digital partner ecosystem – autonomous ICT/network services (in conjunction with digital partnership, operations automation and simplified network architecture/autonomous domains)
- to incorporate for the user stories/use cases, business requirements/framework/architecture and autonomous levels definition
- to implement and showcase the key functions e.g. business/network operations automation systems and simplified network architecture/autonomous domains for user need

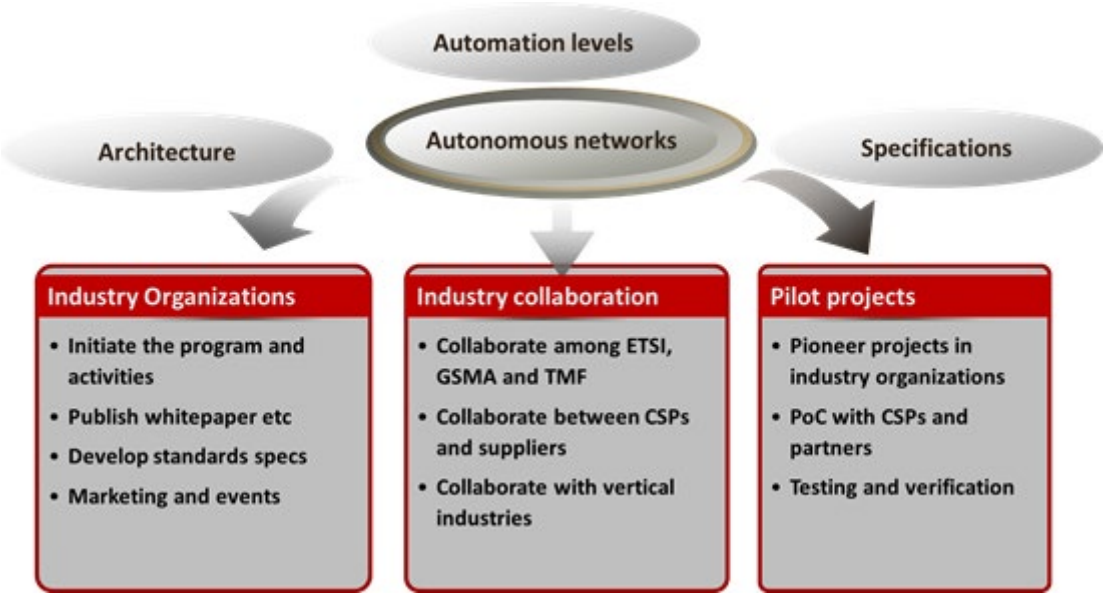



**Figure 7. Industry Collaboration**

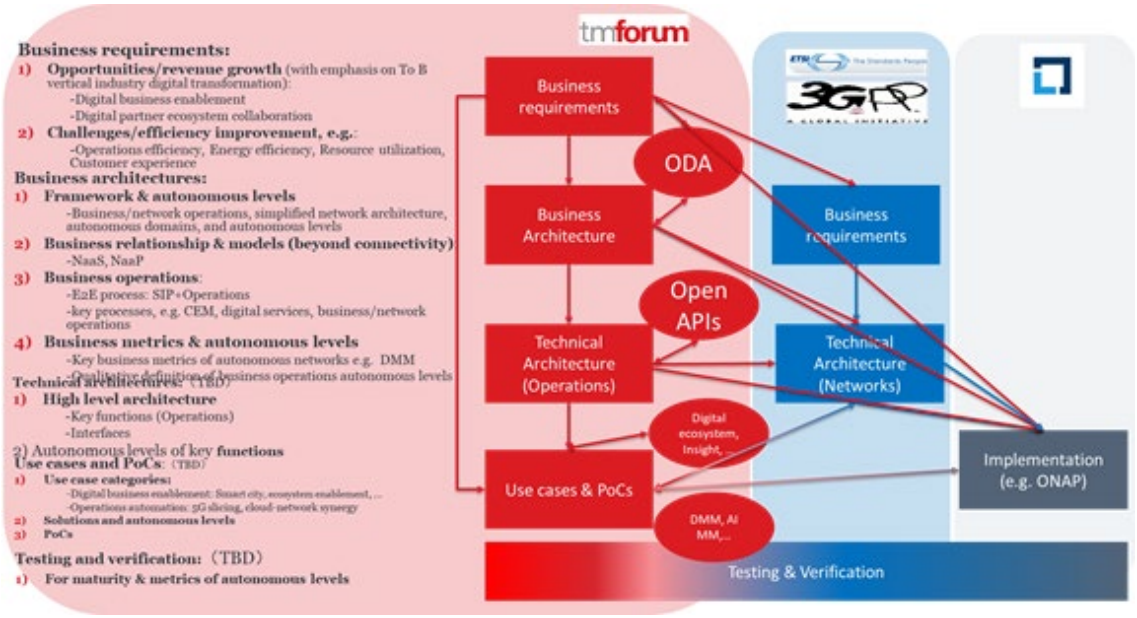



**Figure 8. Examples of relationship with industry organizations**

# 8. Administrative

## 8.1. References


1. SAE J3016 "Levels of Driving Automation".
2. TMF white paper (Release 1.0): Autonomous Networks: Empowering Digital Transformation For The Telecoms Industry.
3. TMF workshop in May 2019 Nice: TM Forum Spotlight: Autonomous networks – building the network of the future.
4. TMF newsletter: CSPs and suppliers seek consensus on autonomous networks.
5. TMF workshop in July 2019 London (member only): agenda, contributions, references and outputs.
6. TMF autonomous networks program work in progress page (member only) – Release 19.5.


## 8.2. Document History

### 8.2.1. Version History

| Version Number | Date Modified | Modified by: | Description of changes |
|---|---|---|---|
| 0.1 | 05 Aug 2019 | W George Glass, Dong Sun | Initial Version |
| 0.2 | 06 Sep 2019 | W. George Glass, Dong Sun | Updated after team review 4/9/19 |
| 1.0 | 04 Oct 2019 | Alan Pope | Final edits for Publication |
| 1.0.1 | 11 Nov 2019 | Adrienne Walcott | Updated to reflect Member Evaluated Status |

### 8.2.2. Release History

| Release Number | Date Modified | Modified by: | Description of changes |
|---|---|---|---|
| Pre-production | 04 Oct 2019 | Alan Pope | Initial Release |

## 8.3. Acknowledgements

This document was prepared by the members of the TM Forum Autonomous Networks project:

- W George Glass (TM Forum)
- Dong Sun (Futurewei)