tmforum

SERVICE ASSURANCE IN THE 5G ERA

Author: Dean Ramsay, Contributing Analyst
Editor: Dawn Bushaus, Managing Editor

servicenow

TM Forum's research reports are free and can be downloaded by registering on our website

Report Author:
Dean Ramsay
Contributing Analyst

Report Editor:
Dawn Bushaus
Managing Editor
dbushaus@tmforum.org

Chief Analyst:
Mark Newman
mnewman@tmforum.org

Senior Analyst:
Tim McElligott
tmcelligott@tmforum.org

Editor, Digital Content:
Arti Mehta
amehta@tmforum.org

Customer Success & Operations Manager:
Ali Groves
agroves@tmforum.org

Commercial Manager, Research & Media:
Tim Edwards
tedwards@tmforum.org

Global Account Director:
Carine Vandevelde
cvandevelde@tmforum.org

Digital Marketing Manager:
Anna Kurmanbaeva
akurmanbaeva@tmforum.org

Report Design:
thePageDesign

Published by:
TM Forum
4 Century Drive,
Parsippany,
NJ 07054
USA

www.tmforum.org
Phone: +1 973-944-5100
Fax: +1 973-944-5110

978-1-945220-90-6

Service assurance in the 5G era

We hope you enjoy the report and, most importantly, will find ways to use the ideas, concepts and recommendations detailed within. You can send your feedback to the editorial team at TM Forum via editor@tmforum.org

The big picture

5G has become synonymous with innovation, IT modernization and a huge broadening of the capabilities communications service providers (CSPs) can provide to their customers, especially enterprises. Reinventing the role of CSPs in this era requires reimagining operational and business support systems (OSS/BSS), which includes embracing automation and AI in service assurance.

The drive for business diversification has put CSPs in uncharted territory, chasing new digital revenue streams and cross-industry B2B2X partnerships. Preparing for this change has meant fundamental transitions in telco operations. Indeed, many operators have taken the first steps on a path away from being a traditional telco. However, they are retaining their largest capital asset: their networks.

CSPs understandably have put much of their developmental focus on 5G in the radio, proving the access technology will work. Now they are turning their focus to building 5G access and core networks at scale. In doing so they are scrutinizing the economics of 5G operations, which puts support systems in the spotlight. Service assurance has become an especially hot topic as it sits at the nexus between network-facing operations and the customer-facing business.

These groups traditionally have been disconnected within CSP organizations, but this cannot continue if they want to deliver on the promises of 5G. The simultaneous maturing of cloud, virtualization, analytics, AI and machine learning, microservices, and DevOps means that all the right tools are in place to achieve long-held goals for assuring quality of service end to end.

CX is a network topic

One of the key challenges for suppliers of service assurance systems lies in being able to identify proactively network issues that impact customer experience (CX). The notion of directly influencing customer service outcomes by improving understanding of network issues has not been an exact science, or at least not an accurately measurable one.

Because of the complexity of networks and OSS, this has been possible only for select service examples, such as in small private networks. The expectation of new service assurance systems is that they can bring together network and service operations to directly equate network issues to their impact on CX.

In this time of network investment, assurance must focus not only on performance management and fault monitoring of existing infrastructure, but also on helping to optimally plan 5G rollouts. In an ideal world, network investments would focus on improving customer experience, while reducing costs and honing operational efficiency, and any improvements in the network should be easily measured in tangible benefits.

In the real world, however, layers of complexities prevent CSPs from precisely identifying network events relevant to specific customer experience KPIs. In the 5G era it should become possible for operators to filter the pertinent information from the noise, understand the consequences and take action to optimize operations, all in a highly automated fashion.

Read this report to understand:

- Why data is critical for service assurance and how orchestration relies on it
- Why assurance is especially important in 5G networks
- What CSPs should look for in evaluating service assurance systems
- How standards such as the TM Forum Open APIs and the Open Digital Architecture guard against data silos
- Why assurance must be proactive
- How assurance can improve CX
- Why fulfillment and assurance go hand in hand, and why they require a "single source of truth"
- The role for automation, AI and machine learning in service assurance

Section 1

Creating service-level insights from the noise of network data

One of the central tenets of modern, analytics-driven operational and business support systems (OSS/BSS) is that communications service providers (CSPs) should be able to cut through the sheer volume of data to find the important information that relates to specific service quality metrics. In its position in the stack, service assurance can act as an abstraction layer collecting network data from below and translating KPIs into service-centric language for use throughout IT operations. As such, OSS can trigger automated workflows to achieve optimization in a service-aware way. While many companies have pursued this line of thinking, the reality of modern operations is that there is still some way to go to cross-correlate network operations data feeds into meaningful service-centric insights.

The role of analytics in this endeavor is clear: Number crunching algorithms are designed to convert quantitative data into qualitative data and processes, acting in a distributed manner in the components of the OSS architecture. It is also important to bring those insights together in a centralized way to provide intelligence for orchestrated master control.

New & old will coexist

The traditional role of service assurance is network-facing in that it monitors and manages data sources from network and element management systems and network probes in physical networks. In many cases CSPs use several assurance systems from vendors associated with different network domains, business units and data sources.

Highly virtualized hybrid network architectures associated with 5G will not replace existing networks any time soon, so the two will live alongside each other as operators try to fully realize the return on their previous investments. So, in effect 5G is adding more noise to the data that is passed into assurance systems and is not removing the existing data sources.

Any new assurance system must have the ability to handle all these disparate inputs and still create a uniform type of actionable insight for each generation of technology.

Taiwan Mobile is a good example of a CSP benefitting from service assurance transformation. As part of a multi-stage effort, the company is deploying end-to-end network and service assurance solutions to gain better insights into network problems by looking at their root causes and impact on customer experience. This helped to consolidate Taiwan Mobile's 2G/3G/4G and fixed network OSS, which includes probing data sources to build a centralized OSS data lake. The company has transformed standalone, siloed applications into an open telco OSS framework with consolidated umbrella applications which share data through TM Forum Open APIs.

Read the full case study:

Cross-correlating service quality

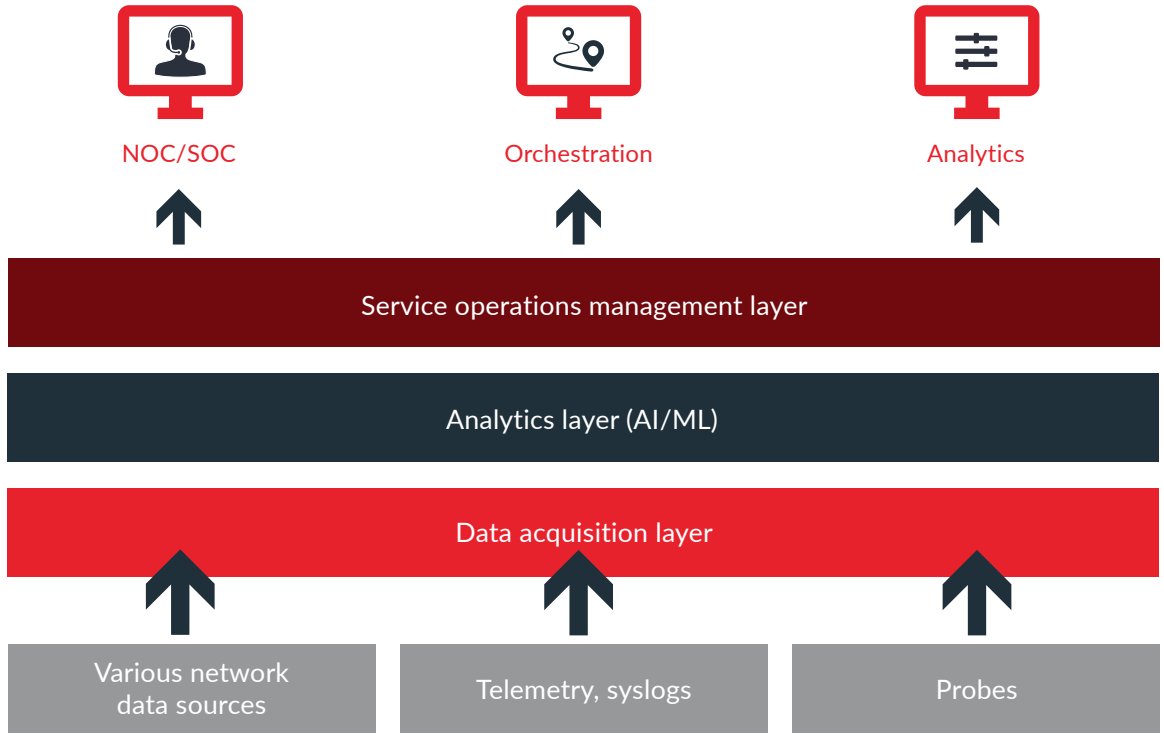
While traditional assurance systems monitor the slew of network feeds for obvious faults or alarms, the current generation creates insights by identifying patterns in the data which may signify less obvious inefficiencies. In the 5G era this must be taken a step further so that service assurance can simultaneously monitor KPIs for network and customer service quality in real time.

Cross-correlating these two data sets in a contextual manner leads to the creation of operational insights that are incredibly useful from a network, service and customer point of view. As CSPs have invested heavily over the last decade in data infrastructure, they already have petabytes of historical data from the network, devices and customers (including usage and billing data) from which to generate highly granular insights.

Achieving this, however, is one of the truly challenging transformational leaps for vendors and operators. Vast amounts of data must be processed in real time, and generating useful insights relies on an extremely agile data model and database architecture that is adaptable to the many disparate inputs and scenarios. CSPs are increasingly concerned about the granular details of software development and have more stringent requirements on the way data models in vendors' solutions interact with upstream automation in OSS/BSS.

Orchestration relies on accurate data

One of the key upstream interfaces for the new breed of assurance systems is the service orchestrator. The concept of service orchestration supporting all tasks in the OSS relies on an assurance solution that can generate high-quality data to be used in the fulfillment of new services and in altering current service orders. High levels of automation result from service orchestration, but automation can be derailed easily if the data the orchestrator receives from other OSS such as assurance is bad.



TM Forum, 2021

In moving away from a siloed approach to gathering network data, CSPs are implementing a horizontal, platform-based approach to assurance that relies on analytics and ingesting and aggregating data from many sources in a multi-vendor environment.

This means that the bottom layer will focus on data acquisition from different network domains (core, transport, access, data plane, customer site, etc.) where it can curate and cleanse data.

This data will be from several sources within those domains, such as telemetry, syslogs, probes, and various test and sensor data, all of which needs to be harmonized as it is sent up to the network operations layer. It is essential at this stage that contextual data relationships are preserved so that a cross-domain, end-to-end service view is maintained.

Above that, the analytics layer starts to convert these pieces of network data into formats that are easily ingested by systems in the service operations ecosystem. Ultimately the service operations management layer provides insights and actions from the application, where it can interface with other northbound OSS through standardized APIs. The data exposed to the OSS should be in a standardized form that interoperates easily with the CSP's service orchestrators, the network or service operations center, and other analytics platforms.

We'll discuss this more in the next section as we address service assurance requirements in 5G networks.

> "In moving away from a siloed approach to gathering network data, CSPs are implementing a horizontal, platform-based approach to assurance that relies on analytics."

Section 2

5G operations – Complex but predictable

Deployment of 5G is different from previous generational changes because it is happening in distinct phases. **Non-standalone 5G** came first, marrying new radio access network (RAN) capabilities with the existing LTE packet core network and utilizing many existing operational and business support systems (OSS/BSS). **Standalone 5G**, which is just getting underway, includes a new 5G core and orchestrated OSS/BSS designed for purpose. These changes allow communications service providers (CSPs) to create exciting new enterprise services (and revenue streams) that leverage features such as very low latency and high availability.

Standalone 5G networks are operationally complex because the core is based on cloud native, containerized architectures that will be orchestrated by Kubernetes or similar platforms. Cloud-native communications networks are significantly more complex than traditional physical, and even current virtualized networks.

That said, the international effort that is going into building standards and defining 5G operational systems surpasses any previous collaborative effort. This combined with the very IT-centric nature of cloud native control environments means that theoretically there should be fewer major anomalies and unpredictable faults.

A containerized network orchestration layer houses all the container network functions, so in establishing these tight orchestration rules, the whole network architecture can be redefined at will to match the needs of service requirements and quality of service (QoS). Data feeds flowing from network operations into assurance systems may contain vast amounts of data, but containerized networks should be significantly less unpredictable than physical legacy networks.

> “ Standalone 5G networks are operationally complex because the core is based on cloud native, containerized architectures. ”

Targeting B2B

For the first time, the majority of new revenue opportunities for CSPs are on the B2B side of their business, as enterprises increasingly demand non-traditional connectivity services to innovate and drive digital transformation in their own industries. The graphic (opposite) shows the types of use cases that are possible with 5G.

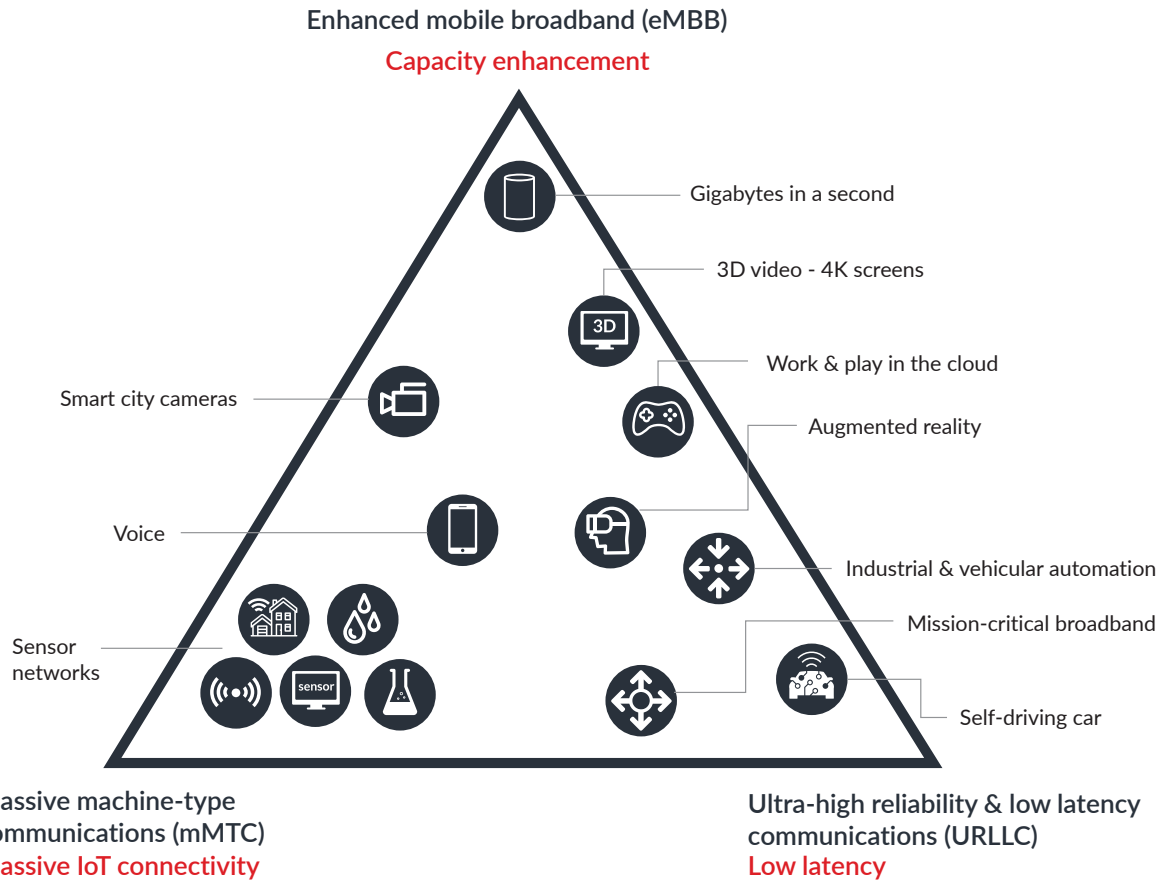
To deliver many of these services, CSPs will need to participate in unfamiliar value chains with customers who have high expectations. One manager of network strategy at a European mobile operator interviewed for this report calls this "an exercise in becoming exactly like your customer, but with a global SDN [software-defined network]."

This illustrates the point that 5G is more than just a supercharged RAN. It is a holistic ecosystem that includes the network, OSS, BSS and customers' systems. Each of these ecosystem components must be fit for purpose in order for CSPs to effectively manage and monetize features such as network slicing.

This is the main driver for marrying network and service operations with service assurance. As an example of this joined-up thinking, Mobily announced in January that it has successfully piloted 4G and 5G fixed wireless access (FWA) network slicing on its live commercial network.

The ongoing pilot in the Saudi Arabian capital city of Riyadh is taking place in a multi-vendor environment and includes sliced access, transport and core networks with management and assurance capabilities.

What are the use cases for 5G?



TM Forum, 2021

What's needed for assurance?

In evaluating 5G service assurance systems, CSPs should look for the following characteristics:

Cloud native – systems should be purpose built to work in a cloud native platform model to give operators the agility needed to easily scale deployments up and down in response to demand from customers. A cloud model also easily allows for DevOps methodologies, microservice architectures and continuous integration and delivery (CI/CD).

Centralized data – most CSPs have different assurance systems or tools for performance management, fault monitoring, alarm management, trouble ticketing, probe monitoring, etc. Indeed, it is not uncommon for a single network operator to have multiple silos of each type of tool. "Swivel chair" operations with multiple user interfaces promote disjointed manual processes, so operators should look for systems that can eliminate silos and centralize data.

Uses AI – AI and machine learning should be embedded into software systems to provide intelligent, contextual analytics at scale. Building the right kind of workflow from a variety of complex data sources requires human-like decision making that basic policy cannot match.

Real-time – systems should be able to build an end-to-end, real-time view of all service-specific data. This is a classic telecoms problem that has been again under the spotlight in recent years as cost-saving initiatives and the drive to operational efficiency were catalyzed by network virtualization. CSPs need to move from being network-centric to a more service-centric model. A service quality approach from the service assurance function will organically drive this cultural change.

Predictive – algorithms that can make predictions in advance of any impact on customers are now genuinely achievable. Root cause analysis remediation routines can be then engaged ahead of any customer affecting fault.

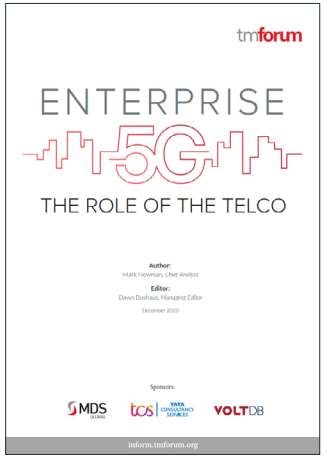
Based on standards – as all the above relies on a multi-vendor ecosystem, it is essential that interoperability and data sharing is optimal among systems. The TM Forum Open Digital Architecture (ODA) and Open APIs can help CSPs manage service assurance end to end (see panel).

From reactive to predictive

Most CSPs keep a keen eye on their Net Promoter Score (NPS) and other metrics to understand how they are performing in the opinion of their customers. They also collectively spend billions of dollars annually on software and third-party services to improve handling of customer interactions across all channels. This is, of course, a retroactive approach to understanding customer experience and satisfaction.

A better, proactive approach to assurance is addressing problems before customers are even aware of them. The shift in customer care from reactive to predictive is being mirrored in assurance as part of the real-time view of all network assets and environments across legacy and virtualized hardware.

For more about enterprise 5G and the role CSPs can play, read this report:



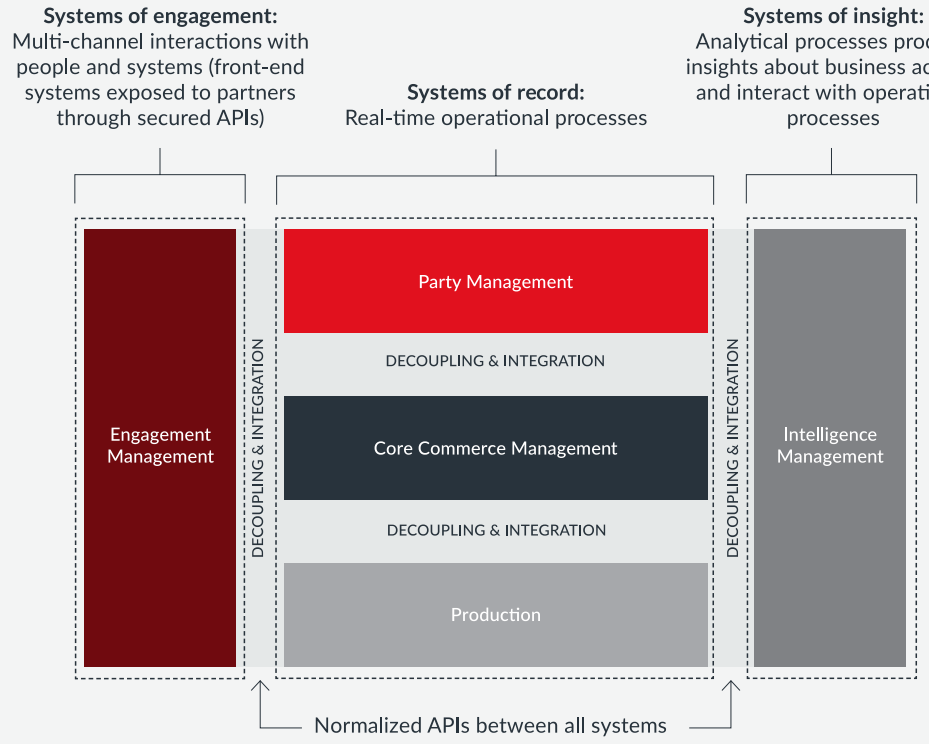
Intelligent, end-to-end operations rely heavily on CSPs not hiding mission-critical data in siloed databases where automated workflows cannot interrogate, extract or alter it. The TM Forum Open Digital Architecture (ODA) uses an architectural framework, common language and design principles to help with this.

The ODA, which is part of the Open Digital Framework (see page 34), defines standardized, interoperable software components organized into loosely coupled domains. These components expose business services through Open APIs built on a common data model. Importantly, ODA provides machine-readable assets and software code, including a reference implementation and test environment.

CSPs have led development of the architecture to reduce the time it takes to create new services from many months to just days or even hours. Today it typically takes about 18 months for CSPs to develop and monetize new services because of requirements to build connections many times over between customer management, service management, and ordering and billing systems across several lines of business. TM Forum members refer to these as systems of engagement, record and insight rather than OSS/BSS. The graphic below illustrates the functional architecture of the ODA.

Read this report to learn more about ODA and Open APIs:

ODA functional architecture



TM Forum, 2021

Ongoing closed loop analysis of granular data allows the surprisingly accurate prediction of traffic spikes and congestion, and even the prediction of a failing piece of network equipment. Proactively modelling the effects of future network failures within assurance systems allows CSPs not only to predict the event, but also measure its severity and take actions to ensure that any exposed services are not dropped as a result.

We'll discuss "closing the loop" more in the next section. Rather than passively experiencing an outage and waiting for customers to complain, service assurance systems should help CSPs proactively address problems in one of three ways:

- With predictive assurance, the assurance solution deals with a fault before it occurs. The customer remains unaware that anything happened, which means that customer satisfaction is unaffected and over time should improve.

- If service-affecting failures are unavoidable (for example, in the case of failing customer premises equipment), the service assurance solution can trigger customer care systems to start notifying and resolving the issue with the customer, in line with their service level agreement.

- If a network fault has occurred and the CSP is unaware of its effect on customer service, it should be possible when a complaint is made to use service assurance to perform rapid root-cause analysis to discover the relationship between a specific fault and the service outage. The assurance solution can then send all the pertinent information about the time of the expected resolution to a customer service representative or directly to the customer via their preferred channel. This is the least desirable action but better than ignoring the fault.

Improving CX

This kind of proactive behavior can have a hugely positive effect on NPS. To achieve it, the assurance solution must rely on analytics to build tight, cross-correlated models for network and service data. The data is already there for all operators; it just needs to be processed intelligently and packaged to create helpful workflows. Doing this well will separate successful and unsuccessful vendors of assurance solutions going forward.

Vodafone, for example, is undergoing digital transformation to provide customer care agents with a 360-degree view via a single platform. This has enabled the company to decommission 24 customer-facing systems that agents previously had to consult in a swivel-chair manner. The challenge of navigating across the legacy apps was compounded by complex service management processes that resulted in unhappy customers and a high cost to serve them.

Now, Vodafone has a single platform with native event correlation. This has led to a 45% reduction in the cost to serve customers, a 45% increase in agent productivity and a 25% increase in customer satisfaction.

"Before digital transformation, Vodafone was a collection of systems," says the CSP's Head of Digital Experience. "It was a really complex environment…a customer would know about a problem before we would. Our agents now have one application that helps them provide excellent service."

In the next section we'll look at the steps CSPs are taking to automate service assurance.

Section 3

Moving towards zero-touch operations & management

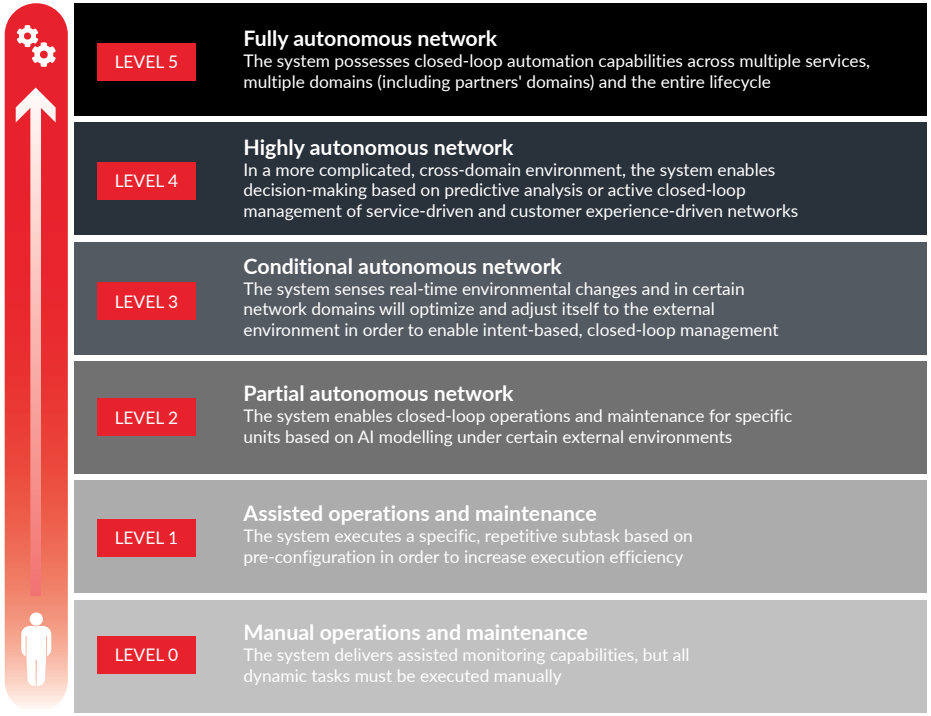
With simultaneous transformations including adoption of cloud, virtualization, microservices and autonomous networks happening simultaneously across the telecommunications industry, shortcomings in the way companies think about software stacks based on legacy operational and business support systems (OSS/BSS) are evident. However, suddenly abandoning traditional methodologies will not happen right away. Instead, CSPs will move toward fully automated end-to-end orchestration of 5G services in incremental steps.

TM Forum members collaborating in the Autonomous Networks Project have identified six stages of advancement towards fully autonomous networks and operations. Most CSPs' service assurance systems are operating at Level 2 with some still at Level 1, meaning there is a great deal of work yet to do.

Progressing towards full automation requires merging service fulfillment and assurance, which until now have been separate disciplines. Digital transformation and the introduction of network functions virtualization (NFV) have promoted a new way of thinking about the interactions of central operations functions. Virtualized networks and software-defined networking (SDN) can help CSPs reduce OpEx and increase agility, but these gains are possible only if cultural change in the structuring of departments and processes is addressed.

As such, it is becoming more common to see OSS job titles such as "Service Fulfillment and Assurance Manager". This illustrates internal commitment within CSPs' organizations to "closing the loop" on complex OSS processes (see page 18).

5G forces automation



TM Forum, 2021

Why do telcos need to close the loop?

In simple terms, closing the loop means collecting and analyzing data to figure out how networks can be optimized, and then implementing those changes in an automated way. This is a critical step toward fully autonomous networks that rely on AI. Theoretically, bringing fulfillment and assurance together is also a simple concept, but redesigning these core processes within working systems has been a classic stumbling block for digital transformation.

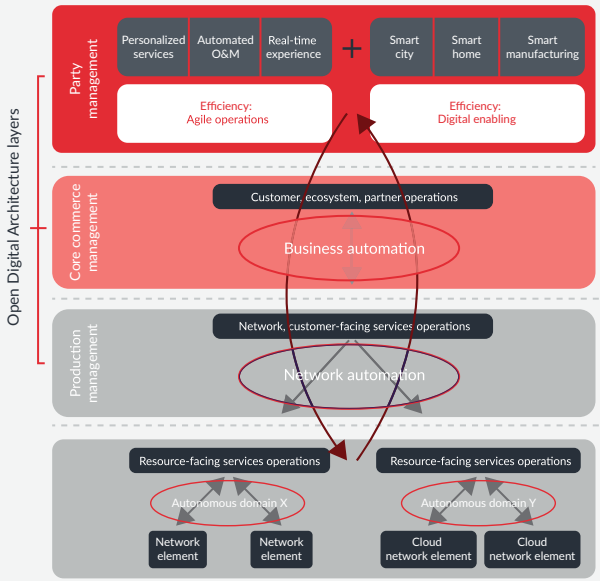
Many of the advancements in this area lie in using orchestrators to enable intent-based, end-to-end management. This approach abstracts the complexity of the network at a high level and then uses a customer's intent along with policy, machine learning and AI to manage it.

It should be possible to orchestrate a network solution to match the intent and then constantly monitor the solution in real-time using assurance. Constant monitoring then organically optimizes how the service is delivered in real-time within the closed loop system.

Implementing this closed loop at several levels within the architecture would then allow CSPs to constantly manage, optimize and remediate issues. TM Forum members are developing architectures and best practices for closed loop operations as part of several collaboration projects and Catalyst proofs of concept. The graphic opposite illustrates the concept as explained in a recent white paper about autonomous networks.

A recent Catalyst project called *Agile and automated digital enterprises*, which was championed by BT and Verizon, demonstrated intent-based service management, showing how a CSP could provide a managed digital workplace solution that included software-defined wide area networking (SD-WAN) and unified communications provided by a partner. In this case, the CSP offered multiple meeting solutions like Zoom to customers using service abstraction and APIs. The CSP did this by mapping meeting product offers to an abstracted meeting service definition, agnostic of supplier which meant that the product and offer definitions were not impacted each time a new meeting solution was added, modified or swapped out.

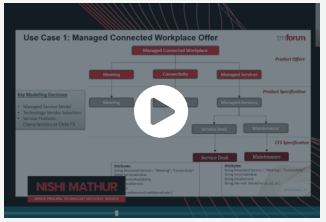
Layers and closed loops of autonomous networks



TM Forum, 2021

Read the white paper:

Watch the video to learn more about the Catalyst:



A single source of truth

Successfully closing the loop relies heavily on alignment of systems in a multivendor environment, and on the quality and synchronization of the data which is stored in disparate databases. Service fulfillment processes for provisioning new orders often refer to network inventory data to make logical and physical allocations for new services. Traditionally these inventory databases were synchronized with the live network data sporadically.

But in the era of virtualization, it has become more important for inventory to reflect a real-time, live view of the network. In tightening this link between fulfillment systems and the assurance view of multiple network domains, the need for a "single source of truth" has become more important than ever.

CSPs often employ data quality teams whose job it is to constantly validate the information stored in network inventory databases. This work, which is accelerating as operators adopt DevOps practices, has taught the industry many lessons about the importance of version control in systems of record. This applies to records for any kind of operational issue, from asset and connection inventories, to service/product catalogs and customer premises equipment logs. Fixing fragmented data storage and retrieval can be costly and time-consuming.

The relationship between a live view of network topology (coming from various network and element management systems, probes, NFV management systems, and other sources) and the data stored in network inventory systems is still a pain point for operators.

The single source of truth becomes critical to avoiding order fallout and manual intervention during the ordering process, as the order management software goes through the actions of order decomposition following the successful validation or the order.

Resource monitoring and topology data in assurance systems and in the network provide key information (device states, equipment availability, cluster configuration, redundancy routing, alarm data, etc.) which is pertinent to the concept of a real-time active inventory. Assurance must support virtual, logical and physical resources equally well in representing the network. This should also apply across legacy networks as well as next-generation software-defined networks in the 5G realm.

The challenge in virtualized networks is keeping network information up to date since virtualized functions are constantly changing. So, functions such as probe systems can poll the network to retrieve a real-time network topology view, including virtualized functions, which should then be instantly reflected in the service assurance system.

> "In the era of virtualization, it has become more important for inventory to reflect a real-time, live view of the network."

This allows the entire operations ecosystem to utilize any network topology information as outages occur to drive the resolution of outages and manage communication with customers through service assurance workflows.

Catalogs & inventories

Several evolutionary changes in service fulfillment since the introduction of NFV and SDN are outlined below. Each has implications for service lifecycle management, meaning the advancement of service orders from instantiation through to decommissioning:

- Centralized product and service catalogs have become a popular way for service fulfillment to address automation problems and drive data quality goals. Catalogs have been "centralized" by becoming a single, detailed reference point for all products and services offered by the company.
- Service orchestration has become the master control process for order management down through provisioning and activation.
- Network inventories have become 'dynamic' to accommodate hybrid virtualized network environments.
- Inventories have also attempted to draw together physical, logical and virtual network records to create a holistic view of the network to better inform ordering, provisioning, planning and optimization.

In the process of fulfilling a digital customer service, the service orchestrator will run a workflow through several OSS to activate the service. For more complicated hybrid cases involving legacy inventory systems and activation of physical network components, service assurance data becomes essential for successfully fulfilling the service without the order dropping out of the automated workflow and entering a manual work queue for operations staff to activate. Consequently, real-time network topology data, performance data and other network-related insights can be used in conjunction with inventory to maximize the efficiency of all service lifecycle activities.

From months to days

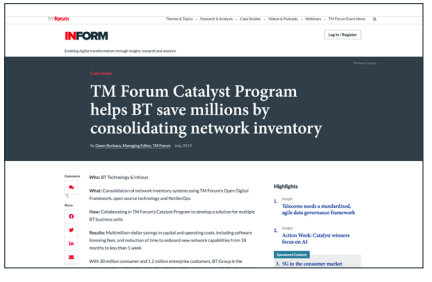
BT recently used the TM Forum Catalyst Program to develop a solution for consolidating network inventory systems, resulting in significant operational savings and a reduction in the amount of time it takes to onboard network components from 18 months to just days.

The company began a project in 2017 to consolidate network inventory systems and digitize business processes in order to introduce automation and improve customer experience. A key objective was to consolidate different types of network inventory – physical, logical and virtual – into a single system to ensure data integrity. BT calls the consolidated system SRIMS (Single Resource Inventory Management System).

This has helped the company save millions in CapEx through network asset reconciliation and in OpEx by reducing software licensing fees.
In the next section, we'll look more closely at how CSPs intend to use AI to improve assurance.

In the next section, we'll look more at the role for AI in service assurance.

Read the full BT case study:



Section 4

The role for AI & machine learning in 5G service assurance

As communications service providers (CSPs) move towards automated orchestration of 5G services, they will retain separate fulfillment and assurance processes along with many other legacy processes. However, establishing a strong overlay in functionality and interoperability is essential to work toward full automation.

Many support system suppliers have been adopting machine learning and AI over the last five years, eliminating repeatable manual tasks and replacing them with programmed tasks automated with software. Assurance has been one of the hotspots within operational support systems (OSS), where the benefits of AI and machine learning are pronounced in real-time performance analysis, contextual analysis for service quality optimization and pattern analysis for predictive fault detection.

Many complex return-on-investment models for 5G operations have scoped the effectiveness of using AI and machine learning to manage the costs of 5G at scale and have included that reasoning in the model. Essentially CSPs are interested in the positive impact these technologies can have on various business metrics, and ultimately the bottom line. For example, fewer service issues and network interruptions should cut the customer churn rate, truck rolls, mean time to repair, network queries into contact centers and mean cost to repair.

Bringing together multiple data sources provides a real-time and accurate view of the interrelation between physical, virtual and logical elements. In doing this, it is possible to provide a much wider topological view for end-to-end service awareness. This is something that leading fulfillment vendors have been trying to achieve in network inventory at the request of CSPs for many years. The latest versions of their logical network inventories include physical and field asset records.

Dynamic automation

The manual tasks associated with performance, fault monitoring, alarms, etc., require highly skilled staff to analyze the data because the right decision is often contextual and dynamic. From this point of view, rules-based decision making lacks the awareness that AI and machine learning can bring, especially in the context of services provided to customers.

It is, however, something that is being addressed with investment from CSPs and vendors. According to research from Omdia, nearly 80% of service providers see the use of AI and analytics, when it comes to the automation of network activities, as an "important" or "very important" IT project for 2021. Nearly 60% of them are planning to increase investment in AI tools.

TM Forum's recent research also finds increasing use of AI in operations (AIOps), although it is still a relatively small proportion of IT spending. CSPs are bullish, however, about the long-term prospects for fully autonomous networks, with more than half believing their companies will deploy them within a decade.

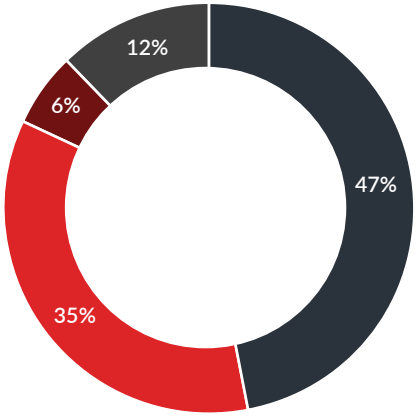
AIOps Catalyst teams develop use cases

The winners of two Catalyst awards at TM Forum Action Week in February have been using AI to automate planning, constructing, operating and maintaining their networks. Their work is providing the foundation for some of the Forum's collaboration projects focusing on automation and AI.

The *AIOps autonomous service assurance* project demonstrates how AI can drive and transform network service assurance by building predictive, closed loop processes. The team demonstrated six use cases including customer experience assurance, fault prediction for multiple types of network technology including 5G, autonomous control desk and NFV service assurance. Champions of the project include China Telecom, Cosmote, LG U+, HKT (PCCW Global), Smart Communications and TIM.

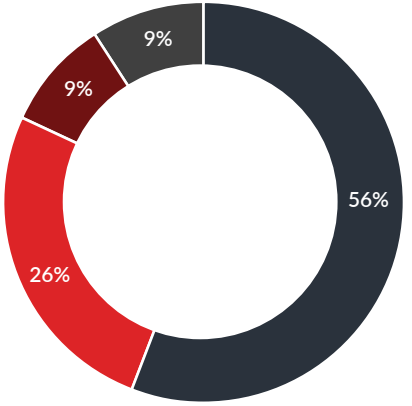
According to the team, the biggest challenges lie in how to combine different use cases, technologies, contexts and solutions, and how to orchestrate them together to ensure consistency. They relied on the AIOps Service Management Framework which has been developed by TM Forum members to prepare IT operations to operate AI at scale and eventually become fully autonomous.

Percentage of CSPs' IT spending on AIOps in next three years



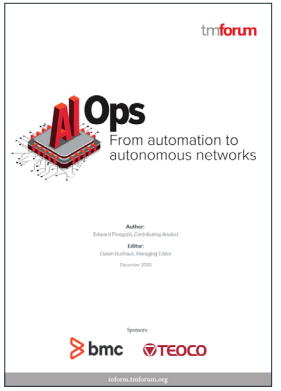
- Less than 10%
- About 25%
- Roughly 50%
- All of it as AI will be part of everything

Will CSPs deploy large-scale, fully autonomous networks run by AI within 10 years?



- Yes, definitely
- Possible but not likely
- Maybe but doubtful
- No

Read this report to learn more about AIOps:



The *AI empowered 5G intelligent operations* project demonstrates how to use AI to boost efficiency; improve customer experience and energy consumption; and reduce OpEx. China Mobile, one of the founders of the TM Forum Autonomous Networks (AN) Project, is the champion of the proof of concept.
The project is important because it demonstrates how to use AI in a controlled way to maintain a live, commercial network – in this case, China Mobile's. In addition, the team was instrumental in creating two TM Forum white papers about autonomous networks.

"The biggest success of the first phase of the Catalyst is practicing the application of AI in the real network and for network planning," said Yao Yuan, Project Manager at China Mobile and leader of the Catalyst project. "It has given us a chance to better understand AI and helped us figure out models. AI is a great but not an easy technology, and sometimes training the AI is as difficult as raising a baby."

To find out more about TM Forum's work on AIOps, please contact Aaron Boasman-Patel.

AI-powered assurance
AI needs to perform human-like reasoning in the case of service assurance to achieve more contextual decision making, at speed and at scale. For example:

- **Patterns in alarm detection** – AI and machine learning can be used together to learn from network events, alarm patterns and resolutions to automatically relate those events against previous similar scenarios to identify root causes for network and service outages. Machine learning can then establish a log of best practice actions for similar future events. The system is self-improving and dynamic: As more data is analyzed, automation levels increase.

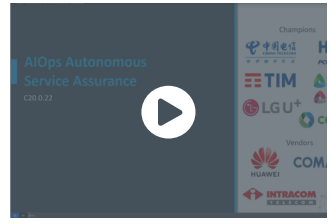
- **Understanding what's normal** – assurance analyzes performance data in the data acquisition layer creating a view of "normal" performance deviations. If access and transport networks are constantly showing some sort of congestion, AI and machine learning can build a more dynamic view of which threshold KPIs are anomalous and must be acted upon versus which are expected and will return to normal if left alone.

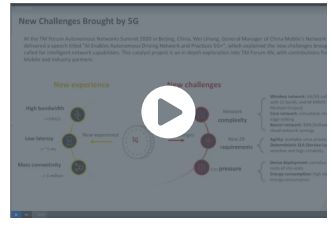
- **Optimization & remediation** – based on pattern analysis or from the autopsy of a catastrophic failure, it should be possible for AI to trigger workflows into the network or service operations center to suggest the optimal fix for the failure. Assurance may even need to trigger a workflow into a system for network planning and optimization, which will bring about a more systemic procedural change in operations.

- **Cross-domain auto-discovery** – AI should be able to automate the discovery of network topology relationships across different network domains without requiring topology information.

In the next section, we offer recommendations to help CSPs advance service assurance in the 5G era.

Watch the videos to learn more about the Catalyst projects:





Section 5

Make it happen – Strategies for service assurance in a 5G world

As communications service providers (CSPs) transform their networks and operations, the demands on service assurance systems are changing. While the systems must be able to handle the same tasks as before, the deployment of 5G demands new capabilities to supercharge operators' ability to deliver new digital services in a wide variety of markets. Following are steps operators should take to transform service assurance:

Think cloud native

CSPs and their suppliers often have a hard time pinning down which new service models will be the big tickets to revenue in the 5G era. But if operators adopt cloud native systems, they don't have to guess. They can use agile operational infrastructure to quickly pivot whenever an opportunity arises.

Merge networks & IT

Service and network operations should be combined, and this merger should be reinforced in process design and internal roles within the company to get the most from the shift to cloud native systems and software-defined networking. This includes adopting DevOps practices, continuous integration and delivery, and microservice architectures to provide agility in both the business and network. The most progressive assurance systems embrace this approach.

Embrace automation

5G operations demand as close to full automation as possible. Interoperability and maximum data exposure are key to ensuring the end-to-end service management that will be needed for features like 5G network slicing. This means that assurance can no longer exist in isolation. Assurance systems should be able to acquire data of all types without manual intervention and interact seamlessly in workflows. This is important now, and it will be essential for assuring QoS in 5G networks.

Improve data quality

Evolving the connection between assurance and fulfillment is an opportunity to tackle a classic problem in telco operations data quality. Granular, live network data can be used to organically audit network inventory shortcomings within the closed loop concept.

Look for new suppliers

Most spending on service assurance over the last decade has been with a relatively small number of vendors. Large deals with incumbent suppliers mean that assurance is often part of a larger bundle. This is changing as vendors from other areas of IT are showing that their knowledge of cloud, VM infrastructure, workflow management, database management, and AI and machine learning are absolutely relevant to modern CSP operations.

Focus on standards

Digital operations are highly reliant on APIs in the network and OSS/BSS. CSPs rightly specify in requests for information and proposal that vendors should comply with industry standards including TM Forum's Open APIs. Standards are especially important in assuring services end to end across partners' boundaries. To learn more about TM Forum's Open APIs and the Open Digital Architecture, please contact George Glass.

> " Standards are especially important in assuring services end to end across partners' boundaries. "

Automating service assurance using industry standards

servicenow

How ServiceNow leverages TM Forum alarm management API to deliver proactive service experiences.

Rising expectations for proactive digital experiences

Digital experience expectations have drastically evolved over the past few years.

It's now standard practice for ecommerce companies to proactively notify customers if there are service issues with orders—such as shipping delays—and how the issues will be resolved. That same consumer-like service experiences are expected of communications service providers (CSPs), and they are under significant pressure to deliver or be pushed even further down the value chain.

Ideally, a CSP needs to proactively identify service issues before or when they happen by predicting certain patterns on the network and proactively finding a remediation path using automation or machine learning (ML) and artificial intelligence (AI). Keeping humans in the loop throughout the entire process is key; Care and network teams need to understand what's happening on the network in order to support resolution, and customers need proactive communication about the impact and resolution process. This type of proactive service experience helps CSPs make big strides towards improving net promoter scores (NPS) and customer satisfaction scores (CSAT).

So why hasn't the telecommunications industry been able to be proactive?

It's time to redefine service assurance

If you look under the hood in any network operations center (NOC), you will likely find an assortment of network management tools that have been installed for years, if not decades. Before next-gen services were born, these tools worked well for fault and performance management, as well as root cause analysis, within specific domains.

In today's competitive landscape—with new assets entering the mix and with increasingly complex networks—this approach no longer works for a myriad of reasons, but primarily because siloed legacy systems cannot deliver end-to-end visibility of all elements across the customer, employee, and partner ecosystem. With 5G and SDN starting to take center stage, there is a need for more modernized, unified approach to service assurance. One that delivers end-to-end visibility of the entire telecom ecosystem, including physical, logical, and virtual layers.

Yet CSPs still struggle to bring the old and new worlds of network resources together in order to deliver proactive experiences and automate service assurance.

Automating service assurance using industry standards

servicenow

Five reasons why proactive service experience is difficult to achieve

The ecosystem of a CSP is massive and will only continue to grow in complexity as networks evolve. ServiceNow has observed five key issues why CSPs struggle to deliver proactive experiences today.

1. **Inability to map resource to customer.** CSPs struggle to map what is happening on a network to the impacted customer because they do not have the customer or service context. As a result, the CSP cannot notify the affected customer(s).

2. **Heterogenous networks.** Multiple different heterogeneous networks are becoming more common. The complexity of these networks and topology makes the resource mapping even more challenging.

3. **Myriad of monitoring tools.** Heterogenous networks come with a set of different monitoring tools that exist in various network environments, making it difficult for CSPs to correlate and link events together.

4. **Lack of orchestration and workflow.** Different organizations and teams need to work seamlessly to resolve an incident. With so many different network monitoring tools, it becomes increasingly difficult to enable orchestration across all the different tools and different organizations to provide a seamless experience.

5. **Growing ecosystem will amplify complexity.** The shift to proactive service experience will get more amplified with the introduction of 5G and SDN, especially when it comes to network slicing. Identifying how service level agreements (SLAs) are impacted, who are the customers impacted, how to notify them, and how to remediate those services and impacted resources all pose significant challenges as networks evolve.

Four key elements to achieving automated service assurance

Network teams know all too well that when an event comes in, it causes a flurry of activity to happen across different tools and different domains. Network teams need the ability to provide cross-domain correlation, root cause analysis, and de-duplication to identify the root cause of the particular network event. They also need to determine dependency mapping of the network and proactively create an incident on the network, identifying which resource needs to be resolved.

In this scenario, achieving automated service assurance means CSPs need the ability to prioritize cases and rank remediation based on SLAs or operational level agreements (OLAs), which requires four key elements:

Automating service assurance using industry standards

servicenow

1. **Map the network.** A CSP likely have multiple heterogeneous network platforms, inventory and discovery systems that exist in their environment. ServiceNow serves as the connective tissue for mapping the entire network; the fundamental core for trying to do proactive notification and resolution paths.

2. **Monitor and detect.** Once the network is mapped, a CSP can now monitor and detect the issues happening and perform root case analysis for those issues.

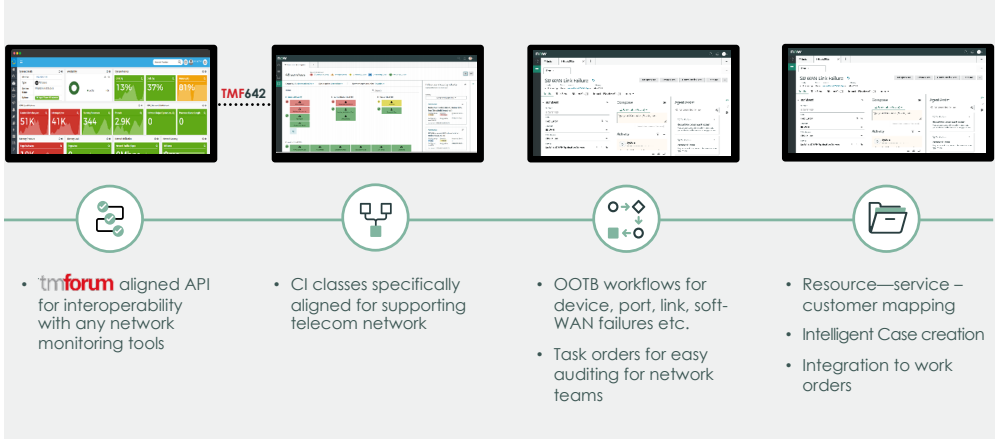
3. **Provide early warning.** The information is then taken and used to proactively notify both internal stakeholders and customers being impacted, creating a notification via an incident to ensure the appropriate remediation path.

4. **Drive resolution.** With early warnings provided, resolution can now be initiated. Resolutions should be recorded and should incorporate AI and ML algorithms running underneath the resolution process in order to learn from those resolution paths, especially if it's human-driven. Resolution can further be automated as confidence builds.

Using TM Forum Standards to enable proactive experiences

Achieving automated service assurance starts by standardizing network monitoring data, which is why TM Forum Open API 642 (TMF642 API) plays such a critical role. ServiceNow leverages TMF642 API for alarm management, which provides a seamless standards-based integration to any network monitoring platform in order to leverage data in a standardized fashion.

TMF642 alarm management for proactive experience



Automating service assurance using industry standards

servicenow

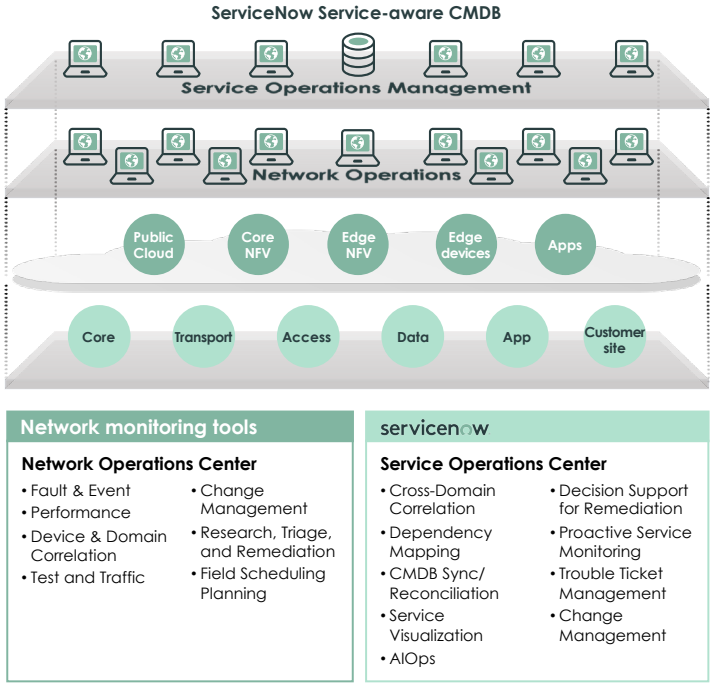
Automating service assurance with ServiceNow

With ServiceNow, CSPs can leverage and enhance existing network planning and inventory tools by consolidating all network data into the ServiceNow service-aware configuration management data base (CMDB).

Think of the ServiceNow CMDB as the service contextualization layer that brings together data from network planning, inventory and discovery tools; A relationship model that provides information such as resources used, services running on top of those resources, and the relationship between different network technologies and domains.

ServiceNow also functions in the Service Operations layer working and integrating with the various tools in the NOC. The business context and instrumentation across a variety of domain-specific network monitoring tools is the key domain where ServiceNow helps increase efficiency in operations for a CSP.

With a single-pane view, CSPs can now increase productivity while reducing mean time to repair (MTTR). Proactive notifications can now be delivered to the customer via the channel of their choice, improving QoS and reducing SLA and OLA breaches. Further, resolution can be automated using assurance workflows tied to field technicians for increased effectiveness and reduced fulfillment time.



ServiceNow serves as the service operations layer for orchestrating service assurance

> “Think of ServiceNow as the connective tissue that brings together data from the network and layers service context on top.”
>
> **Joe Torres, Sr. principal, telecom industry architect, ServiceNow**

Automating service assurance using industry standards

servicenow

The better way to automate service assurance in telecom

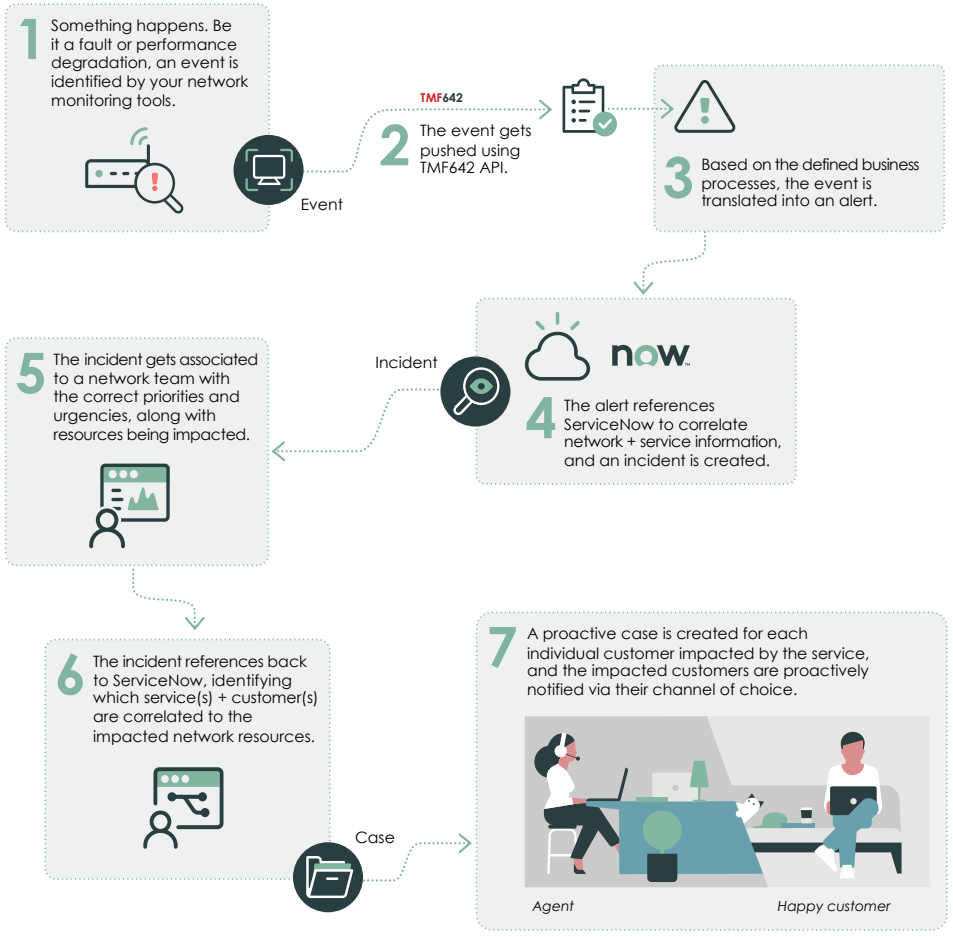
Designed using TMF642 API and ServiceNow's Telecommunications solution, now CSPs can achieve a more efficient process to automate service assurance.

Shifting the paradigm of service operations with ServiceNow

Reimagining service assurance requires CSPs to think out-of-the-box and take bold steps to invest in solutions that have customers, employees and partners in mind. There is also a significant need to pivot and change the way we think about service operations, from traditional resolution tasks to a paradigm that shifts into service operations.

This shift requires customer-to-service mapping, alignment to TM Forum standards, automated workflows all delivered on a single integrated cloud-native platform that breaks down silos and brings customer and network data together, finally.

At ServiceNow we believe that behind every great experience is a great workflow. As CSPs begin to reimagine the customer experience to one that



Service assurance workflow using ServiceNow and TMF642 API.

Automating service assurance using industry standards

proactively informs customers and resolves issues as they occur, it is critical to connect the customer and agents to operations and the network in a simple and streamlined way.

TM Forum's Open API standards ensures interoperability in the evolving digital ecosystem. As the industry continues to transform, these standards allow CSPs to evolve a component of their architecture without disrupting the entire ecosystem.

This paper is a summary of TM Forum Global Architecture Framework webinar: Sounding the Alarm for Proactive Services. **View the webinar on demand** here.

ServiceNow® enables CSPs to streamline and elevate telecom service and operations on one native cloud platform that connects the customer to the network. Give telecom employees the tools to do their best work, and customers the proactive, digital experiences they expect. **Learn more about ServiceNow Telecommunications solutions** here.

ServiceNow is a proud member of TM Forum

Award-winning 2020 catalyst project:
Outstanding Use of TM Forum Assets

Digital Transformation World 2020 executive roundtable:
Service transparency: The next radical change in customer experience

On-demand webinar
Sounding the alarm for proactive experiences: Using TMF642 with ServiceNow

White paper:
Automating service assurance using TM Forum standards

Inform blog:
Enabling the ecosystem: The new role of the vendor

TM Forum Open Digital Framework

A blueprint for intelligent operations fit for the 5G era

The TM Forum Open Digital Framework provides a migration path from legacy IT systems and processes to modular, cloud native software orchestrated using AI. The framework comprises tools, code, knowledge and standards (machine-readable assets, not just documents). It is delivering business value for TM Forum members today, accelerating concept-to-cash, eliminating IT and network costs, and enhancing digital customer experience. Developed by TM Forum members through our Collaboration Community and Catalyst proofs of concept and building on TM Forum's established standards, the Open Digital Framework is being used by leading service providers and software companies worldwide.

Core elements of the Open Digital Framework

The framework comprises TM Forum's Open Digital Architecture (ODA), together with tools, models and data that guide the transformation to ODA from legacy IT systems and operations.

Open Digital Architecture

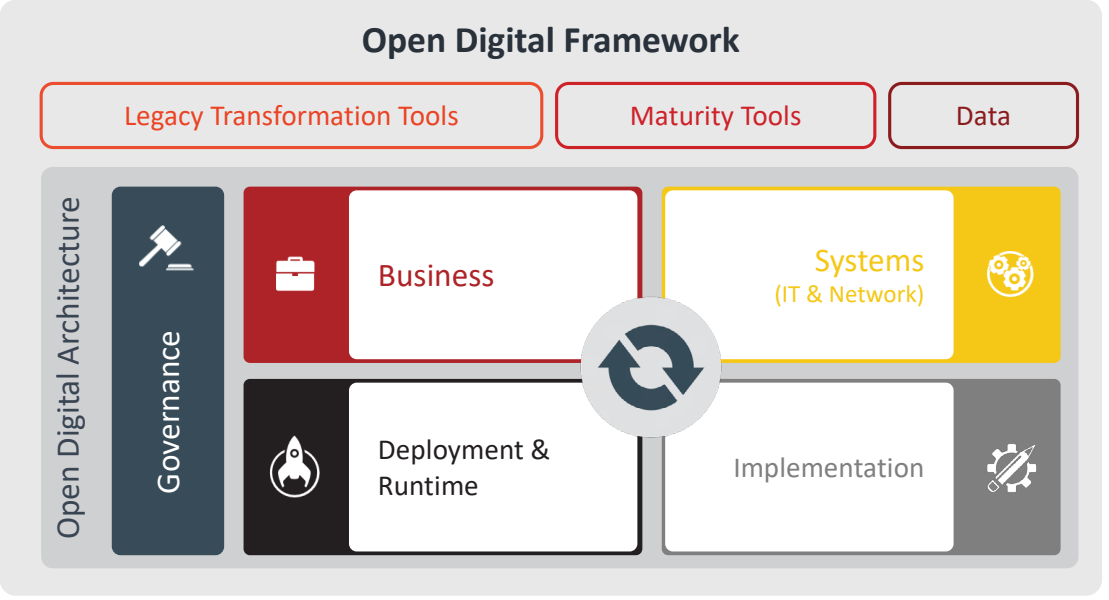
- Architecture framework, common language and design principles
- Open APIs exposing business services
- Standardized software components
- Reference implementation and test environment

Transformation tools

- Guides to navigate digital transformation
- Tools to support the migration from legacy architecture to ODA

Maturity tools & data

- Maturity models and readiness checks to baseline digital capabilities
- Data for benchmarking progress and training AI



Goals of the Open Digital Framework

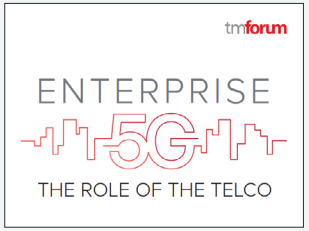
The Open Digital Framework aims to transform business agility (accelerating concept-to-cash from 18 months to 18 days), enable simpler IT solutions that are easier and cheaper to deploy, integrate and upgrade, and to establish a standardized software model and market which benefits all parties (service providers, vendors and systems integrators).

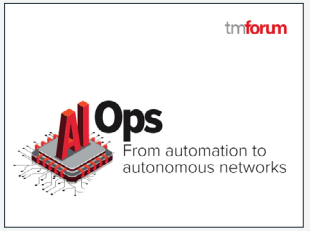
Learn more about collaboration

If you would like to learn more about the project or how to get involved in the TM Forum Collaboration Community, please contact George Glass.

TM Forum Research Reports


How to lead in the
OPEN API
ECONOMY

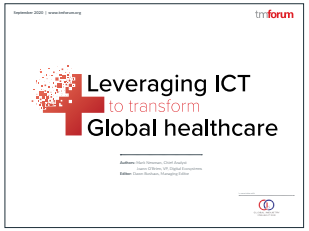

ENTERPRISE
5G
THE ROLE OF THE TELCO


AI Ops
From automation to
autonomous networks


HOW TO BUILD
AND OPERATE
AT THE
EDGE
A TM Forum
benchmark report


OPEN SOURCE
ACCELERATES BEYOND EXPERIMENTATION


DIGITAL
MATURITY
Are we on
the right path?


Leveraging ICT
to transform
Global healthcare


INTELLIGENT
AUTOMATION
IN THE TELCO
CONTACT CENTER


Data orchestration
The key to becoming a data-native organization


INSPIRING INNOVATIVE TEAMS
THROUGH DIVERSITY & INCLUSION


Rakuten Mobile
NO ORDINARY TELCO

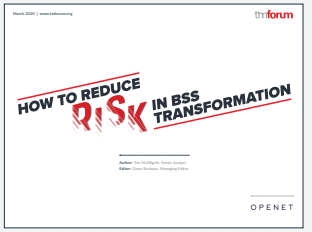

Attaining agility
and beating disruptors
at their own game


MONETIZING 5G
SLICING
Turning a game-changing concept
into an operational reality

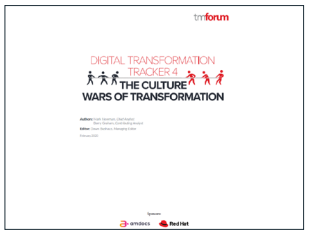

CLOUDNATIVE
OSS BSS


FRAUD
IN THE DIGITAL
EXPERIENCE ERA


Network automation
USING MACHINE LEARNING AND AI


HOW TO REDUCE
RISK
IN BSS
TRANSFORMATION


FUTURE
Customer Experience:
FROM DIGITAL TO OMNICHANNEL

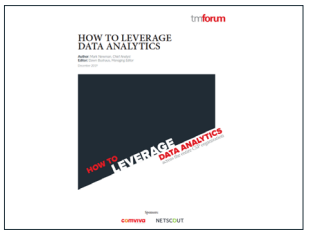

DIGITAL TRANSFORMATION
TRACKER 4
THE CULTURE
WARS OF TRANSFORMATION


FULL STACK
TRANSFORMATIONS:
Do they work and is there an alternative?


FUTURE BSS


PRACTICAL
STEPS
TOWARDS AN
AGILE
DIGITAL
CULTURE


CSPs
An essential
but not singular
solution for
PUBLIC
CLOUD:


HOW TO LEVERAGE
DATA ANALYTICS

Meet the Research & Media team

Report Author:
Dean Ramsay
Contributing Analyst

Chief Analyst:
Mark Newman
mnewman@tmforum.org

Editor, Digital Content:
Arti Mehta
amehta@tmforum.or

Commercial Manager, Research & Media:
Tim Edwards
tedwards@tmforum.org

Digital Marketing Manager:
Anna Kurmanbaeva
akurmanbaeva@tmforum.org

Report Editor:
Dawn Bushaus
Managing Editor
dbushaus@tmforum.org

Senior Analyst:
Tim McElligott
tmcelligott@tmforum.org

Customer Success & Operations Manager:
Ali Groves
agroves@tmforum.org

Global Account Director:
Carine Vandevelde
cvandevelde@tmforum.org

To learn more about TM Forum's Open APIs and the
Open Digital Architecture, please contact **George Glass.**