tmforum knowledge

service assurance

steps out of the shadows

Author: Annie Turner
Editor: Dawn Bushaus, Managing Editor
ISBN: 978-1-955998-05-5

Sponsored by: bmc

contents

setting the scene

Service assurance isn't very visible in telecoms, but its importance is growing quickly. Today it is hidden and mostly reactive, using a combination of fault and event management plus trouble ticketing. It typically involves a high degree of manual copying and pasting across multiple data sources along with "swivel-chair" management to identify what's broken, determine how much it matters and to whom, and figure out how to fix it.

In line with the fundamental changes happening in network technologies and topologies which are rewriting operations, service assurance is undergoing dramatic evolution. It will move from an almost separate discipline to being front and central in supporting operations, especially network automation.

Service assurance will always retain an element of reaction because there will always be unexpected events, but in the future there will be far greater emphasis on being proactive. Communications service providers (CSPs) must aim to prevent issues impacting customers whose expectations are high and loyalty low. Operators cannot differentiate themselves on cost alone – that's a no-win race to the bottom – so they must deliver what they promise. Service assurance plays a fundamental role in this.

CSPs are re-evaluating their operational and business support systems (OSS/BSS), as they aspire to zero-touch or lights-out network operation centers and network automation, although there is little consensus about how to approach automation.

Some things are clear, though: First, service assurance must become cloud native, that is, run on microservices in a containerized environment. Second, Open APIs (such those co-created within TM Forum's collaboration program) are the only pragmatic way to integrate modular, cloud-native, open digital platforms which can be orchestrated using AI, as outlined in the Forum's Open Digital Architecture.

Operators cannot differentiate themselves on cost alone – that's a no-win race to the bottom – so they must deliver what they promise. Service assurance plays a fundamental role in this.

moving to cloud-native solutions

The legacy, silo-based approach to service assurance is already a hindrance and will become unsustainable as CSPs move to:

- Greater levels of containerization and virtualization in the network and IT
- Multi-cloud and hybrid-cloud infrastructures for their own operations and to serve customers
- More working within ecosystems to offer or deliver products and services
- Accessing, assimilating, analyzing and acting on the rising tide of data generated by software-based infrastructure
- Needing ever-higher levels of automation to empower customers through self-care and self-service, particularly as network slicing becomes commercialized over the next three to five years
- Ever-higher levels of automation to support new services including those needing lower latency and at the edge, as well as to reduce the cost of operations while raising customer satisfaction.

As Matthew Halligan, CTO, Optiva, notes, cloud native solutions “are all about low code, no code, no footprint and really a developer-centric model.”

This e-book looks at how service assurance is evolving and can play a significant role in enabling CSPs to achieve their automation goals now and as their networks and operations undergo profound change.

CHAPTER 1

service assurance today: eliminate repetitive tasks & introduce devops

Not long ago, the quality and size of a network operations center (NOC) was measured by number of screens – the most impressive looked like the bridge of Star Trek's Starship Enterprise. Now many CSPs are looking to cut OpEx by 10%-15% in the next 18 months, but their ambitions extend far beyond cost reduction: They want greater flexibility and agility in all operational areas, and in particular to closely align technical data with that from customer-facing systems to improve customer experience.

When the network was a separate physical entity with its own hardware, terminology and technology, it made sense to have different processes and approaches. As many network functions increasingly run on commodity IT infrastructure such as containers using technologies long established in software, it makes sense to use similar, proven methodologies and processes.

The highly skilled, well-paid operatives in telco NOCs increasingly will need DevOps skills, and they should learn how to automate the network because they are best placed to do so. They have unsurpassed knowledge of the problems – and the right remediation steps.

Newer approaches to service assurance can help eliminate repetitive, mundane tasks that consume so much of the operations teams' resources. Seeing people demonstrate good DevOps practices helps other employees learn quickly: It is how to build a culture of excellence.

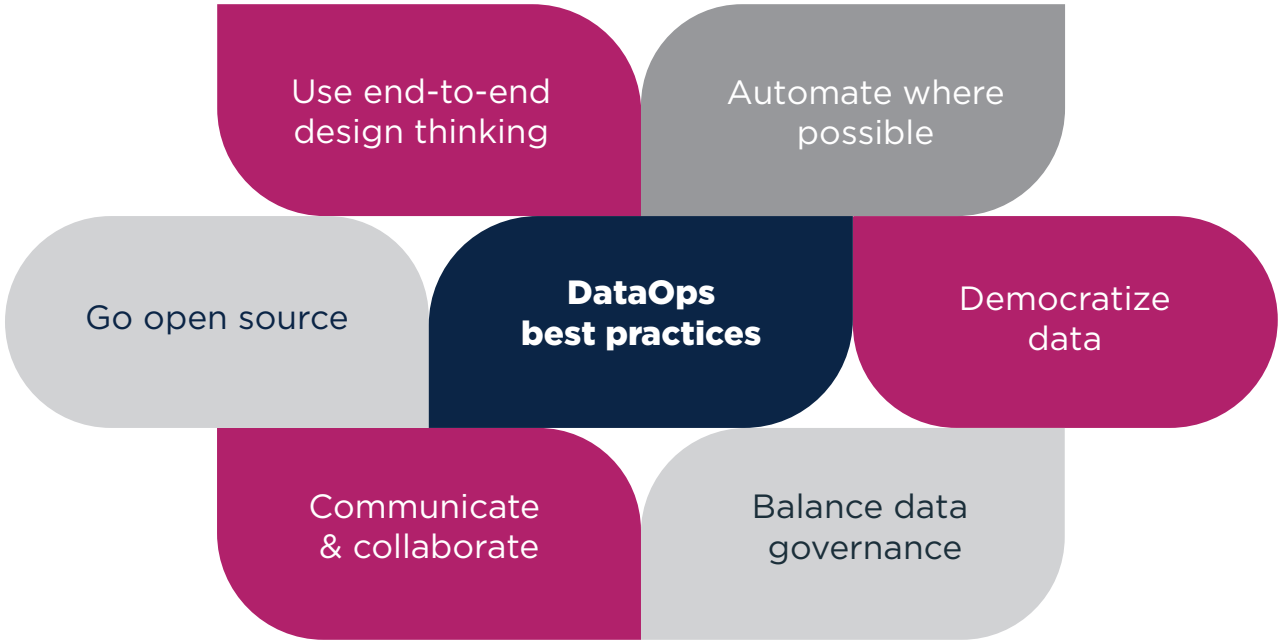
Newer approaches to service assurance can help eliminate repetitive, mundane tasks that consume so much of the operations teams' resources. Seeing people demonstrate good DevOps practices helps other employees learn quickly: It is how to build a culture of excellence.

the trouble with data

The siloed nature of data along with multiple incompatible types of data, remain the single greatest obstacle to network automation.

The siloed nature of data along with multiple incompatible types of data, remain the single greatest obstacle to network automation. Now new network technologies and computing paradigms are driving a sharp increase in the amount and complexity of data that CSPs' service assurance systems must process. In the short term, CSPs should look to improve the quality and accessibility of data by applying DevOps principles to the data pipeline – DataOps.

CSPs have no shortage of data, but it might take six weeks for an ops team to build the initial integration for new data sources. People must be able to access, process, manipulate and act on data as the need arises, so far shorter, faster and more frequent data cycles are needed through DevOps practices like continuous integration and delivery (CI/CD) pipelines. DataOps principles will not solve all the issues with data overnight, but they will make a big difference in some areas quite quickly and can help with assembling the skills and building blocks that are needed.



Another very useful DevOps approach is swarming. In NOCs, intractable, multi-layered trouble tickets often ping-pong between support teams, although such issues often impact customer experience. Swarming brings together people with diverse expertise to work on a specific problem. It can happen routinely, periodically or dynamically as needed. In any case, it has proven to be a pragmatic way of breaking down silos in IT, and as pandemic lockdowns have proven, working in teams remotely is a viable, highly productive option.

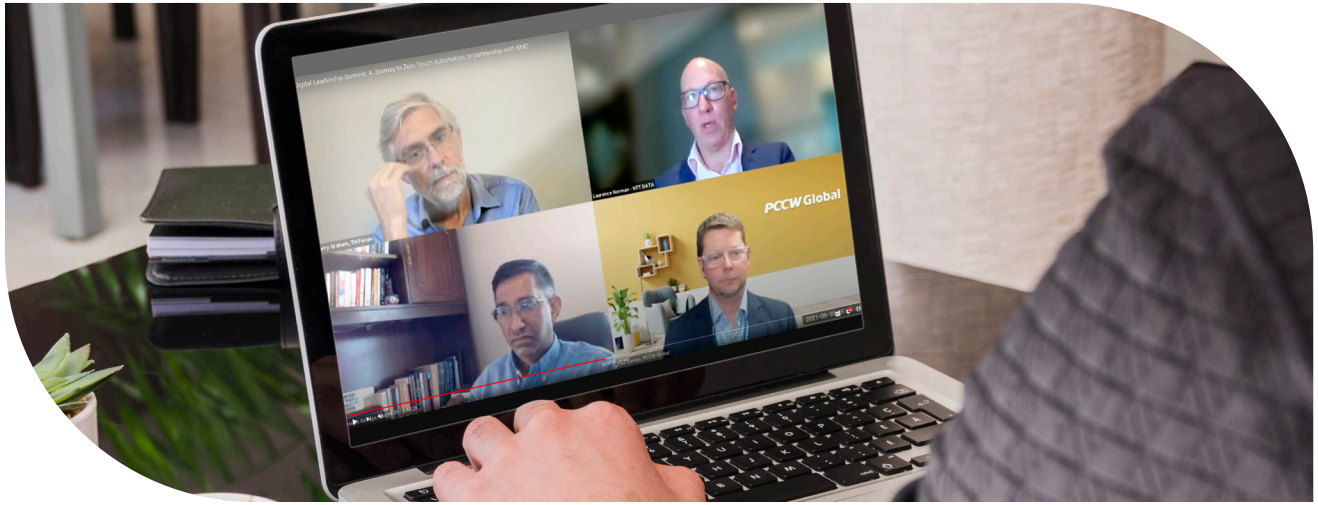
AI in the offing

AI is a key tool in many aspects of digital transformation, including automation, but it needs to be approached thoughtfully and with safeguards from the start. CSPs are in the early days of leveraging AI in operations (AIOps), but if AI is empowered to make decisions, the systems generating it must be accountable to the people who consume the decisions. Algorithms generators need to be able to show which decision was taken, and how the decision was arrived at and implemented.

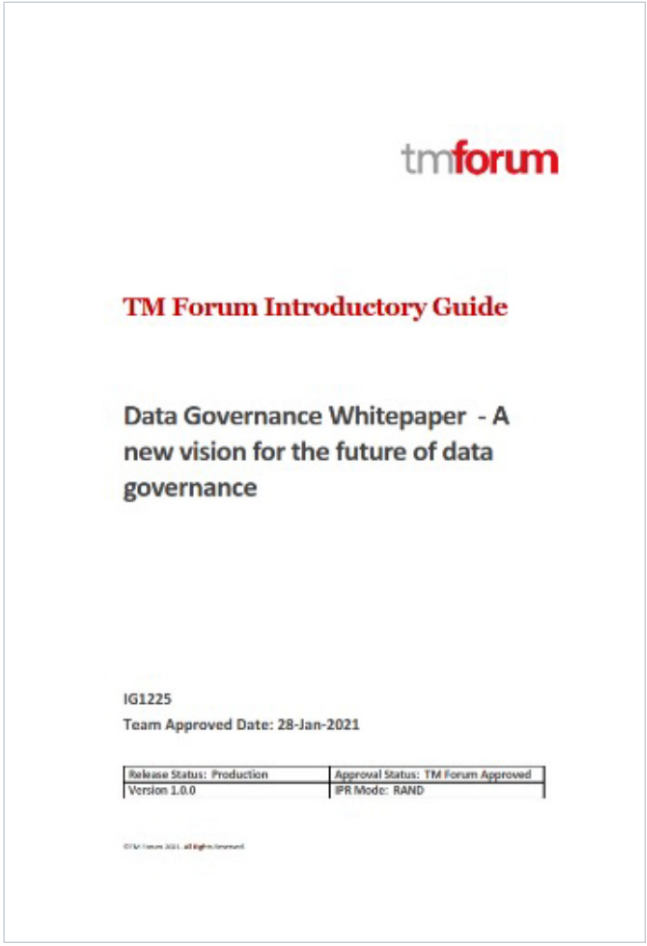
Actions resulting from AI must be traceable, because if AI triggers unexpected consequences operational teams need to "unpick" the reactions triggered by the decision and fix the faulty thinking behind it. Put another way, service assurance needs to oversee the change management of AI itself. We'll explore service assurance's role in change management more in the next section.

The principles of transparency and traceability, backed up by governance, need to be baked into AIOps from the start. There are tools to help, such as the white paper published by TM Forum in 2021, A new vision for the future of data governance.

Digital Leadership Summit:
A Journey to Zero Touch Automation with PCCW and BMC



AI is a key tool in many aspects of digital transformation, including automation, but it needs to be approached thoughtfully and with safeguards from the start.


tmforum

TM Forum Introductory Guide

Data Governance Whitepaper - A new vision for the future of data governance

IG1225

Team Approved Date: 28-Jan-2021

Release Status: Production	Approval Status: TM Forum Approved
Version 1.0.0	IPR Mode: RAND

on the edge

Multi-access edge computing (MEC) is expected to begin mainstream commercial deployment beginning next year, but the time to prepare is now because considerable progress is needed in service assurance to meet this timeline. Today service assurance is about sharing the network; tomorrow it will include customers' workloads running on top of a MEC client, and the MEC could be purchased from a hyperscale cloud provider.

This blurs the line of responsibility. Application workloads are latency dependent and very closely tied to the network, but they're not delivered by the network. Rather the workload is processed by an application sitting on a cloud appliance at the network's edge.

CSPs must answer many questions about MEC: How will they manage customers' expectations when the customers are oblivious of the underlying infrastructure and only care about their application's performance? Who is accountable for what, where? How is stuff fixed quickly – preferably automatically – when so many elements are involved?

The problems become more complicated when latency-specific workloads are accessed by users on the move: If a user is on a fast train from City A to City B while streaming a virtual reality (VR) application, how does the edge move too? Are they to be handed off to different edge sites every time they are handed off to the next cell site?

Again, while there are many unknowns about MEC, one absolute certainty is that a customer's satisfaction level will be extremely low for a VR product that performs poorly when they are on the move.

In the next chapter we'll look at the near future of service assurance.

While there are many unknowns about MEC, one absolute certainty is that a customer's satisfaction level will be extremely low for a VR product that performs poorly when they are on the move.

CHAPTER 2

service assurance tomorrow: increasing intelligence & prediction

During the next 18 to 30 months service assurance will begin to pivot away from tactical remediation to supporting strategic automation as the network becomes increasingly autonomous. This will be achieved through semi or fully automated remediation of issues, which requires adaptive remediations and self-learning. In parallel, service assurance will start to be more about supporting and enabling change – and building a governance layer around that.

Currently, remediation behavior in service assurance is rigid, using an "I see this, I do that" approach. In the mid-term it needs to be: "I saw this; I did that; was it fixed?" If the answer is 'yes', then the system learns. If 'no', then more learning happens. The next time the service assurance system sees a similar event, it can more intelligently predict the success of the prompted action.

Increasingly service assurance can push intelligence to NOC staff and recommend a course of action, or it can take action through closed loop automation. As AI systems learn, and confidence in closed loop networking grows, they will proliferate. This self-learning and adaptive behavior will evolve through a constant, reiterative cycle which in many cases shouldn't need human intervention.

As AI systems learn, and confidence in closed loop networking grows, they will proliferate. This self-learning and adaptive behavior will evolve through a constant, reiterative cycle which in many cases shouldn't need human intervention.

getting schooled by IT

When humans do need to be involved, DevOps and its rapid, iterative development cycles are the order of the day because just as service assurance systems must change, so must the processes that maintain and govern them – and this needs to happen in sync.

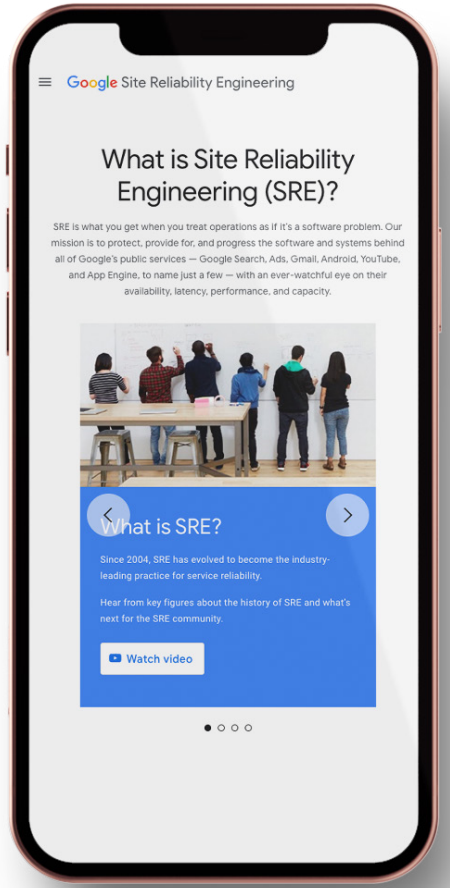
During this phase, forward-thinking CSPs could adopt concepts like site reliability engineering (SRE): Google and other hyperscalers already use this set of principles and practices which applies aspects of software engineering to infrastructure and operations issues.

Another big lesson from IT is that the most successful automation processes are developed and run close to where they are needed. Asking a central automation team to build and test them doesn't work. There is a lot of evidence from DevOps communities showing that teams don't need to run restrictive, complex change processes to implement more successful changes.

Some leaders within CSP organizations are ready and willing to embrace automation and the necessary DevOps practices. Others think it will turn into Skynet, the evil AI system in the Terminator movies. This is where strict governance comes in. Rules that everyone understands are essential, and they must be enforced to build consistency and confidence within operations and business teams.

This is about striking a balance between increasing the speed and agility of the network through DevOps and maintaining the right levels of control. This will lead to a multi-speed model where in some layers of the network, local operations teams have a great deal of freedom. Other areas will be much more tightly controlled because they are critical infrastructure.

Learn about the history of SRE



what's the intent?

Many of today's service assurance tasks that happen in the operations layer will be done tomorrow in the network, depending on the level of maturity of the infrastructure. In the network, service assurance increasingly will be driven by policy or intent, creating a service assurance layer that focuses much more on:

- Processes or functions that teams have tried and failed to automate through some kind of remediation
- Aspects that so far have proved too complex to automate
- Minimizing areas that inevitably require some degree of physical intervention such as truck-rolls.

Progress in this mid-phase needs to have an eye on how to achieve zero-touch operations as the end-game, building on the work undertaken in the short term around data and DevOps to reduce the number of trouble tickets and the number of people required to deal with them. As service assurance evolves, it will provide more context around the failure to help decision-making, such as a view of network topologies and interdependencies, which legacy systems lack.

Understanding the context of different lines of business and domains allows more informed decision-making. The idea is to avoid a 20-minute triage to establish what the failure means, to whom, who needs to know about it and what action they should take.

The ongoing aim of service assurance is to automate everything that can be automated, if not today, then tomorrow. In the next chapter we'll look at the long-term vision for service assurance.

Understanding the context of different lines of business and domains allows more informed decision-making. The idea is to avoid a 20-minute triage to establish what the failure means, to whom, who needs to know about it and what action they should take.

CHAPTER 3

service assurance in 5 years: automation (nearly) all the way

Up to five years out is a long time in telecoms, but by then most of the service assurance layer will be automated. The parts that are not will involve bots pushing information to network operations staff instead of them looking for it. The information sent to operations staff will be highly time sensitive and dependent on context. It will be presented on a single screen via one user interface instead of staff being obligated to scan a wall of screens. CSPs will still run NOCs, but the centers will be much smaller, focusing on issues that for now, at least, can't be fixed automatically.

Traditional event management will diminish, becoming much more focused on IT rather than the network. Service assurance will also move away from fault management, to being proactive and avoiding things breaking in the first place in the shape of predictive maintenance.

Fault management will not disappear but largely will be carried out in the network. There has been much progress within Open Network Automation Platform (ONAP) which develops best practices for orchestration, management and automation of network and edge computing services for network operators, cloud providers and enterprises. ONAP's capabilities mean that CSPs will be able to understand the network and its orchestration layer, plus performance behavior to work out the impact of problems – and how to remedy them – automatically.

blurring boundaries

If containerization and cloud-based services deliver what they promise, the separation between network and IT will all but disappear. A containerized network function in many ways is no different from a containerized IT application. Both will need to be managed in a similar way as they will be running on similar infrastructure with similar management functions.

So, while the CSP will need to understand the network's performance – and information from telemetry on the network, which is slightly different – there will be a greater overlap in terms of capabilities. In this scenario, the service assurance layer will shrink a little, but if the network is much more intelligent, the service assurance layer will adapt to drive closed-loop automation more effectively.

Put another way, assuming the network evolves as expected, service assurance will become a key component of a closed loop service operations model, bringing service fulfillment and orchestration together. This is essential for service operations and monetizing new service models at scale, leveraging 5G having escaped from silos and monolithic architectures.

All of which means change management itself will have to change, and this is an obvious place to deploy AI. People will still be needed, but machines should perform complex assessments – for example, the likely impact of a change on a customer's service level agreement or another service metric. Then, in most cases, machines should carry out the change.

Approvals of changes should be far more intelligent and automated, based on understanding the type of change, the context that the change is being executed against and, critically, executing it. In other words, service assurance steps up to manage complex risks more efficiently and effectively.

Assuming the network evolves as expected, service assurance will become a key component of a closed loop service operations model, bringing service fulfillment and orchestration together. This is essential for service operations and monetizing new service models at scale, leveraging 5G having escaped from silos and monolithic architectures.

Helping CSPs implement autonomous networks & AIOps

TM Forum's Open Digital Framework, which members are developing through collaborative efforts such as the Open Digital Architecture (ODA), Open API and Autonomous Networks Project, can help CSPs create an evolutionary path toward cloud-native, software-defined, autonomous networks and operations. By taking it step by step, operators and their suppliers can realize a return on investment in legacy systems, while at the same time benefitting from new technology.

The ODA is fundamentally designed as a component-based architecture, with the business services of a component exposed as a set of Open APIs. The APIs can be, and typically are, further decomposed into a set of services and microservices. The advantage of using microservices is that they can be managed on scalable infrastructure using Agile DevOps practices.

The Autonomous Networks Project has grown out of the work on the ODA. This team is collaborating with the European Telecommunications Standards Institute (ETSI), the GSMA and ONAP to test many of the concepts through TM Forum's Catalyst Program. The riddle everyone wants to solve is how self-healing and self-optimization will happen in networks. The idea is to look for patterns so that network operators don't have to solve the problem for every specific case. This requires describing the patterns in terms of business outcome, or the customer's intent.

TM Forum members are also leading an initiative to create an industry-agreed AIOps Service Management Framework, which aims to re-engineer the processes in the software lifecycle and service operations management to govern AI software at scale. This will enable operations teams, process owners and business users to exploit AI safely and properly maximize its benefits. The idea is to mitigate risks and ensure the appropriate level of network and service quality.

The AIOps Service Management Framework is part of the Open Digital Framework and is applicable to any type of architecture due to its agnostic design. It can operate as an independent process framework to help CSPs manage the deployment of AI into their current and target architectures. To learn more about TM Forum's collaboration projects focusing on autonomous networks and AIOps, please contact Aaron Boasman-Patel.

Meet the Research & Media team

Author:
Mark Newman
Chief Analyst
mnewman@tmforum.org

Principal Analyst:
Dean Ramsay
dramsay@tmforum.org

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

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

Editor:
Dawn Bushaus
Managing Editor
dbushaus@tmforum.org

Editor in Chief, Inform:
Joanne Taaffe
jtaaffe@tmfourm.org

Digital Marketing Manager:
Anna Kurmanbaeva
akurmanbaeva@tmforum.org

Global Account Director:
Carine Vandevelde
cvandevelde@tmforum.org

Published by:

TM Forum
4 Century Drive,
Parsippany,
NJ 07054
USA

www.tmforum.org

Phone: +1 973-944-5100
Fax: +1 973-944-5110

ISBN: 978-1-955998-05-5

About BMC

From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise. For more information, visit www.bmc.com/csp