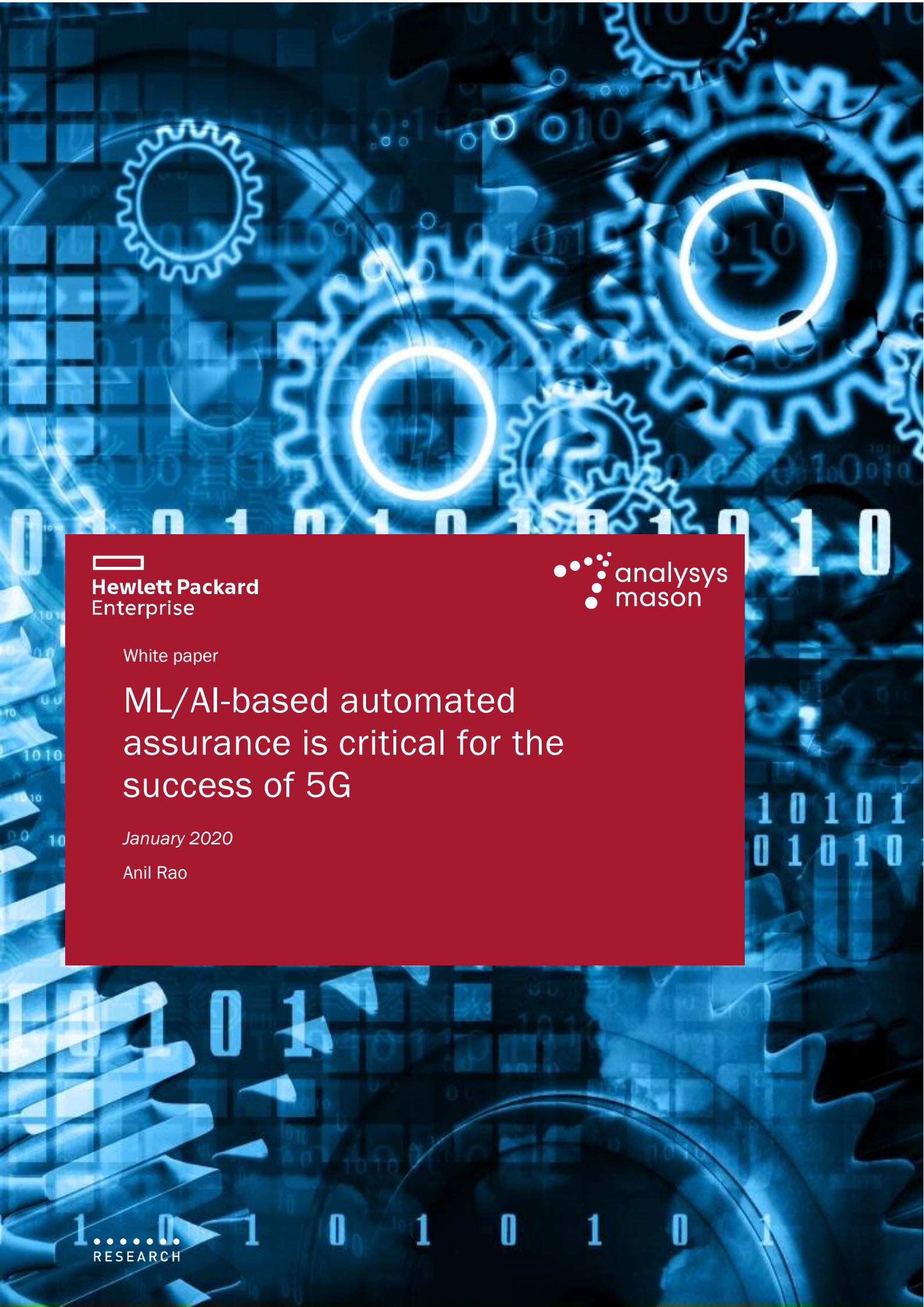


Hewlett Packard Enterprise

analysys mason

White paper

ML/AI-based automated assurance is critical for the success of 5G

January 2020

Anil Rao

RESEARCH

Contents

List of figures

© Analysys Mason Limited 2020

1. Executive summary

5G promises to deliver enhanced mobile broadband services, ultra-low latency and massive IoT communications services for both consumers and enterprises across many vertical industries. Players in the telecoms industry have coalesced around a set of key network design principles that include concepts such as network function virtualisation (NFV), software-defined networking (SDN), cloud-native computing, multi-access edge computing (MEC) and network slicing in order to enable the performance, latency and quality of service that is expected from 5G networks. These capabilities will make networks significantly more flexible and agile, and will enable service providers to rapidly launch new services, reduce capex through infrastructure standardisation and optimisation and deliver superior customer experiences. However, the dynamic nature of cloud-based infrastructure and network functions will introduce unprecedented levels of network and service complexities, and will therefore lead to an increased level of operational complexity and potentially, a dramatic rise in opex.

Analysys Mason's research shows that communications service providers' (CSPs') network opex has been increasing since 2012. Opex as a percentage of revenue grew from 11% in 2012 to 15% in 2017, but revenue declined by 13% during the same period. This is an unsustainable trend that will be exacerbated with the launch of 5G if CSPs stick with their current operational approaches. By using siloed IT and operations tools, network operations departments are forced to rely on manual processes that increase the risk of errors and misconfigurations, lead to longer issue resolution times and subsequently, increase troubleshooting costs.

The emergence of advanced service assurance that uses big data and analytics technologies has alleviated these issues to some extent. Processing massive amounts of network data and applying analytics to post-processed data enables the generation of insights in a matter of seconds or minutes, thereby allowing operations departments to discover and proactively address issues before service impact and customer complaints. Even more-advanced features such as automatic pattern and anomaly detection are emerging, but these require the competence of domain experts and data scientists. CSPs would need to significantly increase the size of their specialist workforces in order to tackle the complexity of 5G networks and the expected increase in the number of potential failure scenarios, which would make the operational economics completely unsustainable. CSPs must reimagine their operations in the 5G era and embrace automated assurance to control opex.

Machine learning (ML) and artificial intelligence (AI) technologies empower assurance and enable CSPs to make the next leap towards autonomous operations. ML/AI technologies are key to achieving predictive operations, which will be critical for managing complexity in the 5G era and controlling opex. By applying ML/AI to assurance, CSPs will be able to perform a plethora of automations, including automated issue identification and root-cause analysis, automated anomaly detection and prediction, automated pattern discovery and automated creation of rules and policies. The auto-generated actionable next steps can be combined with NFV orchestration and SDN control systems to perform open- and closed-loop automation, thereby further reducing the operational costs. This new operations approach will reduce the reliance on manual operations and data scientists, and will allow CSPs to manage complexity in 5G, control opex and make the 5G business case feasible.

© Analysys Mason Limited 2020

2. Virtualised and cloud-native 5G networks will significantly increase service and operations complexity

2.1 The scope of 5G is much broader than that of consumer voice and data services

Previous generations of mobile networks (2G, 3G and 4G) were built for consumer voice and data services, but 5G networks are being built to support a plethora of use cases that in turn support the digital transformation of entire vertical industries. Figure 1 illustrates some of the key differences between the existing 2G/3G/4G networks and the emerging 5G networks.

Figure 1: Differences between 2G/3G/4G networks and 5G networks

2G/3G/4G	5G
Support consumer-focused services.	Support both consumer and business applications.
Networks designed for voice and data use cases.	Networks designed for a very broad array of use cases, ranging from non-critical to highly critical industrial applications.
Used for applications that are not latency-sensitive.	Used for applications with a range of latency sensitivity (for example, 2ms for autonomous driving).
Networks predominantly built for humans.	5G standalone networks built predominantly for machines.
Limited expectations for new revenue.	B2B and B2B2X revenue models.

Source: Analysys Mason, 2020

The variety of use cases that 5G networks are expected to support is quite wide-ranging, but most can be broadly categorised as B2C or B2B/B2B2X services. The B2C category includes high-bandwidth enhanced mobile broadband (eMBB) and fixed-wireless services that are expected to primarily support use cases such as cloud gaming and AR/VR applications. B2B/B2B2X services are used in a wide spectrum of vertical industries to support ultra-reliable low latency (uRLLC) and massive machine-to-machine communications (mMTC) use cases. Examples include smart transportation, critical services and emergency response, sensor networks for smart agriculture and smart cities, AR/VR applications for better human–machine interactions and Industry 4.0 initiatives such as smart wireless factories.

The diverse nature of the 5G use cases and their wide-ranging demands on network performance and network and service dynamicity and latency, as well as the need to support new business models has forced the industry to consider new architectural approaches for 5G.

2.2 5G will lead to a plethora of new network and infrastructure innovations that will increase complexity

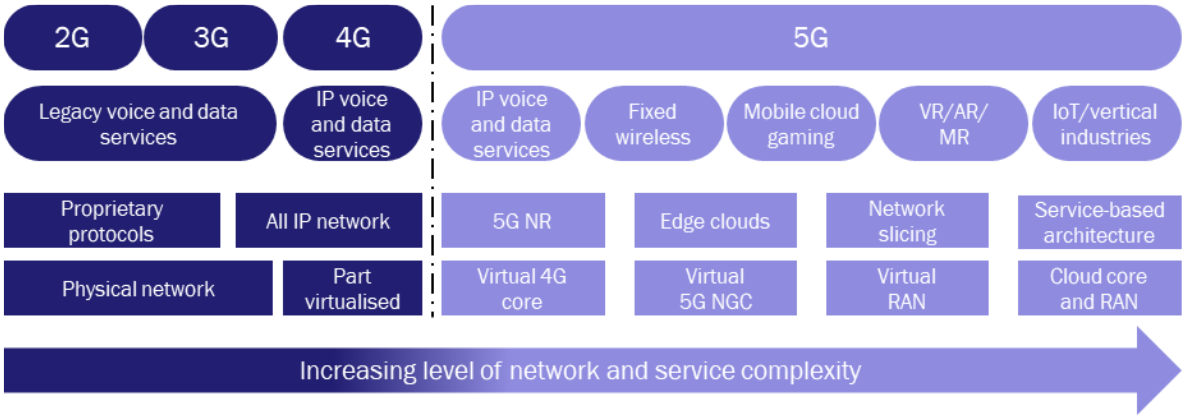
The 5G core network is being built using container technology and a service-based architecture to enable CSPs to deploy and operate the networks in cloud environments, and to support just-in-time scalability, software reusability and extreme network automation. The 5G networks will be further boosted by edge computing, which brings compute power closer to the edge for localised processing and application hosting in order to reduce network congestion and service latency. Additionally, network slicing enables the creation of end-to-end cross-domain virtual logical network slices, and each slice delivers differentiated QoS and SLAs to match service-specific KPIs such as network capacity, latency and reliability.

© Analysys Mason Limited 2020

The RAN has been one of the last frontiers in the virtualisation roadmap due to the complexities involved. In a future scenario where RANs are dominated by a multi-vendor ecosystem, the RAN elements (that is the antenna, the radio and the baseband) will have open and standard interfaces, such that components from different suppliers can inter-operate with each other. To this end, various industry initiatives are in place (such as Open RAN (ORAN) Alliance, C-RAN Alliance and the xRAN Forum) to centralise and virtualise the RAN in order to rapidly respond to changing traffic demands.

Together, these wide-ranging technology enablers (such as NFV, SDN, cloud-native computing, network slicing and edge computing) will provide the basis for new 5G-based digital services (Figure 2), but at the same time, they will increase the complexity of the networks and services to unprecedented levels. This will also significantly increase the operational complexity, rendering the traditional methods of operations obsolete.

Figure 2: The evolution to 5G and the enabling technologies



Source: Analysys Mason, 2020

In the 5G era, CSPs must address new operations challenges including, but not limited to, the following.

- How should dynamic resources and services be monitored in virtual and cloud networks?
- How can unexpected and unknown network/service issues be identified?
- How can CSPs boost the customer experience and service quality for complex services?
- How can CSPs take advantage of the massive amount of data generated in virtual and 5G networks?
- How should operations be prepared in order to rapidly onboard and support future B2B and B2B2X services?
- How can opex be contained while supporting new networks and services?

CSPs cannot apply the old methods of operating 2G/3G/4G networks that were designed for static physical networks supporting basic voice and data services to 5G networks. CSPs must instead embrace a new operations approach that is designed for the telco cloud and is delivered at a fraction of a cost of traditional operations, but that also supports new digital services that have yet to be conceived. Maintaining the status quo is not an option.

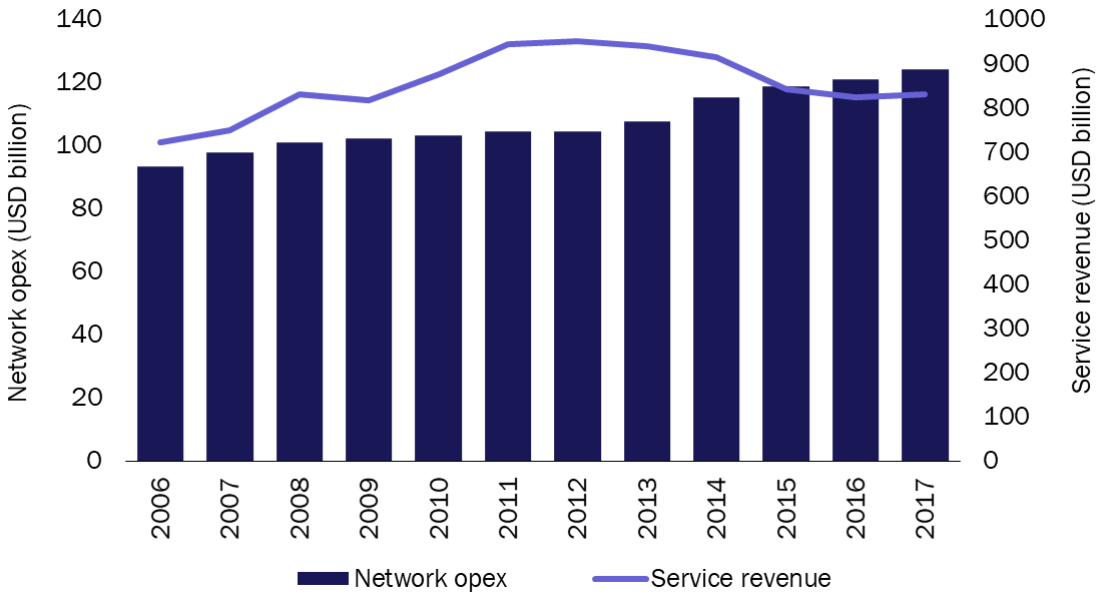
© Analysys Mason Limited 2020

3. Rising opex will make the 5G business case unsustainable

3.1 Network opex as a percentage of revenue is increasing

Network opex accounts for about 22% of the total CSP opex, and has been rising quickly during the past 5–7 years. Network as a percentage of revenue grew from 11% in 2012 to 15% in 2017, but revenue declined by 13% during the same period. (Figure 3). The industry now faces a situation where there is a widening gap between revenue and opex. 5G digital services are expected to deliver new revenue for CSPs, but they will take at least 3–7 years to make a material business impact.

Figure 3: Network opex and service revenue, 2006–2017



Source: Analysys Mason, 2020

Many CSPs recognise that the upward opex trend cannot continue. To contain and reduce opex, even while supporting the new services and operational complexities of 5G, CSPs must make a significant leap in operations efficiency.

3.2 Issue identification and analysis accounts for about 70% of operational time and cost

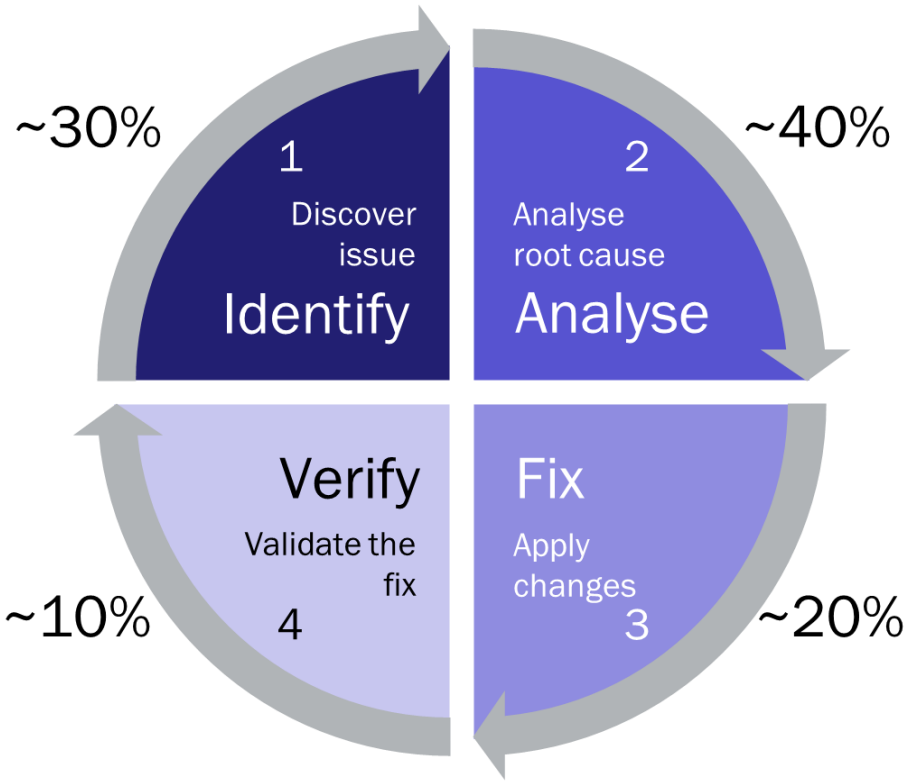
Most large CSPs have hundreds of operations support systems (OSS) for monitoring and assurance in order to identify and report on network faults and performance issues. These monitoring systems have been obtained from a combination of equipment vendors and independent software suppliers, as well as through internal ad-hoc development to support functions that are not supported by commercial software products.

© Analysys Mason Limited 2020

The siloed and fractured tool estate results in swivel-chair operations and manual and error-prone processes that are monotonous and demotivating for operations engineers. Such solutions often lead to reactive operations with extended issue identification and analysis times, and high troubleshooting costs. The NOC front office uses multiple screens to perform the initial diagnosis and often escalates issues to the more-expensive level 2 and level 3 support engineers.

Analysis shows that operational activities can be split into four stages (Figure 4). A total of about 70% of CSPs' time and money is spent on issue discovery and root-cause analysis; these tend to be reactive processes that are triggered when a customer reports a service issue, or the NOC notices a KPI breach. In a worst-case scenario, a network and/or service outage could trigger the process. The other two stages (applying changes and verification) account for the remaining 30% of time and cost, and are usually performed as part of change management and governance processes.

Figure 4: Anatomy of network operations



Source: Analysys Mason, 2020

3.3 Big data analytics enables partial assurance automation, but is insufficient to operationalise 5G at scale

Over the years, assurance and monitoring systems have evolved (Figure 5) from siloed tool farms to unified assurance systems that offer advanced alarm and fault suppression, filtering and de-duplication to significantly reduce the number of incidents and tickets that are handled by operations teams. Assurance systems have further evolved to deliver value beyond network monitoring thanks to the maturity and availability of high-performance big data analytics technologies. By using a combination of diverse network data sources (such as passive wire

© Analysys Mason Limited 2020

data, active test data, streaming telemetry, SNMP, flow data, customer behaviour and application usage data, billing and CRM data and device data), CSPs can now gain a multi-dimensional view of a customer's quality of experience.

Figure 5: The evolution of service assurance to date

Source: Analysys Mason, 2020

The evolution to big-data-based assurance systems has also enabled CSPs to become more proactive in their operations, because big data analytics programmes can process significantly higher volumes of data than their predecessors and can generate insights in a matter of seconds or minutes. Network performance issues or faults that may eventually affect the service can be discovered and pre-empted before the customer complains. Some advanced software also supports the automatic detection of failure patterns for future anomaly detection, but the rules must be created manually at present, which requires the competence of domain experts and data scientists.

The expected increase in the volume and velocity of network data in virtual 5G networks, and the increased number of potential failure scenarios mean that CSPs would need to add an army of specialist engineers and data scientists to operate and support complex 5G services. This would make the operational economics unsustainable and the 5G business case infeasible.

3.4 Rapidly maturing ML/AI technologies can now be used for telecoms operations

ML and AI technologies are fast maturing thanks to their foundation in established big data technologies, and are being applied to a plethora of use cases across industries. Cutting-edge R&D, increased investments in the ML/AI technology ecosystem, leading research by technology companies such as Google and Microsoft and broader open-source initiatives have resulted in fast-paced innovation and increased confidence in ML/AI technology. The availability of large training data sets and low-cost compute and storage has further fuelled the adoption of such technology across companies.

Supervised ML algorithms use reams of historical operations data to learn to spot patterns (such as degrading network performance) and trigger remediation routines (for example, supplementing network capacity). The continuous calibration of algorithms can increase the accuracy of pattern matching and decisioning to a point where there is enough confidence to establish predictive operations. Indeed, models can predict network or service issues hours, days or even weeks in advance, thereby giving enough time to take remedial action.

© Analysys Mason Limited 2020

Reinforced learning is when the machine-learning algorithm makes a single action, receives a notification on how good the decision was and calibrates its next move based on the feedback. Unsupervised learning algorithms do not have prior training on how to classify or label patterns, but employ grouping or clustering to organise data in order to understand potential structures and patterns before predicting outcomes.

Many CSPs are working towards incorporating ML/AI in their operations; this is emphasised in the following statement by a global Tier 1 group CSP based in Europe.

> "Operational automation is important for us as the company has a global transformation program called Zero Touch. Through Zero Touch, we are going to apply different AI techniques in order to solve problems in current 4G and FTTH networks and in future 5G networks (we are currently working on several use cases)."
>
> - Global Tier 1 group CSP

3.5 ML/AI-based automated assurance is necessary to contain opex and operationalise 5G at scale

ML/AI technologies have already been applied to various telecoms use cases such as customer care (virtual assistants), sentiment analysis, customer experience analysis and customer churn prediction. CSPs must now expand the use of ML/AI into operations in order to achieve the level of automation required to tackle the complexities of 5G and operationalise virtual/cloud-native 5G networks at scale (Figure 6).

Figure 6: The evolution of ML/AI-based automated assurance

Source: Analysys Mason, 2020

ML/AI technology will significantly enhance CSPs' existing automated assurance capabilities and will reduce costs by automating issue identification and root-cause analysis processes and enabling CSPs to take a giant leap towards autonomous operations. The key capabilities include automated anomaly detection and prediction, automated pattern discovery, automated creation of rules and policies and automated generation of actionable next steps.

Using the insights generated from ML/AI based assurance platforms, CSPs can implement predictive operations and empower operations departments to perform open- and closed-loop automation. This will also reduce the reliance on manual operations and data scientists, while creating a strong foundation for zero-touch autonomous operations. From a 5G perspective, this approach allows CSPs to operate NFV and cloud-native networks at

© Analysys Mason Limited 2020

scale with confidence, and to launch and onboard new services with marginal incremental operational costs over existing operations.

3.6 ML/AI-based automated assurance with MANO systems enables guided and closed-loop automation, thereby further reducing opex

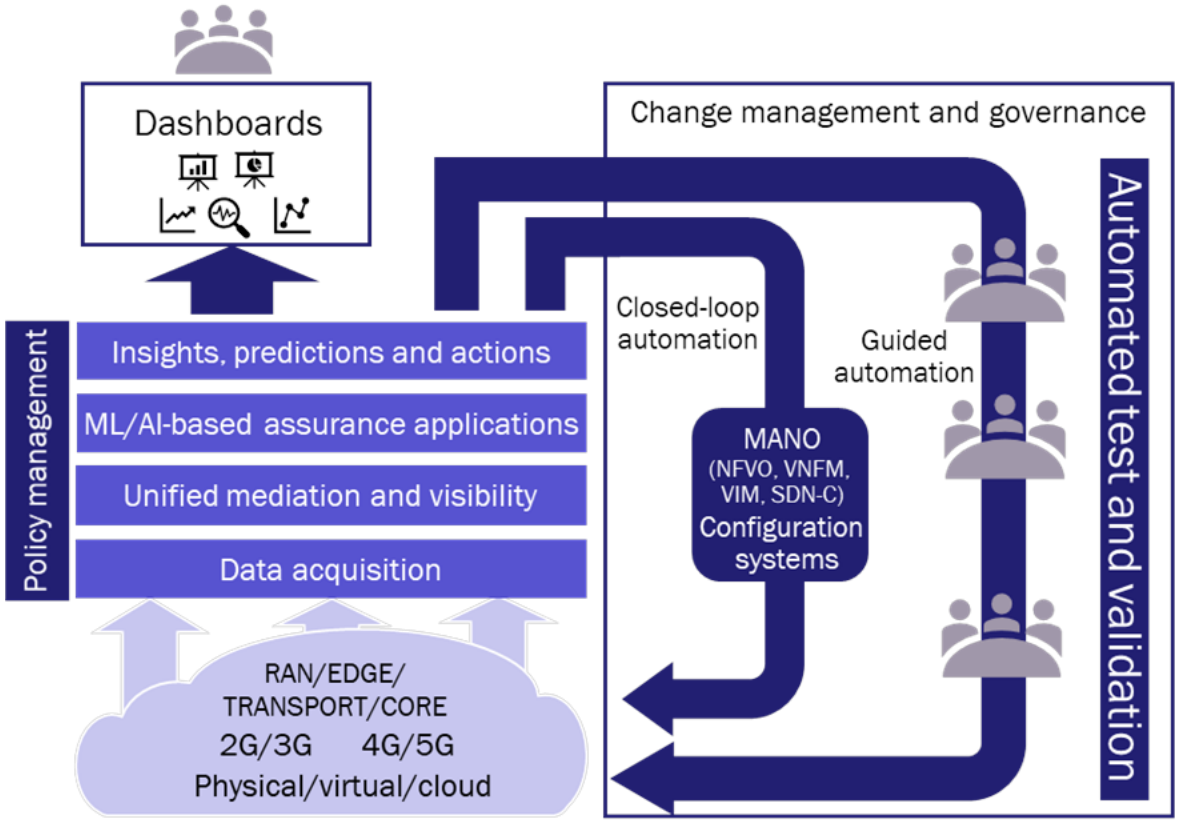
CSPs can gain further benefits from extreme assurance automation by reducing the opex associated with the last two stages of operations (Figure 4): applying network configuration changes and verifying the changes. This can be achieved in the following ways (Figure 7).

- **Guided automation.** This involves automating the network configuration actions via an open-loop automation process that requires human intervention at key decision points. This puts the operations engineers in control of the automation, lets them decide the best course of action and consequently, helps to increase their trust in automations. As more network change processes are codified into automation programmes and applied via guided automations, the expectation is that operations teams' trust will reach a point where they can completely relinquish control and let the programmes drive the changes autonomously. However, this will be a gradual process, and not all automations will be executed in fully autonomous mode from day one.

- **Closed-loop automation.** ML/AI will play an important role in transitioning the operations from guided automations to fully closed-loop automations. By using supervised and reinforced machine learning approaches, operations engineers can constantly tune the models as they make decisions during the execution of the guided automations. This allows for an accurate recording of the decisions and the associated environmental context in which the decisions were made. The models can then replay the decisions when the same environmental contexts manifest again.

© Analysys Mason Limited 2020

Figure 7: Guided and closed-loop automation



Source: Analysys Mason, 2020

CSPs will need a further three key enablers in addition to an ML/AI-based automated assurance platform to successfully implement a closed-loop automation solution.

- **Policy engines at different levels.** The assurance platform itself will require a policy engine to record the trigger rules and the associated actions for issue discovery and root-cause analysis. Another policy engine will be required to enable the rules to trigger automated configuration actions based on the insights and recommended actions from the assurance platform as well as the service and business intent defined in the service models. It is likely that there will be more such engines at various levels, but ML/AI capabilities will play a key role in automatically creating and updating the policy rules.

- **Automated test and validation.** Making automated testing and validation an integral part of change management processes can alleviate some of the risks associated with manual testing. Failure to accurately test and validate changes before switching on services can cause outages, resulting in significant monetary loss and brand value erosion. This will be even more critical in cloud-native 5G networks where changes can occur on short notice.

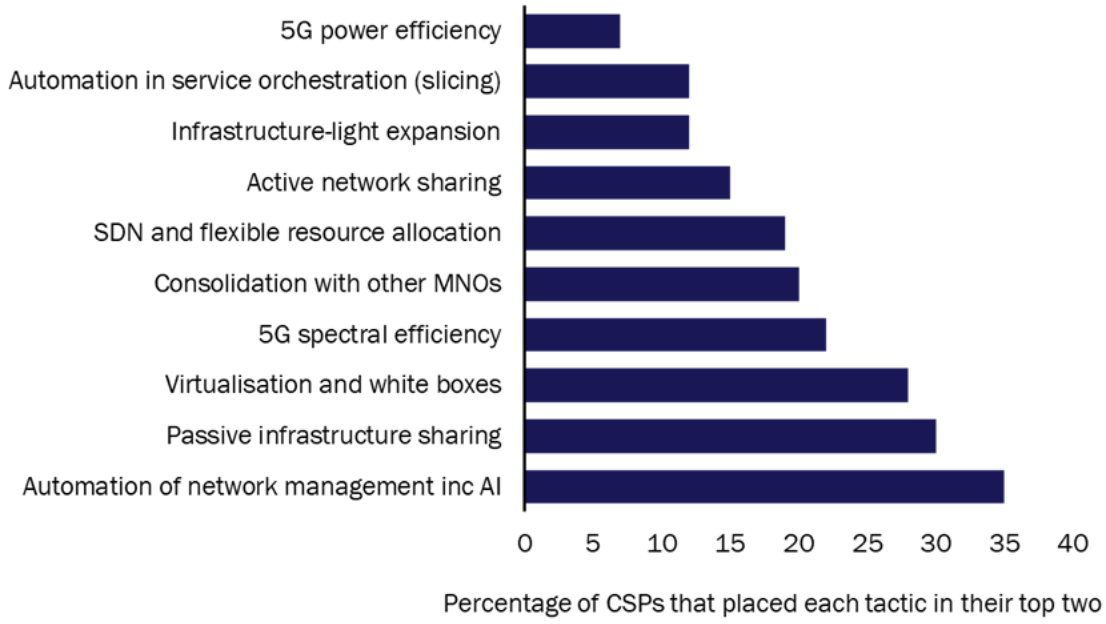
- **Open APIs for easy integration.** Open APIs, preferably standards-compliant APIs, will allow the assurance platform to expose platform capabilities to external applications such as policy engines, test and validation systems and orchestration systems in order to accelerate the level of automation. The APIs also allow open innovation both by the CSP departments and external specialists. Additionally, the platform must use standardised APIs in order to interface with adjunct systems (especially the orchestration and configuration management systems) and drive full automation.

© Analysys Mason Limited 2020

3.7 CSPs have concrete plans to implement ML/AI in operations

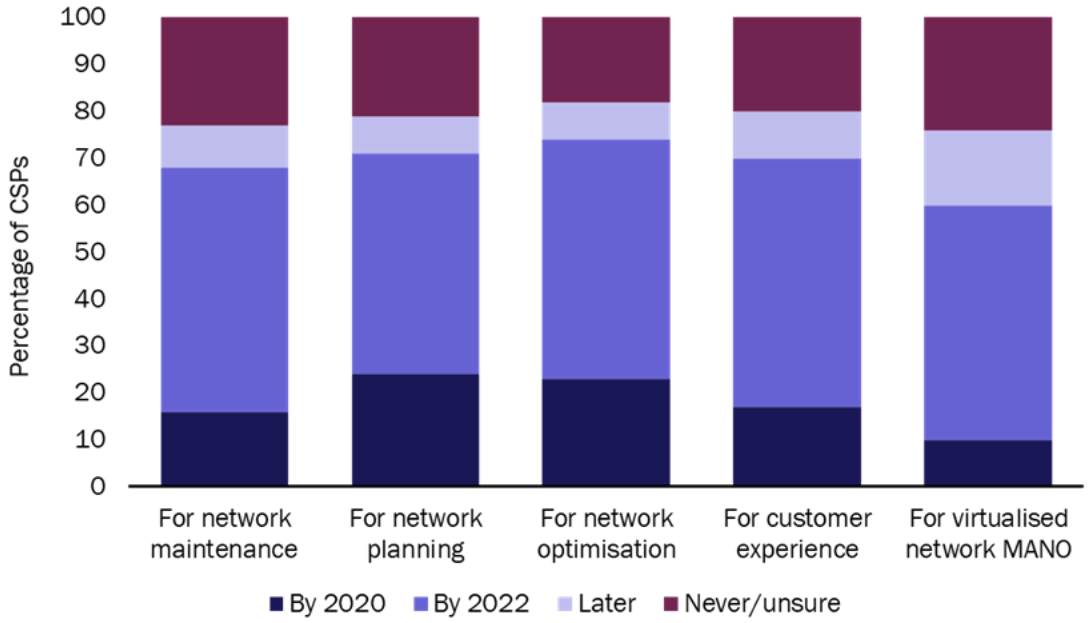
Respondents of Analysys Mason's survey of 55 Tier 1 and 2 mobile CSPs said that they are targeting reductions in absolute network opex of between 13% and 40% by 2025. Figure 8 shows the ten tactics that were most-commonly placed in CSPs' top two priorities for opex reduction. Automation of network planning, management and optimisation (increasingly aided by AI) was placed in the top two by 35% of CSPs. About two thirds of respondents said that they expect to have deployed some elements of AI to enhance planning and optimisation, improve efficiencies in network operations and maintenance, improve overall customer experience and make MANO more intelligent to support virtualised networks by 2022 (Figure 9).

Figure 8: CSPs' key tactics for reducing network opex by 2025



Source: Analysys Mason, 2020

Figure 9: Functions for which CSPs expect to deploy AI/ML in the network



Source: Analysys Mason, 2020

A study by TMForum[1] estimated that CSPs could use AI to reduce the number of network operations personnel by about 30% over 5 years. The study cites World Economic Forum figures and claims that AI-supported network automation could increase the mobile industry's operating profit by USD9 billion because of reduced outages, and could deliver USD27 billion in total cost savings by 2025.

4. Conclusions and recommendations

Many CSPs face rapidly declining revenue and mounting opex. 5G presents great hope and promises new revenue opportunities from enterprises across many vertical industries. However, 5G also introduces significant network, service and operational complexities that cannot be managed using traditional operational approaches. CSPs need a reimagined approach to operations based on the principles of automation. Automated assurance based on ML/AI technologies provides CSPs with the foundational capabilities to reduce their reliance on manual operations and data scientists, to manage operational complexity and to control opex in 5G networks.

CSPs that are preparing to operationalise 5G at scale must make the following considerations when choosing an assurance solution.

- Choose an assurance solution that utilises ML/AI techniques for automated creation of policy rules, automated issue detection and root-cause analysis.

1 TMForum (2017), *AI: The Time is Now*. Available at: http://inform-digital.tmforum.org/tar-ai-report-publication#!/what-is-ai-and-why-is-it-crucial-for-the-telecom-industry

© Analysys Mason Limited 2020

- Demand solutions that maximise current investments for existing operations while providing a clear roadmap for the evolution to fully automated assurance and zero-touch operations for 5G.

- Insist on a platform-based solution that supports open APIs to encourage open innovation and to easily integrate with adjunct systems such as NFV orchestration software in order to develop open- and closed-loop automations.

© Analysys Mason Limited 2020

5. About the author

Anil Rao (Principal Analyst) is the lead analyst for the Automated Assurance and Service Design and Orchestration research programmes, covering a broad range of topics on the existing and new-age operational systems that will power operators' digital transformations. His main areas of focus include service creation, provisioning and service operations in NFV/SDN-based networks, 5G, IoT and edge clouds; the use of analytics, ML and AI to increase operations efficiency and agility; and the broader imperatives around operations automation and zero touch networks. In addition to producing both quantitative and qualitative research for both programmes, Anil also works with clients on a range of consulting engagements such as strategy assessment and advisory, market sizing, competitive analysis and market positioning, and marketing support through thought leadership collateral. Anil is also a frequent speaker and chair at industry events, and holds a BEng in Computer Science from the University of Mysore and an MBA from Lancaster University Management School, UK.

This whitepaper was commissioned by Hewlett Packard Enterprise. Analysys Mason does not endorse any of the vendor's products or services.

Published by Analysys Mason Limited • Bush House • North West Wing • Aldwych • London • WC2B 4PJ • UK
Tel: +44 (0)20 7395 9000 • Email: research@analysysmason.com • www.analysysmason.com/research

Registered in England and Wales No. 5177472

© Analysys Mason Limited 2020

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, mechanical, photocopying, recording or otherwise – without the prior written permission of the publisher.

Figures and projections contained in this report are based on publicly available information only and are produced by the Research Division of Analysys Mason Limited independently of any client-specific work within Analysys Mason Limited. The opinions expressed are those of the stated authors only.

Analysys Mason Limited recognises that many terms appearing in this report are proprietary; all such trademarks are acknowledged and every effort has been made to indicate them by the normal UK publishing practice of capitalisation. However, the presence of a term, in whatever form, does not affect its legal status as a trademark.

Analysys Mason Limited maintains that all reasonable care and skill have been used in the compilation of this publication. However, Analysys Mason Limited shall not be under any liability for loss or damage (including consequential loss) whatsoever or howsoever arising as a result of the use of this publication by the customer, his servants, agents or any third party.