

RESEARCH FORECAST REPORT

SERVICE ASSURANCE SYSTEMS: **WORLDWIDE FORECAST** 2017-2021

Anil Rao

analysysmason.com



About this report

This report provides forecasts for communications service provider (CSP) spending on telecoms-specific service assurance (SA) software systems. It provides details of how spending will vary by delivery type, service type and region across different sub-segments. The report also provides recommendations for how vendors and CSPs can approach the changing demands of telecoms service assurance software.

It is based on several sources, including:

- Analysys Mason's strategy reports and other analysis developed during the past year
- interviews with CSPs and vendors worldwide.

KEY QUESTIONS ANSWERED IN THIS REPORT

- What is the overall size of the telecoms service assurance software market and what will be the key drivers of growth in the next 5 years?
- How will spending vary across different sub-segments of the service assurance market?
- How will spending vary across different regions and service type?
- What are the major drivers and inhibitors that will affect growth rates of CSP spending on service assurance systems?

GEOGRAPHICAL COVERAGE

- Worldwide
- Central and Eastern Europe
- Developed Asia-Pacific
- Emerging Asia-Pacific
- Latin America
- Middle East and North Africa
- North America
- Sub-Saharan Africa
- Western Europe

SUB-SEGMENT COVERAGE

- Probe systems (PS)
- Service management (SM)
- Fault and event management (FM)
- Performance monitoring (PM)
- Workforce automation (WA)

WHO NEEDS TO READ THIS REPORT

- Vendor strategy teams that need to understand where growth is slowing and where it is increasing – according to different sub-segment categories.
- Product management teams responsible for feature functionality and geographical focus, and product marketing teams responsible for growth.
- Professional services vendors that want to understand the growth opportunities for the next 5 years.
- CSPs that are planning digital transformation journeys and want to understand key areas that they should focus on.

Three key trends expected during 2017–2021

1

CSPs will deploy next-generation SA solutions for NFV/SDN and hybrid network environments.

Early use cases, such as active testing using virtual test agents and embedded assurance in MANO to enable localised closed automation, will be implemented by most CSPs. CSPs will also deploy open-source assurance components in OpenStack as part of infrastructure management. More broadly, assurance will become an integral component in the new operational framework for delivering traditional communication services and new digital services.

2

Increasing cost pressure and confidence in cloud-based delivery will encourage CSPs to adopt the SaaS model for service assurance.

In SA, CSPs are most likely to use SaaS deployments for WA software. The IT nature of WA systems makes it highly conducive to SaaS. PS, PM, FM and SM will lag behind WA in terms of SaaS deployment, but will probably accelerate when large dominant vendors start to bring SaaS-based solutions to the market.

3

Demand for NOC consolidation, SOC implementation, and new integration requirements for NFV will drive growth in professional services.

NOC consolidation and managed services will continue to be in demand for traditional networks and services as CSPs attempt to control costs. Implementation of SOC and related process automation will require consulting, custom development and business process reengineering services. Early assurance deployments for NFV require significant systems integration work.

Recommendations for CSPs

1

CSPs should consider virtual service assurance for the operation of physical networks even as they prepare to implement NFV/SDN based virtual networks.

The telecoms industry has arrived at a 'cloud tipping point'. The strong intent shown by CSPs to deploy cloud-based NFV/SDN, combined with an increasing confidence in cloud architecture for telecoms software applications and support systems, is accelerating the innovation towards virtual service assurance. CSPs must exploit the opportunities and business benefits offered by deploying cloud-based virtual SA solutions.

2

CSPs should demand assurance solutions that are designed based on cloud, analytics and automation principles to address the emerging requirements of assurance for NFV/SDN-based virtual networks.

Classic assurance solutions were not designed to exploit the inherent capabilities of NFV infrastructure such as scalability, self healing and flexibility. New SA solutions should employ a plethora of design principles to make it fit for purpose. The new service assurance systems must be designed keeping in mind the new demands of NFV/SDN networks such as platform openness, cloud and analytics to enable high levels of automation.

3

CSPs should make service assurance an integral part of NFV business processes right from the start.

In the new operational approach for NFV/SDN, CSPs should envision the new service assurance as a seamless process across the NFV service lifecycle – test/validation of NFV (NFVI, VIM and VNFs), service testing and operational assurance. As CSPs make the evolution towards a cloud-native era, they should demand assurance solutions that are designed based on the microservices architecture, that will form the basis for the move towards a DevOps model.

Recommendations for vendors

1

Vendors should incorporate advanced analytics technologies to help CSPs reduce the operational costs and allow CSPs to differentiate based on superior service quality.

Assurance solutions have started to integrate network analytics to reduce the time to action for issue resolution. As new analytics technologies based on machine learning and artificial intelligence mature, vendors should integrate them into their solutions to further reduce the cost of operations. Geolocation-based analytics can further bolster the operations use cases in addition to supporting service quality and monetisation use cases.

2

Vendors should embed real-time topology and network discovery into their solutions to assure dynamic NFV/SDN networks.

Traditional performance monitoring and fault management systems have embedded topology discovery modules to perform critical functions, such as root cause analysis. However, the introduction of NFV/SDN requires a redesign of legacy topology discovery technology to make it fit for purpose for the dynamic nature of the virtual networks and service chains.

3

New vendors should focus on specialist areas of assurance and develop strategic partnerships with large prime systems integrators.

To foster innovation and encourage competition, CSPs are trying new vendor solutions in NFV/SDN networks. It is likely that large prime systems integrators with NFV ecosystems and open-source initiatives (such as ONAP, OSM and OPNFV) will drive NFV implementations so new vendors should pre-integrate their solutions into such ecosystems to help CSPs reduce the time to deployment.

CONTENTS

EXECUTIVE SUMMARY

RECOMMENDATIONS

FORECAST

MARKET DRIVERS AND INHIBITORS

BUSINESS ENVIRONMENT

MARKET DEFINITION

ABOUT THE AUTHOR AND ANALYSYS MASON

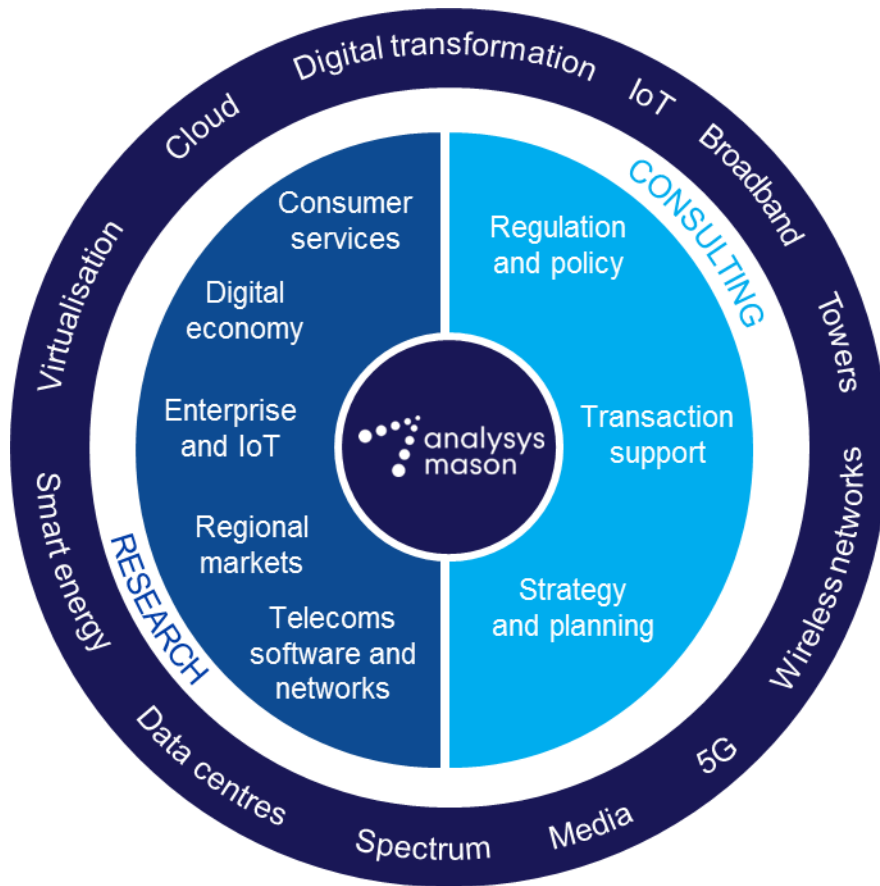
About the author



Anil Rao (Senior Analyst) is a member of Analysys Mason's Telecoms Software and Networks research team and is the lead analyst for the *Service Assurance* programme, focusing on producing market share, forecast and research collateral for the programme. He has published research on IP probes, real-time network analytics and the importance of service assurance in reducing churn and improving customer experience. He holds a BEng in Computer Science from the University of Mysore and an MBA from Lancaster University Management School, UK.

Analysys Mason's consulting and research are uniquely positioned

Analysys Mason's consulting services and research portfolio



CONSULTING

- We deliver tangible benefits to clients across the telecoms industry:
 - communications and digital service providers, vendors, financial and strategic investors, private equity and infrastructure funds, governments, regulators, broadcasters, and service and content providers
- Our sector specialists understand the distinct local challenges facing clients, in addition to the wider effects of global forces.
- We are future-focused and help clients understand the challenges and opportunities that new technology brings.

RESEARCH

- Our dedicated team of analysts track and forecast the different services accessed by consumers and enterprises.
- We offer detailed insight into the software, infrastructure and technology delivering those services.
- Clients benefit from regular and timely intelligence, and direct access to analysts.

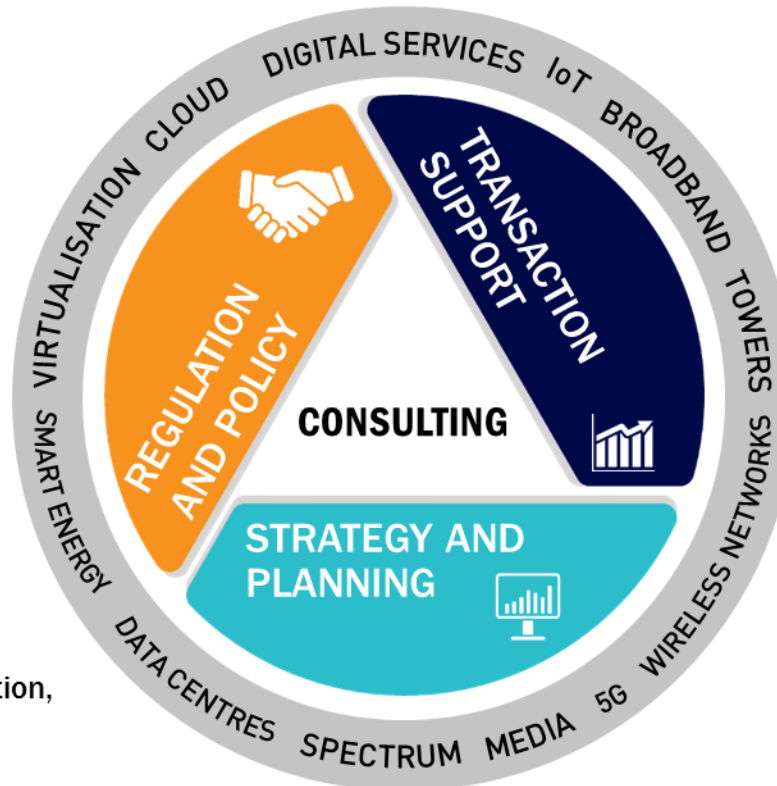
Research from Analysys Mason



Consulting from Analysys Mason

REGULATION AND POLICY

- Quality of service
- Market review
- Margin squeeze tests
- Analysing regulatory accounts
- Regulatory economic costing
- Policy development and response
- Media regulation
- Expert legal support
- Radio spectrum management
- Net cost of universal service
- Radio spectrum auction support
- Postal sector policy: USO, liberalisation, costing, pricing and regulation



analysysmason.com/consulting

TRANSACTION SUPPORT

- Commercial due diligence
- Technical due diligence
- Digital services
- Mid-market finance sponsors
- Data centres

STRATEGY AND PLANNING

- Commercial expertise
- Technology optimisation
- New digital frontiers

PUBLISHED BY ANALYSYS MASON LIMITED IN AUGUST 2017

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 No. 5177472

© Analysys Mason Limited 2017. 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.