



www.pipelinepub.com

Volume 21, Issue 8

The Role of Assurance and AI in Building Level 4 Autonomous Networks

By: [Sandeep Raina](#)

As Communications Service Providers (CSPs) roll out their latest 5G and Fiber Broadband services, the need for automating operations and reducing costs has become a necessity. The complexity of such disaggregated networks introduces errors, only worsened by manual operations. With operational automation based on Assurance and AI insights, not only can high amounts of data be processed efficiently, but operational errors can be significantly reduced. Leveraging AI as a predictive tool is critical to the evolution of Autonomous Networks which will speed up troubleshooting, prioritize resolution, and automate the next best actions for remediation.



In a recent Fiber Broadband survey conducted by Analysys Mason, 34% CSPs reported that they were already working towards autonomous fault resolution with assurance-driven closed-loop automation. Another 34 percent reported that they had started implementing a real-time monitoring solution and some automated fault resolution. When asked about their approach to closed-loop automation of NOC and SOC, 48 percent said that they wanted closed-loop automation only for network and service assurance, and 24 percent said that they wanted closed-loop automation for most of their network and service operation processes.

It's evident that the need for automation is high, yet the progress towards fully autonomous networks is piecemeal and taking time.

Autonomous Networks: How Do We Get There?

The question that arises is what will drive CSPs to automating their networks and to achieve a fully Autonomous Networks status faster? If costly manpower, expensive human mistakes, and low quality of services can be reduced through automation, CSPs will put their money on Automation.

Other than operational efficiency and for cost reasons, CSPs identify business objectives that drive them to Automation. These could include introduction of network slicing for enterprise services, a new

fixed broadband service, or entering a new enterprise market.

Simply put, CSPs would invest in technologies that offer higher revenue at lower costs. Automated operations and Autonomous Networks promise both.

Let's break this down. CSPs need to do the following to remain competitive as new services consume higher volumes of data and require faster data rates:

1. Deliver high performance and high reliability services.
2. Reduce manual operations.
3. Simplify problem investigation in complex networks.
4. Increase workforce productivity.
5. Meet high speed demands of enterprise services.
6. Respond dynamically to changing network conditions.
7. React faster to customer requirements.

The key to achieving some of the targets above lies not in acquiring new tools, but in the data generated in the CSP networks that carries within it the intelligence required for automation. Systems that leverage this data can offer a solid foundation for automation. Let's explore what the network data offers:

- Assurance (Performance, faults, and QoS) metrics.
- Network data when modelled correctly, can unleash AI/GenAI insights.
- Assurance and AI insights together create a powerful combination, underpinning the foundation of Automation.

Network data is already collected by the CSPs for Assurance purposes. However, if this data is manipulated and turned into intelligent AI insights, it can drive the evolution of Autonomous Networks. Only intelligent data in a closed loop feedback system will self-correct the network errors, reduce service delays, and eliminate human errors.

Assurance, AI and Automation: Can They Bring Automated Diagnosis and Remediation?

TM Forum has defined the TMF Autonomous Network Maturity Levels (0-5) with definitions, processes and sample use cases. A recent (2024) Omdia survey shows how CSP autonomous levels are distributed: 20 percent L1 (Assisted Operation and Maintenance), 26 percent L2 (Partial Autonomous), 25 percent L3 (Conditional Autonomous) and only 11 percent L4 (High Autonomous), on an average. This means that less than 50 percent of CSPs have moved beyond L2, where AI is used primarily for monitoring and recommendations rather than autonomous decision-making. In this article, we will focus on the CSPs' journey from L2 to L3 and L4. A direct interpretation of the TM Forum definitions would be to develop an Automation Engine, a software, which leverages Assurance and AI data that can offer capabilities such as workflow automation, trouble ticketing automation, and automated communication with network entities.

The 4 key functions of the Automation Engine could be described as follows:

Workflow Automation: Automating the identification of operational issues including policy violation, site outages, network congestion and network config errors.

Trouble Ticketing Automation: Automating the notification of a degradation and automating the ticketing process.

Auto Correlation of multi-sourced data: Automating the correlation of performance indicators of the CSP network and its underlying IT components.

Remediation Automation: Automating the recommendation of corrective actions to experts or automating the full remediation using AI.

Through a step-by-step Automation process using the 4 functions, CSPs could move from L2 to L3 and then L4. It is important to note that to achieve L4, Assurance and AI data have a key role to play. With the addition of intent-based AI insights for remediation, L5 could also be achieved.

The Steps From L2 to L4 Autonomous Networks

Based on an understanding of Tier 1 CSPs' challenges in evolving from L2 to L4, one can establish the optimum evolution path offered by an Automation Engine that would take a CSP to the desired Autonomous Network level.

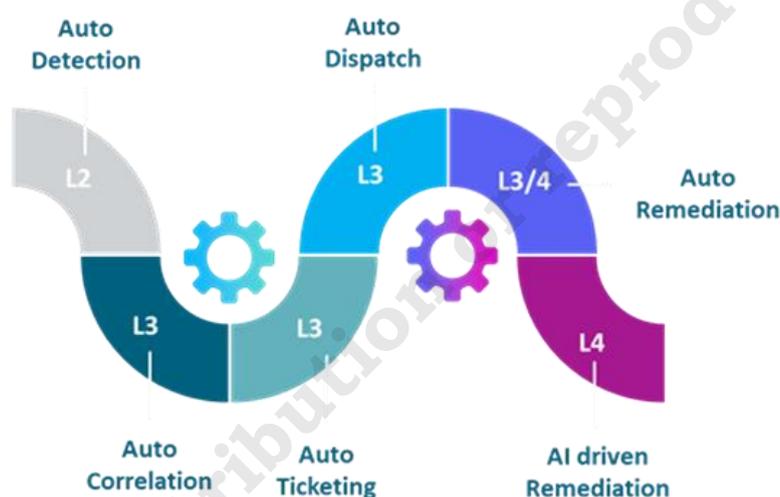


Figure 1: An Automation Engine that drives L2 to L4 Autonomous Networks

The recommended steps to move from L2 (Partial Autonomous) to L3 (Conditional Autonomous) to L4 (High Autonomous), as illustrated in Figure 1, above, are described as follows.

Step 1: Auto Detection of Network and Service problems: This first step detects degradations and faults automatically without human intervention. This is achieved through using accurate service modelling and resource topology through multi-domain correlations.

Step 2: Auto Correlation of event data from network, service, IT and applications: In this step, event data (performance and faults) is automatically correlated across the mobile, fixed, IT, and enterprise networks and processed for resolution, mapping service level problems with the underlying network elements (network, routers, switches, firewalls, etc.).

Step 3: Auto Ticketing: By automating trouble ticketing, operations become efficient and trouble ticket volumes decrease. As tickets get generated automatically for network breaches, email, text, and API based notifications are dispatched out.

Step 4: Auto Dispatch for Field Engineers: This step involves automating dispatches for automated remediation. The auto dispatches are based on predefined criteria and sent out to third party systems, such as orchestrators, for remediation.

Step 5: Auto Remediation: In this step, the Automation Engine triggers automated remediation actions, based on pre-defined rules and then updates the status (Resolved/Failed/No action required) of the incident.

Step 6: AI based Remediation: To evolve the network from L3 to L4, AI for performance forecasting and anomaly detection is needed. By performing predictive AI modelling, and pattern discovery on Assurance data, anomaly detection across different applications and network entities is possible. With GenAI, using natural language prompts, querying complex datasets offers an additional level of remediation.

An Automation Case Study: Tier I CSP offering Mobile, Fixed and Broadband Services

A large CSP with over 60 million subscribers offering mobile, fixed, broadband, data, internet, and managed services had a need to automatically identify the experience of premium services offered on its Fixed Broadband, 4G and 5G networks. This included the impact of network issues on its broadband/enterprise services and customers, and prioritization of remediation of service impacting problems, in a highly automated manner.

An Automation Engine, which comprised Assurance and some elements of AI, was deployed across the mobile, broadband, and enterprise networks. This established a zero-touch network incident lifecycle including proactive and automated issue detection, ticketing, notification, remediation, and dispatching for mobile and home broadband services.

As an outcome, the CSP could offload 86 percent of impacting network events to a zero-touch platform, achieving over a 90 percent reduction in time to trigger customer notifications.

Here are the key KPIs that the CSP achieved over a 12-month period:

- 850+K NOC/SOC person-hours were automated for mobile/fixed services and 72K person-hours were automated for enterprise services.
- Over 80 percent reduction in MTTI (Mean Time to Identify) problems at NOC/SOC.
- 100 percent automation of the ticket creation process was achieved by automating 700+ tickets per day for 160+ service impacting alarms.
- Mitigation of late detection of alarms and performance issues with proactive detection and closure improved the MTTR (Mean Time to Repair) and customer experience.
- Overall problem handling time improved by 92 percent from detection to notification stages.
- There was a 94.7 percent reduction in prolonged broadband outage tickets.

The metrics below show the commercial benefits (in cost savings) achieved by implementing the 6 Automation steps over the 12 month-period.

- Automating mobile and broadband services: 6.5 M USD.
- Automating enterprise services: 1.2 M USD.
- Reducing customer impact: 350 K USD.
- Zero Touch Service Operations Center: 5 M USD.
- Operational efficiency: increase by a factor of 2.3.

With a high degree of 920K+ person hours automated in a year, and with 4.78 million (mobile: 2.79 million; broadband: 1.99 million) notifications sent out to customers informing them ahead of time on outages that hindered their service, the CSP could offer a high level of automated problem resolution across its entire customer base.

This is a true-life example of how TM Forum definitions can be used to build an Automation Engine leveraging Assurance and AI data, helping the CSP to move from Autonomous Network L 1.8 to L 3.3, as exemplified above.

This example is only a slice of the revenue benefits that can be reaped from automated diagnosis, workflows, corrective recommendations and fault resolution, leading to millions of dollars of annual savings for CSPs. Scaling up automation efforts is a necessity and high Autonomous Networks (L4) are a reality. It's now up to the industry to put together the mechanics of exploiting network data, turning it to Assurance and AI insights, and building the Automation Engine which will deliver the high (L4) and full (L5) Autonomous Networks of the near future.

Not for distribution or reproduction