WHITE PAPER

Building Trust in Autonomous Networks

KEYSIGHT

Table of Contents

Executive Summary

Autonomous networks are the most important transformation in telecom service and network management in decades. AI-driven, intent-based, and closed-loop by design, these networks are built to automatically configure, optimize, heal, and protect themselves.

Converging demands are driving autonomous network momentum. High service quality is essential, as enterprises and consumers demand seamless, reliable experiences that meet strict service-level agreements (SLAs). At the same time, performance pressures are increasing, and company boards are mandating reduced operational expenses, improved customer experiences, and faster investment returns on 5G, cloud, and edge deployments.

Meanwhile, the network is undergoing a dramatic and complex transformation into cloud-native, software-based, disaggregated networks carrying diverse traffic workloads with extreme technical requirements, and supporting innovative new capabilities, such as network slicing.

Meeting these new realities requires a level of scale and agility that far exceeds manual management capabilities, making autonomous networks essential.

The TM Forum, a global alliance of 800+ organizations across the connectivity ecosystem, has created a phased autonomous networks maturity model and framework that defines six stages of network autonomy, from manual (Level 0) to fully automated (Level 5). Operators today are advancing toward Level 4, high autonomy.

Automation without confirmed proof of performance risks failure, making continuous testing critical to the success of autonomous networks. When automation is validated in the lab and the live network, it builds trust, accelerates adoption, and ensures outcomes.

Test and assurance play an essential role in autonomous networks, providing a validation layer from lab to live, across 5G RAN, core, and cloud. This is helping operators accelerate progress along the autonomous network roadmap with confidence, safeguarded SLAs, and differentiated customer experiences.

This white paper details why autonomous networks are important and how continuous test and active assurance embedded across lab, staging, and live operations helps operators move toward full and trusted autonomy.

Why Autonomous Networks Matter

Telecom operators are under unprecedented strain as revenues flatten, margins thin, and shareholders demand faster return on 5G and edge investments. Customer quality of experience now impacts competitiveness more than coverage or price.

At the same time, traffic continues to surge and technical complexity is growing exponentially as cloud-native networks require dynamic responsiveness in near real-time and massive scalability. Traditional, manual operations cannot keep pace.

Autonomous networks enable this network revolution with fully automated, self-directed, and adaptive operations.

From Burning Platform to Autonomous Network

Autonomous networks promise a shift from manual, reactive processes to predictive operations that translate business intent directly into network actions.

An autonomous network combines automation, closed-loop control, and AI/ML to reduce repetitive manual tasks and eventually eliminate human involvement. Self-configuration, including automated provisioning and scaling, as well as self-optimized, rapid, dynamic tuning of 5G RAN, core, cloud, and transport resources, streamline network operations.

Because autonomous networks are self-healing, they anticipate, detect, and resolve issues before customers are impacted, ensuring promised service outcomes.

Through self-protection, autonomous networks can rapidly provide adaptive responses to threats.

The overall result is proactive customer-centric operations with zero wait, zero touch, and zero trouble: a “Zero-X” standard.

The TM Forum Autonomous Network Model: An Industry Roadmap

Achieving fully autonomous networks is a journey. TM Forum is developing an industry framework that categorizes network automation maturity into six levels, ranging from Level 0 (manual operations) to Level 5 (full autonomy). The levels are designed to measure an operator's progress toward full network autonomy. Operators can use the **TM Forum Autonomous Network Level Assessment Validation (ANLAV) service to formally determine the autonomous network maturity level and progress as defined by:**

Level 0:	Manual operations; reactive
Level 1:	Assisted operations; task automation
Level 2:	Partial autonomy; event-driven loops in specific domains
Level 3:	Conditional autonomy; AI/ML-supported closed loops
Level 4:	High autonomy; intent-driven multi-domain automation
Level 5:	Full autonomy; self-governing across domains

Most operators are at Levels 1 or 2, with plans to incorporate further automation. Industry leaders are experimenting with Levels 3 and 4 with some, like TDC NET, already demonstrating Level 4 capability. TDC is the first operator to be formally validated for Level 4 RAN energy efficiency optimization via an ANLAV assessment, demonstrating a path toward reducing operational expenditures and contributing to sustainability goals.

Testing and Assurance: The Enabler of Autonomy

As operators progress through the automation maturity model, each step introduces new requirements, capabilities, and risks. Before advancing to subsequent levels, operators must ensure capabilities at the current level are performing as intended.

To this end, testing and assurance form an enabling confidence layer that ensures increasing levels of autonomy operate correctly in real networks and can be trusted.

By embedding testing and assurance across lab, staging, and live environments, operators gain the certainty that event-driven and automated workflows, AI-assisted loops, and multi-domain orchestration behave as intended. Validation provides the confidence to accelerate adoption at cloud speed without instability, and proof that customer experience (CX) outcomes are continuously delivered as promised.

Each level of autonomy brings new risks if left unchecked, as illustrated in this chart.

Autonomous Networks Maturity Phases: Why Testing and Assurance are Essential

Level	0	1	2	3	4	5
	Manual ops	Basic automation	Conditional automation	Closed loops	High autonomy + AI	Full autonomy
Risk	Inconsistent service, slow delivery	Silos, limited validation	Automating errors without validation	Reinforcing wrong behaviors without testing	Opaque AI decisions, CX degradation	Trust gap without continuous validation

Without validation, every step carries new customer experience risk.

Continuous testing and active service assurance

Customer Experience as the North Star

While automation is the operational goal, the real measure of progress is customer experience as defined by responsiveness, reliability, and seamless quality. Testing and assurance connect intent to outcome, delivering measurable business impacts through validation and assurance. KPIs prove whether each autonomous action leads to measurable improvements in customer experience.

Operators progressing along the autonomous network maturity journey can track success with KPI goals such as:

- **Change failure rate (CFR).** Reduction of failed changes or rollbacks by 30–40% with pre-production validation
- **Service availability / SLA fulfillment.** Improvement to 99.95%+ adherence through proactive, real-time assurance
- **Time to detect (TTD).** Cut from hours or days to minutes with automated anomaly detection
- **Time to repair (TTR).** Reduced by 50–70% through closed-loop validation of fixes
- **Automation success rate.** >90% of automated workflows executed without manual intervention

These real-world KPI results prove the value of autonomy not just in technical terms, but in financial, operational, and customer outcomes, with an expectation of improved net promoter scores (NPS) by 10–15 points, as validated automation ensures consistent quality of experience (QoE).

Testing Across the Autonomous Network Journey

As each autonomous network level adds more automation and intelligence, testing and assurance provide validation that each level is safe, measurable, and customer-focused.

Each level involves the addition of important new tests, such as:

- **Levels 1 and 2 (Assisted operations and partial autonomy).** Task automation and domain-level loops must be validated to prevent small errors from propagating network-wide.
- **Level 3 (Conditional autonomy).** AI and ML enter decision-making, requiring models to test for accuracy, stability, and bias to ensure they enhance customer experiences and never degrade them.
- **Level 4 (High autonomy).** Multi-domain orchestration and slicing demand stress testing and SLA validation at scale to prove intent fulfillment.
- **Level 5 (Full autonomy).** Trust becomes the critical currency. Continuous validation and transparent assurance sustain confidence in a self-governing network.

We will now explore in more detail the challenges encountered as operators move from one autonomous network level to another, as well as the additional testing capabilities typically required, the resulting impact on customer experience, and real-world use cases.

Level 0 → Level 1: From Manual to Assisted Operations

Challenge

At Level 0, networks are largely manual, relying on operator intervention and scripts. Moving to Level 1 introduces assisted operations, where tasks become automated and repeatable. The challenge lies in benchmarking what "good" looks like. This includes establishing baselines for performance, validating automation scripts, and ensuring that tasks such as provisioning and fault detection deliver consistent results.

Required testing capabilities

- **Benchmarking and regression testing.** Establish baseline performance metrics against which automation outcomes can be measured.
- **Traffic generation and emulation.** Simulate real-world traffic flows to validate that automated tasks operate correctly under load.
- **Basic security testing**. Inject common fault and attack scenarios to confirm automation can handle them safely.

Customer experience outcome

Eliminate inconsistency by validating task automation early to reduce provisioning errors and speed service delivery. Even small improvements here have a measurable impact on QoE, creating the foundation for customer trust.

Level 1 → Level 2: From Assisted to Partial Autonomy

Challenge

At Level 2, networks begin to operate with partial autonomy, triggering automated workflows based on events within isolated domains. The challenge is verifying that event-driven automation behaves predictably, does not conflict across domains, and delivers measurable improvements over manual intervention.

Required testing capabilities

- **Active service assurance.** Real-time monitoring and synthetic testing to validate event triggers and service health.
- **Lab and test automation.** Integration of automated test suites to validate workflows quickly and repeatably.
- **End-to-end network validation.** Testing automation outcomes across domain boundaries, not just in silos.

Customer experience outcome

Partial autonomy allows networks to react faster to faults and performance issues. Testing ensures that these reactions are correct reactions. Customers see fewer outages, faster recovery, and more consistent service availability.

Real-world use case

A tier-one North American operator replaced manual, technician-led service activation with active service assurance to introduce automated, event-driven workflows. Previously, technicians relied on specialized equipment and repeat site visits to validate tower activations, leading to high costs, errors, and delays. By automating service activation tests and integrating them directly into existing workflows, the operator enabled consistent, repeatable validations that no longer required human initiation at every step. The solution generated “birth certificates” for circuits, validated network health in real time, and automatically diagnosed 80% of trouble tickets. This marked the shift to partial autonomy, where workflows were triggered by network events and verified with

active assurance, reducing truck rolls, cutting activation times by up to 70%, and delivering more reliable service availability.

Level 2 → Level 3: From Partial to Conditional Autonomy

Challenge

Level 3 introduces conditional autonomy, where AI and ML begin to support decision-making in closed loops. Here, testing expands beyond networks to the decisions themselves. Operators must validate AI model accuracy, monitor for drift, and verify that automated root cause analyses are correct.

Required testing capabilities

- **AI-in-the-loop validation.** Test the inference accuracy, false positive rates, and stability of ML models.
- **Anomaly detection validation.** Generate synthetic anomalies to validate whether AI systems recognize and respond appropriately.
- **CNF resiliency testing.** Ensure cloud-native network functions (CNFs) can withstand failures and recover under automated control.

Customer experience outcome

Networks become predictive, fixing issues before they are noticed by users. Testing ensures that predictions are accurate, interventions are timely, and customer experience moves from reactive support to proactive assurance.

Real-world use case

A tier-one North American operator used active service assurance to move from reactive troubleshooting toward closed-loop, AI-assisted assurance across 4G and 5G networks. Initially, the solution automated service assurance with virtual test agents (VTAs). As deployment scaled beyond 1,100 VTAs running 250,000 daily tests, the platform began detecting anomalies up to eight hours before outages occurred. This predictive capability elevated troubleshooting, allowing engineers to act on early warnings, validate root causes, and resolve issues before customers were affected. By automating correlation, root cause analysis (RCA), and anomaly detection, the solution reduced reliance on manual investigation and accelerated decision-making. The teams could seamlessly shift focus from reactive 4G problem-solving to preparing and managing advanced 5G deployments, while also validating new technologies like slicing. This exemplifies

conditional autonomy, where AI-driven insights guide interventions within closed loops, ensuring that predictions and automated responses improve resiliency, reduce outages, and deliver proactive assurance.

Level 3 → Level 4: From Conditional to High Autonomy

Challenge

Level 4 is a turning point, as most operations are automated across multiple domains, guided by intent and optimized through AI. The challenge is validating complex orchestration scenarios at scale: service slices, cross-domain interactions, and new latency-sensitive use cases.

Required testing capabilities

- **Multi-domain orchestration testing.** Validate intent fulfillment across RAN, core, transport, and cloud domains.
- **Scenario stress testing.** Simulate extreme conditions (load surges, topology changes) to ensure orchestration holds.
- **Advanced SLA assurance.** Measure outcomes like 99th percentile latency, slice elasticity, and jitter under real-world conditions.

Customer experience outcome

Autonomy begins to touch enterprise-grade services like private 5G, mission-critical IoT, and low-latency applications. Testing ensures SLAs are met and proven, building the trust enterprises need to adopt new autonomous services with confidence.

Real-world use case

A tier-one North American operator advanced its automation journey by deploying active service assurance to break down siloed operations and deliver end-to-end, multi-domain orchestration. Previously, engineers worked with localized insights that limited ability to detect interconnected issues across RAN, core, and transport domains. This solution supported holistic visibility, correlating performance data across the entire network and generating actionable alerts instead of raw errors. Intelligent alarms were created to detect concurrent anomalies, enabling proactive responses that identified problems hours before outages could occur. This orchestration extended beyond detection, with engineers constructing signatures to automate future responses, ensuring scalability and resilience under complex conditions. The approach optimized engineering resources, reduced war-room escalations, and enabled precise, cross-domain troubleshooting

with fewer staff. This evolution reflects high autonomy, where AI-guided orchestration spans multiple domains, SLAs are proactively safeguarded, and enterprise-grade reliability is delivered with confidence.

Level 4 → Level 5: From Conditional to High Autonomy

Challenge

Level 5 represents a fully self-governing, intent-driven network. At this stage, the challenge is not functionality, but trust. Operators must prove to themselves, regulators, and customers that autonomy is safe, transparent, and reliable at scale.

Required testing capabilities

- **Continuous validation frameworks.** Embed testing so that it runs constantly, validating autonomy in real time.
- **Closed-loop assurance.** Feed test and assurance data directly into orchestration systems to refine actions dynamically.
- **Security and compliance testing.** Simulate sophisticated attack scenarios to ensure the network self-protects.

Customer experience outcome

Customers experience networks that "just work," with zero wait, zero touch, and zero trouble, all without human oversight. Continuous testing and assurance are the only way to sustain this promise, which has yet to be achieved and would require incorporating agentic AI solutions into Level 4 implementations.

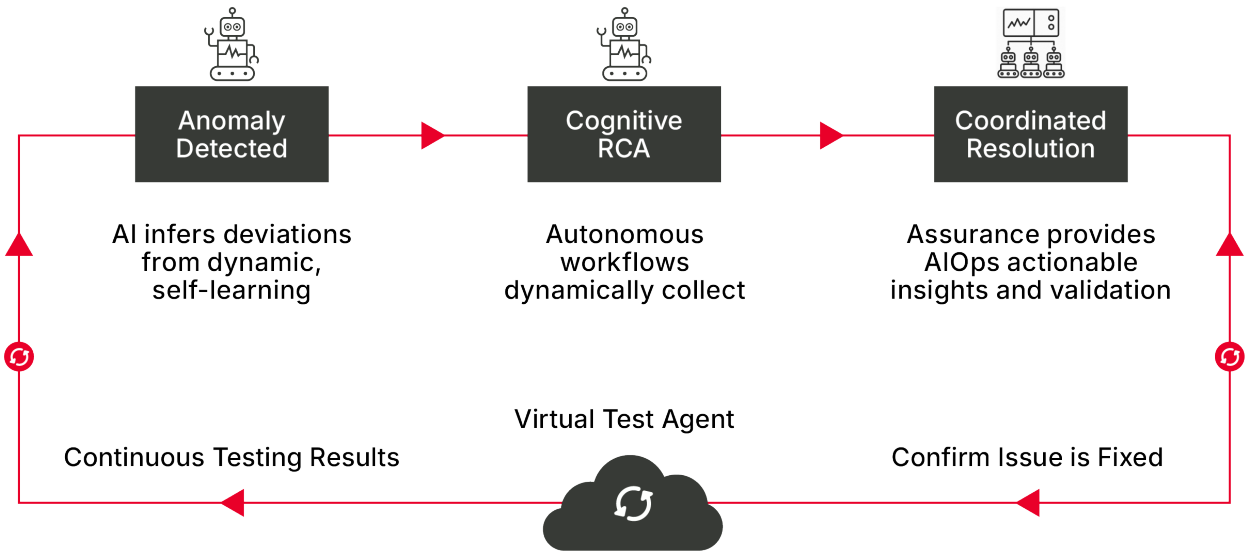

Figure 1. Customer experience outcome flow example

A Sequential Confidence-Building Journey

In this section we summarize how testing and assurance align with the TM Forum autonomous network maturity journey, ensuring that every step in the progression to autonomy strengthens the customer experience. Testing makes automation safe as networks move from scripts to intent. It validates AI decisions so they can be trusted as operations shift from reactive to predictive. It bridges gaps across domains as organizations evolve from siloed to multi-domain. And it sustains confidence in autonomy as the industry moves from promise to trust.

The following table summarizes the focus of test and assurance at each level transition, detailing key metrics captured and the resulting customer experience outcomes.

Level transition	Objective	Validation focus	Key KPIs	CX outcome
0 → 1	Manual → Assisted	Regression testing, traffic generation, fault injection	Provisioning success rate, TTD / TTR baseline	Faster activation, fewer errors
1 → 2	Assisted → Partial	Active assurance, automated workflow validation, end-to-end checks	Automation success rate, incident resolution time	Faster recovery, more stable services
2 → 3	Partial → Conditional	AI/ML accuracy, anomaly injection, CNF resiliency	False positive / negative rates, model drift detection	Predictive, proactive service quality
3 → 4	Conditional → High	Cross-domain orchestration,	SLA adherence %, latency / jitter	Proven enterprise-grade SLAs

		stress testing, SLA monitoring	within 99th percentile, slice elasticity	
4 → 5	High → Full	Continuous validation, closed-loop assurance, compliance testing	Intent-fulfillment rate, compliance audit pass %, security resilience	Trusted full autonomy, zero-touch CX

Summary of test and assurance by level.

The graphic below highlights where specific test and assurance capabilities are required, and how their depth increases across maturity levels.

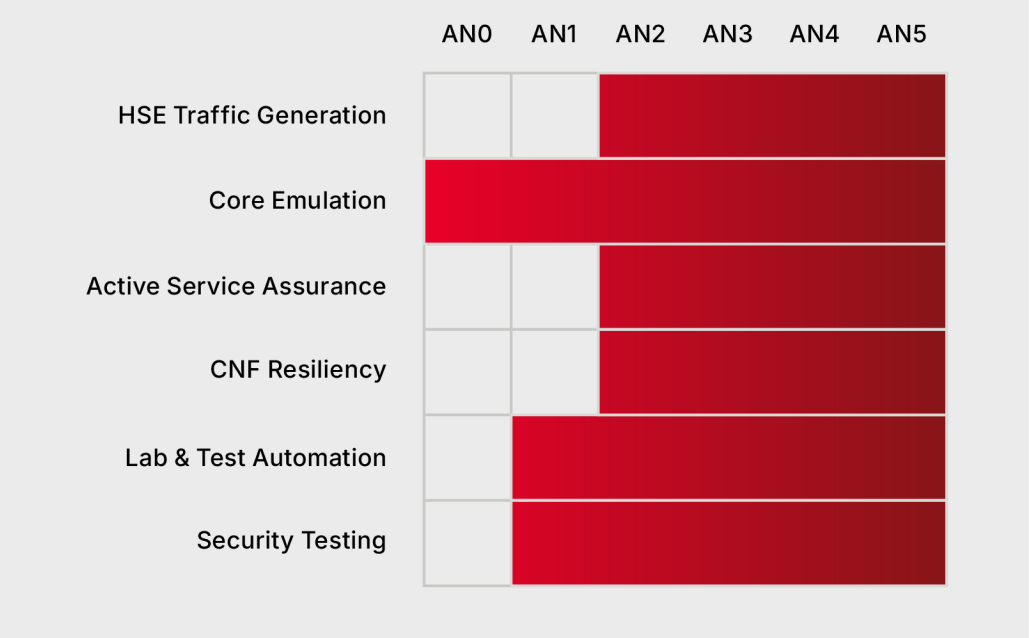

Figure 2. Technology mapped to autonomous network levels

Validation supports safe governance as operators integrate autonomy. It also helps establish guardrails that ensure autonomy is fast, safe and accountable:

- **Safe rollback triggers** automate recovery when KPIs or thresholds deviate from expected performance.
- **Anomaly thresholds** define acceptable tolerance levels for latency, jitter, or loss before corrective action is taken.
- **AI model explainability** ensures visibility into automated decisions to maintain transparency and meet regulatory requirements.
- **Compliance validation** embeds policy checks such as lawful intercept and data sovereignty into the validation pipeline.
- **Staged release and canary testing** deploy updates in controlled subsets before full rollout to minimize risk.

From Lab to Live: Making Autonomy Real

The autonomous network maturity model provides a roadmap detailing how capabilities evolve from manual to fully autonomous. In practice, autonomy only becomes real when it has been executed safely in live operations. This requires validation be embedded across the entire lifecycle, from innovation in the lab, through deployment pipelines, into continuous live operations.

The autonomous network testing lifecycle needs to be continuous, starting early to impact planning and continuing into the production network to ensure continuing service quality. Powerful, automated testing and assurance throughout the lab-to-live lifecycle ensures any changes are thoroughly tested before being deployed in the live production network.

Validation across the lifecycle includes:

- **Lab.** Safely testing new functions, workflows, and AI behavior before they reach production.
- **Staging.** Integrating automated testing into CI/CD release pipelines to keep pace with vendor updates and prevent regressions.
- **Live operations.** Deploying active assurance to measure SLAs in real time, validate closed-loop fixes, and feed insights back to orchestrators.

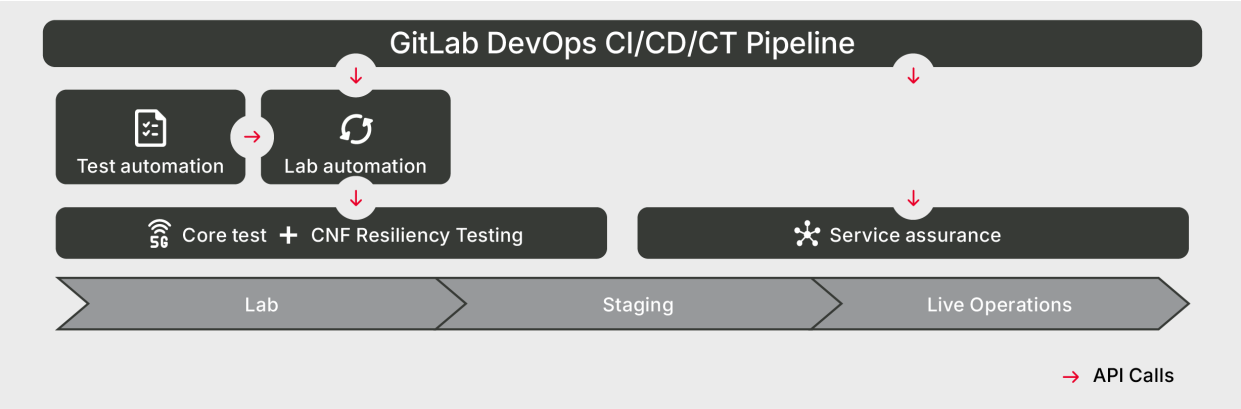

Figure 3. Lab-to-live testing

Testing across this continuum ensures that every innovation, from simple scripts to AI-driven loops, is validated before customers are impacted. This comprehensive testing results in faster time-to-market, reduced risks and costs, and enhanced quality and customer satisfaction.

Test and Assurance Functions for Lifecycle Stages

Test and assurance at each stage of the lifecycle focuses on different test goals and outcomes.

Lab: Safe innovation, proven foundations

In the lab, operators can innovate without risk, testing devices and also automation workflows, policies, and AI behaviors before they touch production:

- Validate automation and orchestration policies in controlled environments
- Simulate real-world traffic, topology changes, and failure scenarios
- Establish performance baselines to measure improvements in autonomy

By using the lab as a proving ground, operators gain confidence to accelerate adoption of new technologies.

Staging and CI/CD: Accelerate deployment

Modern networks evolve at cloud speed, as cloud-native network functions, container updates, and vendor patches are released continuously. Staging environments and CI/CD pipelines are essential for safe agility:

- Integrate automated tests into CI/CD pipelines so every release is validated
- Run regression suites to prevent old issues from reappearing
- Validate cross-domain orchestration scenarios before production rollout

Testing is integrated into the release cadence, reducing risk while enabling faster time-to-revenue.

Live Operations: Active assurance at scale

In production, validation shifts from prevention to continuous assurance with a requirements networks are tested from the customer's perspective in real time:

- Emulate user behavior with synthetic probes, continuously validating service performance.
- Verify closed-loop assurance with automated fixes to improve QoE.
- Detect degradation with proactive SLA monitoring before customers experience it.

Live assurance closes the loop, turning autonomy from a design ambition into an operational reality that customers can trust.

This table summarizes the validation activities and value delivered at each stage of the lifecycle. Lab-to-live is not just an operational detail. It is the operational foundation of trusted autonomy.

Lifecycle stage	Validation activities	Value delivered
Lab	Prove workflows, policies, and AI safely. Simulate traffic and faults. Establish baselines.	Safe innovation, controlled risk, measurable improvements
Staging, CI/CD	Embed automated tests in pipelines. Run regression suites. Validate cross-domain orchestration.	Faster release cadence, reduced risk, early fault detection
Live operations	Synthetic probes emulate users. Closed-loop SLA validation. Proactive monitoring.	Continuous assurance, faster TTR, proactive QoE protection

Lifecycle validation activities and value

The Path Forward

Autonomous networks are the emerging model that will define how communications services are built, monetized, and experienced. Operators are already advancing along the maturity model, but the true measure of success is not the level achieved but the trust that is ultimately earned.

Validation is the foundation of that trust, with testing and assurance instilling operators with confidence they need to automate boldly, innovate at cloud speed, and compete on customer experience. Continuous validation is the difference between autonomy that accelerates failure and autonomy that drives competitive advantage.

The path forward is clear:

- **Embed validation everywhere.** Make testing and assurance intrinsic to the lifecycle from lab to live, not optional checkpoints.
- **Tie autonomy to outcomes.** Measure progress by KPIs that matter, such as SLA fulfillment, TTD / TTR improvements, change failure rate reduction, and customer experience scores.
- **Adopt continuous assurance.** Treat validation as a living process that sustains trust in automation and AI at every level of maturity.

Operators have a significant opportunity to achieve faster time-to-revenue by launching services with confidence. Operational expenses are lowered by reducing firefighting and costly rollbacks. Differentiation in customer experience is achieved by proving, not just promising, intent-driven service quality.

Autonomous networks will define the next decade of telecom. By embedding validation into their DNA, operators can ensure that this transformation is not just ambitious, but reliable, resilient, and relentlessly customer centric.

How Keysight Helps Enable Trusted Autonomy

While many vendors contribute to the autonomous network ecosystem, Keysight plays a distinctive role as the validation layer, ensuring automation, AI, and closed loops deliver trusted outcomes across the lifecycle.

Keysight's lab-to-live capabilities include:

Core capability	Autonomous network level contribution	Lifecycle role
Active service assurance and customer experience monitoring	**L2–L5** (Partial → Full)	**Live:** SLA validation, closed-loop assurance
Core and mobility traffic emulation	**L0–L5** (Manual → Full)	**Lab / staging:** Validate EPC / 5G Core functions, policy, orchestration
Lab automation, regression, CI/CD integration	**L1–L5** (Assisted → Full)	**Lab / staging:** Integrate continuous testing into pipelines
CNF/VNF resiliency validation	**L2–L5** (Partial → Full)	**Staging / live:** Validate cloud-native workloads under dynamic conditions
Security and threat emulation	**L1–L5** (Assisted → Full)	**Lab / live:** Validate resilience, support self-protection

Why Keysight's Approach Matters:

- **End-to-end scope:** Validates across RAN, core, cloud, and transport
- **Vendor neutrality:** Works in multi-vendor, disaggregated environments
- **Lab-to-live continuum:** Embeds validation from design through operations
- **Complementary role:** Feeds validated data into orchestration and AI platforms, providing the "eyes and ears" for trusted automation
- **Proven deployments:** Strongest footprint today at Levels 2–3, enabling operators to accelerate safely toward higher autonomy

Homegrown test and assurance approaches fall short. They lack repeatability across teams and domains, and cannot correlate test, assurance, and orchestration events. Without integrated toolchains, closed loops cannot be validated, as slower mean-time-to-verify changes result in delayed autonomy.

Achieving network autonomy may seem daunting. However, the journey can be decomposed into many successful steps. Operators can start reaping the benefits of autonomy now by focusing on high-value use cases, like private 5G, regulatory compliance, or migration. There is no need to wait.

As a trusted partner, Keysight works with you to accelerate your autonomous network journey. By delivering the lab-to-live expertise and capabilities that make autonomy safe, measurable, and customer centric, you can progress along the autonomous network maturity model with confidence.

Acronym Glossary

Acronym	Term	Definition
AI	Artificial intelligence	The simulation of human intelligence by machines, enabling automation, learning, and decision-making across network operations.
AIOps	Artificial intelligence for IT operations	A framework using AI to enhance and automate IT and network operations, including anomaly detection, root cause analysis, and predictive maintenance.
AN	Autonomous network	A self-managing network capable of configuration, optimization, healing, and protection with minimal human intervention.
ANLAV		Autonomous network level assessment validation
API	Application programming interface	A set of rules that allows software applications to communicate and share data, often used to integrate automation and assurance systems.
CI/CD	Continuous integration / continuous deployment	A DevOps practice for automating the testing and deployment of network updates and configurations.
CNF	Cloud-native function	A virtualized network function designed for cloud environments, offering scalability and resilience.
CT	Continuous testing	Automated testing integrated into the CI/CD pipeline to ensure network changes are validated continuously before deployment.
CX	Customer experience	The overall quality of user interaction with a network or service, encompassing reliability, responsiveness, and satisfaction.
EPC	Evolved packet core	The central component of a 4G LTE network that manages data, connectivity, and mobility.
IoT	Internet of Things	The ecosystem of interconnected devices that communicate and share data over a network, often requiring autonomous network management for scalability.
KPI	Key performance indicator	A measurable value used to assess network performance and customer experience outcomes.
ML	Machine learning	A subset of AI focused on algorithms that enable systems to learn from data and improve decision-making without explicit programming.
TTD	Time to detect	The average time taken to identify a network fault or anomaly.
TTR	Time to repair	The average time taken to resolve a detected issue and restore normal service.
NFV	Network function virtualization	A technology framework that decouples network functions from dedicated hardware, allowing deployment on virtual machines.
NPS	Net promoter score	A customer satisfaction metric that measures loyalty based on likelihood to recommend a service.
QoE	Quality of experience	A user-centric measure of network and service performance based on perceived quality.
RAN	Radio access network	The part of a mobile network that connects devices to the core network via radio signals.
RCA	Root cause analysis	A process of identifying the fundamental reason for a network issue or failure.
SLA	Service level agreement	A contractual commitment defining the expected service performance and reliability metrics.
TM Forum	TeleManagement Forum	An industry association that develops standards and frameworks for digital service providers, including the autonomous networks maturity model.
VNF	Virtual network function	A software implementation of a specific network function that runs on virtualized infrastructure instead of dedicated hardware, enabling flexibility and scalability within NFV and cloud-native architectures.
VTA	Virtual test agent	Software-based testing probes used to simulate user activity and validate service performance in live networks.