
# Testing and Assuring Networks Enhanced with AI

eBook

KEYSIGHT

# Testing and Assuring Networks Enhanced with AI

**The race to deploy AI-powered solutions is projected to drive $632 billion in worldwide spending by 2028 — a CAGR of 29%, according to research firm IDC.**

Communications networks are poised to benefit as AI technologies are integrated to enhance, automate, and optimize network management, performance, and security.

These networks will also be tasked with addressing unprecedented demands.

AI applications require real-time data processing and inference, relying on continuous uplink and downlink network access. This enables the transmission of raw data for processing and the reception of inference results from AI models hosted on edge computing nodes, as well as regional and global data centers. This traffic requires low-latency, high-throughput, and guaranteed connectivity across the edge and IP core, which is accelerating the adoption of 100G, 400G, and 800G technologies.

Modern networks were not designed to support AI's data-intensive, high bandwidth, low latency, lossless, and distributed cloud and edge processing needs. This shift is already driving a complete re-architecting of data centers, while wireless and wireline service providers rush to upgrade networking infrastructure. Dell'Oro has projected data center CapEx will increase to more than $500 billion in 2028.

IDC estimates spending on AI software will reach

$632B

with a CAGR of

29%

by 2028

As AI is integrated into the network, there are concerns about whether it can be trusted to make decisions, handle sensitive data, and defend against the latest hacker strategies. Efforts are underway to rapidly validate that networks built for AI and enhanced with AI perform as expected. Test and assurance are at the nexus of these developments, delivering confidence and predictability in the face of a new frontier.

New methodologies like realistic traffic emulation and network digital twins are speeding comprehensive and reproducible testing of AI situations at scale and under congestion without requiring investment in expensive, proprietary labs.

This eBook explores the latest trends around AI's incorporation into critical network functions. It examines how test and assurance address AI adoption challenges and the invaluable role they play in validating AI use cases. We also draw on Keysight's customer engagements and market experience to reveal recommendations for testing and assuring networks enhanced with AI.

**Let's dive in.**

# Contents

CHAPTER 1

## Using AI to Benefit Networks and Operations

The network functions leveraging AI's capabilities and the challenges slowing AI adoption

GO TO CHAPTER 1 >

CHAPTER 2

## Role of Test and Assurance

How testing helps address AI adoption challenges, key testing methodologies, and testing in the AI network lifecycle

GO TO CHAPTER 2 >

CHAPTER 3

## Recommendations: Testing and Assuring Networks Enhanced with AI

Examples of current practices and recommendations for testing to ensure network function performance

GO TO CHAPTER 3 >

CONCLUSION

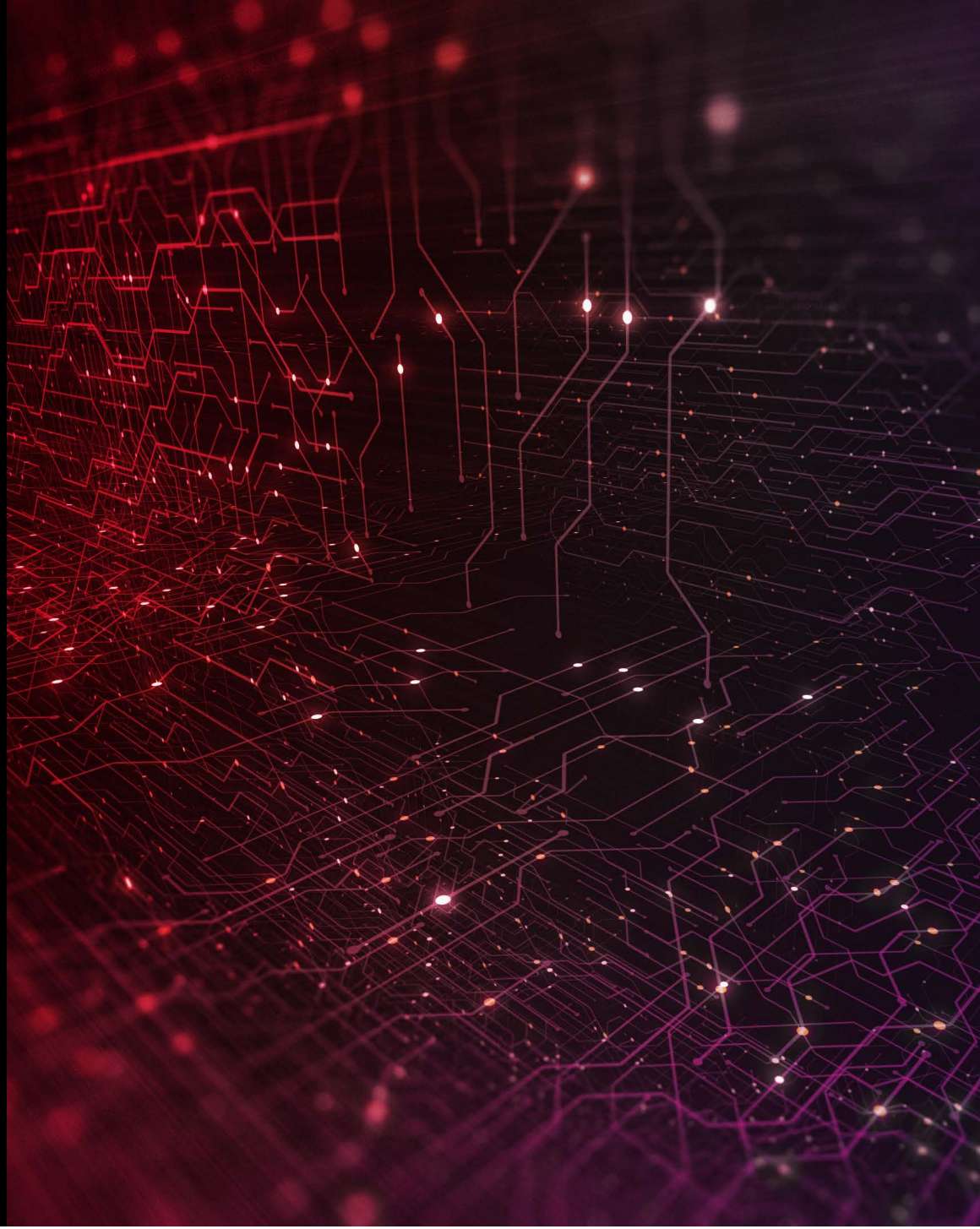
## Keysight: Your Test and Assurance Partner

How Keysight is uniquely positioned to support organizations as they enhance networks with AI

GO TO CONCLUSION >

CHAPTER 1

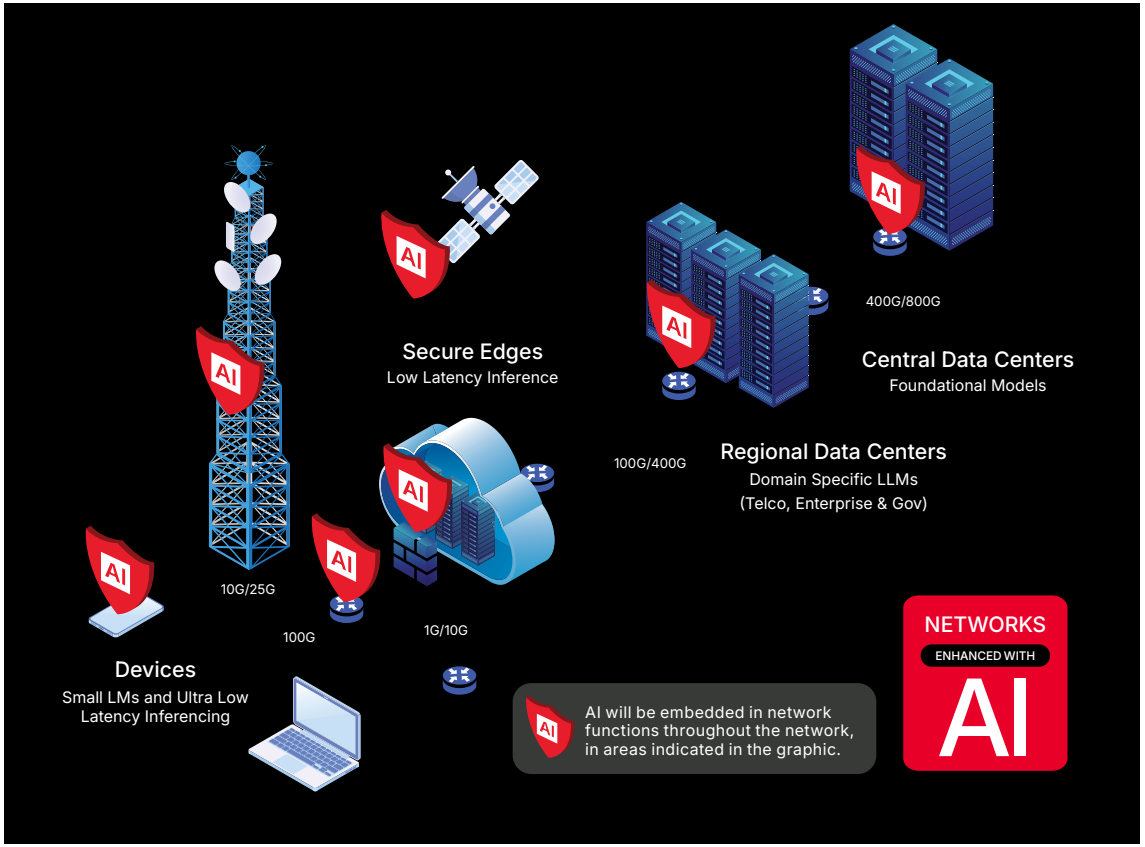
# Using AI to Benefit Networks and Operations



CHAPTER 1

# Using AI to Benefit Networks and Operations

**AI technologies are being integrated into networks as tools to enhance, automate, and optimize aspects of network management, performance, and security. These network functions leverage AI's capabilities, such as machine learning, data analytics, and automation, to make real-time decisions, predict network issues, adapt to changing conditions, and improve overall efficiency.**



## AI capabilities are adding intelligence to the network with use cases spanning:

- **Security systems** to optimize policy and configuration management and enhance attack prevention and threat detection
- The **radio access network (RAN)** to enhance RAN performance and optimize energy efficiency through resource management
- The **IP transport network** to deliver intent-based networking and simplify policy and configuration management
- The **core network** to provide predictive insights and enhance lifecycle management and orchestration performance
- **Global navigation satellite systems (GNSS)** to enable precise positioning in complex areas, interference cancellation and mitigation, and spoofing attack prediction
- **Network management systems** to automate orchestrator and service assurance tasks, optimize configurations, predict faults, and analyze root cause of issues

## Challenges slowing AI adoption

While the opportunities and potential benefits of AI are large, its adoption is being hindered by these kinds of questions and uncertainties:

**Lack of trust in AI decisions and outcomes**
Are they reliable, fair, safe, and consistent?

**Transparency and explainability**
How and why did the AI system predict or decide that?

**Security**
Are malicious actors tricking AI into making wrong decisions?

**Privacy**
How is my data collected, stored, used, and shared?

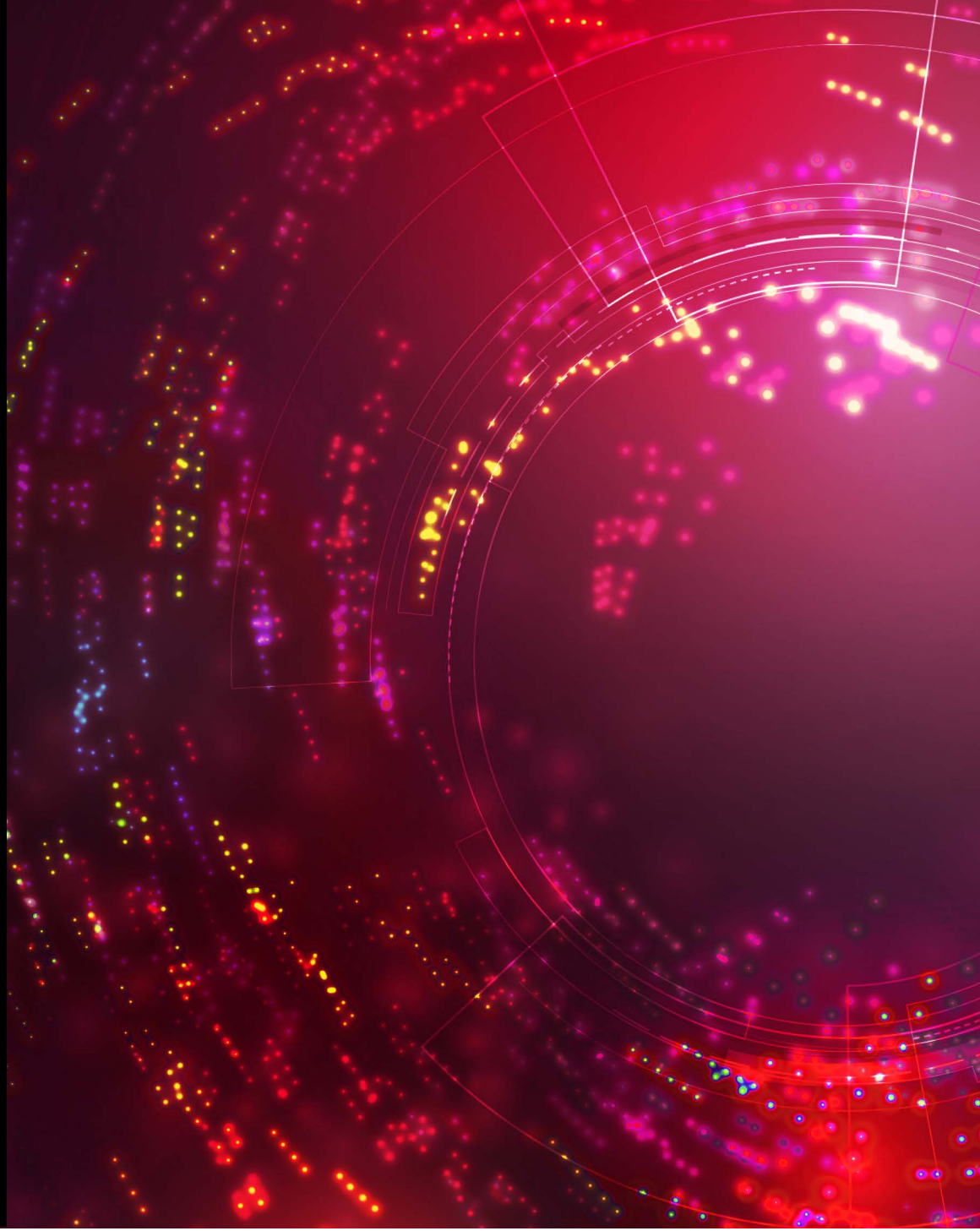
**Regulatory**
What will new regulations be and how will they impact ROI?

**Value versus cost**
Will significant investments in AI systems and networks pay off?

**Energy**
What will be AI's impact on sustainability and costs?

CHAPTER 2

# Role of Test and Assurance



CHAPTER 2

# Role of Test and Assurance

**All eyes are on testing to help address AI's adoption challenges and ensure that networks enhanced with AI are robust, trustworthy, and ready to support heavy investments.**

Testing efforts are already underway to validate performance and compliance with standards and regulations, and mitigate live network surprises in the face of real-world scenarios.

Continuous testing and assurance throughout the lifecycle will play an outsized role given the dynamic nature of software-driven, distributed, and multi-vendor networks. As AI enhances autonomous network operations and drives frequent, real-time changes in an effort to optimize performance, every change demands constant validation. Network operators need to understand in real time whether affected elements still interoperate, maintain performance levels, and remain secure. Continuous testing makes this possible by quickly identifying issues before they become costly failures.

Test and assurance play an important role in overcoming the challenges that are slowing AI adoption by building trust in AI, increasing transparency in its operation, and enhancing governance. The methodologies being used span realistic emulation, use of synthetic test data, continuous testing and automation, active testing, and non-functional testing. Let's explore the role of each in helping to overcome AI adoption challenges.

**ACCELERATE TIME TO MARKET**
Deploy new products and services in weeks with automated testing

**REDUCE COST AND COMPLEXITY**
Manage vendor and provider combinations to keep costs in check

**OPTIMIZE USER EXPERIENCES**
Rapidly pinpoint and resolve issues to optimize user experience

**HARDEN SECURITY DEFENSES**
Prepare for malicious cyberattacks at any stage in the process

Test and assurance help overcome the challenges of accelerating technological change to innovate faster, reduce costs, deliver flawless user experiences, and reduce cybersecurity risks in every step of the technology lifecycle, from lab validation to field acceptance and deployment in the real world.

# Key AI testing methodologies and capabilities

## Realistic emulation and simulation using network digital twins

Network digital twins are emulated replicas that serve as a "known good reference" for the network and traffic. They support realistic, low-cost, and risk-free testing of networks built for or enhanced with AI. Digital twins make it possible to assess AI solutions and network behavior, performance, security, and efficacy ahead of live deployment. For example, data center back-end interconnect fabrics can be tested using extended processing unit (xPU) emulators instead of purchasing actual graphics processing units (GPUs) and compute servers.

## Synthetic test data

Synthetic test data simulates real-world traffic and data for testing. Using data that is free of personally identifiable information but mimicking real data characteristics, it is possible to conduct controlled, repeatable network and system testing, especially when real data is unavailable, sensitive, or insufficient. For example, synthetic test data can generate application security traffic to test known and unknown attacks and evasion techniques in Layer 4–7 traffic emulators.

## Continuous testing and automation

Continuous testing executes automated tests at every stage of the lifecycle to ensure quality, functionality, and performance throughout the delivery pipeline. It serves as a key pillar of DevOps and lab-to-live testing, integrating with continuous integration (CI) and continuous deployment (CD) processes to detect and address issues early. This minimizes risks and keeps devices or systems in a deployable state, ready for the live network.

## Active testing

Active testing injects small amounts of synthetic test traffic into the network to emulate network functions and usage patterns. This generates predictive data to proactively monitor performance, SLAs, and AI-orchestrated network changes. Active testing reinforces AI decision-making through a closed-loop system by quickly identifying and isolating potential faults before they impact the network, offering positive and negative feedback in the process.

## Non-functional testing

Non-functional testing evaluates how well networks built for AI or enhanced with AI perform under real-world conditions. This testing assesses operational aspects like performance, scalability, security, and reliability, ensuring safe, large-scale commercial deployment.

# Testing in the AI network lifecycle

Testing plays a pivotal role in the AI network lifecycle by addressing realism, scale, resiliency, and security efficacy. This contributes to solving fundamental challenges that delay AI adoption and limit its operational use.

Rigorous testing throughout the entire AI lifecycle — from Day 0 design and development to Day 1 deployment and Day 2+ operation — can safely unleash AI's potential while mitigating associated risks.

In the **design and develop phase**, digital twins and emulation solutions simulate networks in a risk-free environment, providing realism and testing accuracy at a fraction of the cost.

The **deployment phase** sees automated continuous testing validate the reliability of AI solutions both pre- and post-deployment, providing the non-functional scalability, resiliency, and security testing critical for safe launch and operation.

Finally, in the **operation phase**, active testing proactively monitors, optimizes, and reinforces AI to ensure it continues to perform as expected and provides feedback loops for continuous AI model improvements.

A continuous testing and improvement loop from design to production ensures networks evolve safely as AI is adopted.

| | Day 0 | Day 1 | Day 2+ |
|---|---|---|---|
| **AI lifecycle** | Design/Develop | Stage/Deploy | Operate/Maintain |
| **Role for testing** | Model/Evaluate/Test | Validate (Pre and Post) | Monitor/Optimize/Reinforce |
| **Challenges testing solves** | Realism/Cost/Accuracy | Scale/Resilience | Efficacy/Transparency |
| **Methodology** | ← SHIFT-LEFT (TEST EARLY) | | SHIFT-RIGHT (TEST IN PRODUCTION) → |

**Digital twins**

(Emulators/simulators and traffic generators)

Allow realistic network design, simulation/emulation, and testing in a risk-free, low-cost virtual environment

**Continuous testing**

(Lab-to-live automated test solutions)

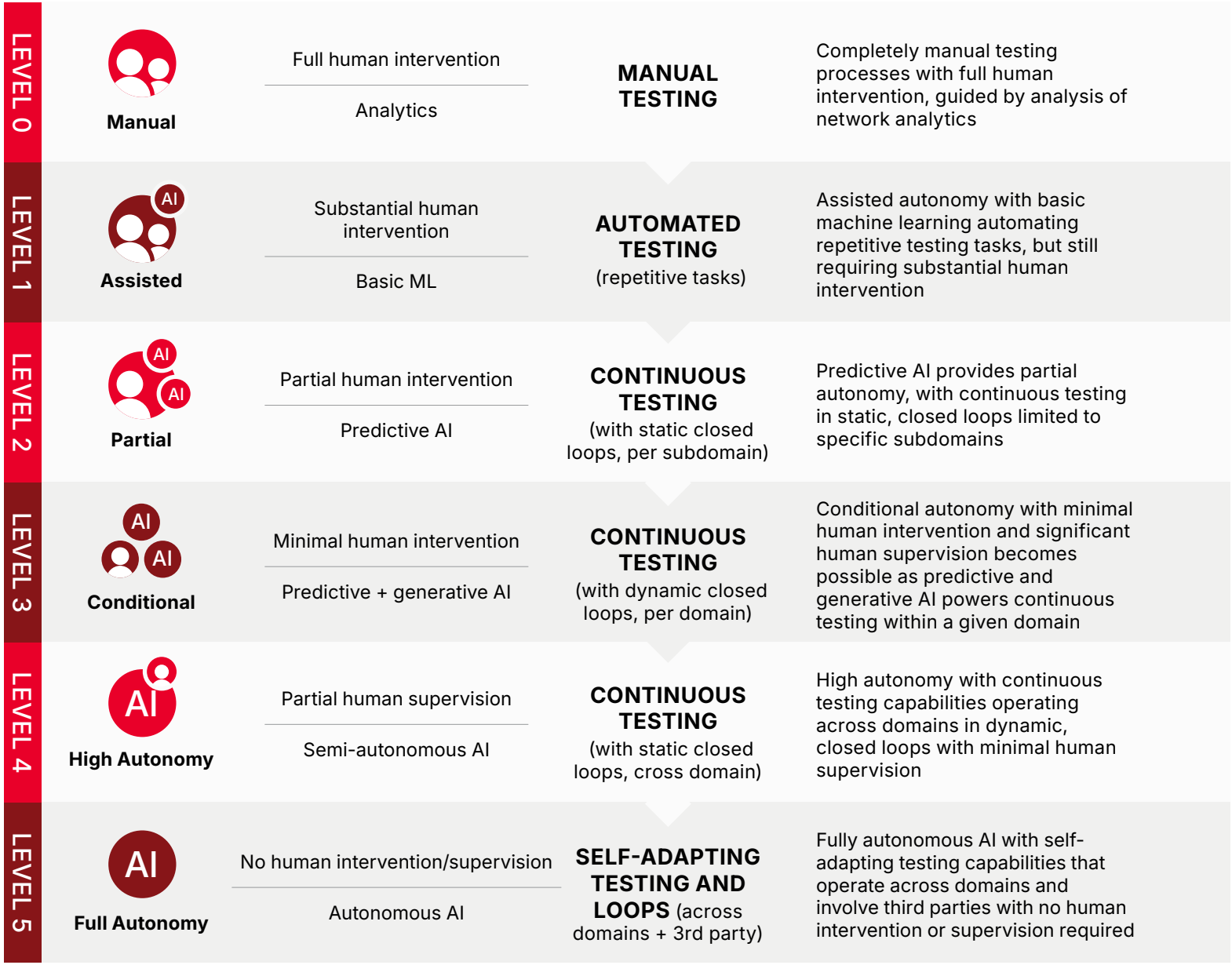
Automated testing to continuously validate efficacy, isolate issues, revalidate changes, and provide feedback loops

CONTINUOUS IMPROVEMENT

# Testing AI-enhanced autonomous networks

Network operators have successfully implemented lower levels of autonomy that decrease manual efforts but still require human intervention. The goal is to continually progress toward full, level 5 autonomy, where AI systems can operate with minimal or no human supervision.

Testing is the linchpin for realizing this vision and safely guiding the journey. A robust testing framework can provide the trust, transparency, and governance necessary for each stage of AI adoption. The graphic illustrates how achieving higher levels of automation involves evolving from manual to fully automated testing.



CHAPTER 3

# Recommendations: Testing and Assuring Networks Enhanced with AI

CHAPTER 3

# Recommendations: Testing and Assuring Networks Enhanced with AI

**In customer engagements, Keysight is seeing the addition of various network functions enhanced with AI.**

Let’s review some examples of current practices and recommendations for testing to ensure network function performance.

# Security firewall / gateway network functions

**AI enhancements:** Manual misconfigurations and thousands of overlapping rules and policies cause 99% of firewall breaches, according to Gartner. AI assistants simplify and optimize complex, error-prone policy and configuration management, and troubleshoot overlapping security rules. AI/ML is enhancing prediction and prevention of advanced and unknown threats, including AI-generated attacks, which are incredibly difficult, time-consuming, and costly to detect without using AI.

AI implementations for security devices and solutions are new, and proactive validation will increase user trust that it is protecting the network effectively.

## Testing recommendations:

Use realistic traffic and attack generation to validate:

- AI changes are implemented correctly
- Efficacy of AI predictive blocking
- Performance impact of using AI
- Any AI hallucinations or laziness

EXAMPLE

### Validating AI next-generation firewall security with attack emulations

**AUTOMATED AND CONTINUOUS SECURITY TESTING**

Realistic user traffic and attack generation validates

- AI changes are implemented correctly
- Efficacy of AI predictive blocking
- Traffic performance impact
- Hallucinations or laziness

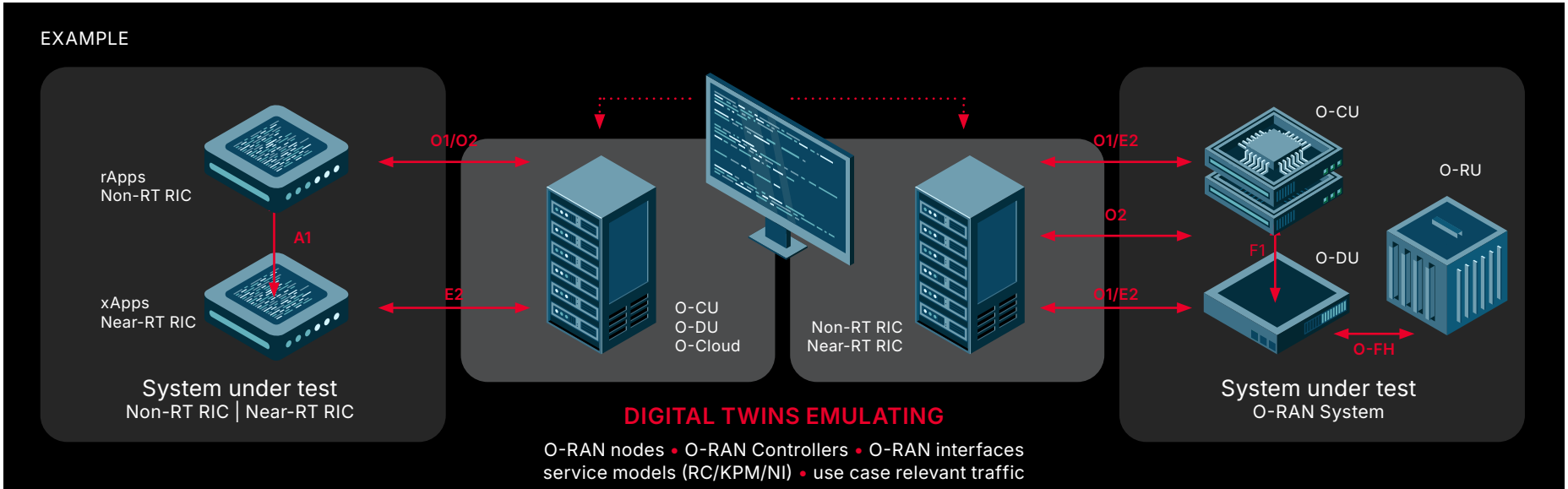
Tests using emulated traffic validate that AI assistant-driven firewall changes do not compromise the network's security or performance. Realistic line rate traffic and attack traffic generation validate that changes are implemented correctly and the performance and accuracy of the firewall blocking is met. Testing should be done continuously against different AI models and AI assistant prompt inputs to validate policies are enforced.

# Open RAN RIC network functions

**AI enhancements:** New RAN intelligent controllers (RICs) enable AI/ML-based near-real-time xApps and non-real-time rApps to control radio resource management decisions that result in enhanced RAN performance and optimized energy efficiency. xApps require 10 milliseconds to 1 second response times, while rApps handle tasks tolerating response times of 1 second or more.

## Testing recommendations:

- Use realistic open RAN network and use case traffic emulation
- Validate the RIC, xApps, and rApps for standards compliance and interoperability
- Stress test for commercial deployment readiness including non-functional tests for performance, adversarial scenarios, what-ifs, and resilience



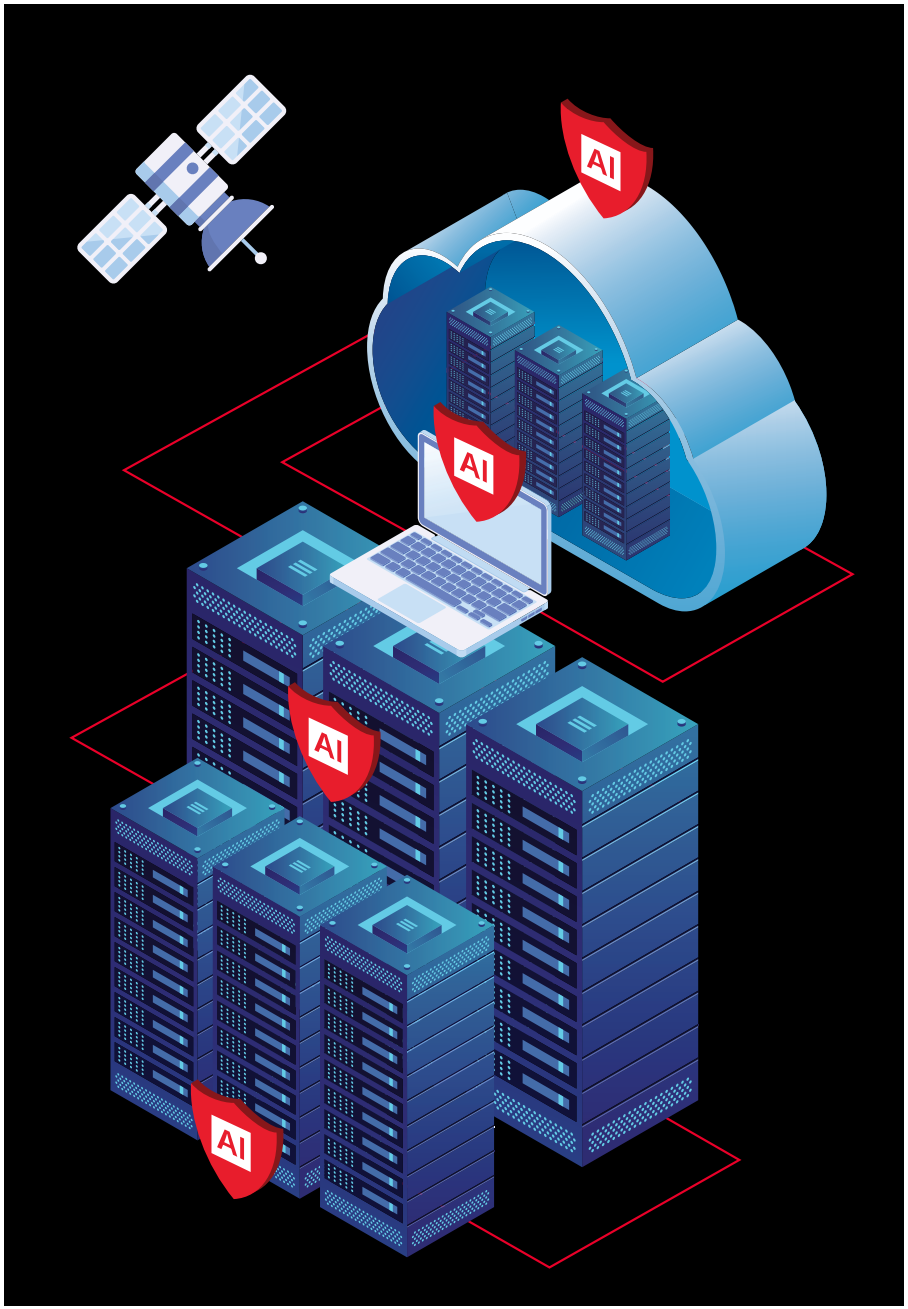

Digital twins realistically emulate the wider open RAN network, including the RU, CU, and DU nodes, and emulate RIC functions and traffic, allowing for two-way testing. Vendor and app developers' RIC and xApps or rApps can be safely tested in an emulated environment to validate and stress test the solutions for commercial deployment readiness, including non-functional tests for performance, adversarial scenarios, what-ifs, and resiliency. Digital twins also enable CU, DU, and RU vendors to validate support for O-RAN standards-based RIC interoperability.

# 5G core network functions

**AI enhancements:** The new Network Data Analytics Function (NWDAF) supports AI/ML predictive insights and actions for dynamic network function and service lifecycle management and orchestration to enhance performance and efficiencies.

## Testing recommendations:

- Validate AI/ML models for both efficacy and interoperability
- Use synthetic test data to help efficiently train and retrain the models




# Network orchestrators

**AI enhancements:** AI/ML powers AIOps to automate network management tasks. By coupling this with active assurance using predictive analytics and actionable insights, self-optimization and self-healing actions can be implemented. This powerful approach allows network operators to confidently implement AI/ML-based tools on their journey to closed-loop automation.

## Network orchestration / AIOps recommendations:

Utilize active assurance to:

- Validate new network functions and create birth certificates before customer traffic is routed to them
- Monitor for and isolate any ongoing performance impacts and degradations
- Determine root cause by isolating faults through specific services, locations, and network functions
- Proactively test orchestrated network changes driven by AI recommendations and validate the efficacy of the change both before and after implementation

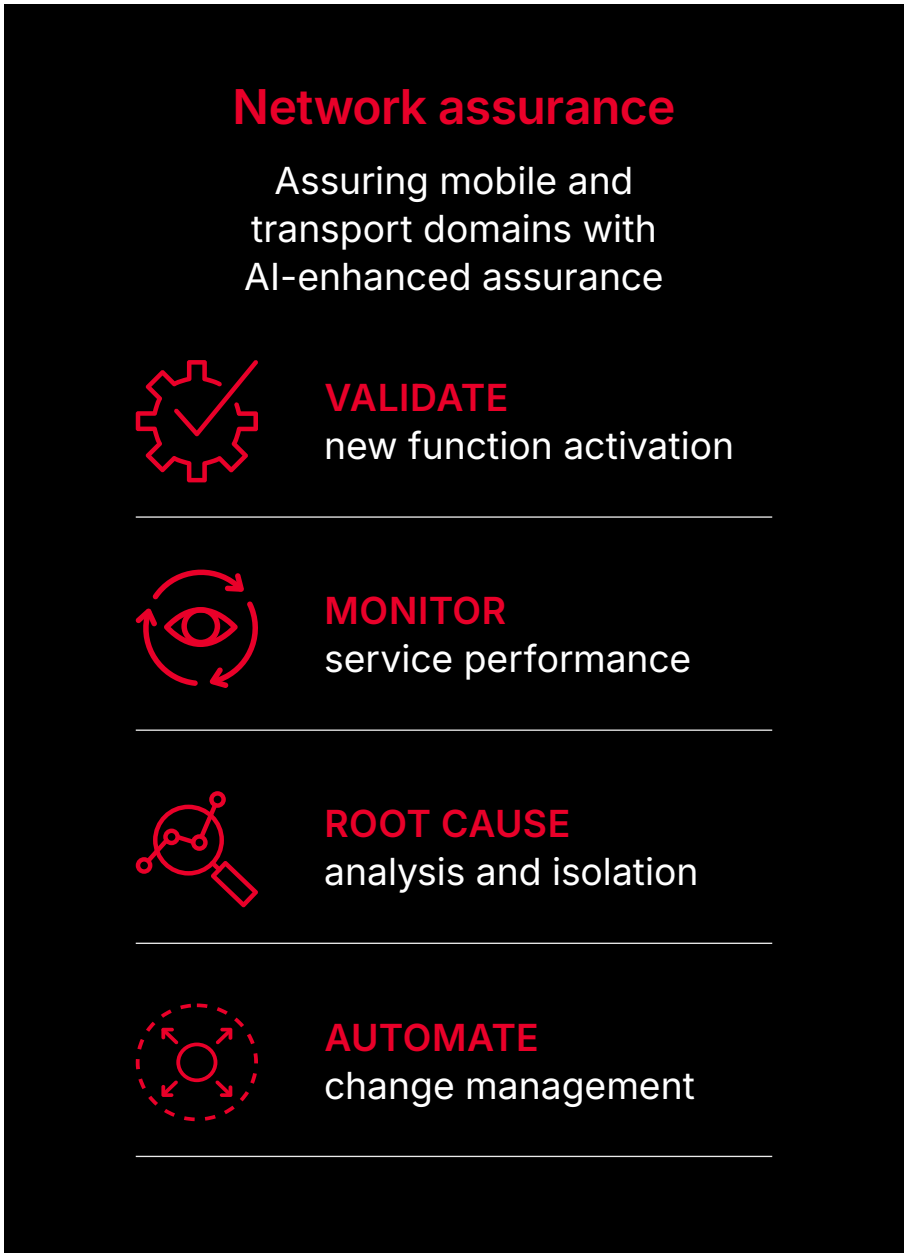
# AI enhances network assurance

**AI enhancements:** Trained AI/ML models are having a positive impact on network assurance by enhancing proactive identification, isolation, and root cause analysis of faults and issues before they impact network performance and user experience.

ML models enable adaptive thresholding of KPIs to learn what is normal/good for a given node in the network for a given time and day. When learned threshold events indicate unacceptable performance, closed-loop active test workflows are triggered to isolate faults and send root cause reports to operations for either automated or manual resolution.

The thresholds learned in the monitoring and fault isolation steps are used to continuously update the thresholds used for automated activation and change management scenarios.

AI/ML also creates new efficiencies through enhanced automation, alarm management, and intelligent prioritization.



# Keysight: Your Test and Assurance Partner

AI's demands are driving a transformation of networking infrastructures, introducing challenges and opportunities. Though these changes unlock unprecedented automation, rigorous testing is essential to accelerate AI adoption and ensure networks enhanced by AI are robust, secure, and trustworthy.

As a neutral and trusted industry leader, Keysight brings deep expertise in navigating AI's impact on networks. With a vendor-agnostic approach and cutting-edge test and assurance capabilities, we are uniquely positioned to support organizations as they confidently embrace AI-driven advancements.

**Keysight is unlocking the power of AI across networks and the infrastructure supporting modern services:**

- In **wireless networks**, our digital twin traffic and network emulators create realistic, repeatable test environments to validate AI-driven networks and AI-enhanced equipment.
- In **live operational networks**, our service assurance solutions enable continuous validation and feedback loops, ensuring trust, transparency, and reinforcement of AI-driven autonomous actions.
- Our **automation frameworks** provide continuous testing capabilities, foundational for AI to supercharge autonomous processes across labs, testing environments, and the entire lifecycle.

## Testing and assuring networks enhanced with AI

| AI-enhanced security systems (NGFWs) | Open RAN RIC and AI/ML apps | 5G Core NWDAF for AI/ML | AI assurance |
|---|---|---|---|
| Security digital twin attack and application performance tester | O-RAN digital twin network and traffic emulators | 5G Core digital twin network and traffic emulators | Service assurance solutions powered by active test |

## About Keysight

Keysight is a leading global provider of automated test and assurance solutions for networks, cybersecurity, and positioning. We provide innovative products, services, and managed solutions that address the test, assurance, and automation challenges of a new generation of technologies, including 5G, edge computing, cloud, autonomous vehicles, and beyond. From the lab to the real world, Keysight helps companies deliver on their promise to their customers of a new generation of connected devices and technologies. For more information visit: www.keysight.com.

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.

This information is subject to change without notice. © Keysight Technologies, 2018 – 2026, Published in USA, June 16, 2026, 7126-1106.EN