

Intelligent framework for autonomous intelligent networks

An autonomous intelligent network is a fully automated, zero-touch deployment and operations infrastructure.

TM Forum has defined a 6-level autonomous network maturity model, with level 5 bringing full autonomy across all services and domains.¹

Introduction

The telecommunications service provider industry (telco) is at an inflection point, powered by the complexities of modern technologies including 5G and artificial intelligence (AI), the proliferation of edge computing, and the increasing demand for cloud-native agility. Automation is no longer a competitive advantage, but a foundational requirement for telco service providers to reduce operating expenses (OPEX) while simultaneously investing in new technologies.

Virtualization and cloudification have provided the platform for automation, open application programming interfaces (APIs) the programmability and integration capabilities, and artificial intelligence and machine learning (AI/ML) is now providing the intelligence for autonomous decision loops.

Telco service providers often struggle to know how to get started among so many possible technologies, techniques and approaches to automation. They need to integrate these to deliver consistent, security-focused, and autonomous intelligent networks that can grow at the speed of innovation.

Automation maturity levels

Achieving a high degree of automation maturity is a multiyear journey. [TM Forum's autonomous network \(AN\) maturity model](#)¹ provides a roadmap, but telco service providers need guiding principles and best practices to transition, with most starting from partial automation (level 2), to conditional automation (level 3), to high automation (level 4), and ultimately full automation (level 5). A brief explanation of the maturity levels are:

Manual and assisted operations levels 0-1

Level 0 describes manual operations with no automation, while level 1 involves assisted operations with some automation and a need for human intervention.

Partial autonomous network level 2

The network has closed-loop automation for certain specific tasks or within certain domains, having the ability to execute some processes automatically. Humans still handle many tasks, and automation is often reactive and prescribed.

Conditional automation level 3

Awareness and adaptability are introduced, with the network sensing real-time environmental changes including traffic patterns, faults, and user behavior, and optimizing itself accordingly. Level 3 systems implement intent-based closed-loop management where service providers define high-level objectives and the system conditionally makes decisions to fulfill those intentions.

Most service providers are still in the early stages of automation, with the vast majority having not progressed beyond partial automation.

Highly autonomous network level 4

Autonomy reaches a high degree across multiple domains, with the network handling complex, cross-domain processes and scenarios with minimal human intervention. Level 4 systems feature predictive or proactive automation, and use AI to anticipate issues before performance is affected. Achieving level 4 requires closed-loop control in each domain, but also coordination between domains by an orchestration layer of automation and a healthy knowledge system.

Full automation level 5

Full automation means the network is fully autonomous across all domains and the entire service life-cycle, including making business-level decisions on its own. This is more of a future vision.

The vast majority of service providers have not progressed beyond partial automation. While they have automated certain processes, their operations still rely heavily on human intervention and isolated automation tools. Some service providers are experimenting with conditional automation in specific domains, such as automated scaling of virtual network functions (VNFs), cloud-native network functions (CNFs), and AI-assisted alarm correlation. Highly autonomous networks are rare, and mostly confined to trials or limited domains.

Challenges of deploying and operating autonomous intelligent networks

Transitioning to an autonomous intelligent network presents significant challenges for service providers, but potentially yields significant opportunities. Understanding both is crucial for a successful strategy:

Technical complexity and integration

Autonomous operations require the integration of a variety of systems, including traditional operational support systems and business support systems (OSS/BSS), new AI and analytics platforms, orchestrators, and domain controllers. As many service providers suffer from fragmented systems, toolsets and stand alone data, this presents a foundational challenge of unifying data management across the network.

A related challenge is the shortage of off-the-shelf automation components for critical functions, including intent engines and cross-domain orchestrators. This is a nascent area, with emerging technologies and approaches that are not yet widely deployed. Service providers often have to build custom solutions, or integrate multiple vendor-specific solutions, both of which increases complexity.

Conventional infrastructure and processes

Service provider networks are typically a mix of outdated physical network elements (e.g., 4G/3G systems) and cloud-native functions (e.g., 5G). Older systems may not support the telemetry or dynamic configuration interfaces needed for closed-loop autonomous intelligent networks.

Additionally, service provider change management processes have historically been cautious and manual so as to avoid outages. Moving to intent-driven changes and automated remediation can clash with existing practices and culture. Service providers often cite traditional mindsets and processes as an obstacle towards automation. The network can not be autonomous if the organization insists on manual checkpoints at every step.

An autonomous intelligent network is where everything is automated, with data analytics and AI models providing deep learning (DL) for advanced decision making, and autonomy and governance providing policies to enforce compliant deployment and operational decisions and actions.

Organizational and skills gaps

Autonomy demands a new skillset in the service provider workforce, shifting toward data scientists, automation engineers, AI specialists, and fewer command line interface (CLI) configuration-type of personnel. Most service providers have a critical skills shortage in areas such as artificial intelligence and machine learning (AI/ML), and also need to adapt their organizational structure to become cross-domain to facilitate effective automation.

Breaking down traditional silos of the radio access network (RAN), core, and transport teams is needed to foster an automation culture. However, organizational inertia can be high, with staff potentially resisting due to fear of job losses. Therefore change management and upskilling programs are essential, but can be challenging to execute at scale.

Trust, transparency, and regulation

Handing control to algorithms raises questions of trust and accountability. Ultimately, service providers have to ensure AI does not make a bad decision that causes an outage, as networks have become business critical and form an integral part of society and economies. In order to build trust, there is a need for explainable AI in operations so that humans understand why an autonomous agent or process made a decision.

Regulatory bodies in some countries may also require a level of human oversight, especially in areas affecting safety (e.g., emergency communications). Also, an autonomous network could potentially react to a cyberattack faster than humans, but if proper security is not in place, the automated closed-loops could be targets for exploitation (e.g., feeding false data to AI to mislead it). Thus, comprehensive governance and security frameworks must be in place.

Uncertainty of investment and return on investment (ROI)

Implementing autonomous networks requires substantial investment in new systems, including AI platforms, data lakes, orchestration software, and the overhaul of existing processes.

ROI and timeline is often difficult to quantify, as they accrue with time, reduced OPEX, fewer outages, and an accelerated time to revenue for new services. Telco service providers can struggle to build a solid business case to justify the move towards an autonomous intelligent network, especially as most have invested heavily on 5G spectrum and deployments.

Benefits of autonomous intelligent networks use cases

Operational efficiency and cost reduction is seen as the most immediate benefit of autonomous intelligent networks. Automation significantly reduces network deployment time and streamlines operation processes. A related benefit is an accelerated time-to-market because services can be deployed in less time when compared to conventional means. Improved network resiliency and increased performance are achieved as the network is able to continuously monitor itself and make adjustments. These advantages help contribute to the enhanced customer experience and help generate new revenue opportunities, including network-as-a-service (NaaS) that are offered on a per customer basis to deliver a specific service level agreement (SLA).

The following autonomous intelligent network use cases being adopted, especially in more advanced markets:

By adopting Red Hat's autonomous intelligent networks framework, telco service providers can automate operations and processes to cut costs and accelerate new service deployment.

Radio access network (RAN) optimization

Open RAN and the RAN Intelligent Controller (RIC) support use cases including automated interference management, anomaly detection, and dynamic spectrum allocation. AI-driven RAN optimization can reduce dropped calls and improve throughput by dynamically tuning parameters. Radio network optimization delivers measurable outcomes by double-digit percentages without human intervention.

Predictive maintenance and self-healing

Telco service providers are implementing AI models to predict equipment failures and to trigger preventive maintenance to dramatically reduce outages. This leads to significant reductions in network incidents.

Service assurance and customer experience

A major benefit of implementing an autonomous intelligent network is to improve customer experience by resolving issues before they occur. Traditional operations react after a user complaint. With an autonomous intelligent network, using AI to correlate network events and user experience metrics can fix problems preemptively, reducing outages and ultimately improving customer satisfaction.

Dynamic resource optimization and slicing

AI-based closed loops are being used to auto-scale 5G network slices and allocate resources on demand. Autonomous slice management is where the network can instantiate or adjust a 5G slice based on traffic predictions, for example, spinning up extra capacity then tearing it down with no human in the loop. This yields significant OPEX savings and increased agility, turning networks into elastic platforms.

Energy efficiency

Automation is being used to achieve telco sustainability targets and objectives. AI can autonomously turn off parts of the network during low traffic periods, for example, shutting down RAN sectors and cells at night to save energy. AI energy management features can cut energy usage by double-digit percentages, contributing to OPEX reduction and sustainability objectives.

A framework to realize an autonomous intelligent network

Red Hat has developed an autonomous intelligent network framework using a modular, open source approach. This framework is not a single product but a combination of technologies, architecture guidelines, and ecosystem partnerships. The philosophy of the framework is to provide end-to-end automation and AI-driven operations on a common cloud-native platform, using open-source innovation and avoiding proprietary software and hardware.

Red Hat OpenShift

[Red Hat® OpenShift®](#) serves as the common telco cloud-native foundation of the framework, providing a consistent and scalable runtime environment for the deployment of CNFs (5G, RAN, OSS/BSS), AI and applications across a service provider's network. A unified experience is crucial to achieving an autonomous intelligent network so that automation policies can be applied uniformly across the network.

Red Hat OpenShift also includes [OpenShift Virtualization](#) which allows for the coexistence of virtual machines (VMs) and containers. This helps with the gradual transition to cloud-native and ensures vendor-agnostic flexibility.

Red Hat's approach becomes the natural choice for telco service providers who view open source as a strategic advantage.

Red Hat Ansible Automation Platform

[Red Hat Ansible® Automation Platform](#) plays a pivotal role in orchestrating and executing network automation tasks. Ansible Automation Platform uses agentless, declarative automation scripts and has wide adoption in network configuration automation. Ansible Automation Platform serves as the unifying automation layer that can configure and integrate across various network elements defined within the framework, and provides closed-loop execution when the network decides a change is needed.

[Event-Driven Ansible](#) can respond in real time to events and alerts. If a monitoring system detects a failure, an event triggers Event-Driven Ansible to automatically instantiate a new instance of that function, effectively self-healing the network. [Red Hat Ansible Lightspeed](#) (an AI-powered code assistant for Ansible Automation Platform) provides AI-driven automation within the framework, allowing networks to self-heal, self-optimize, and proactively respond to changes.

Red Hat Advanced Cluster Management for Kubernetes

[Red Hat Advanced Cluster Management for Kubernetes](#) is designed to address multicluster and multicloud management of distributed telco service provider networks. In the framework, Red Hat Advanced Cluster Management provides a single control plane to manage the lifecycle, configuration, and policies of OpenShift clusters at scale. Having a centralized and automated cluster management is vital for autonomous intelligent networks.

Red Hat Advanced Cluster Management integrates with Ansible Automation Platform to facilitate the automatic scaling out of computing capacity when needed, and making it more effective to apply consistent autonomous operations including rolling updates or auto-scaling policies.

Red Hat AI

[Red Hat AI](#) provides the AI engine component of the framework, and delivers intelligent decision-making. [Red Hat OpenShift AI](#) provides a set of capabilities to operationalize AI on Red Hat OpenShift, including the necessary tools for the training and deployment of AI/ML models within the telco service provider environment.

With OpenShift AI, telco service providers can feed network telemetry into an AI pipeline running on Red Hat OpenShift, train models for anomaly detection and traffic prediction, then deploy models as containerized microservices that continuously analyze network data in real-time. Red Hat AI enables AI at scale for operations, transforming the network to be AI-native.

Beyond technology, a Red Hat framework relies on an open ecosystem of partners and access to vibrant open source communities. Red Hat recognizes that telco service providers will implement autonomy with multiple vendors and system integrators, so collaborates with suppliers, independent software vendors (ISVs), and standards bodies to ensure interoperability.

Conclusion

Telco service providers should transition through the different levels of autonomy incrementally, use case by use case. Rather than trying to automate everything at once, service providers should identify high-value use cases for automation and tackle them 1 at a time.

Red Hat believes in an evaluation methodology where potential use cases are categorized based on business value (effect on OPEX, customer experience, and revenue potential) and technical feasibility (is the technology ready, and is the data available), and prioritize those.

Red Hat supports the notion of starting in one domain, achieving a specific and measurable level of autonomy, then federating across domains. For instance, implementing conditional automation (level 3) in the service provider core to handle automated scaling and healing of core network functions, and separately in the RAN using automation for coverage and capacity optimization. Once each domain has a degree of closed-loop control, service providers can then connect them together through higher-level orchestration to transition to a highly autonomous network (level 4).

By adopting Red Hat's autonomous intelligent networks framework, telco service providers gain access to a dynamic and open foundation on which to embark on their automation journey. They can achieve short-term gains by automating processes to cut costs and reduce human error, and position themselves for long-term innovation by taking advantage of AI and cloud-native agility.

Learn more

[Contact](#) a Red Hat representative today

[Watch](#) a video: Automation & Zero-Touch Provisioning for the RAN

[Read](#) an overview: Maximizing the value of telecommunications automation

[Check out a blog](#): Telco autonomous networks choosing the right cloud and framework



About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with [award-winning](#) support, training, and consulting services.

f facebook.com/redhatinc
x @RedHat
in linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

**Europe, Middle East,
and Africa**
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com