



www.pipelinepub.com

Volume 22, Issue 11

From Legacy OSS to Autonomous Networks: Rethinking the AI Foundation

By: [Ram Ramanathan](#)

AI is already transforming network operations, but realizing its full value begins with understanding the problem it is meant to solve. AI assistants, copilots, and analytics tools offer meaningful benefits to teams managing increasingly complex networks with limited resources. These technologies can surface relevant information, summarize events, identify anomalies, and recommend next steps. While such improvements represent a practical first step toward AI adoption, they should not be confused with autonomous operations. True autonomy requires a fundamental change in how networks are managed and operated. Faster processes layered on top of fragmented data, manual intervention, and reactive workflows may improve efficiency, but they do not transform operations.



This distinction is becoming increasingly important for communications service providers. Many organizations are turning to AI extensions as the fastest path toward automation and operational transformation. While these capabilities deliver clear benefits, a more strategic question remains: can the operational architecture beneath them support the next generation of intelligent networks, which rely on real-time data, contextual understanding, and increasingly autonomous decision-making? AI extensions may be a practical starting point, but they are unlikely to deliver the full level of autonomy operators ultimately seek. Achieving that objective requires a foundation built on unified data, contextual awareness and automation.

When AI Runs into Legacy Limitations

Operators have made significant investments in infrastructure, operational systems, processes and skills over many years. Those investments cannot simply be discarded as new technology cycles emerge, making the idea of introducing AI into existing OSS environments understandably appealing. AI extensions offer a relatively efficient and minimally disruptive way to introduce new capabilities into established workflows while reducing manual effort and improving productivity.

But achieving autonomous operations requires more than incremental efficiency gains. Traditional OSS platforms were designed to support human-led, reactive workflows rather than real-time, autonomous decision-making. AI extensions frequently rely on customized integrations connecting multiple legacy systems together, making it difficult to create the unified operational environment autonomous networks require. As a result, AI often improves existing workflows without fundamentally redesigning them.

The consequences extend beyond technical complexity. Fragmented operational environments slow decision-making, increase operational costs, and make it difficult to scale automation across the network.

In many environments, data remains incomplete, delayed, or disconnected from related systems. An AI assistant may successfully identify an anomaly, but engineers may still need to consult multiple operational systems to determine business impact, identify root cause, and execute remediation. The workflow becomes faster yet remains fragmented.

This is the central weakness of treating AI as an add-on rather than as part of a broader operational redesign. Extensions can improve access to information and streamline user interactions, but they do not automatically solve the underlying issues of fragmented data, limited context, and manual execution. In some cases, they may simply make existing processes more efficient rather than helping operators rethink how decisions should be made and acted upon.

As networks become more dynamic, distributed, and interconnected, these limitations become increasingly difficult to overcome through AI overlays alone. To move beyond incremental gains, operators must evaluate the operational foundation that supports AI, not just the AI capabilities themselves.

Autonomous Operations Require the Right Foundation

Autonomous operations require timely, trusted, and connected operational data across domains, systems, and network layers. Modern networks generate enormous volumes of telemetry, alarms, logs, performance metrics, configuration data, and service information. Collecting this information is no longer the primary challenge. The challenge is creating a unified view that enables AI to interpret conditions accurately and act with confidence.

AI systems must understand how events, services, and infrastructure relate to one another across the network in order to support meaningful autonomy. An alarm on a network component may indicate a hardware failure, a configuration issue, a capacity constraint, or a downstream service problem. Without visibility into broader operational context, AI can identify symptoms without understanding their significance.

This becomes even more important in today's multi-vendor, multi-domain environments. Modern networks span physical infrastructure, virtualized functions, cloud-native applications, transport networks, routing domains, and customer-facing services. Events occurring in one layer frequently affect another. A domain-specific view may fail to reveal how a performance issue affects service quality, customer experience, or operational risk elsewhere in the network. Autonomous operations require end-to-end visibility and systems capable of understanding these relationships. This is where observability becomes more important than traditional monitoring. Monitoring tells operators that something happened. Observability helps them understand why it happened, what systems are affected, and how events relate to one another. In cloud-native and highly distributed environments, operational conditions can change rapidly, and components may be dynamic and short-lived. Continuous telemetry, analytics, and event correlation provide the context required for both human

decision-making and AI-assisted automation.

Moving from Insight to Action

Insights alone do not create autonomous operations. To move from reactive management toward autonomy, insight must be connected to action. This does not eliminate human oversight. In many operational environments, especially those supporting critical services, human expertise remains indispensable. Rather, it elevates automation from a collection of isolated scripts into a coordinated operational capability.

With the right foundation in place, AI can support progressively more advanced forms of automation. It can reduce repetitive manual work, identify probable causes, recommend remediation steps, simulate the impact of operational changes, and initiate workflows with appropriate approvals. Over time, some workflows can evolve into closed-loop systems that detect, decide, and act within established policies and guardrails.

This incremental progression is both realistic and manageable. Network operations teams need confidence in the data, recommendations, and automation logic before reducing levels of human intervention. Organizations can begin with targeted use cases such as fault correlation, predictive maintenance, lifecycle automation, or security compliance while maintaining human oversight. As trust and operational maturity increase, automation can gradually expand to support broader operational objectives.

A New Operating Model

The transition to autonomous operations represents a shift in operating model, not simply a technology upgrade. As a result, it requires new architectural thinking. Platforms supporting AI-driven operations need access to real-time data and the ability to ingest, correlate, and analyze information from multiple operational systems. They must integrate openly with OSS platforms, business systems and automation tools while allowing operators to embed operational knowledge into workflows efficiently. They also need to support multiple levels of control, from recommendations and guided workflows to fully automated execution where appropriate.

Emerging operational platforms are beginning to combine observability, analytics, automation, and AI within more unified environments. While approaches vary, the common objective is reducing fragmentation and improving the movement of information between systems. The broader goal is not replacing every existing investment, but ensuring legacy systems no longer constrain how AI accesses data, understands context, and executes workflows.

A practical approach is often incremental. By preserving and augmenting existing investments, operators can prioritize use cases according to operational need, business value, and organizational readiness while gradually establishing a more unified operational fabric.

The Journey from Reactive to Autonomous Networks

Most network operations environments remain largely reactive today. Teams respond to alarms, investigate incidents, and restore services once problems become visible. AI and automation create an opportunity to move earlier in the lifecycle by identifying patterns, detecting degradation, anticipating capacity constraints, validating changes, and preventing issues before customers are affected.

Achieving autonomous network operations is an ongoing journey rather than a discrete destination. Organizations must progressively develop the ability to identify and resolve issues before they occur.

Doing so can reduce service disruptions, lower operational effort, and improve customer confidence. AI and automation support this evolution by helping teams identify trends, detect anomalies and forecast potential issues earlier in the operational lifecycle.

Autonomy does not mean removing people from the process. The most effective operating models will continue to combine automation with human judgment, particularly where risk, security, compliance and customer impact are involved. Engineers will remain responsible for defining policies, managing exceptions and continuously refining how intelligent systems operate.

AI extensions can play a valuable role in this transition. They help teams become more efficient and more familiar with AI-assisted operations. However, they should be seen as a step along the journey rather than the end goal. The larger objective is to establish the operational foundation that autonomy requires: unified data, contextual understanding, observability, automation, and governance.

The industry's challenge is no longer determining whether AI belongs in network operations. The challenge is ensuring that the operational foundation beneath AI is capable of supporting increasingly autonomous decision-making. Organizations that solve that challenge will be better positioned to transform AI from an efficiency tool into a genuine driver of operational autonomy.

Not for distribution or reproduction