From Outages to Outcomes

Building The Action Layer in Telecom Network Operations

> Network downtime today isn't driven by lack of data — it's driven by the gap between insight and action, especially across multi-vendor, multi-domain ecosystems. Closing this gap is where real business value is created

Ritesh Karan, Director of Telco Strategy and Presales, UST

Executive Summary

Telecom operators have invested heavily in monitoring systems, analytics platforms, and domain-specific tools that generate a constant stream of alerts. But alerts create awareness, not resolution. Teams still lose critical minutes interpreting alarms, correlating cross-domain impacts, and deciding next steps. In multi-vendor 5G environments, that delay between detection and action is now a primary driver of downtime. As Ritesh Karan, Director of Telco Strategy and Presales at UST, explains, "Most network downtime today is driven less by hardware failures and more by complexity of multi-vendor, multi-domain environments." He notes that alerts "show symptoms without context, root cause, or resolution steps — overwhelming teams with noise and slowing remediation. The real challenge is the delay between detection and action, which is where AI-driven automation becomes essential."

The Action Layer is designed to close this gap. It is a governed decision-and-execution plane that sits above existing OSS, assurance, orchestration, and ticketing systems. Using Agentic AI-based correlation to isolate likely causes and automation to trigger approved responses ensures every detected issue has a consistent, traceable path to remediation. For operators, this protects current investments, reduces mean time to repair (MTTR), and enables outcome-driven operations without replacing core tooling.

The State of Network Operations

Most operators run a mix of RAN, transport, IP, core, and cloud domains, each supported by different vendor tools, data formats, and operational workflows — these silos slow correlation when incidents span multiple layers and force teams to maintain parallel interfaces and playbooks. The result is fragmented visibility and inconsistent execution across the end-to-end service chain.

Alert volume continues to rise as networks densify and software-defined functions expand. During peak periods, operations centers may face thousands of alarms per hour, yet only a small fraction map to actionable incidents. Teams spend more time responding to alarms and less time executing improvements that directly affect the customer experience.

This overload necessitates heavy reliance on manual filtering, resulting in slow, inconsistent decision-making. Senior engineers spend a disproportionate amount of time filtering noise, and resolution quality often depends on a small group of senior specialists who understand how specific patterns behave in that environment. This makes operations fragile, limiting scalability.

Procurement teams feel the strain, as multi-vendor ecosystems significantly raise integration costs. Each new platform introduces a unique set of telemetry, APIs, and lifecycle requirements. Maintaining connectivity among legacy monitoring systems, orchestration layers, and ticketing tools becomes a persistent OPEX burden and slows modernization.

Additionally, these challenges slow down modernization efforts. Even when operators invest in advanced analytics or new orchestration tools, these solutions struggle to deliver their full value because the surrounding processes remain manual or disconnected. What operators need now is not another visibility layer, but a way to normalize insights across domains and convert them into reliable, governed actions. The Action Layer is designed to provide that structure.

Why Networks Still Fail

Network failures rarely stem from a lack of visibility. They stem from delays and inconsistent responses. Even when the correct data exists, teams still must interpret alerts, identify cross-domain patterns, and decide on remediation steps. This “last mile” between detection and action is where MTTR and end-customer experience converge.

Alerts typically show symptoms without context or recommended steps. AI correlation reduces noise and highlights likely causes, but intelligence

alone does not resolve incidents. Operators also need standardized, policy-approved execution so that responses are fast, repeatable, and auditable.

This combination is critical. Operators need intelligence that narrows down the problem and automation that delivers a reliable response. Without this, teams are left with knowledge that does not translate into action, and downtime remains higher than it needs to be.

Manual incident handling and troubleshooting remain common: engineers move between tools to validate impact, check history, coordinate across teams, and confirm compliance. Each handoff adds time. Different engineers may also respond differently to the same event, creating operational risk and unpredictable MTTR — a problem that worsens under strict service-level agreements and regulatory requirements.

Closing the detection-to-action gap requires both intelligence that narrows the problem and governed automation that consistently executes the correct response.

The Action Layer: From Detection to Resolution

The Action Layer serves as a unified decision-making and execution environment that integrates with existing OSS systems, orchestration tools, and monitoring platforms. It uses the information they already provide and applies AI and policy logic to determine the next steps. Ritesh explains that traditional tools focus on reporting and orchestration but often operate in silos tied to specific vendors or domains. UST's Action Layer "sits above these systems as a governed, vendor-neutral decision and execution plane."

Three core capabilities define it:

AI-driven correlation

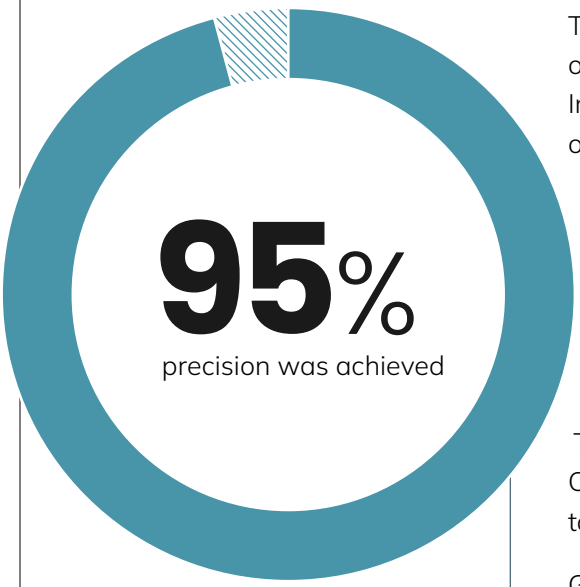
Reduces alarm noise, links related events across domains, and identifies likely root causes and recommended actions.

Policy-based automation

Executes responses only within pre-approved rules, with risk-based approvals, audit trails, and compliance checks.

Vendor-neutral integration

Applies the same policies and workflows across multi-vendor environments through standard interfaces, avoiding domain-by-domain rework.



as Ritesh highlighted real examples where predictive monitoring and preemptive fault resolution pinpointed root causes and recommended fixes.

The Action Layer turns fragmented visibility into unified, outcome-driven operations and improves how teams interface with existing systems. Instead of relying on custom scripts or vendor-specific workflows, operators can define policies centrally. These policies dictate how the network should respond to specific triggers. Because they reside in the Action Layer, they apply consistently across vendors and domains, improving predictability and simplifying governance.

AI correlation within the Action Layer does more than filter alarms, as it identifies relationships across the network, such as how a transport event may cause downstream service issues in the radio access layer. This gives teams actionable intelligence rather than isolated alerts. Operators can understand not only what happened, but also what is likely to happen next, and what the recommended response should be.

Governance features also allow for built-in controls for approvals, auditing, and compliance checks. Operators can implement guardrails that prevent automation from taking actions that do not meet internal standards. This allows large organizations to scale automation without increasing risk. Each action is recorded with full traceability, which supports operational reviews and external audits.

It can also support repeatable workflows. For example, a recurring congestion alert might require coordinated actions across multiple systems. Without the Action Layer, this process might involve several manual steps. Instead, the workflow can be automated using a single policy that triggers the correct response every time.

Building Blocks and Roadmap for Transformation

The Action Layer supports a phased adoption model, letting operators start with bounded, high-value workflows and expand automation safely over time. A typical transformation cadence looks like this:

First 90 Days: Quick Wins

Teams can begin with prebuilt playbooks that target common bottlenecks. These include SLA management, energy optimization, early fault detection, and noise reduction. Ritesh highlights real examples, in which predictive monitoring and preemptive fault resolution “identified faults up to 7 days early, pinpointed root causes, and recommended fixes with 95% precision.” Alarm noise reduction and automated ticketing “achieved 93% alert suppression,” which helped teams focus on the alerts that required meaningful action. These early improvements build trust in automation and reduce manual workloads.

First 180 Days: Smarter Scaling

After early successes, operators can expand automation into areas that require predictive decision-making. Predictive capacity and utilization playbooks help align scaling decisions with actual demand. This supports both OPEX and CAPEX planning. As Ritesh notes, these capabilities help operators "defer unnecessary expansions, reduce OPEX through better utilization, and make smarter CAPEX investments tied to actual demand."

First 360 Days: Toward Autonomous Operations

As policies, audit controls, and automation coverage mature, operators can begin to explore enterprise-wide orchestration. Digital twin models help test changes, optimize configurations, and validate actions before they reach production. This creates a pathway toward predictive and autonomous operations. Ritesh describes the direction in which networks will "anticipate failures, mitigate congestion, and dynamically reconfigure themselves — all without human intervention." The Action Layer enables this evolution by connecting AI insights with the systems that perform the work.

Conclusion

Operators don't need more alerts. They need a consistent process for resolving issues once detected. The Action Layer from UST provides this capability by combining AI, governed workflows, and vendor-neutral automation. It strengthens operational accountability, reduces downtime, and supports the long-term shift toward self-optimizing networks. As Ritesh summarizes, "The Action Layer is essentially the bridge between knowing and doing in network operations." It gives operators a predictable, scalable way to translate insights into outcomes and integrates with existing systems, enabling them to advance automation without significant replacement efforts. As networks modernize and service expectations rise, the ability to translate insights into reliable action will become a core operational requirement. Operators that build this action capability now will be better positioned to scale 5G complexity and progress toward higher-autonomy network operations.

UST helps service providers reduce operational noise, increase agility, and build the foundation for more autonomous operations. If your organization wants to move from reactive firefighting to proactive and resilient network operations, the Action Layer can guide that transition. Reach out to learn how UST can support your automation journey and help you achieve measurable business impact.