www.pipelinepub.com
Volume 22, Issue 7

Level 4 Is Not The Destination: What Matters Is The Direction of Travel

By: Aaron Boasman-Patel

For more than a decade, the telecom industry has spoken about autonomous networks as a destination, something mapped neatly across maturity curves, debated at conferences, and positioned as just over the horizon. What we are now seeing across the industry is not the arrival of fully autonomous networks end to end, but the steady emergence of autonomy as an operational capability, already taking shape in live environments, already solving real problems, and already influencing how networks are run day to day.

Recent TM Forum data reflects this shift, although it needs to be read carefully. According to "Assessing CSPs' progress towards Level 4 autonomous networks: Benchmark Report", around one fifth of operators report that they are operating at Level 3 or above at an overall level, and while Level 4 is beginning to appear in more advanced scenarios, it is not yet widespread, nor is it consistently deployed across domains. What matters is not the headline number, what matters is the direction of travel.

Across production networks, we are seeing repeatable, scalable use cases where systems are able to act with a high degree of independence within defined boundaries, handling complexity in ways that would previously have required constant human intervention. These are not isolated experiments, and they are not theoretical constructs. They are practical implementations, grounded in operational need, and they are quietly reshaping expectations of what is possible. The industry has not changed its ambitions. It has changed its approach.

From Automation to Understanding

For years, automation in telecom was largely about efficiency, replacing manual tasks with predefined workflows and rule-based processes that could execute faster and more consistently than people. As networks became more dynamic, more distributed, and more interdependent across domains, rigid automation struggled to keep up. Systems could follow instructions, but they could not adapt meaningfully when conditions changed beyond what had been anticipated. The shift we are now seeing is from pilot to production, and from execution to understanding.

Operators are no longer asking systems simply to do what they have been told. They are asking them to interpret intent, to assess context, and to make decisions that balance multiple objectives at once, whether that is performance, resilience, cost, or energy efficiency.

Intent driven control sits at the heart of this shift. When intent is defined in a way that systems can continuously interpret and enforce, it creates the conditions for autonomy to scale, not because every action is predefined, but because every action is aligned to an outcome. The challenge, as many operators will recognize, is not defining intent in isolation. It is applying it consistently across domains that have historically evolved in silos, with different data models, interfaces, and operational ownership.

Artificial intelligence plays an important role here, although not in the way it is often portrayed. The value is not in handing over control to opaque systems, but in augmenting the network's ability to perceive, to anticipate, and to prioritize. AI helps interpret vast amounts of telemetry, identify patterns that would otherwise be missed, and evaluate trade offs in real time. Crucially, it operates within guardrails defined by architecture and policy, reinforcing rather than replacing operator control.

Autonomy, in this sense, is not about removing humans from the loop. It is about changing how control is expressed, moving from manual intervention to continuous, policy driven oversight.

Turning Capability to Measurable Value

As autonomy matures, the conversation is also shifting in a more fundamental way, from what networks can do and towards what they deliver.

For a long time, progress in autonomous networks has been described in terms of levels, maturity models, and technical capability. These are useful, but they are not enough on their own. What ultimately matters are the business outcomes that autonomy enables, and whether that impact can be measured.

Operators are increasingly focusing on how autonomy translates into measurable impact, whether that is improved customer experience, faster service restoration, lower operating costs, or more efficient use of energy and resources. This is where the role of clear metrics becomes critical.

Key performance indicators remain essential for tracking operational efficiency and network behavior. Alongside these, there is a growing emphasis on key business indicators, which connect autonomous capabilities directly to outcomes such as revenue protection, customer satisfaction, and service reliability. What is emerging is a more complete picture of value, where autonomy is not assessed purely on technical sophistication, but on its ability to move the metrics that matter most to the business.

This is also an area where the industry still has work to do. One of the priorities for the industry is to help define and standardize how these outcomes are measured, so that operators can consistently evaluate their level of automation against real business impact, rather than relying on subjective or fragmented indicators.

When this alignment is in place, autonomy becomes easier to justify, easier to scale, and far more meaningful at an executive level. It shifts the conversation from capability to consequence.

Why Digital Twins Are Becoming Essential

Digital twins have been part of the conversation for years, often positioned as a future capability with broad potential. What is different now is that they are being applied in focused, practical ways that directly support autonomous operations.

In areas such as service assurance, fault management, and troubleshooting, operators are using digital twins to simulate network behavior before changes are applied, to test how intent policies will perform under real conditions, and to validate decisions without putting live services at risk. This creates something the industry has historically struggled with: confidence at scale.

As networks become more complex, it is no longer feasible for human operators to anticipate every possible outcome of every possible action. Digital twins provide a way to explore those scenarios safely, allowing systems to learn not only from live environments, but also from modelled ones. What is important here is that successful implementations are not attempting to model the entire network in one go. They are targeted, domain specific, and incremental, building trust over time rather than attempting transformation in a single step.

Building Coordinated Intelligence Across Domains

Much of the progress the industry has made so far has been within individual domains. Operators have successfully applied autonomous capabilities in areas such as fault management, transport optimization, and energy efficiency, often delivering strong results within those boundaries. These achievements matter, and they are an essential part of the journey.

But networks do not operate in isolation by domain. Customer experience, service performance, and operational efficiency are all shaped by interactions that cut across network layers, technologies, and organizational boundaries.

To move beyond partial autonomy, the industry needs to shift from single domain intelligence to cross domain orchestration, where systems can coordinate decisions across multiple layers of the network, balancing competing priorities and responding to change in a holistic way. This introduces new challenges, particularly around data consistency, policy alignment, and control across domains that may have evolved independently. It also raises the bar for architecture, requiring a level of integration and standardization that many organizations are still working towards. However, it is also where the real value of autonomy begins to unlock.

When decisions can be made across domains, rather than within them, operators can optimize end to end services rather than individual components, reduce unintended consequences between systems, and deliver outcomes that are aligned to both operational and business objectives. In that sense, cross domain orchestration is not just a technical step forward. It is the point at which autonomy becomes truly systemic.

Architecture as The Enabler of Scale

If there is one area where the industry has learned hard lessons, it is in the importance of architecture. Many early automation initiatives delivered promising results but struggled to scale because they were built on fragmented systems, bespoke integrations, and inconsistent data models. Success in one domain did not translate easily to another, and each new use case required significant reinvention. This is where architectural alignment is becoming a critical enabler.

By moving towards shared information models, standardized interfaces, and modular capabilities, operators are creating an environment where autonomous functions can be reused, composed, and governed more consistently. This does not mean forcing uniformity, but it does mean reducing unnecessary complexity, so that autonomy can move across domains rather than being confined within them.

The impact is already visible. Operators are moving more quickly from proof of concept into production, and lessons learned in one area are increasingly transferable to others. Autonomy

starts to look less like a collection of isolated successes, and more like a system that can evolve coherently.

Trust, Not Just Technology

As autonomy increases, trust becomes an operational requirement rather than an abstract concern. Operators need to understand why decisions are made, to verify that they align with policy, and to intervene when necessary. Without this, even the most advanced capabilities will struggle to gain traction. This is why observability, explainability, and auditability are not optional features. They are foundational.

Autonomous systems need to expose their reasoning, to provide clear lineage for models and decisions, and to demonstrate outcomes in ways that can be measured against intent. This is particularly important as the industry moves towards more objective indicators of effectiveness, such as service restoration times and fault recovery performance. Trust is not established through claims. It is built gradually, through consistent, transparent performance.

Scaling Level 4 With Discipline

The path to Level 4 autonomy is not defined by a single breakthrough moment. It is defined by accumulation. Each successful use case expands what is possible. Each improvement in architecture reduces friction. Each instance where a system handles complexity reliably builds confidence to go further. At the same time, it is important to remain grounded where the industry is today.

While ambition is high, and many operators expect to reach Level 4 within the next few years, current deployments remain uneven, and progress continues to depend on the less visible work of integrating systems, aligning data, and establishing clear operational accountability. The operators that succeed will be those that treat autonomy as a core operational capability, not as a series of innovation showcases. They will invest in the foundations, even when those investments are not immediately visible, because they understand that scale depends on consistency.

The Future Is Already Delivering Value

It is easy to continue talking about autonomous networks in terms of levels, as though progression alone is the goal. In reality, levels are only meaningful if they translate into outcomes. Autonomy is already being built, incrementally, in live networks, shaped by practical decisions, operational constraints, and real-world demands. It is not uniform, and it is not complete, but it is already delivering measurable value where it is applied effectively. The question for the industry is no longer whether Level 4 is achievable.

It is whether we can connect autonomy to the outcomes that matter, scale it across domains rather than within them, and align around the architectures and metrics that allow it to be trusted, measured, and sustained. Those that do not just advance along with a maturity model. They will redefine how networks are designed, operated, and governed in a world where success is measured not by the level you reach, but by the value you create.