ERICSSON

In partnership with

How to build an autonomous IoT network

Using 5G to enable reliable decisioning and response for autonomous operations

Image courtesy of Adobe Stock

"Informed" is not autonomous

Enterprises have made major progress in connecting assets and improving visibility into device status, operating conditions, and system performance. Data now flows continuously from equipment, field devices, meters, cameras, and control systems. Teams can monitor conditions more closely than ever before. Yet in many environments, a human must still review the output and decide what should happen next.

Autonomous IoT closes the gap between detection and action. An autonomous system can recognize a condition, interpret it within defined bounds, and trigger a timely response. This is often framed as an AI story, but connectivity is just as important. If telemetry arrives too late, if systems can't stay synchronized, or if control signals fail under pressure, the loop breaks. The system may still generate insight, but it can't deliver dependable action.

5G is essential for enterprises moving from connected IoT to autonomous operations, which need a network foundation built for timely response, secure coordination, resilient mobility, and distributed decision-making. They also need an architecture that supports edge computing, because many autonomous decisions create the most value when they occur close to the asset, machine, or event.

If autonomy is the destination, connectivity is the prerequisite.

⊗

Myth

IoT is just sensors.

✓

Reality

Autonomous IoT is a distributed control system.

Autonomous IoT does more than collect data from connected assets. It creates a closed-loop system that senses conditions, interprets their meaning, and triggers action across devices, applications, and control environments. The value comes from reducing the gap between detection and response.

Image courtesy of Adobe Stock

Why autonomous IoT is agentic by design

Autonomous IoT is the next step beyond connected and automated systems.

Connected IoT gives enterprises visibility. Automated IoT adds predefined actions when known conditions appear. Autonomous IoT goes further by evaluating multiple signals, interpreting conditions in context, and deciding what should happen next. Agentic AI becomes relevant at this stage.

An agentic system can do more than notice a problem. It can decide whether a response is needed and initiate it on its own. But it doesn't have unlimited freedom. Humans still define the boundaries, including which actions the system can take on its own, which conditions require escalation, and when control returns to a human operator.

Most enterprise environments aren't trying to remove human oversight entirely. The goal is to let systems handle routine decisions faster, while people retain authority over exceptions, escalations, and higher-risk calls. In practice, the model often appears as adaptive control, automated remediation, or a shift from predictive to prescriptive operations.

⊗

Myth

AI makes it autonomous.

✓

Reality

Autonomous IoT requires reliable real-time input and output loops.

AI can help determine what should happen next, but intelligence alone does not create autonomy. Autonomous systems depend on telemetry arriving in time, decisions being made in the right place, and control signals reaching the endpoint before the moment for action is lost. When that loop is unstable, AI becomes advisory instead of operational.

Image courtesy of Adobe Stock

Connectivity: The hidden constraint of autonomy

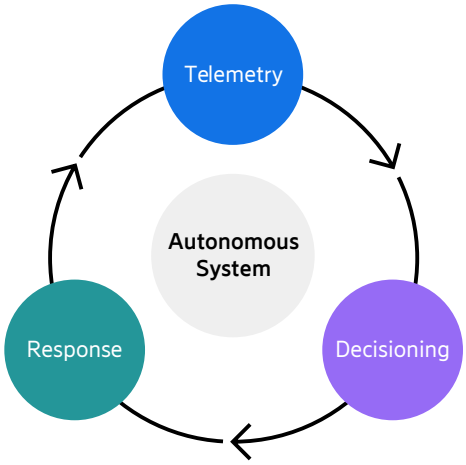
Autonomous IoT is often thought of as a matter of smarter software. In practice, many deployments stall because the communications environment isn't built to support autonomy at scale.

A functioning autonomous system requires a continuous loop of telemetry, decisioning, and response. Data must move quickly enough to inform a decision before the decision loses value. The signal must then be processed in the right place, and the resulting instruction must reach the endpoint without delay or disruption. If any part of the loop becomes unstable, the system falls back to manual operations.

Connectivity determines whether autonomy scales. Pilot programs can often succeed in controlled environments, but scaling across a production network, utility territory, or fleet exposes where the network is too slow, too inconsistent, or too fragile to support reliable action. The difference between a successful pilot and a scalable autonomous system often lies in the communications layer that supports telemetry, control, and coordination in real time.

Several factors shape whether the loop can hold together in the field. Latency and jitter affect timing and predictability. Uplink capacity matters in environments with heavy telemetry, video, or sensor traffic. Coverage and mobility are critical when assets move between locations or when monitored assets span geographies. Resilience and security are important because the system still needs to function when conditions are challenging or deteriorate, or when trust boundaries weaken.

When those requirements are missing, organizations end up with autonomy islands that work in narrow pockets but don't coordinate across the broader environment. Manual overrides become routine, which defeats the purpose of autonomy. AI may still generate insights, but it becomes advisory instead of operational.



5G is the strongest foundation for autonomous IoT

The case for 5G is not simply speed. 5G is better aligned with the needs of distributed, time-sensitive operations. Closed-loop control relies on timely exchange between endpoints, decisioning systems, and control environments. Autonomous IoT also calls for stronger uplink performance, especially in environments that rely on video, machine vision, or dense sensor traffic.

Older wireless approaches can struggle with operations that are simultaneously mobile and continuous. 5G is better suited to both requirements. For moving assets such as robotics, vehicles, and field equipment, the advantage is uninterrupted connectivity as conditions change.

Segmentation is another differentiator. In autonomous environments, control traffic and operational telemetry should not have to compete with less critical data. 5G enables a more intentional model by separating security and performance concerns.

SASE helps isolate autonomous operation data within defined trust boundaries, keeping it separate from less critical traffic or from other sensitive data accessed by different users or systems. 5G network slicing ensures the bandwidth availability, low latency, and predictability required by autonomous control loops by assigning this traffic to a dedicated slice protected from congestion elsewhere on the network.

⊗

Myth

Connectivity is just plumbing.

✓

Reality

Connectivity is the autonomy layer.

In autonomous IoT, connectivity does far more than move data from one point to another. It determines whether telemetry, decisioning, and response can operate as a secure, coordinated system under real-world conditions. It is what allows isolated pilots to become scalable, repeatable operating models.

Image courtesy of Adobe Stock

5G and edge compute accelerate the control loop

Autonomy is shaped not only by connectivity but also by where decisions are made.

If every signal must travel back to a distant cloud before action can be determined, the loop becomes slower and more dependent on centralized infrastructure. A cloud-first model may work for some workloads, but it becomes limiting when response time affects outcomes. This is why 5G and edge compute belong in the same conversation.

Edge computing brings inference and decision-making closer to the machine, site, or field asset. The shift reduces backhaul dependence and shortens the path between signal and response. The cloud remains essential for policy, orchestration, analytics, and system-wide optimization. Autonomous IoT increasingly follows a distributed model in which the edge handles time-sensitive decisions near the environment, while the cloud governs and optimizes performance across the wider system. 5G is the communications layer that makes the architecture practical.

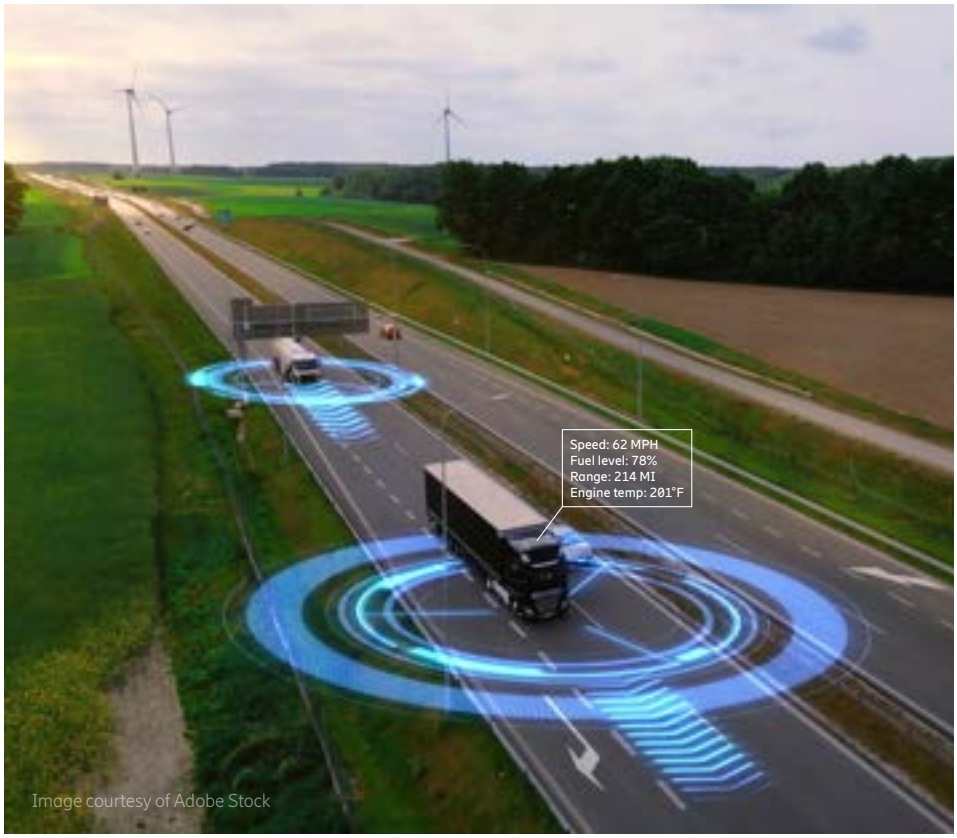


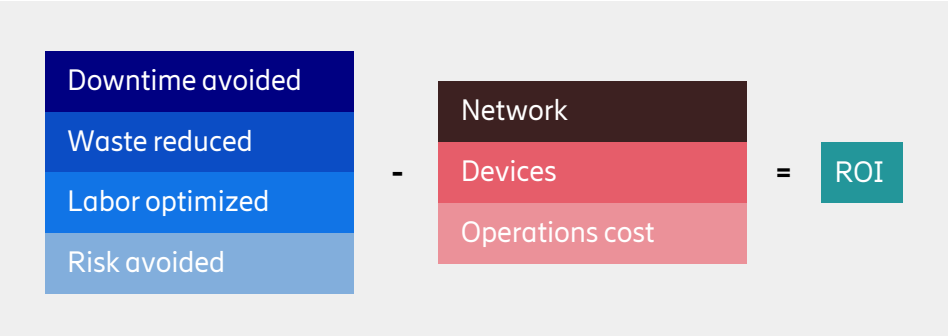
Image courtesy of Adobe Stock

ROI framework: How 5G-based autonomy creates value

The business case for autonomous IoT built on a 5G foundation should be framed in operational terms. Value comes from shortening the gap between detection and response, then converting that speed into steadier performance, lower risk, and better use of existing assets. In high-impact scenarios — such as leaks in large water or gas lines or a downed power line — time is critical. Autonomous systems can detect issues and act immediately, cutting waste, limiting environmental damage, and, in some cases, saving lives.

The return often begins with fewer manual interventions and faster operating cycles. It also appears when systems catch problems early enough to keep deviations from spreading. In many environments, the result is stronger continuity, faster recovery, and less exposure when conditions shift.

The value equation is straightforward:



With 5G in place, organizations do not need to wait for full-scale use to prove value. Early signs often appear in lower latency and jitter, faster mean time to detect and respond, higher closed-loop automation rates, and fewer manual overrides. In practice, that can mean quicker fault isolation, fewer truck rolls, lower wastage, and more consistent uptime.


Image courtesy of Adobe Stock

Industry proof points for autonomous IoT

Utilities

Grid-wide coordination

Utilities may offer the strongest long-term case for autonomous IoT. The modern grid is bidirectional, variable, and increasingly distributed — and all of it must communicate fast enough to keep the whole system in balance.

Connected field assets continuously sense conditions, and the system responds when intervention is needed. The response may involve rerouting power, adjusting resource use, isolating a fault, or preserving service elsewhere on the network.

A 2025 power outage that left large parts of the Iberian Peninsula without power for hours showed how quickly a stressed grid can break down when volatility outpaces the system's ability to coordinate a response. In a grid with more variable and distributed generation, utilities need systems that can communicate and respond fast enough to prevent local instability from becoming a wider disruption. That is where an autonomous Distributed Energy Resource Management System (DERMS) becomes important for throttling generation, storing excess energy, redirecting power flows, and isolating faults before a local issue becomes a broader outage.

Better coordination via autonomous IoT can help avoid or contain outages, restore service more quickly, and protect critical assets before instability spreads. Over time, the same capabilities can support higher renewable penetration with less operational strain and help defer capital investment by using existing infrastructure more intelligently.

Manufacturing

Keeping production inside tolerance

Manufacturing is one of the clearest illustrations of autonomous IoT because the business value of fast response is easy to quantify. A production environment constantly generates signals. Traditional IoT surfaces those signals, and autonomous IoT acts on them.

In a closed-loop quality environment, the system can correlate visual and sensor data, determine whether the issue is process-related, and correct it while production is still underway. The response may involve adjusting settings, isolating a problem area, or slowing part of the workflow before waste spreads. Here, autonomous IoT can reduce downtime and line stoppages while protecting yield and uptime.

Smart cities

Continuity under disruption

Smart city autonomy is tested most clearly when conditions break down. For example, San Francisco power outages disrupted Waymo's rideshare service by disabling traffic signals, roadside sensors, and supporting network infrastructure. This showed how quickly autonomous systems can reach operational limits when the surrounding infrastructure becomes unstable.

For smart city autonomy to withstand disruption, the system needs more than intelligent software. It needs redundant connectivity, priority treatment for safety-critical traffic, always-on telemetry, and safe degradation so operations can continue locally or shift into a lower-risk mode instead of failing outright. Real-time kinematics (RTK) positioning can further improve autonomy in mobility and robotics, but only if correction data is delivered reliably enough to preserve accuracy and continuity.

The payoff of autonomous IoT often appears in service continuity and faster recovery during disruption.

Implementation: A phased path to scale

Most organizations will not move directly from connected IoT to full autonomy. A phased approach is more practical and more credible.

1

Assess the workflow

Start with the operational problem. Identify where fast response most directly affects outcomes and where shortening the path between detection and action would create the most value.

2

Design the control loop

Map what needs to be sensed, where the decision should happen, what system executes the response, and what the operational bounds are. At this stage, organizations also need to define technical requirements, segmentation, coverage, redundancy, and edge placement.

3

Pilot for scale

A useful pilot does more than prove technical feasibility. It should validate whether the system behaves reliably enough under real conditions to justify broader deployment.

4

Operationalize the model

Shift from a working use case to a working operating model, including management, observability, security, policy, and human oversight.

5

Scale with control

Extend a proven pattern across sites, fleets, or business units without degrading performance or trust. Safe degradation is a major consideration here. A credible autonomous system should not simply fail when conditions deteriorate. It should move into a known lower-risk operating mode.

Build autonomy on a network that can keep up

Autonomous IoT marks a significant change in how enterprise systems operate. Connected IoT gave organizations visibility. Automated IoT reduced some manual effort through predefined responses. Autonomous IoT goes further by allowing systems to sense, evaluate, and act within trusted bounds while human oversight remains in place for governance and escalation.

Autonomous systems still need the right network. Without reliable telemetry, strong uplink, predictable performance, resilient mobility, and secure coordination, the control loop breaks. The result is a system that may be smart, but not operationally autonomous.

For autonomous IoT, 5G provides the strongest foundation. It supports real-time responsiveness, stronger mobility, better segmentation, greater device density, and a cleaner path to distributed edge architectures. More than enabling autonomous IoT in theory, 5G helps make it repeatable in practice.

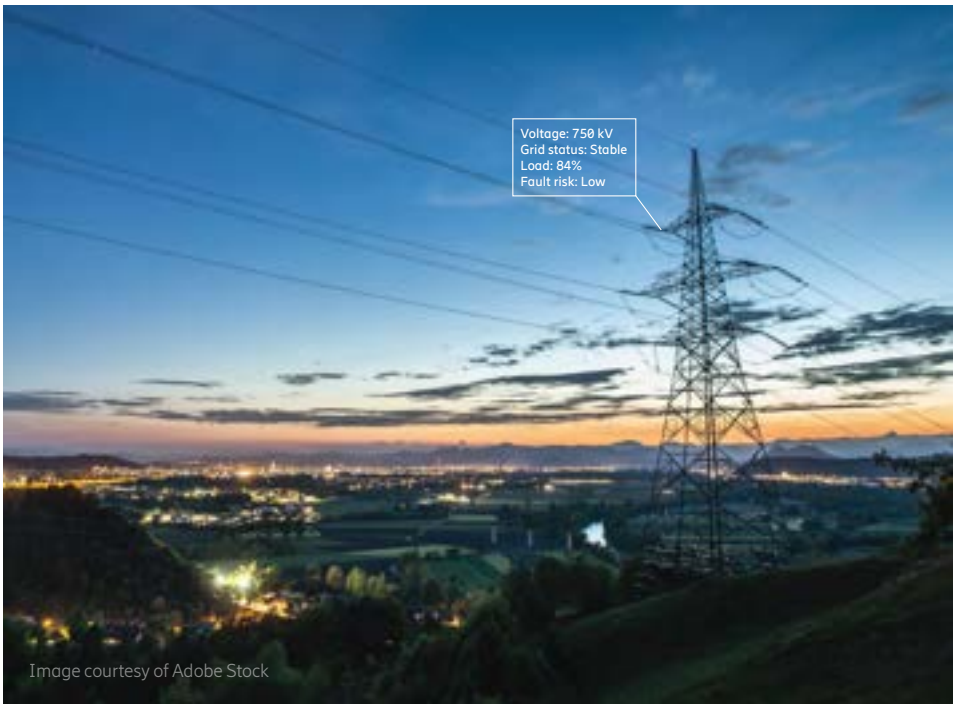


Image courtesy of Adobe Stock

Learn more about enterprise wireless solutions

What leaders must know about autonomous IoT

- **Autonomous IoT is about action, not just insight.**
  The goal is not to collect more data. The goal is to help systems detect conditions, make decisions within defined limits, and respond quickly enough to change the outcome.
- **5G is what makes that possible at scale.**
  Autonomous operations depend on reliable connectivity, fast response times, strong uplink, mobility, and secure coordination across distributed environments.
- **The payoff is operational and measurable.**
  With 5G, enterprises experience faster detection and response, fewer manual interventions, more closed-loop actions, higher uptime, and steadier performance.

The bottom line: Autonomous IoT succeeds when systems can turn signals into action quickly, reliably, and at scale. 5G is the foundation that helps make that possible.

Learn more about enterprise wireless solutions

Five questions for leadership teams

1

Where would a faster response create the most value?
Focus on workflows where shortening the gap between detection and action improves cost, continuity, safety, or service.

2

Can the network support real-time coordination?
Autonomy depends on latency, jitter, uplink, mobility, resilience, and segmentation, not just basic connectivity.

3

Where should decisions happen?
Some decisions belong in the cloud. Others create more value at the edge, closer to the machine, site, or field asset.

4

What happens when conditions degrade?
A credible autonomous system should move into a safe, lower-risk mode rather than fail outright.

5

How will success be measured early?
Track operational indicators before waiting for full enterprise-scale return.