Velotic.

From Point-to-Point Chaos to Streamlined Connectivity

Manufacturing is generating more data than ever—from sensors, machines, PLCs, assembly lines, and beyond. But more data doesn't mean better insights. Most of this data is trapped in siloed systems, stored in inconsistent formats, and disconnected from the context that makes it insightful.

The root of this challenge is the cost of building and maintaining point-to-point connectivity and integrations. What works for a handful of systems quickly becomes unmanageable across lines, sites, and the enterprise—creating brittle architectures that are expensive to maintain, impossible to scale, and difficult to govern and secure.

More than 90% of respondents say they expect to maintain or increase smart factory and production technology investments in 2026, according to the Manufacturing Leadership Council. The pressure to modernize is real. But AI, analytics, and automation can only deliver when the data beneath them is structured, scalable, and accessible. Here's what's driving the complexity—and what it's costing manufacturers.

What's fueling the increase in point-to-point connectivity?

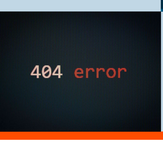
- **More devices coming online:** Manufacturers are connecting more machines, sensors, and assets than ever before to support AI, analytics, and digital initiatives. In fact, the number of IoT devices in 2025 is forecasted to **reach 39 billion** by 2030. Each new device adds another endpoint—expanding the number of required connections across the environment.
- **More applications demanding data:** OT data is no longer confined to a single system. It feeds analytics, MES, ERP, cloud platforms, and AI initiatives—each requiring direct access to consistent, trustworthy insights. Without a standardized, scalable foundation, this growing demand drives a surge in one-off connections.
- **More business-as-usual connectivity:** Many architectures were never designed to orchestrate, contextualize, and govern data across the enterprise and connectivity has always been an afterthought. Instead, integrations are added incrementally—creating fragmented, point-to-point connections that become increasingly complex as environments evolve.

What drives point-to-point chaos?

Direct, custom integrations: Point-to-point architectures connect each device to every application (SCADA, MES, ERP) individually—without a standard layer in between. As environments expand, this creates a dense web of dependencies that is difficult to scale, manage, or change.

Insecure, legacy communication protocols: Many industrial protocols such as Modbus weren't designed for modern, connected environments. When exposed beyond the manufacturing network—to cloud applications or enterprise systems—they introduce new risks, expanding the attack surface and making it harder to secure data flows.

Inconsistent, ungoverned data: Disparate protocols, tag naming, and data models result in inconsistent data across systems. Without standardization, data becomes difficult to normalize, contextualize, and govern—limiting its usability for analytics and AI.



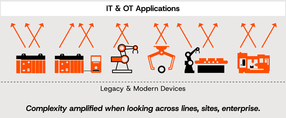
Architectures that can't handle demand: As more applications poll the same devices for data, legacy systems reach their limits. Excessive polling strains devices and infrastructure—leading to performance issues, instability, and unreliable data delivery at scale.

What's the Real Cost of Point-to-Point Chaos?

- **Stalled scalability:** Point-to-point integrations may work for a few systems—but they collapse under the weight of enterprise-wide IT-OT integration, leaving manufacturers stuck with architectures that can't scale.
- **Slower access to data:** New devices require point-to-point integrations to each application, and new applications require point-to-point integrations to each device. This process is slow, expensive, and prone to security challenges.
- **Increased security risk:** Every custom integration is another potential attack surface. As point-to-point connections multiply, so do the vulnerabilities—making it harder to monitor, secure, and defend the network. Fragmented architectures also slow the rollout of software and firmware updates, increasing exposure to known threats.
- **Weakened data governance:** Privacy and regulatory compliance become more challenging when a single governance or policy cannot be applied to readily accessible, uniform data.
- **Lost context:** Advanced technologies like AI and analytics depend on data with context—what it means, where it came from, and how it relates to other data. Fragmented point-to-point architectures make that context increasingly difficult to deliver, limiting the value of every downstream investment.

Today, connecting to the source of OT data is difficult

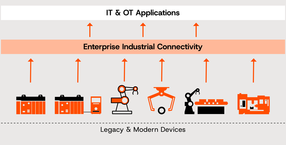
Current state: Many point to point integrations, disparate and out of date OPC servers, and insecure protocols

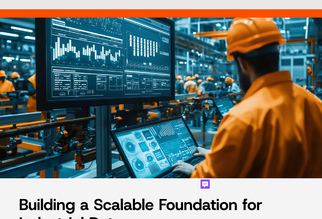


Complexity amplified when looking across lines, sites, enterprise.

Standardized connectivity creates a foundation for OT data

Enterprise industrial connectivity creates a single source for OT data while modernizing protocols and securing OT networks.





Building a Scalable Foundation for Industrial Data

To successfully scale data-driven operations, manufacturers need to move away from fragmented architectures toward a more structured, enterprise-ready approach:

- **Treat connectivity as a strategic foundation—not an afterthought:** Establishing a scalable data foundation is the first step to unlocking reliable insights, faster innovation, and enterprise-wide transformation.
- **Introduce a standard connectivity layer:** Abstract devices from applications with a centralized layer that connects, normalizes, and secures data—minimizing the need for custom integrations.
- **Adopt architectures built for scale:** Shift to flexible, event-driven data architectures that can grow with evolving environments—without adding new complexities.

A Better Approach to Industrial Connectivity

Explore how standardized connectivity can help manufacturers address today's data challenges while future-proofing automation operations for tomorrow.

Explore the Role of Standardized Connectivity →