

Siemens Industrial Automation DataCenter Pairs AI Readiness with Lifecycle-Managed OT Infrastructure

ARC VIEW

October 15, 2026
By David Humphrey

ARC Advisory Group

VISION, EXPERIENCE, ANSWERS FOR INDUSTRY, ENERGY, & INFRASTRUCTURE

KEYWORDS: Siemens, Industrial Automation DataCenter, Managed IT/OT Infrastructure, IT/OT Convergence, Industrial AI, Virtualization, Cybersecurity, Availability Care – Operate, NVIDIA, Palo Alto Networks, Prisma AIRS, Industrial DMZ, Digital Transformation

Overview

When ARC first wrote about Siemens' Industrial Automation DataCenter (IADC) in 2022, the main story was IT/OT convergence: an engineered approach that moved automation systems into modern, IT-like infrastructure while preserving OT requirements for availability, safety, lifecycle support, and cybersecurity. Since then, virtualization has become broadly accepted. The competitive question has shifted from whether automation systems can be virtualized to what infrastructure can support future industrial operations, cybersecurity, AI, remote service, digital twins, and lifecycle management.

IADC is no longer just about virtualizing automation servers. Siemens now positions it as a secure, AI-ready, lifecycle-managed OT infrastructure layer for software-defined industrial operations.

Siemens' answer is to broaden IADC into a managed IT/OT infrastructure foundation. The updated positioning preserves IADC's role as an on-premise, pre-installed, pre-configured, and system-tested OT platform, while expanding the message to AI-ready operations, cyber protection, faster deployment, scalability, and lifecycle support through "Availability Care – Operate" (formerly Remote Industrial Operations Services).

This ARC View examines how Siemens IADC has evolved, why the company is expanding it around AI-ready managed IT/OT infrastructure, and what this shift means for industrial users seeking secure, scalable, and lifecycle-managed foundations for software-defined operations.

Key Takeaways for Buyers

- Look beyond virtualization: demand secure, lifecycle-managed, AI-ready OT infrastructure.
- Use IADC as a benchmark for pre-configured, secure, AI-capable OT infrastructure close to production.
- Choose the right adoption path: platform first, managed operations when accountability matters.
- Press vendors on what happens after the AI pilot: governance, tested versions, controlled updates, and single-point accountability.

From Engineered Virtualization to Managed IT/OT Infrastructure

In 2022, ARC described IADC as an individually engineered "data center" for production IT. Siemens assembled and configured rack-based infrastructure using proven IT components and industrial networking devices, then installed the hypervisor layer, virtual machines, operating systems, automation

applications, backup and recovery, security components, and supporting services around the customer's requirements. This approach helped users adopt IT-based infrastructure without treating the OT environment like a generic enterprise data center.

That distinction remains important. OT systems operate physical assets and must prioritize safety, availability, determinism, maintainability, and long lifecycle support. IT systems focus more heavily on confidentiality, integrity, data availability, resource utilization, and rapid technology refresh. IADC was designed to bridge these priorities by applying IT infrastructure concepts in an engineered OT context.

The new IADC positioning builds on that foundation while expanding the scope. "Managed IT/OT Infrastructure" reflects a broader architecture and service model that combines the on-premise infrastructure platform with ongoing monitoring, maintenance, cybersecurity services, and support. Siemens positions IADC as the physical and virtual foundation for industrial applications, while Availability Care – Operate provides the optional operational wrapper that helps keep that foundation secure, current, and available throughout its lifecycle.

How IADC Has Evolved

Industrial users today have a clearer need for secure, standardized, and managed OT infrastructure. Digital transformation initiatives have moved beyond connectivity pilots and isolated analytics projects. Users increasingly want to run advanced analytics, AI copilots, machine vision, digital twins, simulation, historians, asset performance applications, engineering tools, and cybersecurity applications close to production. These workloads require compute power, reliable networking, protected data exchange, and lifecycle governance.

Dimension	2022 IADC Emphasis	Current IADC Direction
Market framing	Engineered virtualization and IT/OT convergence	Managed IT/OT infrastructure for software-defined, AI-ready operations
Primary value proposition	Consolidate and modernize automation infrastructure while preserving OT requirements	Provide a secure, validated, lifecycle-managed OT infrastructure foundation
Technology scope	Rack-based infrastructure, hypervisors, virtual machines, automation applications, backup, and security components	Pre-configured OT infrastructure, controlled data exchange, lifecycle services, cybersecurity, and optional accelerated compute
Cybersecurity role	Core design element based on defense-in-depth, segmentation, patching, backup, and recovery	More strategic emphasis, including AI-related cyber protection and optional OT cybersecurity extensions
Service model	Project-oriented engineering and support around customer requirements	Optional Availability Care – Operate layer for monitoring, maintenance, security operations, and lifecycle support
Lifecycle support	Classic lifecycle support for the engineered IADC platform	Expanded proactive and preventive lifecycle support through remote monitoring with Availability Care – Operate
Customer decision criteria	Can automation systems be virtualized reliably?	Who owns lifecycle governance, updates, security, availability, and operational accountability?

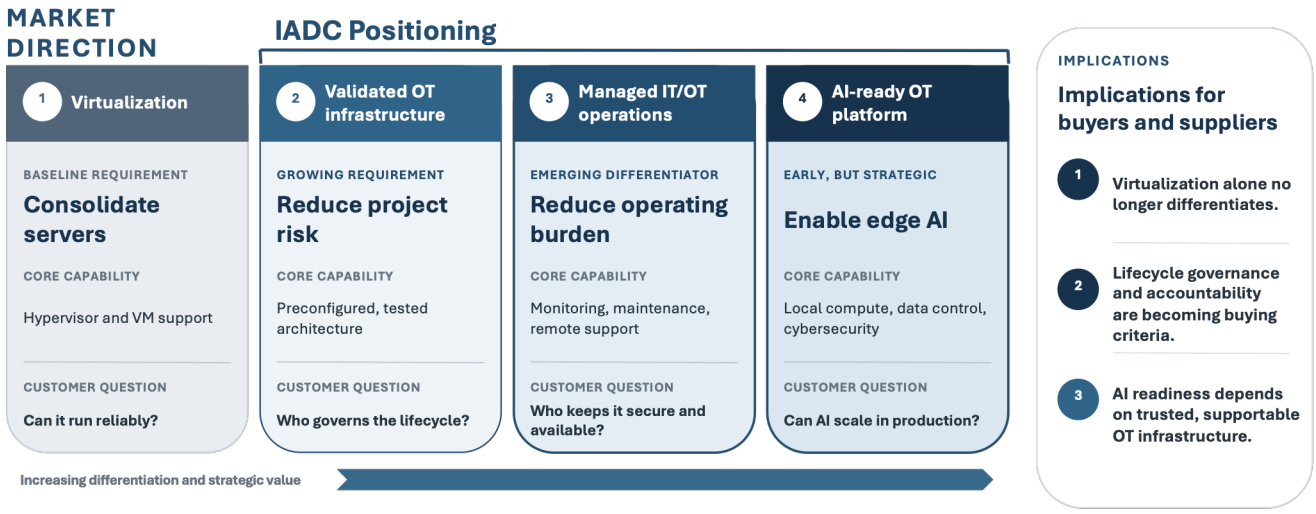
What has changed?

At the same time, the cybersecurity environment has become more demanding. Industrial cyber risk is now widely discussed as a business risk, not simply an IT risk. Remote access, cloud connectivity, software updates, and AI-enabled applications all increase the need for disciplined segmentation, monitoring, threat detection, and incident response. The traditional separation between IT and OT remains useful, but it is no longer sufficient by itself. Users need a secure exchange layer, consistent governance, and infrastructure that can be managed without compromising production availability.

The third major change is the acceleration of industrial AI. Siemens argues that AI is transforming industrial operations, that real-time decisions are becoming business-critical, and that complexity is slowing innovation. This reflects a broader market trend: industrial AI will not scale in production unless the underlying compute, networking, cybersecurity, and lifecycle infrastructure is available and trusted. Siemens is positioning IADC as an AI-ready platform that can provide this foundation on-premise at the industrial edge.

AI-Ready at the Industrial Edge

Siemens' updated IADC concept is a modular, pre-configured IT infrastructure platform for AI-ready industrial use cases. The company highlights pre-installed and pre-configured systems, aligned hardware and software, consulting and planning, and remote monitoring and management throughout the lifecycle. In practical terms, Siemens aims to reduce the integration burden for customers that would otherwise need to design, procure, assemble, configure, secure, and support their own industrial IT infrastructure.



OT Infrastructure Differentiation Is Shifting Beyond Virtualization.

Optional AI-ready configurations can include NVIDIA GPU and DPU technology to support advanced AI and cybersecurity workloads. GPUs provide accelerated computing power for AI workflows, while DPUs can support specialized infrastructure and security functions. According to Siemens, this enables OT applications such as copilots, AI manufacturing assistants, advanced analytics, and other AI-enabled workloads to run closer to the production environment.

This is significant because many industrial AI use cases are constrained by latency, data sovereignty, cybersecurity, or operational continuity requirements. For many plants, sending all production data to the cloud for analysis is neither practical nor desirable. An on-premise, AI-ready OT infrastructure can support use cases that require local compute, controlled data exchange, and integration with automation, historian, and engineering systems. For Siemens, this creates an opportunity to position IADC as more than a host for virtualized automation applications and as a deployment platform for industrial AI.

Cybersecurity Moves to the Center of the Offering

Cybersecurity was already a core part of IADC in 2022. ARC described defense-in-depth concepts, industrial DMZs, network segmentation, firewalls, endpoint protection, vulnerability management, patch management, backup and disaster recovery, and log management. What has changed is the level of strategic emphasis and the tighter link between cybersecurity and AI-enabled edge workloads.

In the new Managed IT/OT Infrastructure message, Siemens positions cybersecurity as an important supporting capability for IADC, not as a replacement for the platform's central purpose: hosting OT applications on a secure, lifecycle-managed infrastructure foundation. The partnership with Palo Alto Networks and the use of Prisma AIRS should be understood as a new optional cybersecurity extension for OT environments, particularly as customers begin to deploy AI-enabled workloads at the edge. This extension can help protect AI applications, models, and data through Zero Trust and AI-specific cyber defenses, but it is not a general standard across the installed IADC base.

As automation environments become more software-defined, connected, remotely supported, and AI-enabled, their vulnerability profile expands. Customers need protection that does not disrupt operations, along with clear accountability for monitoring, incident response, maintenance, and compliance. Siemens' OT domain knowledge is important here. Generic IT security practices cannot simply be imposed on automation environments without considering availability, safety, update windows, validation, and lifecycle constraints.

Managed Services Add the Operational Layer

One important addition to the IADC story is the explicit role of Availability Care – Operate, a 24/7 managed services layer for IT/OT infrastructure. Here, Siemens offers two related but commercially separate layers: IADC is the infrastructure layer for hosting OT applications, while Availability Care – Operate is the modular operations and service layer for monitoring, maintenance, security operations, and lifecycle support. Customers can adopt the IADC platform without the managed service, or they can add Availability Care – Operate to reduce the operational burden over time.

This addresses one of the most persistent barriers to IT/OT convergence: the skills gap. Many industrial sites lack enough personnel with combined expertise in automation systems, virtualization, industrial networking, cybersecurity, backup and recovery, patch management, and compliance. Even companies with strong IT departments can struggle when plant-level OT requirements create unclear ownership and

accountability. IADC without lifecycle support could shift complexity from physical hardware to virtual infrastructure. IADC with Availability Care – Operate can reduce that burden by giving customers a managed operating model.

The managed-service layer offers a clearer operating model: Siemens can monitor, maintain, secure, and support the OT infrastructure while customers retain flexibility in how they adopt the platform.

The service component also strengthens Siemens' differentiation, provided the distinction between platform and service remains clear. Many suppliers can support virtualization, but few can credibly combine automation domain expertise, validated infrastructure, lifecycle services, industrial cybersecurity, and remote operations support. Siemens' commercial offer should not be read as requiring customers to buy the platform and managed service as a single package. Rather, IADC provides the validated infrastructure foundation for OT applications, while Availability Care – Operate adds an optional managed operating model for customers that want Siemens to take on more responsibility for keeping that foundation secure, current, and available.

Virtualization Is Now the Baseline Requirement

By 2022, Siemens had already delivered a substantial IADC installed base. Today, that early experience remains valuable, but the market context has changed. Major automation suppliers now offer virtualization or high-availability infrastructure options for their control system environments, and most position some form of virtualized, software-defined, or infrastructure-managed automation environment. The competitive issue is no longer whether a supplier supports virtualization. The issue is how far the supplier can go in delivering a validated, secure, lifecycle-managed, and open OT platform.

This creates both an opportunity and a challenge for Siemens. The opportunity is that the market has validated the original IADC premise. The challenge is that Siemens must now differentiate above the hypervisor layer. Customers will evaluate IADC not just as an infrastructure solution for Siemens applications, but as a potential platform for broader OT workloads, AI use cases, cybersecurity services, and future software-defined operations.

Openness Is Key

As IADC becomes more platform-like, openness becomes more important. Industrial users often welcome a single point of accountability, but they resist infrastructure lock-in. Customers want validated architectures and supportable configurations, but they also want flexibility in servers, storage, networking, backup, cybersecurity, hypervisors, applications, and system integration partners. These priorities can conflict if openness is not clearly defined.

©2026 • ARC Advisory Group • 3 Allied Drive • Dedham, MA 02026 USA • 781-471-1000 • arcweb.com

For Siemens, "open IADC" does not mean unmanaged freedom to install anything, since that would undermine the value of a validated OT infrastructure. Instead, openness means certified third-party application support, transparent support boundaries, defined integration interfaces, a published lifecycle governance model, and some flexibility in infrastructure components from approved vendors. Customers should understand which workloads are supported, which are validated, which are allowed but not supported, and which would compromise lifecycle responsibility. This distinction becomes more important as Siemens expands the IADC message beyond process automation. The updated Managed IT/OT Infrastructure message now supports SCADA, MES, historians, PLC programming software, AI applications, digital twins, and advanced analytics, and it gives IADC a clearer solution path for discrete industries as well as process environments.

IADC's durable value lies in lifecycle governance, validated updates, and a single point of responsibility for the OT infrastructure foundation.

ARC Perspective

Siemens' expanded IADC positioning reflects where industrial automation infrastructure is headed, but some of its key differentiators are operational rather than AI-specific. For many customers, the strongest value lies in Siemens' ability to deliver centralized manufacturing, standardized configuration, tested software versions, controlled updates, clearly defined lifecycle responsibility, and a single point of responsibility. These capabilities reduce project risk, simplify ownership, and make the platform easier to sustain over time. AI readiness strengthens the IADC story, but the day-to-day customer case often rests on the confidence that the infrastructure foundation is engineered, validated, governed, and supported as a coherent OT platform.

Conclusion

Siemens introduced IADC before many industrial users were ready to think of automation infrastructure as a managed IT/OT platform. That early move gave the company valuable experience and credibility. Since 2022, the market has caught up in one sense: virtualization is now widely accepted and increasingly expected. At the same time, the discussion has moved beyond virtualization toward secure, governed, and service-supported OT infrastructure.

The next phase is about secure, AI-ready, lifecycle-managed OT infrastructure. IADC provides the foundational IT/OT backbone for shopfloor operations: a factory-tested, validated infrastructure layer for hosting OT applications and supporting future software-defined, AI-enabled use cases. Availability Care – Operate is not automatically bundled with IADC; it is an optional, modular managed-services layer that customers can add when they want Siemens to take on more responsibility for monitoring, maintenance, security operations, and lifecycle support. Together, the platform and optional service layer close the loop for a Managed IT/OT Infrastructure model, while still allowing customers to decide how much operational

©2026 • ARC Advisory Group • 3 Allied Drive • Dedham, MA 02026 USA • 781-471-1000 • arcweb.com

freedom or managed support they want. The competitive issue is not who can deliver the most complex rack, but who can provide the most reliable foundation for industrial operations. If Siemens keeps the offer sufficiently open, clearly governed, and supportable, IADC can provide the trust layer industrial operators need to scale with confidence.

For further information or to provide feedback on this article, please contact your account manager or the author at dhumphrey@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC, and no part may be reproduced without prior permission from ARC.