ARC VIEW

DECEMBER 1, 2022

Siemens Industrial Automation DataCenter: An Engineered Solution Puts Process Automation Systems in an IT Environment

By David W. Humphrey

Keywords

Siemens, Industrial Automation DataCenter, IT/OT Convergence, Digital Transformation, Industry 4.0

Summary

A consequence of digital transformation is the growing influence of information technology (IT) in operational technology (OT, or classic automation systems) as industrial solutions increasingly use technologies based on open IT standards. Even the most conservative industrial companies are convinced of the need to adopt these technologies as part of their digital transformation journeys. IT-based solutions offer a multitude of advantages, ranging from universal connectivity to rapid application development to highly efficient asset management of hardware and software. Industry users are well aware of the often-diverging priorities of IT versus OT systems, so how can these differences be resolved?

The IT/OT Dilemma
IT systems *ensure data availability, integrity and confidentiality of data, while* ***OT systems,*** *which operate physical assets that could cause harm if mishaps occur, prioritize equipment availability and safety.*

To help customers achieve the best of both worlds while addressing these differences, Siemens developed the Industrial Automation DataCenter (IADC), an engineered solution for process industry users that solves the practical challenges of delivering classic process automation solutions in an IT environment.

The IT/OT Dilemma

The benefits of employing a modern IT architecture in any environment are countless, ranging from lower hardware costs and greatly improved data accessibility to solution scalability, better maintainability and ubiquitous cybersecurity. Industry users would flock to modern architectures immediately if it weren't for the IT/OT dilemma: the fact that IT and OT systems have fundamentally different priorities. With IT systems, the top priority is to ensure availability, integrity and confidentiality of data for applications. OT systems, on the other hand, operate expensive physical assets with the potential to cause harm if mishaps occur. For this reason, these systems prioritize equipment availability and safety.

Delivering Traditional Process Automation

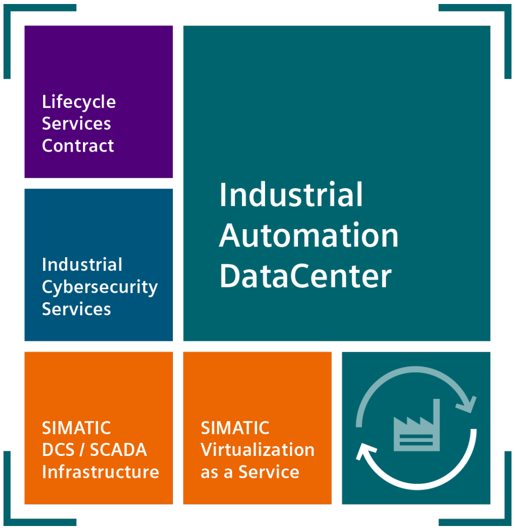
Process automation systems have evolved gradually over decades, but architectures are still mostly proprietary. Commercial "office" technologies such as Ethernet and desktop operating systems were often spurned in favor of home-grown solutions that addressed industry-specific requirements for redundancy, determinism or intrinsic safety.

Plant automation is designed and built to be robust and reliable with high availability. Hardware may be hot-swappable and is often set up in redundant configurations so that continuous processes and mission-critical applications cannot be interrupted. While regular maintenance is critical to reliable operation, software updates are treated with suspicion and subject to rigorous testing. These requirements are critical for the safe and secure operation of process plants.

The use of open technologies based on commercial IT standards has grown in areas such as connectivity and virtualization as industrial communications standards continue to evolve, and some equipment suppliers now deliver non-critical systems using virtual machines. However, adopting these technologies doesn't mean that modern plant automation systems must completely redesign their architectures. Instead, the key is to deploy these systems in a modern IT-like environment while preserving the integrity of mission-critical control systems. This is what Siemens set out to achieve when the company developed IADC.

What Is IADC?

Siemens' IADC is not a product, but rather an individually engineered solution that packages process automation systems in an IT infrastructure. According to Siemens, the system is designed to facilitate entry into the forward-looking, digitalized infrastructure of the industrial environment of the


Lifecycle Services Contract
Industrial Cybersecurity Services
Industrial Automation DataCenter
SIMATIC DCS / SCADA Infrastructure
SIMATIC Virtualization as a Service

IADC Serves as a Platform for Plant IT Infrastructure

future. According to the company, the development work on IADC took into account the fact that digital developments common in office IT environment for years are becoming increasingly important in the OT environment. It also recognized that OT requirements differ greatly in terms of long asset lifecycles, high system heterogeneity, and the need for high plant availability. Finally, Siemens recognized the need for a solution that combines expertise in automation, digitalization, and cybersecurity.

The solution is an individually engineered “data center” offering high performance computing with high availability, IT/OT networks, back-up and disaster recovery, process data archiving, an uninterruptible power supply and an IEC 62443 compliant security architecture. As an engineering solution, Siemens takes a holistic approach by offering services for consulting, configuration, and lifecycle support.

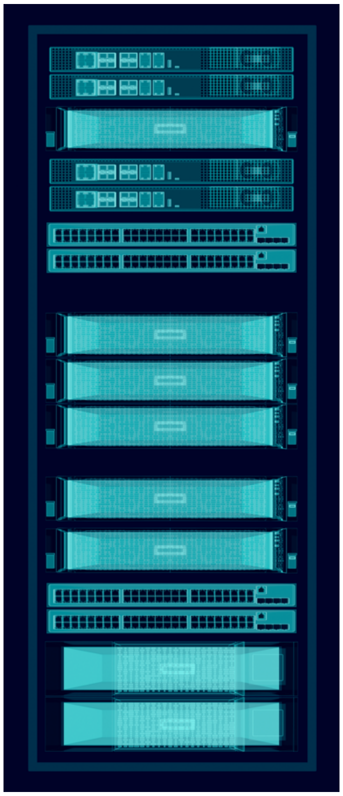
Virtualization at the Core

The IADC hosts a wide variety of Siemens process automation systems and software, ranging from process control to visualization, engineering and simulation. These applications are deployed as virtual machines (VM) on servers mounted in the IADC rack, allowing the user to benefit from typical VM advantages. These include lower total cost of ownership (TOC), lower hardware costs, higher system availability (lower downtime), faster application deployment, and faster disaster recovery response. Siemens brands this solution “SIMATIC Virtualization as a Service,” or SIVaaS.

The IADC engineering services provided by Siemens start with the specification, purchase, assembly, and installation of proven technology from market leading vendors. These solutions include front & back firewalls, industrial DMZ, IT & OT networking, computing, backup & disaster recovery, process historian, and uninterruptible power supply. The operating system, VMs, and applications are then installed and configured to the customer’s requirements.

Built-in Redundancy

To ensure high system availability, hardware components such as fans, power supplies, network cards, and system components such as firewalls and switches are always set up in a redundant configuration. Redundancy options are available that offer a two-host configuration using PCS 7 OS Server redundancy only for hot standby availability, or a three-host configuration using PCS 7 redundancy as hot standby and VMware vSAN as additional cold standby high availability. The vSAN concept is also capable of providing redundancy for a complete cluster, for example, if hosted in separated fire zones.



Siemens Recommends Rack Servers for IADC

Rack Server Preferred

The requirements of OT application software such as PCS 7 regarding the underlying hypervisor layer are significantly higher compared with typical IT applications, a fact that can lead to conflicts during the lifecycle of the asset. To address this, Siemens recommends separating OT applications from other IT applications by using different IT infrastructure environments. Blade server architectures are also feasible, but at significantly higher costs. According to Siemens, all known cases where blade servers were used, eventually reverted to rack servers.

Dedicated OT Networks

Siemens recommends physically separating OT networks from IT networks and using industry-proven infrastructure devices like the company's own SCALANCE switches. The reason is that cross-communication between automation devices may use protocols not supported by commercial switch providers, possibly causing malfunctions. In particular, the parallel usage of redundancy protocols such as MRP and RST within the same network has been known to cause malfunctions in existing plants.

First Priority: Cybersecurity

Cybersecurity is top priority for any IT solution, but once again the security requirements for OT systems may differ from those common in the IT world. Siemens addresses security with a holistic approach around the Defense in Depth (DiD) concept based on IEC 62443, which puts up multiple layers of security around the plant, network and system. Hardware, software and services for network security and system integrity are already integrated, so that two of the three layers of the DiD concept are served.

For network security, the solution includes next generation firewalls, IT/OT network segmentation, and industrial DMZ (jump host, remote access). For system integrity, the solution supports these features: computing (hardening, authentication), backup & disaster recovery, log management, endpoint protection, vulnerability management, and patch management.

Application Support

The table below lists the functions and Siemens applications currently supported. As a platform, users can easily integrate a wide variety of third-party applications with these functions.

Function	Application
Process Control	SIMATIC PCS neo, SIMATIC PCS 7
Engineering	SIMATIC Step 7, TIA Portal, COMOS
Visualization	SIMATIC WinCC, BRAUMAT
Building Management	DESIGO CC
Simulation	SIMIT

Siemens Supports These Own Applications on IADC

Conclusion

Forward-looking concepts like Industry 4.0 and digital transformation have been around long enough for even the most conservative process industry users to see them as a key part of their future. But these concepts represent a journey guided by principles and ideals, attainable only with the application of new technologies. Engineered solutions like Siemens' IADC are designed to help users cross the digital chasm and modernize their automation architectures to reap the benefits of digitalization.

Since its introduction in 2015, Siemens has delivered more than 2,100 IADC hosts with 37,000 cores and 59,000 VMs at over 200 customer sites. That is quite a lot of experience in IT/OT integration – a domain that many still consider new in industrial applications. Process industry users should consider such engineered solutions that rely on both domain knowhow and IT expertise. However, few users have personnel with the right IT skills in place, so such solutions must be accompanied by a package of lifecycle services to help users get started along their digital transformation journeys.

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 of it may be reproduced without prior permission from ARC.