SIEMENS
Ingenuity for life

Case Study

Modernized Siemens Industrial Network virtually eliminates downtime while providing a backbone for digitalization

As a large Siemens plant in Texas set its sights on fully digitalized manufacturing, it deployed an advanced OT network to gain greater reliability, flexibility, and security

As industrial enterprises around the world accelerate their journeys toward end-to-end digitalization, they're finding that secure, deterministic networks must be the strategic backbones of their operations. That's because data drives digitalization, but not all data is the same. Control data differs from a web page in that it must get to its destination – an actuator, a valve, a motor, or other field-level devices – at the precise moment a process requires that device to do its job. If not, all sorts of consequences can result.

Over the years, many plants built their production networks as extensions of their front-office, enterprise IT networks, resulting in a host of performance and security issues. IT networks operate on a best-effort, packet-delivery basis, with data latencies many orders of magnitude higher than what operational technology (OT) networks can allow. While office users won't notice one or two-second delays in sending an e-mail or accessing a database, such delays can cause costly production disruptions, possibly endangering personnel, the environment, or both.

In fact, production disruptions were a big issue that the giant Siemens switchgear and circuit breaker plant in Grand Prairie, Texas, aimed to reduce when it conducted a fundamental overhaul of its OT network. The plant's offices cover nearly an acre of ground while its manufacturing operations, including fabrication and two assembly lines, are about four times that size. Its network that interconnected the sprawling operations was many years old, built on enterprise IT network principles, and not well-optimized for production.

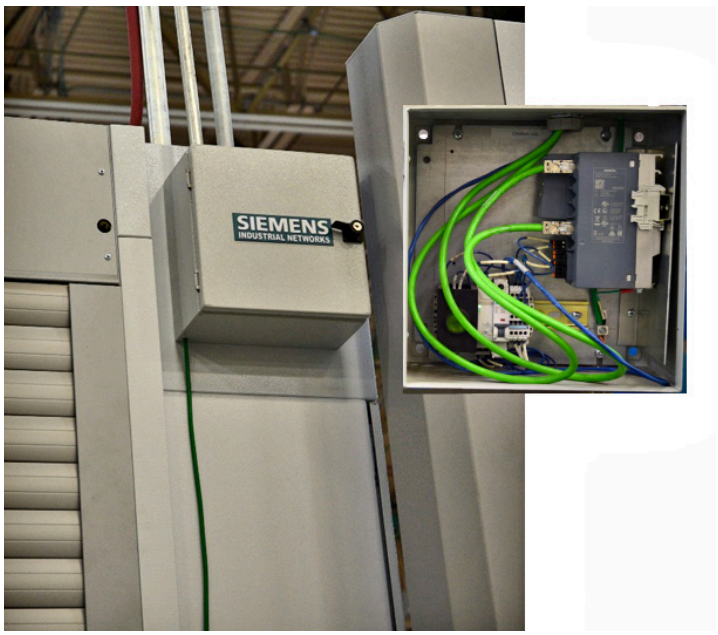

Figure 1: One of 38 SCALANCE SC636-2C firewalls securing the automation network

Challenge: Poor network reliability, causing frequent production disruptions

The plant suffered from poor network reliability that was due to many factors. “Basically, we had a very standard IT network topology,” says Brian Nappier, Siemens business excellence specialist. “We had one switch in our server room, a firewall back to all our remote applications, and then switches throughout the facility to support all the office PCs, plus the PCs on the shop floor. And our production team had no control over those firewalls or switches.”

Another problem was due to faulty IP addressing schemes that caused devices to lose their IP address, effectively disabling the machines to which they were connected. “Typically, you didn’t know it happened until an operator reported it,” Nappier says. “And when it was reported, it took a day to fix, but meanwhile the machine stood idle, along with its operator.”

Patching servers and PCs across the network also disrupted production, especially when they were sent without notification. “In addition to our production software, our shop-floor PCs had standard office and collaboration applications on them, despite not needing them, so when a patch would be pushed across the network to them, they’d be down for as long as an hour while the patch was applied,” Nappier said.

In addition, the existing IT network lacked flexibility. Relocating a CNC machine and its work cell as part of reconfiguring assembly workflows could take up to two weeks, mostly due to rewiring and reconfiguring the network. And if one of the machines had a problem, its OEM supplier had no way to remotely connect to it through the network, so a service call was required that took time and expense.

It turns out all these issues and their disruptions were taking a huge toll on productivity, according to a study Nappier conducted. He found that an hour of downtime in the fabrication area impacted assembly productivity by three hours, idling workers and affecting delivery schedules. “In the two-year period we investigated, network connectivity interruptions occurred in 21 of the 24 months,” he says. “Over half of those periods sustained multiple network connectivity incidents.”

Solution: Overhaul the plant’s OT network to facilitate fully digitalized manufacturing

Clearly the plant needed a new OT network, separate from the IT network but bridged via a so-called demilitarized zone (DMZ). Fortunately, the plant’s plans to become a fully digitalized enterprise required just that. Management wanted to integrate and automate many manual processes to improve workflow efficiencies and output. Other goals included greater operational visibility, support for mobile applications, central alarm reporting, and secure remote access for suppliers, including OEMs.

“As part of our larger digitalization effort, we knew that we had to start by totally reengineering our network,” says Nappier. “After all, digitalized production relies on a secure, reliable, and flexible network to move vast streams of many different data types to where they need to go and needs to be separate from our IT network.”

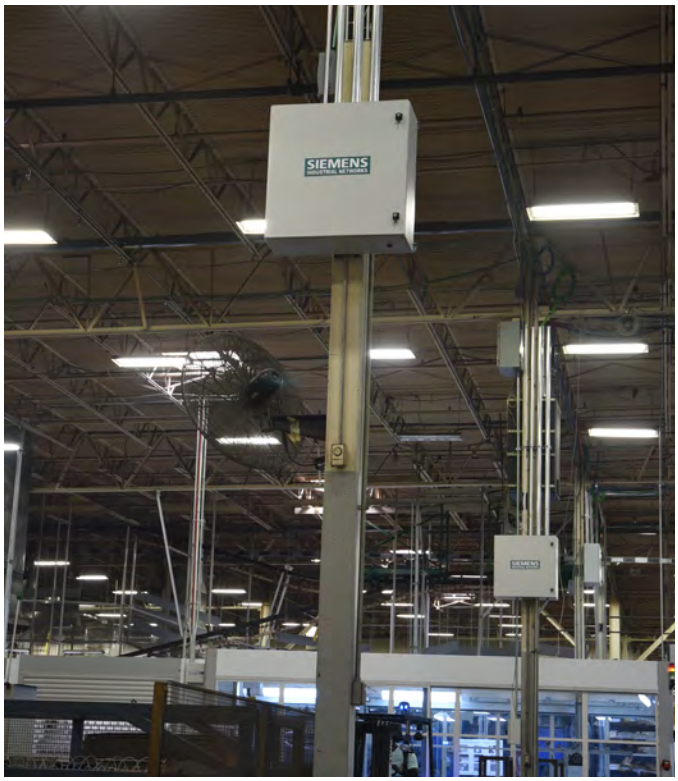

Figure 2: Enclosures house a SCALANCE X416-4C to establish the network backbone with a ring

Siemens assembled a cross-functional team to create the strategy, design the solution and implement the new network architecture. Siemens OT network experts devised the new network configuration and security measures while collaborating with Corporate IT. Prism Systems, a Siemens Solution Partner, assisted with the implementation.

“It was truly a team effort,” Nappier says. “In the end, our OT network’s modernization became the upgrade template for five other Siemens plants as well as for customers, too.”

The team started by carefully defining its objectives for the new plant network. Those included:

- A design specifically for the factory’s requirements with highly deterministic data delivery
- High availability via redundancy to prevent disruptions and improve asset utilization
- Network security internally and externally, with OEM remote access for diagnostics and issue remediation
- Flexibility to enable easy reconfiguration of shop-floor workflows and equipment relocations
- Scalability to easily expand the network as plant requirements grow
- Powerful diagnostics to flag performance issues and enable fast and effective resolutions
- Real-time alerts when network performance degrades or disconnects occur
- Redundant power supplies as back-ups in case of power outages

To meet these requirements – about as good a list for a modern OT network as there is – the plant deployed the following Siemens networking and power components in a redundant ring topology with subnets for each of the 45 CNC machine work cells:

- **RUGGEDCOM RX1400 firewalls,** with two redundant, rack mounted units installed in the plant's secure computer room as part of the DMZ for secure IT / OT collaboration
- **SCALANCE XR524-8C Layer 3 switches,** with two redundant, rack mounted units also installed in the computer room, and each communicating with the industrial firewalls and forming redundant rings with the Layer 2 switches.

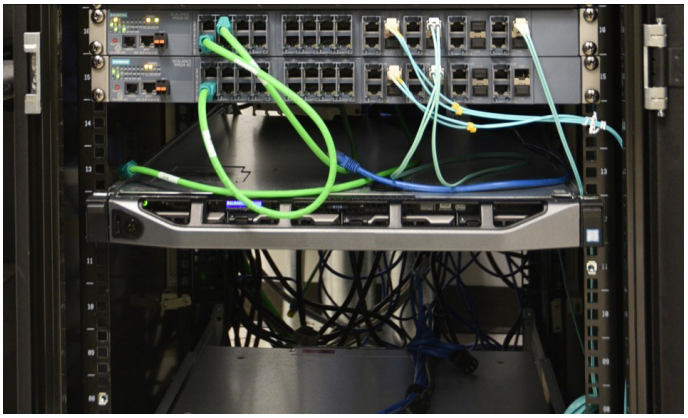

Figure 3: SCALANCE XR524-8C Layer 3 switches on the server rack as part of IT / OT collaboration

- **SCALANCE XM416-4C Layer 2 switches**, with 13 units installed on DIN rails attached to the vertical roof-support columns in the fabrication area and providing interconnects for the network ring.
- **SCALANCE SC636-2C firewalls,** with 38 units installed, virtual private network (VPN) capability, and an on-board SINEMA Remote Connect for secure remote access
- **SITOP power supplies and Ethernet enabled UPS1600 (uninterruptible power supply) battery backups,** with redundant 24 V DC UPS to provide at least one hour of network uptime in case of power failure.
- **SINEMA Remote Connect,** a secure remote access platform to manage access rights and encrypt communication with OpenVPN.
- **SINEMA Server,** for centrally managing the entire network, access privileges, including OEM, all from a single console dashboard.

Gigabit speed with High Speed Redundancy Protocol (HRP) was implemented to provide high availability. The reconfiguration time in the case of a defective ring is a maximum of 300 ms. Multiple security measures were implemented as part of the Defense in Depth strategy. A DMZ with redundant firewalls, manufacturing cell segmentation with firewalls, secure remote communication with SINEMA Remote Connect and OpenVPN as well as network monitoring form multiple security layers.

"We wanted to isolate our plant OT network from the IT network, so we could optimize its performance, which would in turn improve overall plant performance," Nappier says. "Ultimately, we wanted to know about network and work cell issues before even our operators did, so we could take proper steps to mitigate or remediate problems before they disrupted production."

Results: Greater network reliability, flexibility, and security – plus network-caused downtime virtually eliminated

Nappier reports the plant's new OT network meets all of its design objectives – with significant upside benefits. What's more, once the new OT network was fully deployed, he commissioned penetration testing to gauge the strength of its cyber safeguards and found them to work as expected. "The testers called us and said, 'hey, we can't see the machines at all…' and we told, them, 'Good. You're not supposed to.'"

Now the plant's OEMs can gain secure access to their machines only for diagnostics and firmware upgrades. In addition, the plant now has greater flexibility to configure and move their machines around. Nappier cites the case of retrofitting one critically important CNC bus-punching machine that would have previously required two weeks to be fully networked and operational. "We had the machine on the network and able to communicate with its operator in just two hours," he says.

In another example, Nappier recalls having to move 12 CNC machines on the shop floor, which he estimates would have taken 1,700 hours in total, but with the new OT network in place, the job took just 23 hours. "We added eight new work cells to the network, taking just 16 hours," he says. "Before, those tasks would've taken us 640 hours, so that's a time reduction of almost 98 percent."

In terms of performance, Nappier conducted speed tests and found the plant's new OT network operates 50 percent faster than the enterprise IT network that was previously used. "In addition to installing the latest available network hardware, we configured the network to operate at the fastest possible speeds including gigabit bandwidth to the operators' PCs," he says.

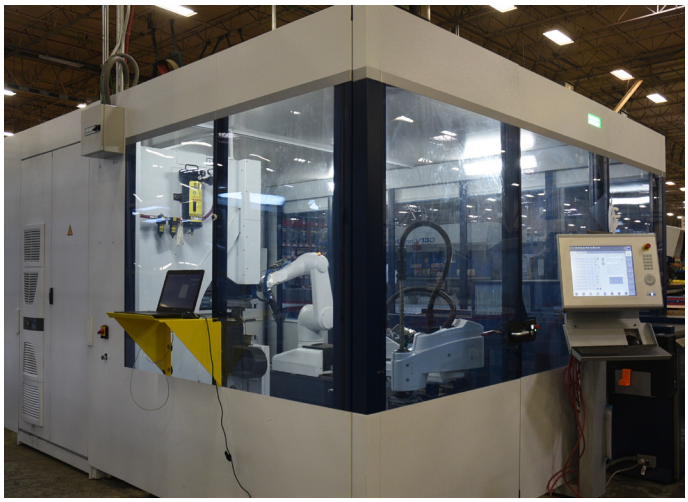

Figure 4: The SCALANCE networking components throughout the facility and in the enclosure in the upper left, support the automation devices.

Disruptions due to network downtime have been virtually eliminated, too. Security scanning and OS patching of operators' PCs are scheduled during non-production hours. Also, their PCs have been cleared of all but the applications needed to run the machines. "After-hours support calls have been cut by 80 percent," Nappier says.

"Even more important," he adds, "we reduced the downtime in our fabrication department due to any sort of network disruptions from 3,083 production hours to just 15.4 hours, the latter occurring during the network commissioning.

> "That's huge for us, especially since we found that an hour of downtime in fabrication impacts assembly by three hours. This new OT network has been nothing short of transformational."
>
> – Brian Nappier

Learn more:

Network Security:
usa.siemens.com/network-security

Professional Services:
usa.siemens.com/industrial-network-services

Industrial Networking:
usa.siemens.com/future-ready-networks

Published by
Siemens Industry, Inc. 2019.

Siemens Industry, Inc.
5300 Triangle Parkway
Norcross, GA 30092

For more information, please contact
our Customer Support Center
Phone: 1-800-241-4453
E-mail: info.us@siemens.com

usa.siemens.com/future-ready-networks

Order No: NTCH-GPNET-1019
Printed in U.S.A.