

PROTECTING HIGH-AVAILABILITY OT ENVIRONMENTS

SECOMEA

From legacy VPNs to segmented, scalable OT remote access for automotive manufacturing

Operating in a highly regulated and performance-driven environment, a premium UK automotive manufacturer needed to modernize how external connectivity into its production facilities was governed.

*The goal was to **replace fragmented, manual access methods with a secure, scalable solution** that would protect uptime, enable rapid supplier collaboration, and provide a robust, long-term security foundation for future production expansion.*

THE CHALLENGE

Production lines relied on PLCs running critical processes across robotic cells, assembly stations, and industrial equipment.

External vendors required remote connectivity for diagnostics, troubleshooting, and configuration – but existing access methods **lacked standardization, visibility, and centralized control**.

The new remote access approach had to improve security without introducing operational friction, while also:

- Support Siemens S7 communication and TIA Portal workflows natively
- Provide granular, role-based access to defined endpoints only
- Enable third-party connectivity without exposing the wider OT network
- Minimize on-prem infrastructure overhead through a cloud-based approach that could scale across lines, plants, and supplier ecosystems

THE SOLUTION

External connectivity into PLC-driven production systems is unavoidable in modern automotive manufacturing. The differentiator is how securely and efficiently that connectivity is governed.

Following a structured RFI and RFP evaluation process involving IT security, NetSec, and engineering stakeholders – Secomea achieved the **highest technical score among all reviewed vendors**.

The deployed architecture delivered:

- Proven Siemens compatibility – validated support for Siemens S7 PLCs and TIA Portal workflows
- Segmentation by design – least-privilege, time-limited sessions
- Secure third-party access – centrally governed authentication and authorization
- Centralized, SaaS-based management with minimal local footprint and high scalability potential

THE RESULT

Uncontrolled access paths, legacy VPN constructs, and unnecessary jump hosts were eliminated.

With Secomea's purpose-built Secure Remote Access solution, this manufacturer transitioned **from reactive access management to a structured OT security strategy**.

The implementation led to:

- ☑ Improved production uptime and cyber-physical systems (CPS) security governance
- ☑ Stronger alignment between IT security and operations
- ☑ Secure supplier enablement without onboarding friction
- ☑ Reduced architectural complexity
- ☑ Enterprise-wide scalability aligned with automotive production growth

The organization established segmented, auditable connectivity into production systems that balances security and usability across stakeholders.

THE BUSINESS OUTCOME

Production uptime is protected. Supplier collaboration is streamlined. Infrastructure complexity is reduced while control is strengthened. And the model scales with manufacturing growth.

Security that protects production – without slowing it down.

secomea.com

Built for OT, Trusted by IT

IEC 62443-certified

Based on a Zero Trust architecture