KONSEC
make things real

Cybersecurity

Kosu Zero Trust Strategy

Martin Konold

Dr. Simon Heugel

KONSEC GmbH

06.11.24, Stuttgart / Filderstadt

Securing Next-Gen Manufacturing: Zero Trust Cybersecurity Strategies for Commissioning of Industrial Production Lines

Executive Summary

As manufacturing evolves, embracing digital transformation and Industry 4.0 technologies, cybersecurity becomes paramount. Manufacturing Execution Systems (MES) and Programmable Logic Controllers (PLCs), essential to modern production lines, face unprecedented threats due to global supply chains, remote contractor involvement, and legacy system vulnerabilities. Kosu, a secure platform as a service (PaaS), addresses these challenges by enabling a robust zero-trust security model, tailored for industrial control systems. This whitepaper explores the Kosu platform which provides secure, efficient production line setup, reducing risks associated with contractor access and enabling compliance with standards such as ISO 27001. The Kosu platform offers an agile, cost-effective approach to safeguarding commissioning of new production lines with lifetime benefits while improving Start of Production (SOP) times.

Introduction: Manufacturing Cybersecurity in the Age of Industry 4.0

The shift to Industry 4.0 has brought new efficiencies to manufacturing but also heightened cybersecurity risks. Digital transformation means traditional MES and PLCs must integrate with a range of connected devices, often sourced from multiple suppliers, creating potential entry points for cyber threats. Legacy systems designed for functionality over security are especially vulnerable, as evidenced by incidents like Stuxnet, which exposed risks inherent to industrial control systems (ICS).

For organizations to achieve resilient operations and remain competitive, cybersecurity must be seen as an enabler rather than a burden. Manufacturing businesses, in particular, stand to gain from proactive cybersecurity strategies that enhance operational resilience, compliance, and client trust. Kosu's secure platform as a service (PaaS) offers a zero-trust model that isolates contractors and suppliers, enabling secure remote access without requiring extensive provisioning at the manufacturing plant.

Cybersecurity Challenges in Manufacturing Today

Contractor and Supply Chain Risks

With the integration of globally sourced components, manufacturers often rely on contractors to configure and deploy production line components. However, granting contractors on-premises access creates significant risks. Multiple contractors may work simultaneously within the same network segment, and their systems may lack consistent security standards. Additionally, contractors often send junior engineers with senior supervisors accessing systems remotely, which increases the risk of unauthorized access via VPNs or unsecured devices.

MES and PLC Vulnerabilities

MES and PLCs are frequently integrated without strict security protocols, primarily due to concerns over production downtime if patches or updates are applied. As a result, these systems often operate without the latest if any security measures, making them vulnerable to malware and other threats. Additionally, PLCs, which control production processes, are configured to communicate with MES but can be a gateway for malicious attacks if compromised.

Perimeter Security Gaps

Traditional perimeter security approaches, such as VPN-based remote access, fail to provide adequate control over contractors and third-party vendors. Contractors who connect remotely from various jurisdictions introduce compliance concerns, and the production line network often lacks sufficient isolation, increasing the risk of unauthorized access to other sensitive areas within the plant.

Current Workaround Solutions and Their Limitations

Remote Pre-Integration by Contractors

Many manufacturers attempt to mitigate risk by having contractors configure systems offsite and then perform the final integration onsite. While this approach reduces direct network exposure, it still requires contractors to connect their devices to the production line network, leading to potential security and compliance issues.

On-Site Device Use

Commonly, contractors bring their own devices (BYOD) to the client site, creating security risks as these devices may lack consistent security protocols or be difficult to monitor. Additionally, on-site engineers often rely on unsecured VPN access, which lacks the stringent access control needed to prevent malicious intrusions.

Simulation Limitations

Pre-deployment testing is often attempted through simulations or emulations, but with the wide variety of PLC architectures and the complexity of integration, this approach rarely replicates real-world conditions effectively and is in many cases not feasible due to the lack of appropriate support for exotic PLCs.

Zero Trust Security Architecture: A Proactive Approach

In contrast to traditional methods, a zero-trust architecture offers a secure, proactive solution to manufacturing cybersecurity. By assuming that all devices and users are potential threats, zero trust minimizes the risk of breaches and secures access at all levels. Kosu's zero-trust approach enables

manufacturers to implement a secure framework without extensive configuration changes or reliance on untrusted third-party systems offering a simple but transparent security framework.

Key Principles

Mutual Authentication Kosu uses cryptographic certificates to verify all devices, ensuring secure access without default trust.

Attribute-Based Access Control (ABAC) ABAC provides granular control, allowing access only to specific resources based on defined attributes.

Network Segment Isolation By isolating different contractors and network segments, Kosu minimizes the risk of lateral attacks within the production environment. No contractor can see the presence of its competitors.

Disposable Infrastructure To limit exposure, Kosu's zero-trust model leverages disposable computing infrastructure, ensuring that each session operates in a controlled, isolated environment. Hardware is reassembled newly for each project with newly programmed firmware, BIOS, operating system, fixed project specific configuration and security tokens.

Impact on Compliance

Zero-trust security architecture supports ISO 27001 compliance, offering an agile, scalable cybersecurity solution. By removing the human factor, Kosu reduces reliance on the training, awareness and monitoring of third-party engineers, further enhancing security and reliability.

Introducing the Kosu Platform

Kosu Box

Kosu Box is a preconfigured device that provides secure, zero-configuration network access for contractors. Kosu Box uses a secure, temporary security token to identify and authenticate the device, which connects to the Kosu platform via cellular network, enabling global access. With remote monitoring, Kosu Box ensures a secure connection without requiring access to the client's network or local DSO involvement. All access control is implemented in the Kosu Cloud and therefore not prone to security breaches in the realm of the contractor.

Kosu Cloud Instance

Each project deploys a dedicated, isolated Kosu Cloud instance, complete with MES, database management systems (DBMS), and network segmentation using infrastructure as code. This on-demand, disposable infrastructure operates independently of the internet, offering strict control over contractor access while ensuring a secure, authenticated environment for client engineers.
Access for MES engineers is strictly controlled via mutually authenticated web access.

Kosu Services

Kosu provides end-to-end services to streamline deployment, including ISO 9001 and ISO 27001 compliance, incident response, and flexible configurations. With a pay-as-you-go model, Kosu offers global support and seamless integration across regions, including areas with restrictions such as the Chinese Great Firewall.

Case Study: Bosch and Remote Production Line Deployment

During the lockdowns of 2021 and 2022, Bosch required secure, remote setup for production lines in China. Kosu enabled Bosch to achieve this without travel. In addition reducing both environmental impact and logistical costs. Kosu's platform-as-a-service model allowed Bosch to maintain productivity and resilience, setting a precedent for secure, remote manufacturing in restricted environments.

Conclusions

Kosu's zero-trust approach enables manufacturers to secure contractor integration and reduce cybersecurity risks, enhancing reliability and accelerating time-to-market. Manufacturing businesses stand to benefit from Kosu's robust, compliant solution, which not only reduces travel costs and carbon footprint but also shortens the Start of Production (SOP) timeline. With Kosu, manufacturers can achieve resilient operations, protecting assets while meeting global cybersecurity and compliance standards.