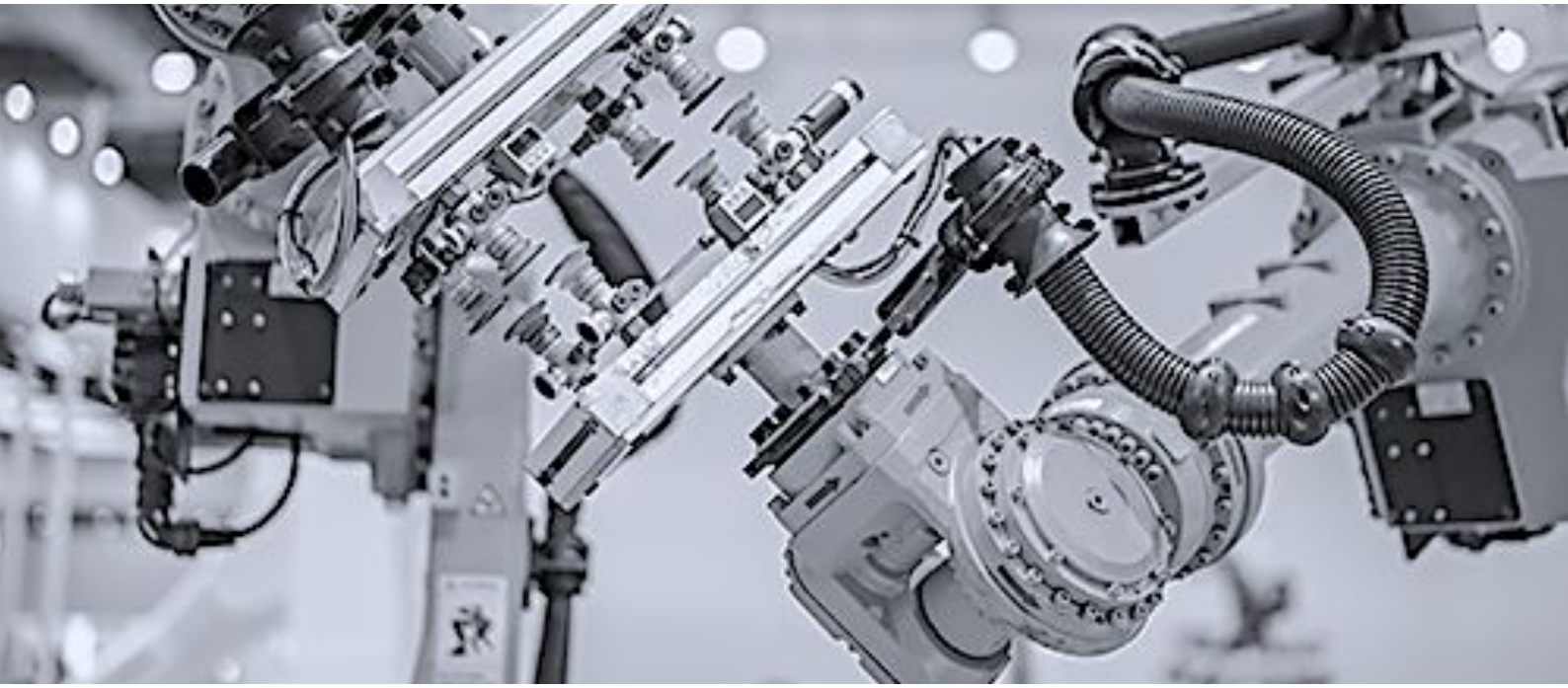
Case Study

Addressing Transformation Challenges With Zero Trust From Industrial Automation to Industrial Autonomy



Background

The era of the pandemic has shed light across many industries for the need to be resilient in providing steady-state and dynamic connectivity between remote workforce, services and machines.

The drive to future-proof industrial control systems in supporting more efficient, sustainable, and safe manufacturing plants is imminent - integration of robotics, autonomous software technologies in production lines, and process control systems, plant operators can achieve long-term operational benefits.

However, there are digital transformational challenges - Connectivities, Infrastructure/Networking and Security across cyber-physical systems (smart factories), the mobility of operators, and the need for interconnection across other operations in the supply chain.

By taking advantage of the benefits of Industry 4.0 and innovative technologies supporting integration capabilities in multi-protocols heterogeneous systems, industries can reduce the integration risks and costs as they transform from Industrial Automation to Industrial Autonomy.

Challenge

The varying conditions and needs of each plant imply that there isn't any standard "to-do list" that we can adopt to achieve digital transformation. Similarly, the degree of transformation required varies from plant to plant. In this very complex scenario of heterogeneous systems, in many cases still relying on legacy systems, OT managers and CISOs are challenged with new complexities, including integration, increasing workloads, costly compliance efforts and the rise of cyber and operational risks.

Industry

Industrial Automation(AI), Industrial Autonomy(AI), Industrial Control System (ICS)Operational Technology Plants

Challenges

- Continuity of operations
- Limited computing resources
- Legacy Systems
- Limited bandwidth
- Hard updating and restarting
- Poor security of industrial protocols

Goals

- Implement network virtualisation and segmentation for greater isolation and protection against plants' supply chain attacks
- Seamless lightweight security integration into legacy and resource-constrained devices
- Reduce plants operational costs

Solution

SE*link*™ provides a zero trust security model combined with software-defined network segmentation, privileged access management, whitelisting practices and lightweight security. Delivering Data, Device and Network Security and Control in one single solution.

Solution

Industrial autonomy is a crucial part of Industry 4.0 enabling industrial assets and operations with adaptive capabilities. By harnessing big data analytics, logs and machine learning through Artificial Intelligence (A.I), autonomous control systems will respond with zero or little human interaction to situations within secure domains that were not anticipated in the system designs. Industrial autonomy lets industrial companies harness innovative technologies (e.g. SE*link*™) to create true digital transformation of operational strategies.

SE*link*™ is a Zero Trust, Service-oriented, Secure Virtual Networking solution to address challenges in connectivities, networking and security of endpoints (e.g. human operators, production machines, robots, sensors, analytics cameras, etc) and networks alike.

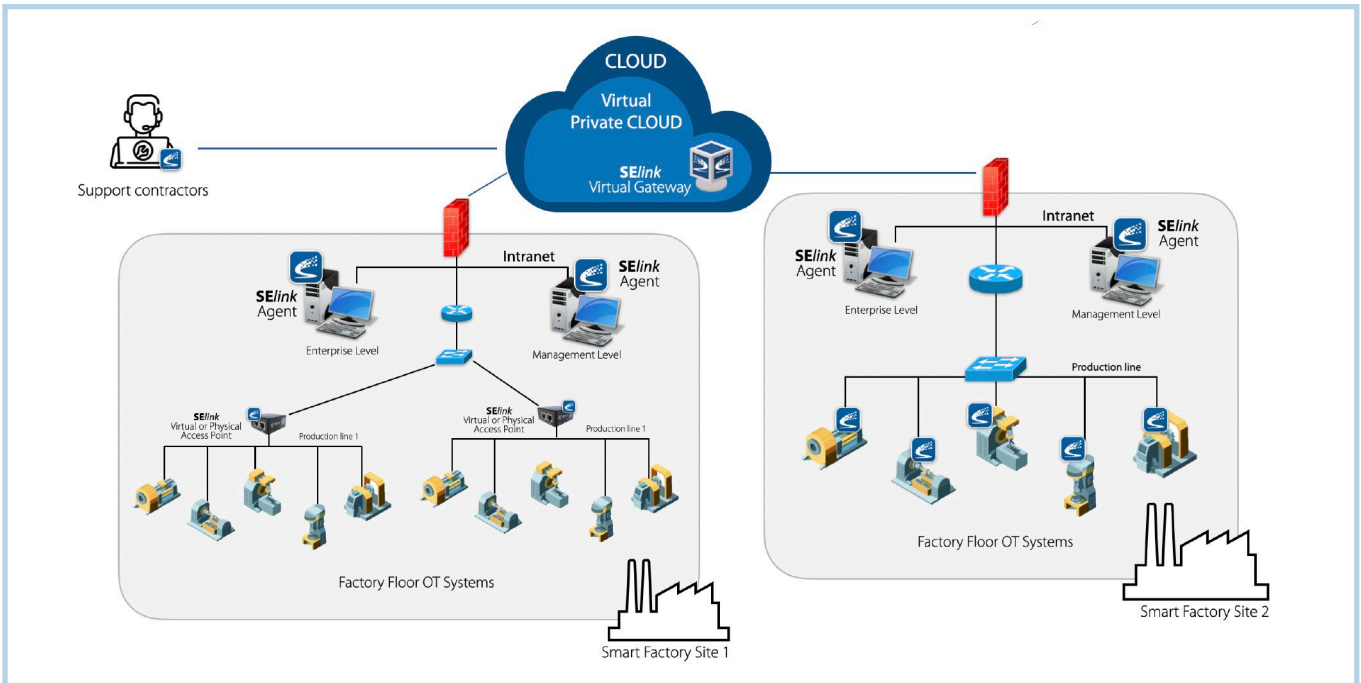
SE*link*™ replicates seamless heterogenous behaviours as in a physical private LAN of a production line. All network resources, intermediaries and endpoints will be virtualised on a virtual LAN regardless of their physical geographical location in the world.

As industrial companies gearing towards Industrial Autonomy, data-hungry driven analytics technologies (e.g. A.I.) requires continuously flow of uninterrupted data feeds from multiple endpoints and servers from any kinds of network topologies. The inherent design of SE*link*™ context-based granular access control is part of ZTNA model. Each singular data traffic is vigorously authenticated, authorised and encrypted (i.e. based on industrial and quantum safe cryptographic schemes), and transported over assigned micro channels to reach its respective destination(s).

8 Compelling Benefits

1. **Zero Trust Network Access (ZTNA)** simplifies implementation of ISA/IEC-62443 Series of Standards
2. **Rationalisation of Operational Costs** No VPN, No PKI Infrastructure, No Public IPs
3. **IT-IIOT Integration** of Security into Heterogeneous Devices, inc. Legacy Assets
4. **Lightweight Protocols** guarantee Low Latency, Less Bandwidth, High-Speed & Scalability
5. **Zero Encryption Overhead** vs commonly used TLS/SSL
6. **Cyber Resilience** to Quantum Attacks
7. **Enhanced System Longevity, Redesign-free** through Crypto Agility
8. **Easy & Efficient Management** with access from anywhere Management Suite

From a single pane of glass, SE*link*™ gives OT managers true Accessibility & Isolation control over the entire network. Assets in the IT/OT network are isolated and protected. No Public IP addresses nor opened inbound ports are needed, preventing any possibility for remote attackers to reach the assets. Yet, OT managers can grant dynamic access to remote workers / 3rd party vendors to access their respective device(s) of interest (e.g. maintenance or upgrades) while completely blindfolded from seeing nor accessing any other resources or machines in the network - stops propagation of threats. That's Zero Trust for IA.



Blu5 Group
info@blu5group.com
www.blu5group.com