Case Study

# Reaching Industrial Control Systems Resilience through a Zero Trust Model

## Background

Digital technology has been broadly implemented across various industries, successfully automating production processes and machinery as well as delivering greater production efficiency. The implementation of plant control networks and SCADA systems became the foundation of today's Operational Technology.

These implementations may not have foreseen the need to support communication across cyber-physical systems, the mobility of operators, nor the need for interconnection across the operations value chain to enable a smart, integrated factory. This, however, does not mean that these existing systems necessarily have to be replaced to take advantage of the benefits of Industry 4.0. Through innovative technologies that support seamless integration capabilities in multi-protocols heterogeneous systems, industries can reduce the risks and enable full visibility and control of their Industrial Control Systems (ICS) networks.

## 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 Control Systems
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
- Increase stability and longevity of ICS systems
- 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

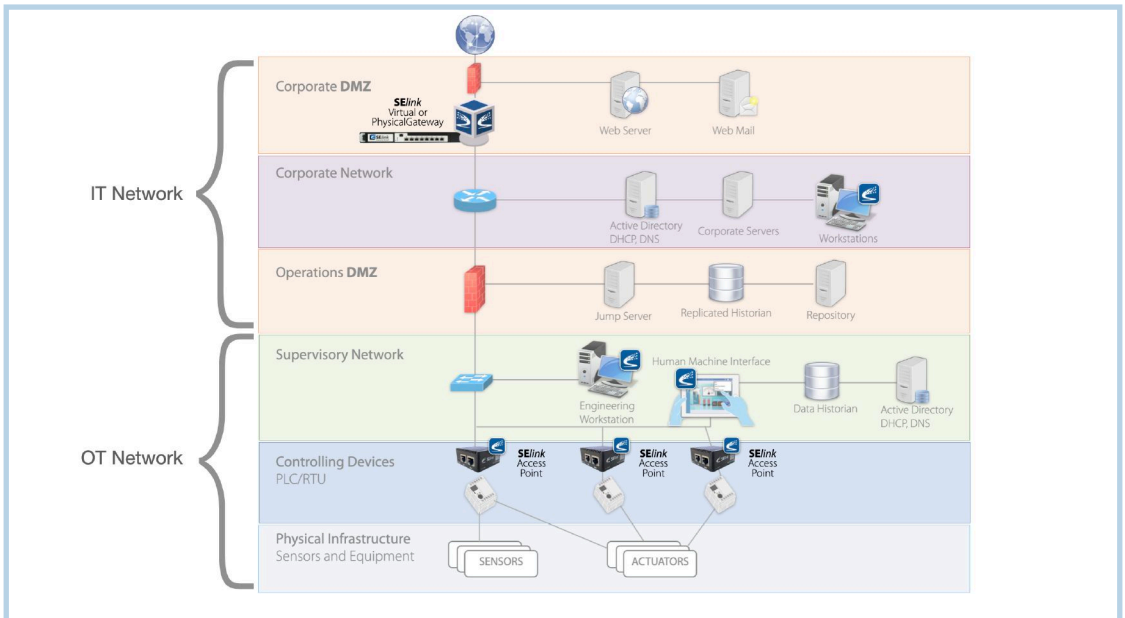
Cyber-physical systems (CPS) that support critical infrastructure industries are highly dependent on OT and IT systems for their command and control. Industrial control systems (ICS) are connected to the IT infrastructure providing remote connectivity for real-time data and remote support. This is challenging OT and Security teams with new complexities, including the rise of cyber and operational risks and increasing workloads. Enterprise techniques, processes and tools are not as effective, can be incredibly costly to implement and can cause issues. Not to mention the fact that legacy systems cannot be updated, secured or replaced without considerable cost and risk.

**SE*link*™ is a service-oriented, secure, virtual networking solution** to protect end-points and networks alike. Able to replicate heterogenous clients and server behaviours in a seamless way, as in a private LAN; when the OT is inter-connected to IT network, through SE*link*™, both networks and endpoints are all virtually relocated in the same server LAN regardless of their actual geographical location.

**The SElink™ Gateway performs endpoints "virtualisation"**, showing to the server the original MAC address and a unique, registered, identifier for each managed device. The advantages are overwhelming. SElink™ protects both the data channel, the access to a micro channel and a specific service, which is only created and used by authenticated and authorised processes through context-based granular controls. This ensures that all assets in the IT/OT network are hidden and protected even in the event that a device is compromised, for example in the event of a supply chain attack. Endpoints no longer need public static IP addresses or open ports willing to accept connections, to the benefit of a reduction of the attack surface as well as operational costs. Lightweight protocols and zero encryption overhead make band availability and the integration of security into legacy assets no longer a limit. Easy to be integrated in any environment, over any protocol, portable, multi-device with the benefit of crypto-agility to guarantee system longevity, SE*link*™ security techniques, are resilient and resistant to quantum computing attacks. Continuous monitoring and logging from a single pane of glass gives OT managers true visibility and control over the entire network overcoming the challenges of siloed environments.

## Benefits

1. **Zero Trust Network Access** strategies simplify the implementation of the ISA/IEC-62443 series of standards
2. **Lightweight protocols** for bandwidth sensitive and resource-constrained devices
3. **Zero Encryption Overhead** compared to TLS/SSL
4. **Smart mechanisms** guarantee low-latency, high-speed and scalability
5. **Flawless IT/OT integration** of security into heterogeneous devices, including legacy assets
6. **Enhanced system longevity and resilience** to quantum attacks
7. **Seamless encryption updates, redesign-free** through Crypto agility
8. **Rationalisation of operational costs:** NO VPN, NO PKI infrastructure, NO static IP addresses
9. **Efficiency and ease of management**




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