Deloitte.

# Achieving a Zero Trust Architecture in an industrial environment with multiple facilities

## A success story from a major industrial organization that leveraged a Cyber Security Program to transform their infrastructure security

**Highlight**

A major chemical industrial organization with multiple critical facilities detected weaknesses in their Industrial Control Systems (ICS) security posture namely access management (internal and remote), network security and security monitoring and engaged Deloitte to increase their security maturity level.

Deloitte designed a Zero Trust reference architecture specific for the client's industry and critical facilities needs which included IT (including cloud services) and OT systems for the multiple sites and industrial facilities.

**Business & Issues**

Growing ICS threats and attacks – as organizations are connecting more components of the OT infrastructure to IT networks and internet (IoT) – amplifies their attack surface, making them more vulnerable to compromise. Moreover, considering these facilities are handling dangerous chemicals that need extreme control and surveillance, these cyber threats can have a catastrophic impact and cause harm to human lives. Additionally, a major incident in a critical industrial organization can compromise the environment, business advantage and even put their survival at risk.

This presented a major shift for the organization that leveraged the new security architecture to upgrade current infrastructure and use it for future implementations in other industrial facilities.

Deloitte was engaged by a chemical organization with critical facilities which demand strict controls due to the usage of dangerous chemical products. The main challenge was to mitigate their risks related to their industrial infrastructure due to incomplete segregation between IT and OT networks and OT isolation from the internet, nonexistence network and remote access controls and lack of network monitoring and incident response capacity.

## Starting point

Deloitte leveraged the Purdue Reference Model, which is a reference architecture for ICS composed of five levels, namely:

**Physical Process (Level 0)**
Defines the actual physical processes of the manufacturing facilities;

**Intelligence Devices (Level 1)**
Sensing and manipulating physical processes (sensors, analyzers, actuators and other instrumentation);

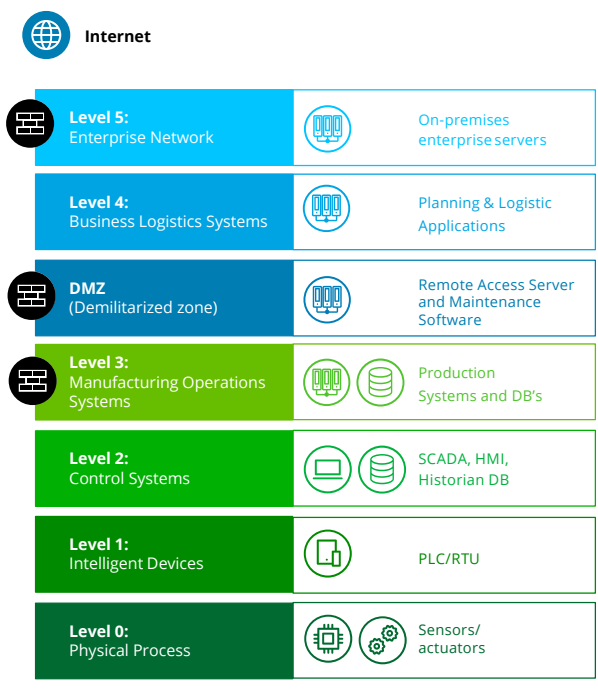
**Control Systems (Level 2)**
Supervising, monitoring and controlling physical processes (real-time controls, DCS, HMI, SCADA software;

**Manufacturing OS (Level 3)**
Managing production workflow to produce the desired products;

**Business Logistic Systems (Level 4)**
Managing business related activities of the manufacturing operation.

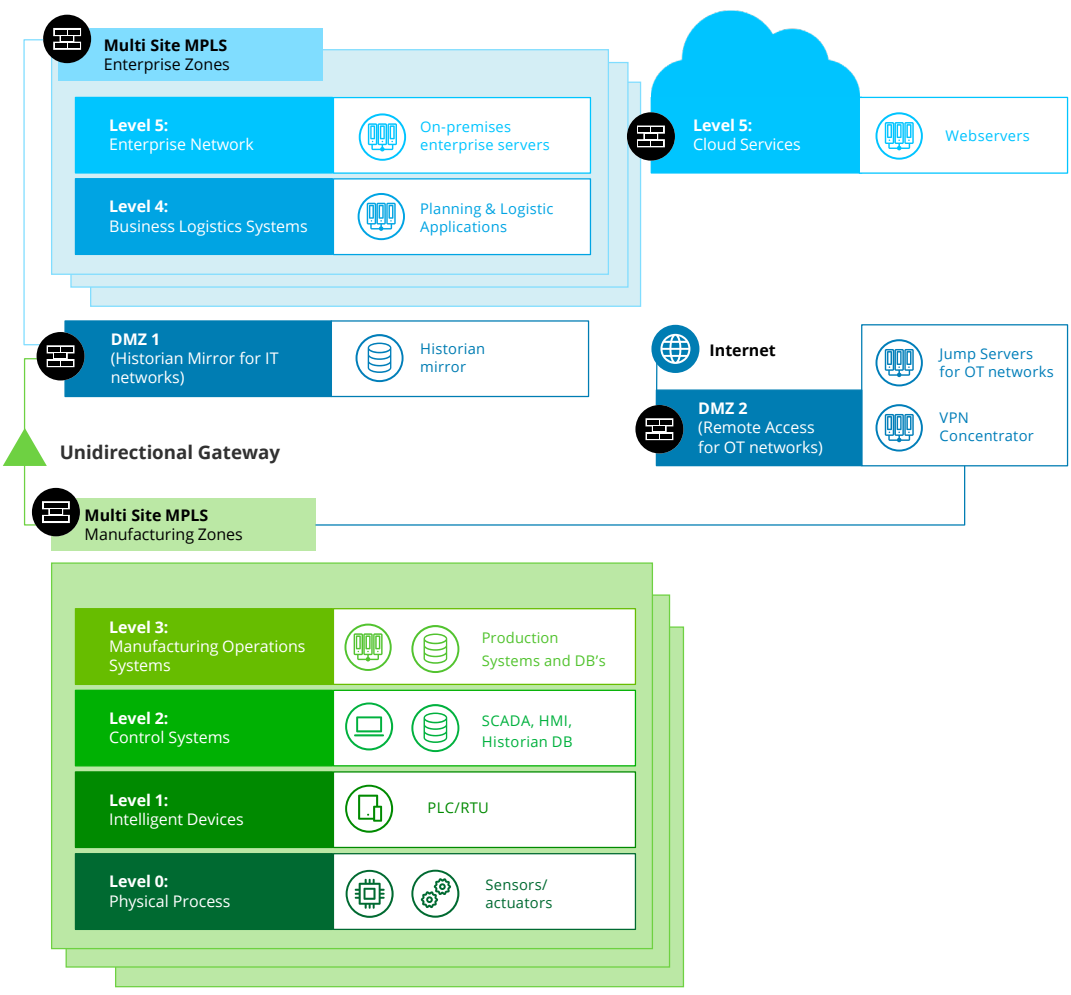
**Enterprise Network (Level 5)**
Managing IT infrastructure and applications (e.g. webservers, VPN access).

Starting with **Purdue Model** as a baseline for secure architecture for Industrial Control Systems (ICS)




Source: ISA99 Committee (2004). Manufacturing and Control Systems Security Part 1: Models and Terminology. Retrieved from http://isa99.isa.org/

Deloitte's approach to achieve a **Zero Trust Architecture in a multi site industrial environment:**




We extended and tailored Purdue Model in order to accommodate specific organization requirements such as communications between multiple sites, namely communication between ICS networks from different sites (dedicated network across multiples sites for ICS environments) controlled points of contact between ICS and IT networks achieving a Zero Trust as a reference architecture.

**Results**

Deloitte was able to design a security reference architecture that fits specific industrial needs, including Information Technology (IT) Systems, Cloud Services and Industrial Control Systems (ICS) across multiple sites and critical industrial facilities. This included a 3-year roadmap that emphasized the zero trust model and depicted client's current, interim and future state. Implementation of this architecture will deliver impact in the following areas:

**Architecture & Governance:**

- Reference Architecture focused on Zero Trust Framework and specific for industry operations;
- Asset inventory and prioritized global services as well as dependencies for migration from on-premises to the cloud;

**Network Security:**

- Achieve IT and OT segregation, through a **Unidirectional Gateway**: a specific hardware that allows data to flow from OT to IT networks, but makes physically not possible to send any information at from the IT networks to the OT networks;
- Implement **microsegmentation** in all levels - a security technique that involves dividing perimeters into small zones to maintain separate access to every part of the network.

**Security Policies:**

- Achieve ICS environment isolation, through security policies and rules related to access and remote access controls through **least-privilege access** principle.

**Identity and Access Management & Secure Devices:**

- Remote Access through VPN connections (including **conditional access such as MFA**) only allowed through hardened Jump Servers with anti-malware and remote session recording solutions;

**Real-time monitoring:**

- **Monitoring capability**: deployment of a Security Information and Event Management Solution (SIEM) and Intrusion Detection Systems (IDS) throughout the network, including OT monitoring capacity.

## Contacts




**Frederico Mendes Macias**
Partner
+351 966850347
fremacias@deloitte.pt



**André Correia de Sousa**
Manager
+351 962753775
andrsousa@deloitte.pt


Deloitte.