Deloitte.

The Future of Industrial Networks

Shaping the industrial towards a new era of digital transformation

Telecom Engineering Centre of Excellence (TEE)

Introduction

Industry 4.0 (I4.0) and Industrial Internet of Things (IIoT) transformation is increasing the need for connectivity between industrial assets.

Industrial businesses are evolving and becoming more digital and cloud-oriented, therefore, organizations need to evolve their network infrastructure and connectivity between industrial assets, local, central applications and systems. As they move forward in this digital journey, it will require to face challenges across multiple domains, such as health & safety, network security, performance and governance.

Traditional industrial networks were designed to support the connection between industrial assets and enable the monitoring and control of every device and systems within the industrial environment. Therefore, these networks, also known as Operational Technology (OT) networks, focus on workers & customer safety and network availability, which differs from Information Technology (IT) networks priorities (*i.e.*, data integrity and protection). As the need of full connection between devices and systems becomes more relevant, IT and OT will need to progressively converge.

Predictive maintenance & analytics, remote asset control and process monitoring & improvement are examples of core Industry 4.0 and IIoT use cases, that rely on the successful implementation of OT networks. To achieve the network ambition and target state, and overcome the challenges of these use cases, it will require Industrial organizations to work across several technological capabilities, aligned with an appropriate governance model.

This paper intends to provide a view of the Industrial networks importance for the main use cases of Industry 4.0 and Industrial IoT and provides a maturity model that will help organizations to understand their current maturity level and to design a tailored roadmap, that will accelerate the transition to the long-term network maturity ambition.

Pedro Tavares
Lead Partner
Telecom Engineering Centre of Excellence (TEE)

Luís Abreu
Partner
Telecom Engineering Centre of Excellence (TEE)

The importance of industrial connectivity

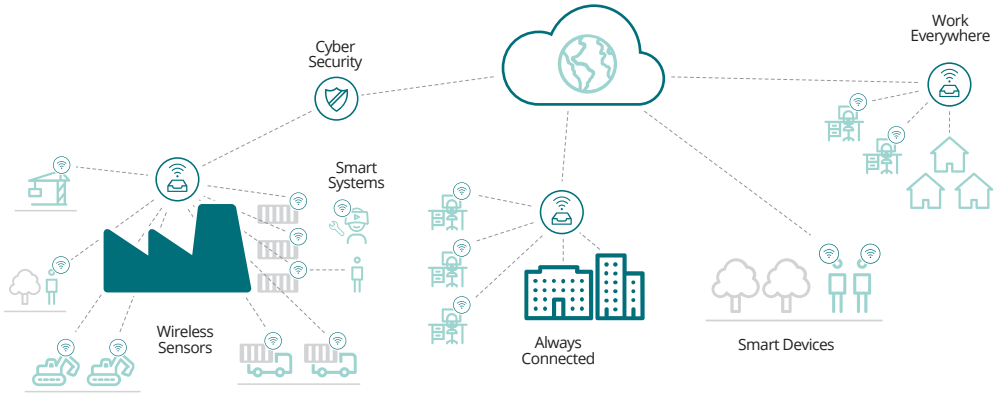
Industry 4.0 and IIoT transformation is increasing the need for companies to invest in industrial networks in order to improve communication of operational data.

Digital transformation is creating a major impact in Manufacturing and industrial companies. Across different industries, there is an increasing focus on growth leveraged by the implementation of I4.0 solutions, as well as Industrial Internet of Things (IIoT) use cases. These disruptive technologies are transforming companies, specially after COVID-19 pandemic, that forced to implement remote access solutions, among others.

While companies invest in technological solutions to improve productivity and performance, such as process automation, monitoring of sensors-based data and remoted controlled machinery, there is an increasing need to connect industrial assets and devices. According to Bosch Connected World Blog, it is expected there to be 14 billion connected devices worldwide by the end of year 2022 and, although the manufacturing sector only represents a small part of this, it is foreseen a major positive impact in uptime increase and productivity improvement as a result of the implementation of solutions to connect industrial devices.

Industry 4.0 and Industrial Internet of Things transformation is increasing need for **connectivity between industrial assets:**

Companies are investing in automated and remoted controlled machinery as well as in sensors-based data capture for process monitoring and predicative maintenance with the aim of improving productivity and performance.



14 billion connected devices[1]

Forecasted for 2022 will be concentrated in 4 industries:

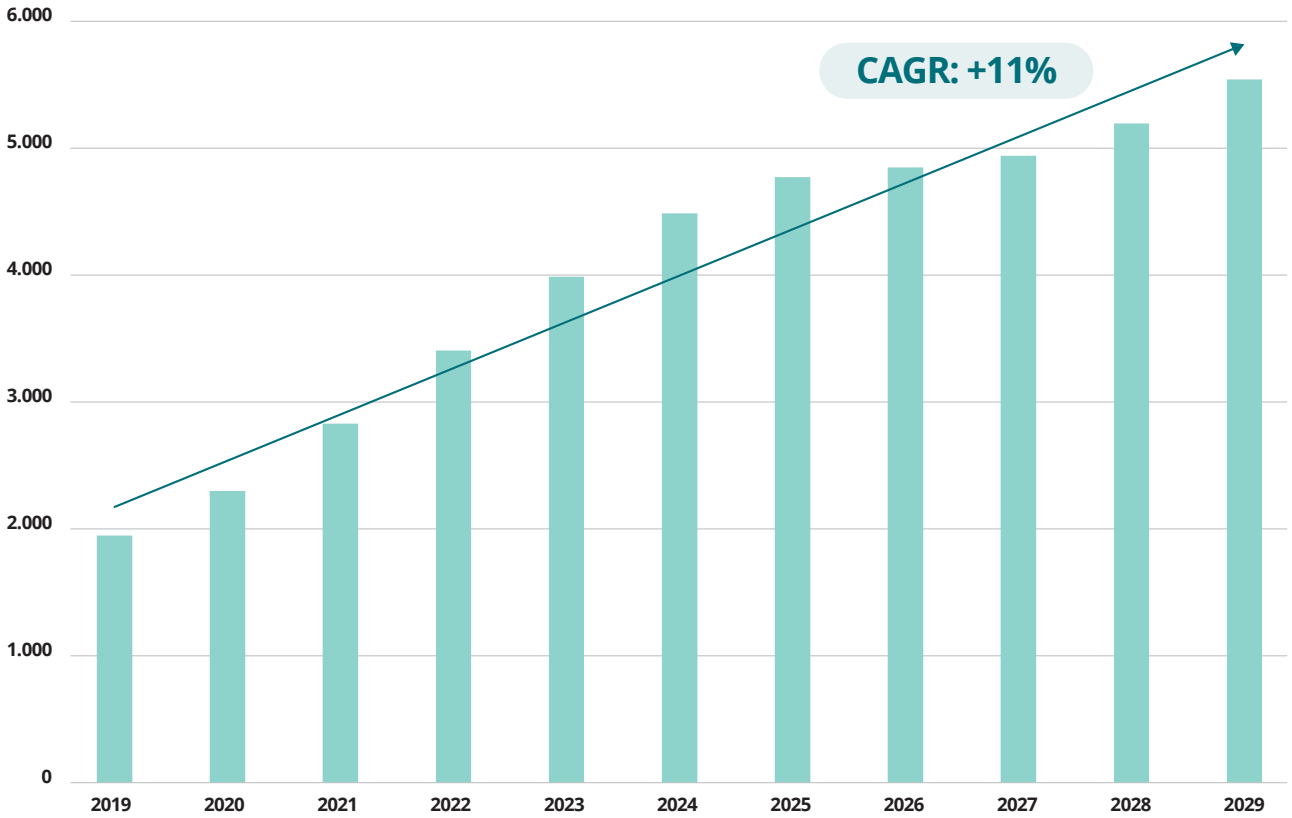
Intelligent buildings;
Automotive;
Healthcare;
Utilities.

Therefore, industrial organisations are looking at improving the connectivity of plant devices and industrial local systems, as well as with central systems and the cloud. This means that it is paramount to invest in communications performance in order to retrieve the highest value from I4.0 use cases. In fact, according a Gartner Forecast, it is expected that the manufacturing sector increases spending in IoT communications by 11% a year (CAGR), from 2019 until 2029.
To sum up, I4.0 and IIoT transformation is, indeed, leading to a major increase in the need to invest in industrial networks that improve communication of operational data in order guarantee the success of the technological solutions being tested and implemented on the shop floor.

As the proportion of connected industrial assets and devices will continue to rise, manufacturing investments in IoT communications and networks is also forecasted to **grow 11% per year until 2029.**

... resulting in a need to invest in communications to connect the devices with local and central applications and systems:

Worldwide Manufacturing Spending in IoT Communications [2]
2019-2025 (Millions of Current USD)



Sources: 1 Bosch ConnectedWorld Blog; 2 Gartner Forecast

Industrial networks and operational technology

Industrial networks are commonly called "Operational Technology" (OT) networks and support the connection between industrial assets and enable the monitoring and control of every device and systems within the industrial environment.

There are some key differences between OT and IT networks that should be taken in mind when investing in the development of industrial assets connectivity. Therefore, it is important to understand the OT Network main characteristics, and how their differ from the IT environment.

Industrial Networks

Industrial networks are the mean to **connect all the operational technology available in an organization**, supporting the data exchange between the different devices and systems in place.

What is Operational Technology?

"**Operational Technology (OT)** is hardware and software that detects or causes a change, through direct monitoring and/or control of industrial equipment, assets, processes and events." in Gartner Glossary

Main characteristics of OT Networks:

Purpose	Enable monitoring and control of industrial assets			
Priorities	**1.** Safety (worker and costumer)	**2.** Availability	**3.** Reliability	**4.** Confidentiality
	Traditionality	Current and Future Trend		
Systems Approach	Standalone applications	As the need of full connection between all devices and systems becomes more relevant, IT and OT will progressively converge in all aspects and become interconnected.		
Architectural Model	Close and proprietary			

IT and OT networks have traditionally been completely disconnected, and therefore only IT equipment has been connected to external systems and networks. However, as companies move forward with the implementation of I4.0 and IIoT technological solutions, they are connecting industrial assets and systems to IT networks, creating a new trend of IT and OT convergence.

The convergence of IT and OT networks is bringing additional challenges and concerns to be overcome. One of these challenges is the difficulty to clearly understand the differences between the IT and OT infrastructure.
The **Purdue Enterprise Reference Architecture** provides a **hierarchical classification of the different levels of critical infrastructure that are used across the OT and IT networks.** When planning a security strategy for de OT environment, the Purdue Model **can help provide industrial communication security** through its separation of layers and definition on how network devices and systems should function and interact.

Industrial networks play a key role in the successful implementation of the main use cases that IIoT and I4.0 offer to organizations. Therefore, it is important to understand what are these use cases and which are the challenges that will come ahead.

Purdue Enterprise Reference Architecture

Industrial networks' role in Industry 4.0 and IIoT use cases

Core I4.0 and IIoT use cases rely on the successful implementation of OT networks. There are three main use cases that can be leveraged with industrial networks.

Process monitoring & strategic improvement

Companies are applying Artificial Intelligence and advanced analytics to better understand the production processes and identify **drivers of lower performance and operational inefficiencies.**

To enable process monitoring, sensors must be in place and **connected with central systems to maximize process efficiency and product quality.**

Improve product quality and reduce defects

4%
Estimate of detective outputs [2]

Improve productivity by increasing throughput

83%
Estimate of production vs. machine maximum potential [2]

Remote asset control

Remote asset control is becoming crucial to enable skilled **workers flexibility** while drastically improving health and safety. In addition, **response times are also improved**, allowing for cost reduction.

A strong network with **connected devices to central and external systems** is crucial to implement remote access.

Improve health and safety when human involvement is hazardous

Facilitate problem solving and maintenance and reduce costs

28%
Estimate for time spent waiting for maintenance [2]

Predictive Maintenance & Analytics

Applying **machine-learning technologies** to process **historical performance and failure data** enables companies to forecast and plan maintenance in advance, reducing impacts of equipment failures.

Companies must install **connected machine sensors** in order to collect data and make data-driven decisions.

Reduce downtime costs

50 billion €
Estimate for unplanned downtime costs [1]

42%
of unplanned downtime is caused by equipment failure [1]

Although there are **enormous advantages from IIoT** applications, it's crucial to be aware of the **network challenges that come ahead**

Sources: 1 WSJ; 2 STL partners

The key challenges ahead and how to overcome them

Looking at market evidence, it is possible to identify some key challenges that industrial organizations face that can have serious financial and operational impact in the business. These challenges can be overcome by the development of industrial networks.

Market evidence

82%
of industrial organizations are unable to identify all devices connected[1]

$170 billion
is the cost of work injuries in 2017 in the US, equivalent to $1.100 per employee[2]

40%
of industrial enterprises believe OT networks are less secure than their IT networks[3]

$50 billion
is the estimate of unplanned downtime costs at manufacturers[4]

90%
of organizations have reported a breach of their OT networks[5]

50%
of organizations have reported a breach of their OT networks[6]

Key challenges that industrial organizations face:

Asset Visibility
Most of industrial companies struggle to have visibility over its resources and assets, which prevents them from having a **complete control over network and infrastructure, equipment and material**

Health & Safety
Safety challenges will **always be present despite evolving technologies** in Industry 4.0. **Human health and safe environment will continue to be a requirement for operating the business**

IT & OT Convergence
Bringing together IT & OT will require companies to focus on overcoming culture and governance issues in order to **enable operational continuity and maintain a digitally secure environment**

Network Performance & Availability
As more devices are connected, the network will need more capacity and the **OT network vulnerabilities** can result in costly damages, mainly as a result of **downtime of OT Systems**

Cyber Threats
Traditional OT organizations were not connected, and as organizations connect more devices and equipment, the surface attack increases and **more cyber attacks are targeted to OT networks**

Interoperability & Standardization
Typical OT networks include **numerous devices**, sensors, and gateways that potentially communicate using different protocols, creating a **difficult-to-maintain network architecture**

It is clear that there is a **big potential in the evolution of industrial networks to address the challenges described** and bring several benefits to manufacturing companies

Sources: [1] Fortinet [2] National Safety Council (NSC); [3] Claroty; [4] IndustryWeek; [5] Fortinet; [6] IIoT World

Industrial Networks maturity model

Industrial organizations need to understand their current network maturity level and work across several capabilities (people, processes, technology) to reach the network ambition and target state

Deloitte's view on Industrial network development encompasses 4 stages of maturity. Pursuing an evolution of the network does not assume that the company will need to always start from the 1st stage (Traditional), as there are critical existing foundations which should be leveraged on to accelerate the Industrial network transformation. From our experience, most Industrial organizations tend to be around the 2nd stage (Essentials).

Industrial Network Maturity Model Phases

1 Traditional
Lag behind the competition, with flat and complex network

- No governance model defined for IT & OT
- Processes not aligned with OT needs
- Flat and open network
- Reduced visibility over OT assets

2 Essentials
Early improvements with key tools and technologies

- OT roles & responsibilities defined
- Processes improved for critical activities
- IT & OT network segmentation
- Improved visibility over OT assets

3 Advanced
Improved maturity with new OT digital capabilities

- IT & OT teams integrated
- Processes defined and reviewed
- Levels 3 & 2 network segmentation
- Visibility & Monitoring tools integrated

4 Optimal
Industry leader with efficient and reliable OT infrastructure

- Centralized SOC for OT & IT teams
- Zero Trust based operating model
- Micro segmentation for lower levels
- End-to-end assets visibility and Control

The evolution and transformation to a network maturity optimal stage involves **much more than an architecture transformation or the implementation of a standard solution.** There are several capabilities that need to be developed and improved, and therefore **organizations need to analyse their status and define a clear strategy** to achieve the optimal stage.

For each phase described in the Industrial Network Maturity model, several **technology capabilities** as well as along the **people** and **processes** can be established. **None of these capabilities or solutions should be addressed in isolation.** Therefore, it is critical to analyze and specify the different **dependencies** and **integrations** within the Industrial ecosystem, to achieve the desired outcomes.

Deloitte's identified several technologies that are commonly used in each maturity model phase, and the distinct characteristics that better describe each phase.

Industrial Organizations need to understand what is their maturity level for People, Processes and different Technology areas, so they can clearly define a strategy that fits their needs and future maturity goals.

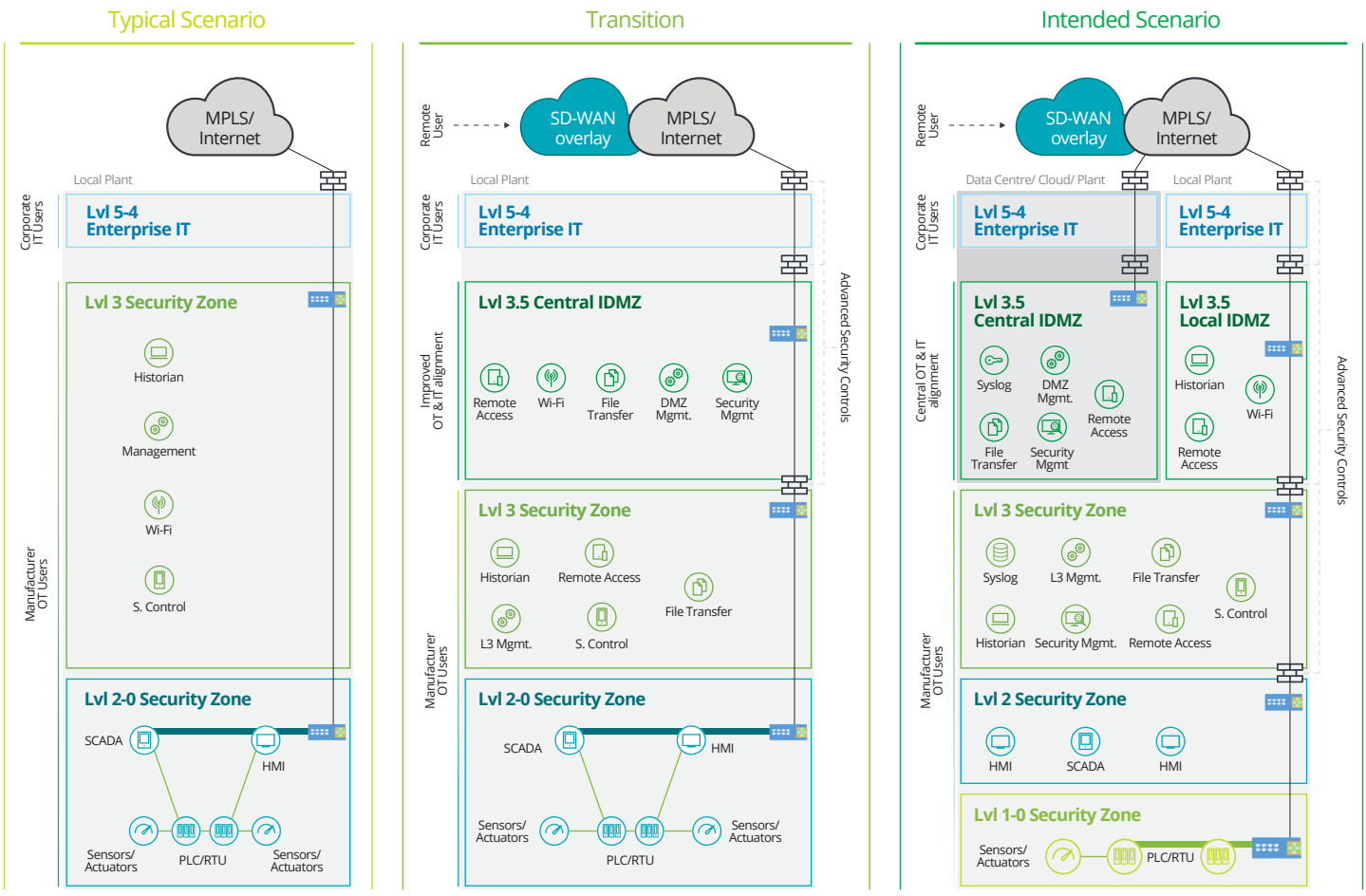
Industrial Network Maturity Model		Traditional	Essentials	Advanced	Optimal
People		Reduced Network & Security expertise in OT environments	Network & Security expertise increase in OT environments, SOC for OT networks	IT & OT teams integrated and aligned with roles and responsibilities defined	IT & OT network and security teams aligned and centralized SOC created
Processes		Minimal processes defined for Network Management and Maintenance	Network Infrastructure Change Management processes defined	Vulnerability Management and Incident Response plans created	Processes defined and regularly updated for Network Management and Maintenance
Technology	Segmentation	Flat & Open Network	Segmentation Between IT & OT	Segmentation for Levels 3 and 2	Micro Segmentation for all Levels
	Security Controls	Static and basic Firewall ruleset controls	NGFWs, IDS/IPS and Anti-bot	DDOS and SSL inspection of all traffic	Cloud sandboxing and Identity awareness
	Remote Access	VPNs for critical Applications only	VPNs for all Industrial Applications remote access	Cloud based SWG & CASB	Zero Trust based remote access model
	IAM	Roles and Responsibilities defined but without proper privilege distribution	Roles and Responsibilities defined and reviewed for OT Network Environment	Privileged Access Management solution for main users and OT systems	Identity and Access Mgmt. mechanisms implemented for all users and OT systems
	Visibility, Control & Hardening	Reduced Visibility over OT network Assets and reduced patching	Network Visibility & Monitoring tools deployed and patching for critical assets	Network Visibility & Monitoring tools optimized and patching for all network devices	Network Tools fully integrated for end-to-end assets visibility, Control and Patching
	LAN Connectivity	Legacy wired based connections	Wired, Wi-Fi based WLAN, POCs for SD-LAN	Industrial Ethernet, Wi-Fi + Mobile based WLAN, SD-LAN	Industrial Ethernet, Wi-Fi 6 + 5G based WLAN, SD-LAN
	WAN Connectivity	MPLS based WAN	Hybrid WAN (MPLS + Internet), POCs for SD-WAN	Hybrid WAN (MPLS + Internet), SD-WAN	Internet + 5G based WAN, SD-WAN
Main Characteristics		**Complex governance model with reduced alignment between IT & OT** **Enterprise IT intranet as the main defense perimeter for OT network**	**IT & OT network segmentation and creation of an Industrial DMZ** **Improved asset visibility and monitoring capabilities with new tools and services**	**Governance model defined and IT & OT teams integrated** **Firewall security controls implemented, and SD-WAN/ LAN solutions deployed**	**Connections secured independent on the user/ device location** **Automated network security management and monitoring**

To better deploy the capabilities identified in the previous section, Industrial organizations need to understand which network scenario its currently deployed across their OT network. The typical scenario relies on traditional network security strategies, with a complex governance model and no segmentation between IT and OT networks. In this situation, once an attacker penetrates the security perimeter, it is extremely difficult to ensure that the OT network environment is not compromised. It is important for Industrial organizations to clearly define the scenario and technologies/ services that better fit their business needs.

Deloitte identified three different scenarios and several services/ technologies that are commonly used in Industrial environments, and the distinct characteristics that better describe each scenario.

Industrial Network Maturity Model Architecture and Main Features

Traditional — **Optimal**



MAIN FEATURES

- Complex governance model for IT
- Flat and open network without network segmentation
- No standard security and remote access solutions
- MPLS/ Internet enterprise
- Limited firewall security controls

- Governance model defined and aligned with IT & OT needs
- IDMZ and IT & OT network segmentation
- Security and remote access standardized services
- SD-WAN connectivity
- Firewall security controls

- IT & OT teams integrated
- Centralized IDMZ and segmentation for lower levels
- IAM, data and services redundancy
- OT services standardization and automation
- Advanced firewall security controls

Deloitte expertise

Our team as a proven track record supporting different clients across several industries and geographies over a multitude of Industrial network initiatives

Deloitte has a proven track record supporting different clients across several industries and geographies over a multitude of industrial network initiatives. We have been working with several clients in industries ranging from chemicals/ petrochemicals, steel and iron, shipping and ports and technology solutions.

The initiatives Deloitte supports can start with strategy definition (e.g.: IT/ OT network convergence strategy), perform a technical assessment, develop a business case or operational model and can also end with the actual implementation of the technical solutions.

Key experience

Petrochemicals

Secure modern integrations between enterprise and industrial networks by **protecting the boundary between IT and OT with advanced security capabilities**

Key Outcomes

- Network design requirements defined
- Asset inventory created
- Network architecture designed
- Technology catalogue created
- Network architecture test strategy and report
- Service model designed and procured

Steel & Iron

Assess the client's **current state of their IT/ OT network security implementation** and review the existing solutions under discussion

Key Outcomes

- Network security architecture strategy reviewed
- Potential gaps in network security roles and responsibilities identification
- 4 different firewalls scenarios implementation analysis
- 6 major risks identified & 15 short term actions defined
- Recommendations defined on 'the way forward' for all the potential options

Chemicals

Mature the client's integrated IT/OT cyber security capability that was marked as strategic priority, with high involvement from executive management

Key Outcomes

- Programme scale up and costs optimisation
- Deployment roadmap of security controls created for more than 130 sites worldwide
- Suppliers and implementation parties management
- Network segmentation reference architecture management and firewall ruleset definition for both the IT and OT environments

Shipping & Ports

Ensure the **network became more secure, resilient & recoverable**, as part of a larger **cyber security programme**

Key Outcomes

- Network Segmentation Strategy defined
- Network Topology created
- Tooling Strategy, Firewall Rulebook and Secure Baseline Configuration defined
- 42 instances of IPS/IDS implemented
- 135 firewalls patched with the latest software version
- Capabilities implemented to sustain the defined strategy

Technology Solutions

Craft a compelling **Zero Trust (ZT) business case** and **roadmap** in order to secure funding for a transformation programme

Key Outcomes

- Business and risk drivers assessment, Zero Trust ambitions definition
- Business case definition by articulating for the 'why', 'what' and 'how'
- ZT assessment model to assist the client's decisions along the journey of ZT
- Client's expertise on ZT enhancement
- Roadmap definition

Packaging Solutions

Understand, analyse and aid recovery of the client's network as a result of a **ransomware incident**

Key Outcomes

- Management and configuration of ~380 business applications into Zscaler Private Access (ZPA)
- Perimeter security improved, by removing ~500 rules from 38 Firewalls and standardized FW change management process'
- Full high-level global NW architecture visibility provided (7 critical vulnerabilities identified; 8 remediation initiatives; 17 sec. design principles)
- Inventory of VPN connections created and defined an approach for decommission

Legend: Network security architecture definition; Business cases and operational models design; Enhanced network visibility and technical assessments; Software Defined Networks and threat detection & protection implementation; IT/OT networks convergence strategy

Lessons learned and key success factors

Our experience within the industrial environment has allowed us to identify six key lessons learned that should be taken into account when planning an industrial network transformation.

Lessons learned

Minimise impact on Production downtime

Temporary production downtimes are usually needed to implement the new solutions designed for the OT networks. The roadmap should be defined in a way that reduces the downtime to a minimum

Guarantee worker and customer safety

Worker and customer safety is the top priority for industrial organizations and, therefore, it must be on the top of our minds when designing, planning and implementing an industrial network transformation

Minimise impact on Work processes

Processes are difficult to change and differ across different plants, so it's important to minimize the changes in processes and to take into consideration the particularities of the various sites

Consider Technological diversity and avoid generalisation

Existing infrastructure is probably going to vary across plants and some assets are potentially aged beyond their useful life. From the start solution, it's crucial to avoid generalization to all sites

Ensure transversal Employee involvement

The lack of common vision of the benefits from the transformation impacts its success, so it's crucial to communicate properly and involve employees from the different plants upfront in the design phases

Consider OT and IT divergences and promote alignment

IT and OT have siloed teams and governance, leading up to different work cultures and priorities. While IT is more focused on data protection, OT is more concerned on operational efficiency

The following success factors should be considered to ensure a successful industrial network transformation

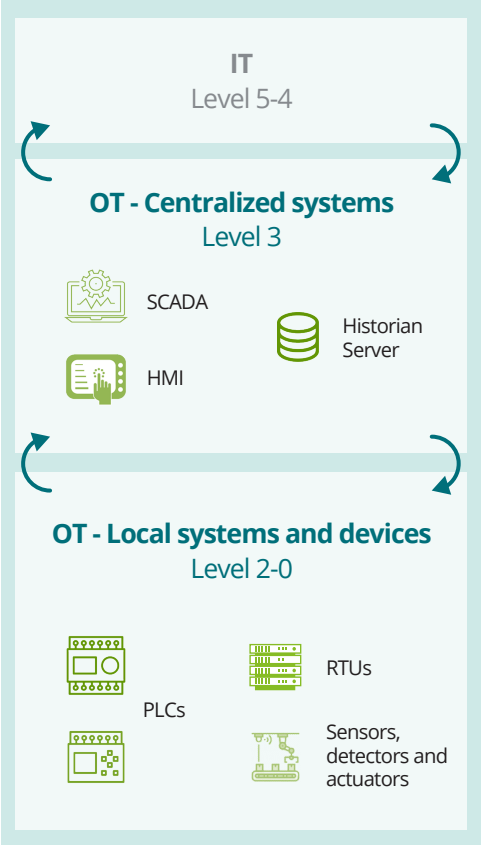
1. **Align the benefits** with site workforce and **communicate key changes**
2. **Minimize the impact** in operation and downtimes
3. Guarantee **worker safety** during and after implementation

Our Offer

Deloitte proven experience results in a holistic **OT networks offer that covers all stages of project lifecycle**, from assessment and strategy definition, to solution implementation and operations and maintenance.

In addition, Deloitte is capable of helping clients on transformation journeys that involve not only **all OT environment levels but also the integration with IT infrastructure and networks.**

Finally, one of the crucial factors that allow Deloitte to leverage strategic partnerships with key players is the **consistency of our offer across all the domains of a business infrastructure:**



Enterprise and plant/ Factory Networks

- Site to site and plant to plant connectivity, leveraging software defined WAN (SD-WAN) solutions based on connectivity models (MPLS and Internet)
- On-site and on-plant connectivity, levering software defined LAN (SD-LAN) solutions for both wired and wireless access networks
- Remote access solutions, including next generation VPN services and software defined Perimeter (SDP) technologies
- Network performance enhancements, including redundancy and scalability, bandwidth, latency and SLAs
- 4G/ 5G Mobile Private Networks, including network design, planning, and sizing

Datacentre and Cloud connectivity

- Datacentre infrastructure, including consolidation, disaster recovery, migration and decommissioning of DCs
- Next generation DC solutions, leveraging software defined networking datacentre (SDN-DC) and hyperconvergence
- Micro-segmentation solutions, focusing on on-premise connectivity, hybrid cloud and multi cloud implementations
- Cloud connectivity models and containerization, within the organization network (plants, branches, warehouses, Data Centre)
- Enterprise/ Industrial edge computing strategy definition, including sensors and servers connectivity, and cloud integration

Network Security

- IT & OT governance model and network segmentation, including zoning, Industrial DMZ, micro-segmentation, lateral movement security, among others
- Network security controls, including next-gen security features
- Hardening IT and OT network devices, including firewall and router patch management, vulnerability management, intelligent rule design, etc.
- Risk assessment and compliance based on audit-ready reports for all major regulations (e.g.: PCI and HIPAA) and industrial and network security standards (e.g. NERC, ANSI, ISA, IEC, NIST)

Network Automation

- Network Planning and Engineering, including configuration and policy automation and capacity management in Industrial environments
- Network and Service operations, including NOC automation, predictive network maintenance and self-healing solutions
- Network orchestration to automate security and workflows for repeatable network and security operations tasks in heterogeneous OT Networks

Contacts

Luís Abreu
Telecom Engineering Excellence Partner
labreu@deloitte.pt

Filipe Leonardo
Telecom Engineering Excellence Senior Manager
fleonardo@deloitte.pt

Bruno Pires
Telecom Engineering Excellence Manager
brunpires@deloitte.pt

Luís Pinto
Telecom Engineering Excellence Senior Consultant
luisspinto@deloitte.pt

David Andrade
Telecom Engineering Excellence Senior Consultant
davandrade@deloitte.pt

Marta Campos
Business Consulting Senior Consultant
martacampos@deloitte.pt

Maria Galarza
Business Consulting Senior Consultant
mgalarza@deloitte.pt

Margarida Esteves
Business Consulting Consultant
mesteves@deloitte.pt

Acknowledgements

Special thanks to whom contributed to this publication in terms of researching, providing expertise, and coordinating:

Hugo Pinto | Maurício Pereira | Paulo Costa | Gonçalo Pessoa

Deloitte.