Delivering your Global Manufacturing Strategy in times of Remote Working

How to Securely and Efficiently connect to Production Lines and Teams across the UK and Europe

Webinar's Full-Memories

polestar. industrial IoT

DISPEL

Delivering your Global Manufacturing Strategy in times of Remote Working.

How to Securely and Efficiently Connect to Production Lines and Teams Across the UK and Europe

Contents

The Manufacturing Scenario in 2021

In this session we discussed the effects that dual forces - the global COVID-19 pandemic and Brexit, have had on the manufacturing industry in Europe and the UK, testing business resilience and pushing forward Global Manufacturing Strategies. We will show you how it is possible to achieve efficiencies through secure industrial connectivity.

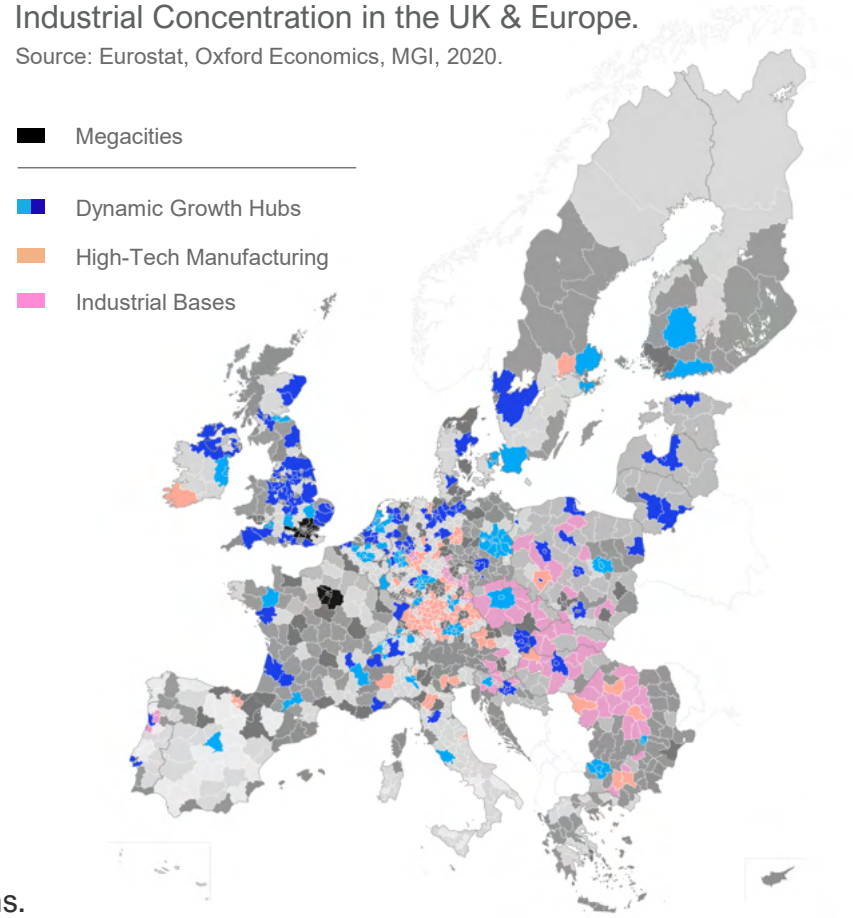
We all have seen that beyond COVID-19, automation and the regulations imposed by Brexit are shifting the geography of manufacturing in Europe. But, in terms of priorities in both the short and mid-term for businesses to achieve or maintain manufacturing efficiencies and leadership, what does the future of this industry look like?

Before these two events we were noticing how the manufacturing scenario in Europe and the UK was taking shape. Manufacturers were dispersing operations across different regions according to the degree of specialization that each of their processes and products required, as a solution to maintain or improve quality, speed to service, and to keep profit levels healthy.

As you can see in the graph below, developed by Eurostat, Oxford Economics, and MGI in 2020, locations for manufacturers were divided into 3 main segments: Dynamic Growth Hubs, High-Tech manufacturing Centers, and Industrial bases.

Dynamic Growth Hubs include the megacities of London and Paris with strong innovation capabilities, a highly educated, young workforce; 46 superstar hubs, including Oxbridge, Copenhagen, and Munich, which have a wide range of high-growth industries; and Sevice-based economies of which most of them are concentrated in the UK.

Industrial Concentration in the UK & Europe.
Source: Eurostat, Oxford Economics, MGI, 2020.



Next, we have 78 **High-Tech Manufacturing Centres**, of which more than 70% are in Germany, including Wolfsburg and Stuttgart, focusing on advanced manufacturing and producing numerous high-tech patent applications.

Then we have 72 **Industrial Bases** focusing on basic manufacturing, located mainly in Eastern Europe, Southern Germany and Portugal. The working-age population in these clusters is decreasing due to ageing, outmigration, or both.

These location and specialisation trends have been further intensified by the restrictions on mobility that have been imposed to handle the pandemic and by the consequences of Brexit. In turn, these pressures have accelerated the need to establish resilient remote working infrastructures.

To respond to this demand, hundreds of remote work solutions and initiatives flood the market. This has made the evaluation of suitable technologies time consuming and costly. During the pandemic, manufacturers have learned some hard lessons; a well-planned and executed digital transformation can bring real and lasting operational value, but fail to adapt fast enough and your business will struggle to survive.

We have seen through our own experience and through the media, that the companies who had already started their digital transformation, or had prepared beforehand

experienced greater resilience and business growth, despite the crises they have faced this past year. The world economic forum mention Lighthouse Manufacturers of the likes of Foxconn, Arcelik, Henkel, and Rold as examples of the most advanced Global factories that thrive even during economic downturns.

Their strategic approach is based on three main pillars: Work reduction, or aiming at being leaner, Waste reduction, or becoming greener, and Worry reduction, which simply put is agile planning. These manufacturers redefine the configuration of their management, ensure that their ERP & IoT systems are hyperconnected, and all of their devices and machinery synchronised and automated. They decided on an early stage that they will be investing in becoming more efficient in terms of deliverability, maintenance, and availability. Furthemore, every year they train their workers in data sharing, performance improvement and the usage of digital tools to maintain their global leadership.

Not all manufacturers have reached these levels of integration, but we are witnessing how things are changing quickly.

In fact, PWC's Global Manufacturing Pulse Survey in 2021 indicated that to improve effectiveness and to stablish operational priorities for manufacturing, businesses have started to intensify activities in the areas of:

1. **Workforce Development**: Manufacturers are increasing their activities in digital enablement (robotics, workflow automation), next-generation talent (digital upskilling), and flexible working.

2. **Operational Technology**: Cloud and Internet of Things (IoT) will be the mainstays of manufacturing technology, prioritised by nearly 70% of companies to modernise production processes.

3. **Cybersecurity**: As digital transformation moves forward, more access points for remote working need to be created. Therefore, Response and Recovery plans (50%), investing in Security Applications such as Firewalls and Encryption (43%), the Coordination of Data Privacy and Security (33%), and Improving Governance and Access (30%), are all priority areas.

4. **Supply Chain**: Manufacturers will increase their focus on network optimisation and demand forecasting capabilities.

Considering these trends, and facing the uncertainty of what is to come in the geopolitical, social and economic scenario, remote manufacturing will keep playing a key role in the delivery of Global Manufacturing Strategies, pushing forward businesses into digital transformation.

The wide adoption of Remote Work during the pandemic has shifted how companies will operate from now on. But still, many people will be returning to the workplace as

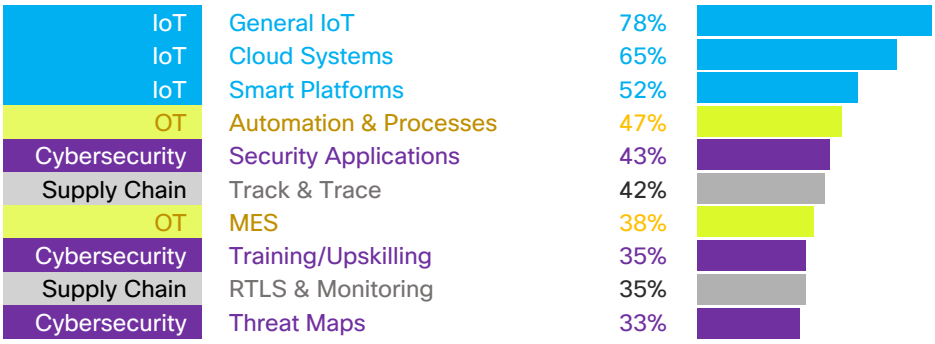
economies reopen. Considering the technological infrastructure of businesses, the majority could not work remotely at all. From an analysis of 2000 tasks and 800 jobs performed by MGI in 2020, about only 20% of the workforce could work remotely from three to five days a week, and more than half the workforce has little or no opportunity for remote work, as some tasks require collaborating with others, using specialized machinery on-site, or performing corrective maintenance on location.

In contrast, activities such as information gathering and processing, coding data, communicating with others, coordinating predictive maintenance, managing teams, processes, and automated workflows, and performing training can theoretically be done remotely.

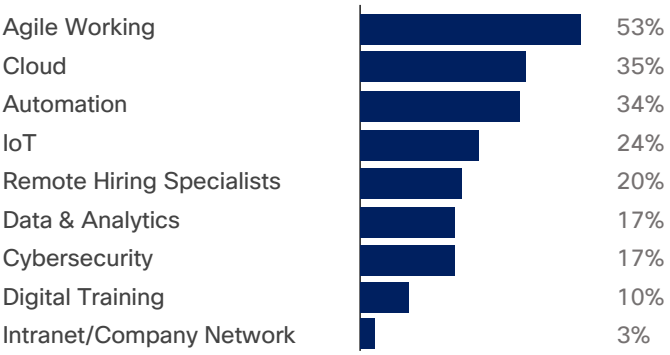
That is a clear indicator of what is left to achieve on digital transformation for European and British manufacturers. In MGI's analysis, executives indicated that hybrid models of remote work are here to stay, especially if they support, besides sanitation and workforce safety, Agile ways of working, Automation, the operation of Cloud Systems & IoT, and Cybersecurity. MGI's analysis indicates that businesses will be hiring more professionals in such areas as a result of COVID and Brexit.

As we keep working towards achieving efficiencies in terms of deliverability, maintenance, and availability through connected manufacturing facilities, we will still face more challenges. The following are expected risks that will be present when starting to operate through Remote Teams and Facilities.

Overarching themes in Manufacturing, PWC (2021)



Top Hires in the UK & Europe after COVID-19 + Brexit, MGI (2020)



Efficiency Risks of Remote Manufacturing Initiatives.

When deploying remote manufacturing activities, a series of changes within the organisation are required, specially to prevent efficiency risks that come up from factors such as not having the right leadership and skillset on-board, not ensuring proper communication and team engagement, and allowing unexpected downtime. These refer to:

In terms of **Leadership & Skills**: To engage in the process and technologic improvement that remote manufacturing requires, and receive support from stakeholders, there should be clear IT | OT governance policies. When OT is the sole responsibility of CISOs, CTOs, CPOs, or Production Directors by themselves, and is not streamlined between all of them, efficiency risks increase.

This implies that there will not be a clear guidance on what data management structures and digital skills are needed. Also, technological solutions will not appropriately be planned and/or implemented. We have seen that leaders that are not flexible in their approach and don't plan clear Operational and Technology strategies tend to focus on vanity measurement, instead of looking for key outcomes and strategic process optimisation that impacts efficiency.

When speaking of **Communication & Team Engagement**: Both managers and engineering teams play a critical role in maintaining efficient remote operations. Technical staff and Engineers must have a deep understanding of the manufacturing processes and data to diagnose and solve problems. While managers must be able to react to issues on the factory floor that impact production scheduling and equipment effectiveness.

Leadership & Skills:
IT | OT Governance
Lack of Digital Talent
Vanity Metrics

Communication:
Information Gaps: IT, OT & Management
Unfamiliar Working Environments
Information Security

Downtime:
Legacy Systems
Corrective Maintenance
Process Disruption

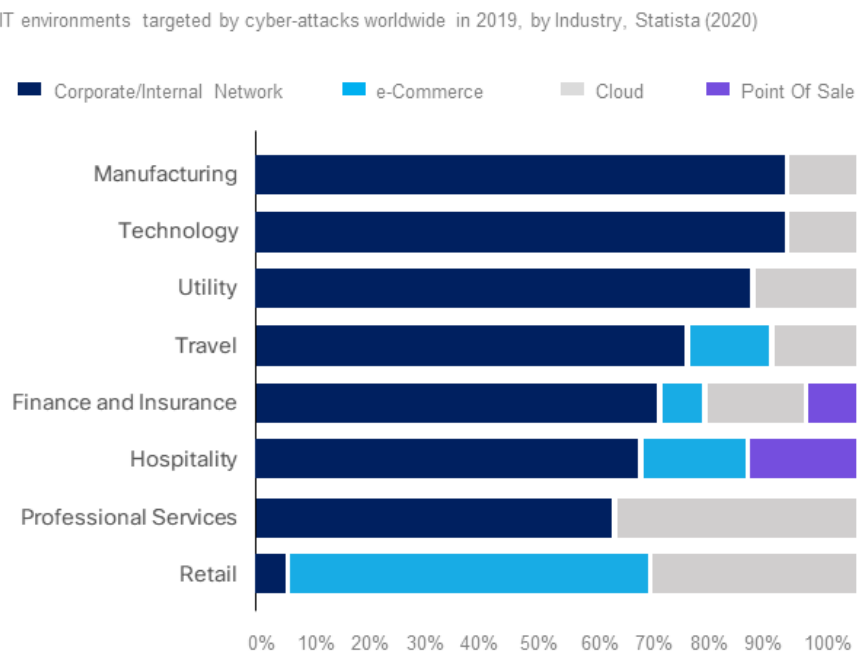
But when communication doesn't occur between these teams, there will be an information gap that can cause disruption. This happens frequently in Remote Work environments, as teams that are used to working and communicating in shared physical spaces will find the change in daily work challenging or isolating. Remote communications can also bring along security risks as seen in the following section.

When facilities, teams and management are not fully, securely and efficiently connected, activities such as keeping the machines running and gathering manufacturing data will still need to be done on-site and manually, which can generate delays in decision making and process optimisation. We have seen that addressing variability in production demonstrates a great challenge: sites can vary enormously between the very small, with people making products manually, to the very large, with process areas across several buildings on multi-acre sites.

Assuming that preventive maintenance is not being performed, and without full control over the real-time status of your machinery and systems, **Unexpected Downtime** can occur. During unplanned downtime, your top priorities are safety and getting your systems back online, especially given that every minute of having your production systems stopped can cost on average about £100,000.

Security Risks of Remote Manufacturing Initiatives.

In addition to the efficiency risks mentioned, research suggests that we will likely continue seeing cyber attacks targeting manufacturers. The ongoing COVID-19 pandemic has also had a major impact on cyber security. Online scams spiked by more than 400% in March 2020 compared to previous months, according to international law firm Reed Smith. Additionally, Google revealed it was blocking more than 18 million malware and phishing emails related to COVID-19 every day.



According to EEF/MAKEUK, 48% of manufacturers had at some point been subject to a cyber security incident, and half of those organisations suffered financial loss or disruption to their business. Statista also shows how the Manufacturing sector was, at the beginning of the pandemic, the top scorer in receiving attacks to their corporate or internal networks (88% of attacks).

Most manufacturing systems today were made to be productive, but not fully made to be secure. Historically, manufacturers have been concerned with securing their physical OT environment, whilst often neglecting IT security.

When you implement IoT systems to ensure Data Availability, Data Aggregation and BYOD policies to make remote manufacturing work, your facilities acquire an increased exposure to threats such as data breaches, hacking, malware & ransomware, phishing, insider attacks, and breaches caused by lack of attention or poorly designed internal processes. Some of the risks include:

Information Security: Losses caused by information leaks on patents, financial records, commercial information, or unwanted violations on GDPR.

Business continuity and resilience: A single cyber attack on your industrial network can cause multiple weeks of downtime, resulting in millions lost from stopped production and reputational damage.

LSD+T approach to reduce Risks in Remote Manufacturing

To every new challenge there is a solution. Risks present in Remote Working stemming from inappropriate leadership and communication, lack of digital skills and poor information security management can be mitigated through a comprehensive planning of your business Leadership, Skills, Data and Technology, which is what we call the LSD+T approach.

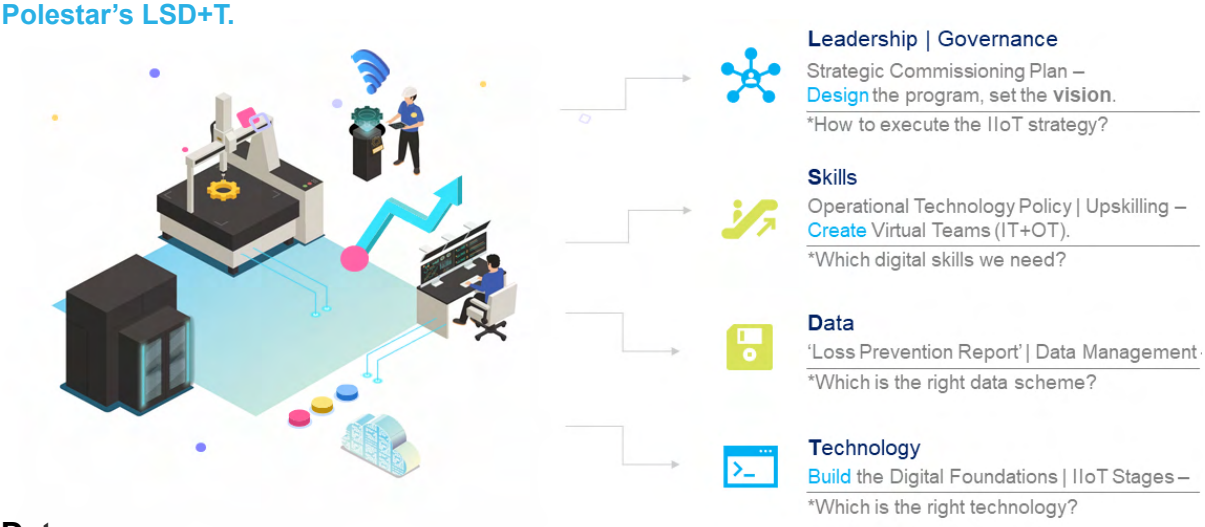
Leadership:
Through the years we have witnessed how collaborative work with directors, managers, engineers, and operators from key departments such as Automation, OT, IT and Security improves the delivery of the Strategic Intent and increases the efficiencies when implementing Digital Transformation projects. Remote Work in particular requires resilient leaders across enabling functions to evolve the organisation's approach. Remote leaders need to be savvy in the benefits of IIoT technologies, the implementation of IT/OT Convergence & Policies, and willing to build and upskill cross-functional teams.

Skills:
We believe that Automation & IT departments need to work together, and staff need to be trained on each other's systems in order to make Operational Technology work. To kick-start this process, we set up virtual teams consisting of departmental stakehold-

ers and recommend peers in other companies or industries we deal with, who have already 'been there and done it'. Internally, we help our customers 'learn lessons' and share knowledge across the different business units.

Critical areas in which future workforces will need special training will be in Data Analytics Skills, Cyber security and ICS. Businesses that actively adopt Cyber security expertise and more importantly improve their security infrastructure, data analysis, and process optimisation are more likely to be successful. These businesses have come to see cyber security as an enabler to everyday operations. With security expertise becoming so difficult to source and retain, organisations should consider cultivating this talent organically.

Polestar's LSD+T.



Data:
For implementing remote manufacturing strategies, we suggest the creation of defined data management structures or special training in Data Management, so your teams can reach:

Data Availability: Data obtained from sensors and qualitative data that provides context for processing is critical to successful remote monitoring. When your manufacturing team use and understand a platform that provides both real-time and easy-to-access historical information it enables them to remotely address problems as they occur. This helps factories avoid long-lasting issues with significant impact and provides constant continuous improvement efforts with access to historical data.

Data Accuracy: While having automated sensors removes the need for human intervention, there are still contextual components that need to be captured. Understanding the reason why a machine is down is critical to providing accurate remote support. Processes that establish data capture must be in place before remote monitoring can be successful. Expectations and transparency are important for both factory floor personnel and remote teams to ensure accurate decisions are being made. Ensuring data quality, defining, monitoring, maintaining data integrity, and improving data quality.

Data Aggregation: To provide additional context, factory data from machines, sensors and floor personnel should be aggregated with data from ERP, MES and quality systems through a Historian, SCADA or OPC UA server. Once data is centralised it can be displayed through various data visualisation or exploration tools that allow remote employees to compare manufacturing performance across lines, shifts, products and more. The data can also be used by machine learning and applied analytics technologies to provide predictive alerts and performance optimisation recommendations. Managing analytical data processing will enable access to decision support data for reporting and analysis.

Data Governance: Your teams must be able to define who within an organisation has authority and control over data assets and how and what those data assets may be used for (roles, responsibilities, and processes for ensuring accountability and ownership of data assets, ensuring privacy, confidentiality, and proper access). Also, by producing reports such as 'loss prevention reports' that include cyber security recommendations, we can jointly design new systems, new processes and new procedures to fit our customer's needs.

Technology:
Your business needs tools to effectively onboard remote work and remote manufacturing. Otherwise, how will your organisation communicate with remote workers, and how will remote workers communicate with one another and their equipment?

For instance, remote monitoring solutions provide the operational visibility that these teams need to track performance and make the necessary recommendations without having to physically be on the factory floor. Ensuring that quick and simple to use remote access tools are available in the workspace will give employees one less excuse for not engaging. It also allows access to critical information, a smooth experience for employees, reduces time spent accessing critical systems and information, troubleshooting, and keeps productivity high. A robust **Remote Access System** should allow complete control for your OT network admin with full security features built-in that align with the NIST Cybersecurity Framework 1.1, the IEC 62443, NERC-CIP, and the NIST 800-82 at a minimum.

Some of the specific measures that manufacturing companies can put in place to ensure their networks are protected from cyber attacks are implementing or enhancing logging information, adopting multi-factor authentication (MFA) for all public-facing access, managing user privileges, monitoring and reviewing user permissions, integrating endpoint security capabilities, IP whitelisting from the corporate address space, and applying patches to affected assets as soon as they become available should become second nature for all IT departments.

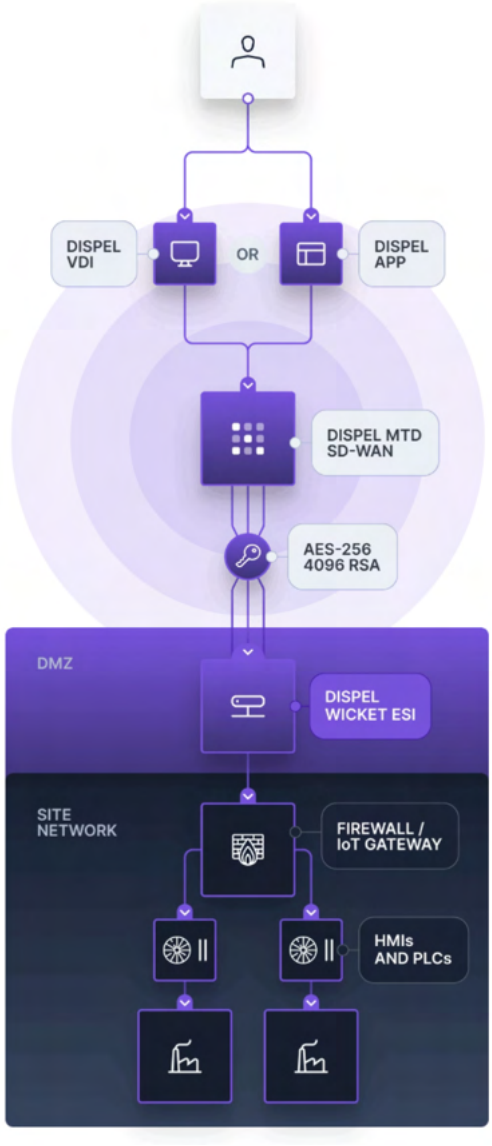
Implementing **policy iteration algorithms** (iteration rollouts) for learning how a good cyber security policy should be structured is also critical. At each iteration, a new policy is produced using training data obtained through rollouts of the previous policy on a simulator. The aim of these rollouts is to identify better action choices over a

subset of states to form data for training the classifier, creating an improved policy.

Using **agile processes** can help promote network and system readiness as a part of your rollout. This iterative methodology improves readiness by accelerating the identification of problems within an application or system. For instance, if a conformance test fails and there is a network segmentation configuration error, you will know to work with NetOps to address this issue. When the conformance test passing through the system is not working as expected, you know the network configuration is valid so there must be an application or system-level error, which requires escalation to the owners of the impacted application and/or system.

When we put together these measures under an **enterprise architecture with multiple layers** (following the PURDUE model), we start creating a Secure-by-Design Architecture, in which security, redundancy and connectivity are ensured for each of its levels: the physical processes, intelligent devices, control systems, manufacturing operations systems, and business logistics systems.

Our experience demonstrates that this approach is not only useful for implementing remote manufacturing successfully, but also for achieving process efficiencies, cost savings and global manufacturing leadership.



A secure and efficient remote access architecure:

Users authenticate against a website, receive access to a single-use virtual desktop and reach their equipment. In the background, their connection traverses a moving target defense SD-WAN down to the relevant OT network.

At the edge of the OT network sits a virtual machine that provides user-session-protocol specific whitelisted access to equipment.

Classic vs Cloud Remote Work Implementations

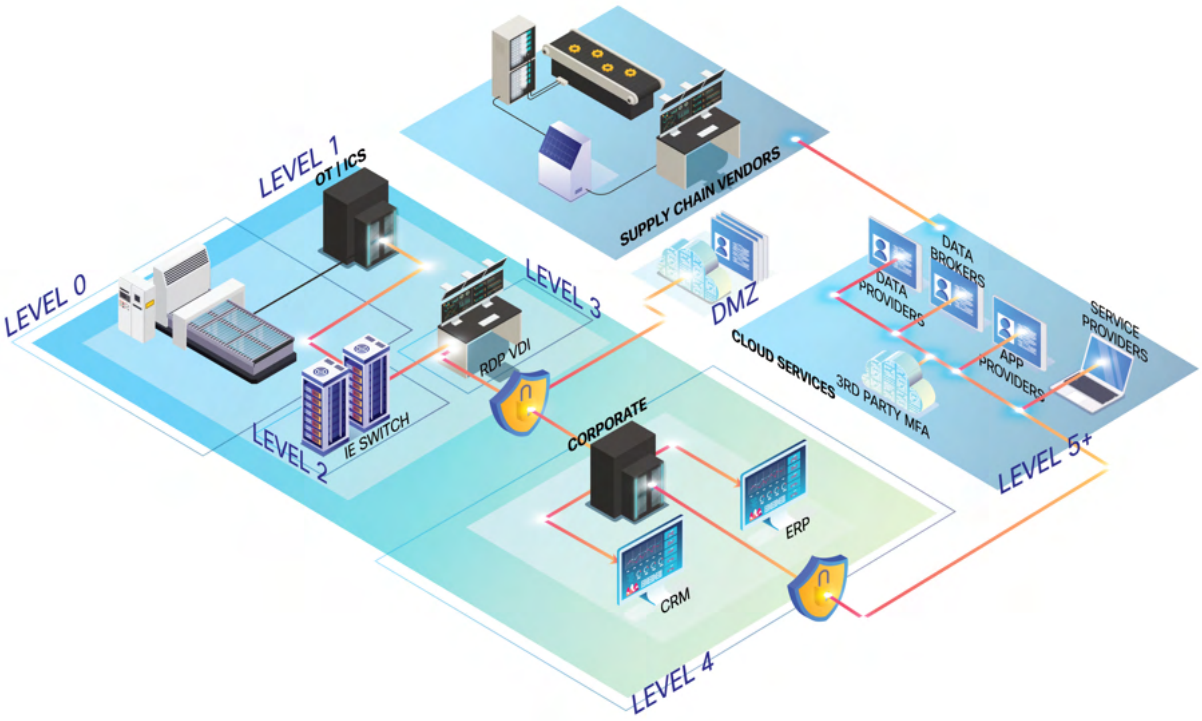
Something that we find in **89% of our customers** is that they are running factories with technology that is up to and sometimes over 30 years old. Getting visibility on those assets is a major problem and even if you have the knowledge within the business to make the right decisions about which devices can communicate with each other, the approach that is taken is usually to ringfence the assets by installing multiple firewalls at zone and cell level.

This requires exposing data points from their control systems to the enterprise to drive efficiencies. A common problem is that IT departments do not have the time, resources or knowledge to protect the actual systems that make the business their money. Collaboration, Office365, standardisation around cloud-first projects for Corporate applications and also cyber security in the enterprise, all contribute to the problem for IT teams to stay current and up to date.

Standards like **IEC62443** for OT teams can be effective, especially when protecting Industrial Control Systems for Critical National Infrastructure, but for manufacturers, this can be too costly due to the management overhead as they have a very large number of disparate assets in some very large factories.

Most of the time, perimeter protection is installed using firewalls, and the OT and Automation teams are left to their own devices. This does not solve the problem as most hacks come through Enterprise services and not as you would probably expect, through Industrial Control Systems and this is due to the high number of services that are require to be open in an Enterprise in order for information workers to do what they need to do.

What can be done to minimise risk without having to rebuild a production network from scratch?



Remote access with segmentation by firewalls.
Ringfencing of assets by installing multiple firewalls at zone and cell level.

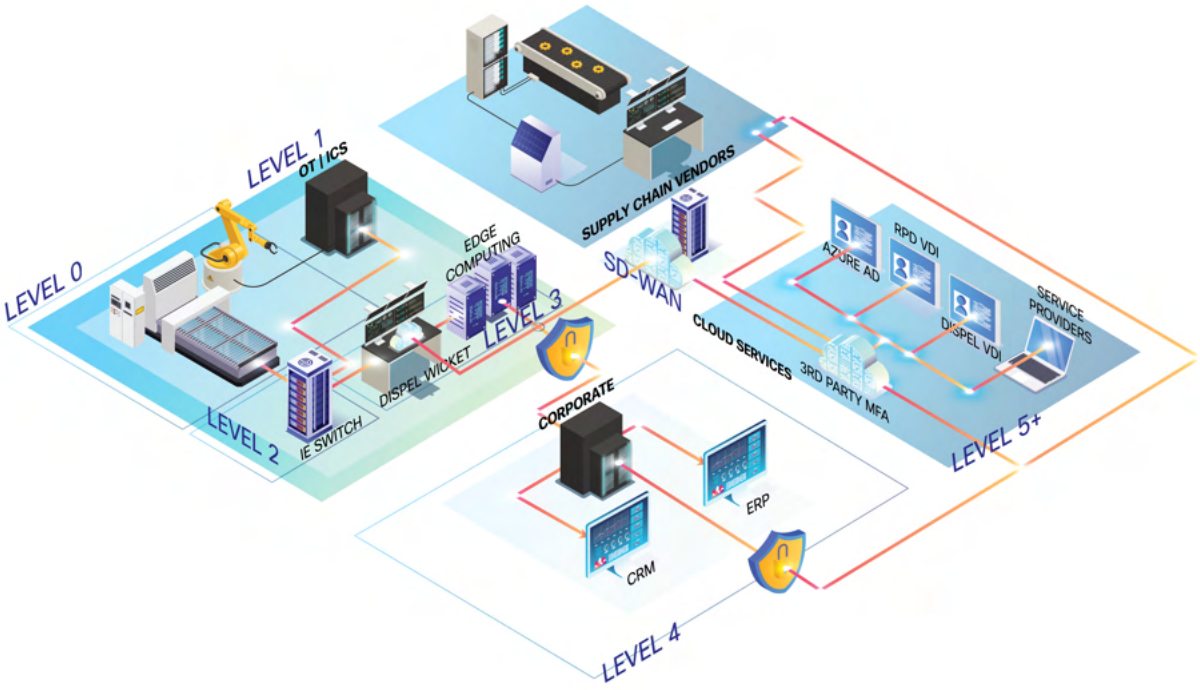
No Visibility to Assets.
Asset Ringfencing with Multiple Firewalls.
OT & Automation are not Connected.
Enterprise Services receive most Hacks.

Cloud services provide an opportunity to bring IT/OT and Automation teams together. Cloud platform security can arguably be said to be more secure than any number of perimeter and access firewalls - if implemented correctly.

Transitioning to a hybrid cloud platform will provide transparency and security by design that only needs to be built once. By routing industrial data through more securely controlled cloud systems, you are reducing the attack surface and the number of data points that are being exposed across the entire enterprise.

However, using some of these new technologies does not come without potential high risk. By not having the means to monitor what is going on at the industrial level and by not having the means to implement the right policies and controls, you can end up in the situation where there are multiple routes into the production systems from the enterprise and from supply chain vendors.

What we are currently seeing is customers running 24x7 production schedules with the emphasis firmly on keeping the 'lights on'. This doesn't give much headroom to quickly implement new technologies such as secure remote access for support, maintenance and commissioning. Our approach is to move the remote access risk to the cloud where it can be carefully managed, and, at the factory level build **robust and resilient OT networks.**



Optimisation through SDX network segmentation, secure RDP and non-repudiation screen recording.

Visibility of all Assets & Data Points, Cloud Platform Security & Software Defined Segmentation. IT, OT & Automation Integration. Hybrid Cloud Platforms & Edge Computing for increased Security & Efficiency.

A Playbook For Finding New Technologies

Follow this guide to choose the best fit Remote Access Solutions for your Security & Efficiency requirements.

polestar industrial IoT

DISPEL

Remote Manufacturing Solutions

Many manufacturers and enterprises, not fully understanding the security risks, opted to install a quick-fix remote access solution to maintain productivity. Whether it was an unprotected access point or a shadow Android phone plugged into the OT network, manufacturers tried their best to configure a remote access setup within a tight deadline. Unfortunately, the security risk is very high —29% of all cyber attacks in the UK were targeted at manufacturers last year.

Quick fix methods often satisfy OT's need for efficiency but leave IT's security requirements unattended. In order to optimise your remote manufacturing strategy, you need a system that bridges the gap between IT and OT: a tool that both meets cybersecurity requirements mandated by IT, and maximises plant efficiency for OT.

The good news is that this gap is bridgeable. Done properly, remote access to industrial control systems fulfills the needs of both IT and OT, providing substantial enhancements to uptime, system availability, and safety. More specifically, a successful secure remote access solution should be tailor-made for industrial environments, and should also facilitate:

- Delivering operations from different countries
- Vendor access, for maintenance purposes
- Training, that would otherwise require a physical location

A Playbook For Finding New Technologies

When it comes to finding the right technology, start by considering your end goal. Most companies answer this with "to find a technology", "to find a secure technology", "to maintain cyber security", or to "implement remote access". However, these are not the end goal.

The real end goal is **plant efficiency**. To accomplish this, you need to:

- Maximise performance
- Minimise downtime
- Maintain system control

To properly evaluate the new technologies you are looking to implement, you must place a relentless focus on plant efficiency. Here are the 3 key considerations you should make when evaluating a new technology.

1. **Security and Compliance:**

   A robust remote access system should allow complete control for your OT network admin with full security features built-in.

If you are looking for a baseline of security best practices, a good place to start for those in the UK is the NCSC framework. Similarly, NIST 800-82, and IEC 62443 are also helpful resources to give direction to how you shape your security posture.

Too often, security is seen as the enemy of efficiency. Especially in OT environments, security must be designed to boost plant efficiency. Make sure to ask:
Is the product's access control built to improve productivity, minimise downtime, and maintain system control?

Ask a consultant to walk through how you would onboard, give access, and revoke access for a third-party vendor technician. A good consultant should tell you about:

- Access control
- Regulatory frameworks
- Secure architecture
- Resilience and fault tolerance

2. **Time-to-Equipment:**

Every minute of downtime is money lost. Your technology should be actively helping you minimise downtime, so it is essential that your technology is fast and easy to use.

Ask your consultant to show you how the technology considers:

- User experience
- Connection time
- Accessible design

3. **Long-term Viability:**

Factories are built to last decades. Is your digital technology built to keep up through 2050? New digital technology should bring you towards resilience and flexibility, not bog down your systems further.

Ask your technology consultant:

- How often do I have to buy new hardware to stay on the most up-to-date version of this technology?
- Do I have to restart/re-install software on my equipment?
- How will this technology work with our Digital Transformation initiatives through 2050?

How to Measure the Efficiency Impact

If you are looking to measure the efficiency impact of a technology, the best place to start is with a simple back-of-the-napkin comparison. To accomplish this, here are the steps you should take, and the data you need to collect:

STEP 1: Collect Baseline Data Before Pilot	STEP 2: Install a Pilot	STEP 3: Collect Pilot Data
Concrete numbers you need to collect:	Concrete numbers you need to collect:	Concrete numbers you need to collect:
# of minutes to log in and access equipment	# of hours for installation of pilot	# of minutes to log in and access equipment
# of minutes to grant access to new user or vendor	# of hours for new admin training	# of minutes to grant access to new user or vendor
# of hours per week managing access	# of minutes for new user training	# of hours per week managing access
Survey-based feedback to collect:	**Extrapolation needed:**	**Survey-based feedback to collect:**
User happiness: How easy is it for you to log in?	# of hours for installation at all sites	User happiness: How easy is it for you to log in?
Admin confidence: How confident are you in keeping this as your long-term solution?	# of hours per year for upgrades	Admin confidence: How confident are you in keeping this as your long-term solution?

STEP 4: Extrapolate Efficiency Gains
After a month at a single site, you should have clear qualitative feedback, and promising quantitative feedback.

Please download our Efficiency Calculator to enter your inputs for your efficiency gains. Enter your findings into the "Executive Summary View" page, and look at the box at the top for your results.

polestar industrial IoT

DISPEL

Contact us for more information or to schedule a discussion on digital transformation for your manufacturing organisation.

+44 115 911 6699
www.polestarinteractive.com
info@polestarinteractive.com
@ polestar iiot