SECURING OPERATIONAL TECHNOLOGY **IN THE MANUFACTURING INDUSTRIES**

FOUR KEY CONSIDERATIONS

BAYSHORE

Introduction

Connecting industrial equipment, networks, and applications can drive significant economic benefits for automobile, heavy equipment, and machinery manufacturers, creating the opportunity for smarter factories, safer workers, and better business outcomes. In fact, "the Industrial Internet will dramatically improve productivity and efficiencies in the production process and throughout the supply chain. Processes will govern themselves, with intelligent machines and devices that can take corrective action to avoid unscheduled breakdowns of machinery. Individual parts will be automatically replenished based on real time data. Every handheld digital device in the factory will report the status of every fixed device, giving personnel mobile access to real-time, actionable information. Wearable sensors will track the location of each employee in the factory, in case of emergency. The list goes on and on."[1]

While there are many benefits, Internet-connected devices can introduce the potential for new cyber threat vectors and larger attack surfaces that result in safety concerns, downtime, operational disruptions, IP risk, and costly physical damage to equipment, products, and people. Manufacturers have a primary requirement to ensure worker safety, and recent cyber attacks on industrial plants have put safety at risk, causing damage, explosions, and shut-downs. Meanwhile, the cyber threat to intellectual property – from state sponsored actors and competitors – increases annually.

This white paper will examine the rise of the Industrial Internet, also called the Industrial Internet of Things (IIoT), and the concurrent increase in cyber risk within the manufacturing sector, the opportunities and challenges created by the convergence of information and operational technology, and four key considerations when protecting industrial assets against cyber threats. Lastly, it introduces Bayshore's Industrial Control Platform, which stops cyber threats before they can damage critical manufacturing assets and systems, and allows secure connection to the Industrial Internet, including secure remote access.

[1]Industrial Internet Consortium, http://www.iiconsortium.org/vertical-markets/manufacturing.htm

The Explosive Growth of the Industrial Internet of Things

According to Frost & Sullivan, 80% of manufacturing companies around the globe will have adopted the Industrial Internet of Things by 2021.[2] In fact, it is estimated that by 2020, between "30 billion and 50 billion objects will be connected. These connected objects will automate processes, find and self-correct problems, and record and send data to central servers. All of this data can be analyzed to modify and improve products and processes."[3] IIoT is also known as Industry 4.0, which "creates what has been called a 'smart factory.' Within the modular structured smart factories, cyber-physical systems monitor physical processes, create a virtual copy of the physical world and make decentralized decisions."[4]

Much of the value from the rise of Internet-connected devices on the manufacturing floor is derived from the industrial data that is collected and analyzed to:

- **Predict Maintenance Schedules**
  For example, sensors detect whether machinery is operating within normal limits as benchmarked against previous performance and predict when it might need to be worked on. Predictive maintenance enables manufacturers to stay ahead of repair schedules and costs as well as keep systems up and running for optimal productivity. This enables manufacturers to optimize production because they can now know when there is a slowdown or less-than-ideal performance through sensor data and analytics, garnered through remote monitoring without the need for massive human oversight.
- **Integrate and Optimize the Company's Supply Chain**
  "Traditional, linear supply chains are no longer fit to compete. What companies need now is a new supply chain strategy—a strategy structured around the flexibility and scalability that digital technologies can enable. With such a strategy companies unlock their supply chain to be an engine for growth, enabling quick movement into new geographies, supporting new value-delivery approaches, and creating new products and services."[5]

These two use cases increase the ability of the plant to operate at maximum uptime, reduce waste from manufacturing processes, and increase safety via equipment and employee monitoring. These benefits, however, are countered by the challenges of securing OT on the plant floor as well as its interconnection with the corporate network. While IIoT "enhances digital capabilities throughout the manufacturing and supply chain processes and drive revolutionary changes to connected devices, it also brings with

---

[2]Frost & Sullivan, "Cyber Security in the Era of Industrial IoT," sponsored by Bayshore, 2017.
https://www.bayshorenetworks.com/cybersecurity-in-the-era-of-industrial-iot

[3]Stefan Guertzgen, "Chemical Industry: 4 Opportunities Provided by Internet of Things," Internet of Things Institute, December 14, 2016.
http://www.ioti.com/industrial-iot/chemical-industry-4-opportunities-provided-internet-things

[4]https://en.wikipedia.org/wiki/Industry_4.0

[5]Gary L. Hanifan, "Is Your Supply Chain a Growth Engine?" Accenture, 2015.
https://www.accenture.com/t20150923T080445Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_13/Accenture-Is-Your-Supply-Chain-Engine-Growth.pdf

it new cyber risks for which the industry is unprepared."[6] That's because IIoT increases the potential attack surface with billions of interconnected devices, all of which can be searched on dark web search engines, such as Shodan, for vulnerabilities.

Unfortunately, Internet-connected sensors and devices are built for 24x7 uptime and reliability, not security. The majority of operational systems is not up-to-date or patched regularly. Moreover, corporate IT networks can act as a gateway for cyber attackers to infiltrate the OT network through lateral movement, and different protocols and systems use enterprise networks and the plant's operational technology, making them difficult to secure holistically. Meanwhile, IT and OT staff have different priorities and skill sets, making it challenging for them to align with cybersecurity priorities.

These risks and challenges have deep consequences. "When supply chains, factories, customers, and operations are connected, the risks posed by cyber threats become all the greater and potentially farther reaching."[7] These threats include but are not limited to:

- Espionage on corporate systems
- Sabotage of plant systems, leading to the manufacture of incorrect specifications and possible plant shutdown
- Physical hazards such as fire and explosions
- Public and employee health issues

Let's look at some specific examples of manufacturing companies recently affected by cyber attacks.

ThyssenKrupp

Stolen IP: "ThyssenKrupp, one of the world's largest steel makers, said it had been targeted by attackers located in southeast Asia engaged in what it said were 'organized, highly professional hacker activities.' In breaches discovered by the company's internal security team, hackers stole project data from ThyssenKrupp's plant engineering division and from other areas yet to be determined."[8]

Hacked Control System: It is believed that ThyssenKrupp is also the same company that lost control of its blast furnace in 2014. "Given that blast furnaces contain molten metal heated to thousands of degrees, it was a dangerous situation. Fortunately, there were no reported injuries, and the only result was "massive damage" to the facility.

[6]Stefan Guertzgen, "Chemical Industry: 4 Opportunities Provided by Internet of Things," Internet of Things Institute, December 14, 2016.
http://www.ioti.com/industrial-iot/chemical-industry-4-opportunities-provided-internet-things

[7]René Waslo, Tyler Lewis, Ramsey Hajj, Robert Carton, "Industry 4.0 and cybersecurity: Managing risk in an age of connected production," Deloitte University Press, March 21, 2017.
https://dupress.deloitte.com/dup-us-en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html

[7]Eric Auchard, Tom Käckenhoff, "ThyssenKrupp secrets stolen in 'massive' cyber attack," Reuters, December 8, 2016.
https://www.reuters.com/article/us-thyssenkrupp-cyber/thyssenkrupp-secrets-stolen-in-massive-cyber-attack-idUSKBN13X0VW

More concerning, though, was why the accident happened. Hackers had infiltrated the mill's control system and wreaked havoc, according to a report from BSI, the German government's office for information security."[9]

Georgia Pacific

Damage via VPN: "A system administrator...had worked at paper maker Georgia-Pacific for years until the Valentine's Day 2014 when he left the company and started attacking it.... [He] maintained an active VPN connection to the systems at Georgia-Pacific even after he left the company and accessed the servers to install its own software and interfere with industrial control systems (ICS) in the plant. The former sysadmin launched the attack against the company that lasted two weeks and caused roughly $1.1 million dollars in damage."[10]

Renault

Production Downtime: "Renault and its Japanese partner are the only major car manufacturers so far to have reported production problems resulting from Friday's WannaCry ransomware worm attack that spread to more than 150 countries. The cyber attack halted or reduced the output of at least five Renault sites over the weekend. Besides Douai, they included a van plant in Sandouville, France; a small-car plant in Slovenia; the no-frills Dacia plant in Pitesti, Romania; and a factory shared with Nissan in Chennai, India."[11]

Cadbury

Production Downtime: "Production at Cadbury's chocolate factory in Hobart has stopped after its parent company found itself engulfed in the ransomware cyber-attack that has spread through the US and Europe.... the Hobart chocolate factory's 500 employees, who produce about 50,000 tonnes of chocolate a year, turned up for work on Wednesday but it was unclear how long it would take to restore the computer systems so production could resume."[12]

---

[9]R.A. Becker, "Cyber Attack on German Steel Mill Leads to 'Massive' Real World Damage," Nova Next, January 8, 2015, http://www.pbs.org/wgbh/nova/next/tech/cyber-attack-german-steel-mill-leads-massive-real-world-damage/

[10]Pierluigi Paganini, "Former employee hacked paper maker Georgia-Pacific and caused $1m damage," Security Affairs, February 18, 2017. http://securityaffairs.co/wordpress/56396/cyber-crime/paper-maker-georgia-pacific-hacked.html

[11]Reuters staff, "Renault-Nissan resumes nearly all production after cyber attack," Reuters, May 15, 2017. https://www.reuters.com/article/us-cyber-attack-renault/renault-nissan-resumes-nearly-all-production-after-cyber-attack-idUSKCN18B0S5

[12]Guardian staff, "Petya cyber-attack: Cadbury factory hit as ransomware spreads to Australian businesses," The Guardian, June 27, 2017. https://www.theguardian.com/technology/2017/jun/28/petya-cyber-attack-cadbury-chocolate-factory-in-hobart-hit-by-ransomware

Royal Canin

Product Shortages: "Britain is in the grip of a shortage of cat food after a cyber attack hit one of the country's biggest. Some pet shops are still reporting low stocks of Royal Canin after the company's headquarters in France were attacked by hackers on June 27. Although production has been put back up to full capacity, many British suppliers have been unable to fulfill orders or restock shelves. Shortages have been reported across London and the Home Counties. At one pet shop in Sydenham, south London, customers were faced with a two-week wait for kitten food."[13]

At the heart of these attacks are three ransomware attacks, known as WannaCry and Petya, which targeted and ecrypted older Windows systems such as Windows 7, and NotPetya. Both WannaCry and NotPetya propagated via an exploit developed by the U.S. National Security Agency.

Protecting Against Cyber Threats: Four Key Considerations

So what can manufacturers do to secure their systems? What's clear is that enterprise IT cannot be assured by operational technology. A way must be created for data to transit the network securely and be policed at the same time. Identifying and blocking cyber threats is a mandatory first step before connecting plant processes, networks, and applications. Here are four key considerations when assessing potential solutions:

1. Improve End-to-End Asset Visibility: You Can't Protect What You Can't See

Ensure your solution continuously maps and monitors industrial traffic, learning as it adapts to observations. You'll want to combine advanced threat intelligence from public and private sources with out-of-the-box policies to establish and maintain a baseline of acceptable behaviors in order to block known malware. Look for an approach that helps you optimize and protect your OT environment, including protocols, sources, destinations, manufacturers, models, and anomalies or violations of baseline policies. Also, ensure that the solution can inspect full messages (regardless of protocol) for both content and context at the transaction level and that all reporting can be integrated into your SIEM/SOC and forensic analysis tools of choice.

2. Mitigate Cyber Threat Risks: Just Seeing a Threat Won't Stop It

Look for an approach that stops cyber threats in real time, before they can damage your industrial infrastructure or the environment. Look for active alerting and proactive blocking of unauthorized communication and commands, preventing cyber threats from reaching and affecting targeted objects and data, as well as anti-springboard technology that stops malware from making horizontal jumps. You'll want a solution that operates at line speed, providing protection at a fine-grained transaction level, enabling authorized traffic and standard workflows to continue unimpeded even in the face of ongoing cyberattacks.

---

[13]Richard Hartley-Parkinson, "Cat food shortage after cyber attack hits one of UK's biggest suppliers," Metro News, August 24, 2017
http://metro.co.uk/2017/08/24/cat-food-shortage-after-cyber-attack-hits-one-of-uks-biggest-suppliers-6875065/#ixzz4sNzXy9HN

3. Provide Managed Remote Access: Protection Means Control Over Access and Actions

Allowing vendors to access industrial equipment for maintenance and troubleshooting remotely offers distinct advantages. Providing industrial data to service providers may help improve business outcomes. However, opening industrial infrastructure to these third parties creates significant risk. Traditional VPNs can help with controlling access, but once a connection is made, manufacturers have no way to know or control the actions that remote users undertake on their open ports. The lack of cyber protection provided by VPNs is just unacceptable in the industrial world: customers must be in charge of their networks, not their vendors. Look for a Managed Remote Access solution that goes far beyond traditional VPNs to create an on-demand, encrypted, policy-protected, bi-directional tunnel between remote users and your industrial infrastructure.
Ensure that every element of communication between you and third parties is verified, managed, and blocked if necessary. Look for Managed Remote Access that enforces authentication, authorization, white lists, and other security controls at the device command and individual transaction level. Your Managed Remote Access solution must limit ability to access plants remotely, and control activity during remote access sessions, with no VPN access allowed.

4. Secure Your Industrial Internet: Protect Your Assets Before You Connect

When you are ready to interconnect your industrial infrastructure and data to take advantage of all the Industrial Internet has to offer, look for a solution that provides bi-directional, access-controlled, and policy-protected tunnels between your organization and your chosen IIoT partners. This means that not only is access limited to specific sources and destinations, but also that content and context is controlled by policy so that every element of communication between the organization and its external IIoT ecosystem can be verified, alerted, and blocked if necessary.

How Bayshore Networks Can Help

The Bayshore Industrial Cyber Protection (ICP) platform stops cyber threats before they can damage critical industrial assets and systems, and allows secure connection to the industrial internet of things (IIoT). Bayshore has extensive experience providing cyber protection for massive manufacturing networks, while allowing manufacturers to take advantage of the promise of connecting their industrial infrastructure. Bayshore operates at the machine transaction level, enabling the extremely granular filtration, segmentation, and isolation required to secure large-scale manufacturing infrastructure.

The Bayshore ICP platform delivers a comprehensive set of capabilities required to protect and defend against sophisticated, complex attack systems. Bayshore empowers industrial enterprises with safe and efficient production, operational insights, and improved business outcomes while blocking cyber threats to industrial plants, machinery, and people. It is designed to support manufacturing customers throughout the entire industrial cyber protection life cycle, leading to improved business outcomes.

The journey begins with mapping networks assets and progresses to identifying anomalies, preventing attacks and incidents, optimizing business efficiencies, and finally, to enabling innovation and digital transformation, such as creating new revenue sources and product markets. The comprehensive industrial cyber protection platform uniquely offers customers a long-term solution by providing a single, tightly integrated, extensible, and scalable architecture. Bayshore Secure Remote Access, which uses two factor authentication, stops unnecessary access to equipment and limits the actions remote users can take.

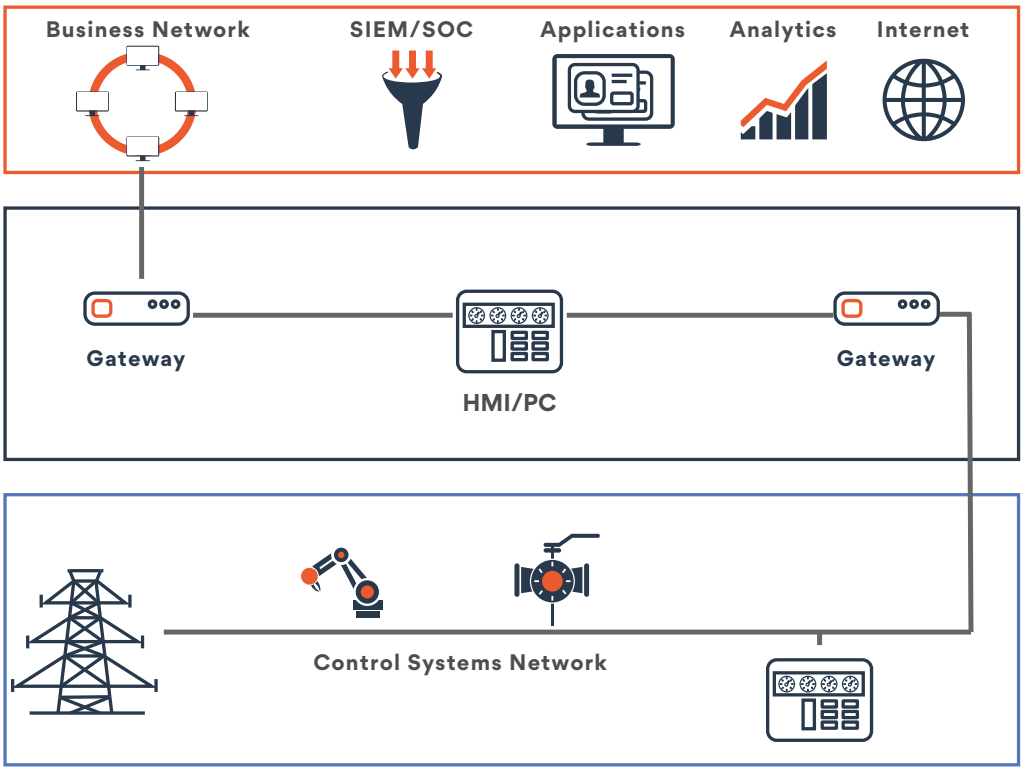


Figure 1: How the Bayshore ICP Platform works

Gateways blocks unauthorized commands from reaching end points, preventing malware from entering server farm and affecting HMIs, Engineering Workstations, other susceptible endpoints. Bayshore Gateways can detect network scanning, even with industrial protocols and prevent unplanned firmware patching to the ICS network. Bayshore Gateway inspection points alert on unnecessary access to the control network and alert or block disruptive commands. The Bayshore Management Console rapidly deploys policies across gateways, blocking cross-contamination. Policy enforcement blocks unauthorized commands and firmware downloads while the expropriation of data is blocked by deep content filtration and enforcement of DLP policies.

The benefits of Bayshore's native OT protocol and content-based cyber protection for manufacturers include:

- Visibility across global-scale OT infrastructure
- Increased worker safety, factory uptime, and reduced downtime
- Enhanced predictive maintenance
- Improved operational efficiency leading to increased revenue, reduced OPEX
- Simplified reporting and compliance

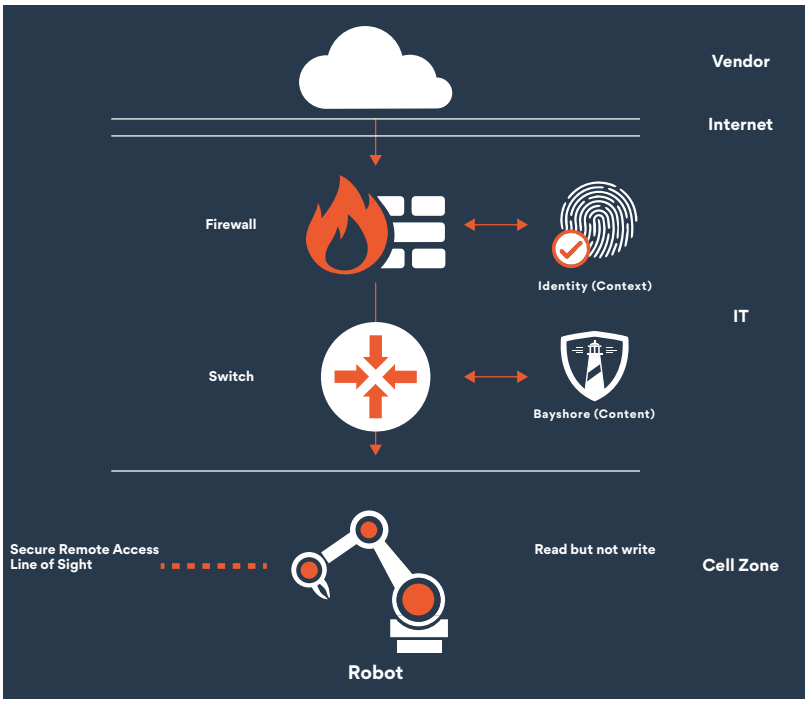
Case Study: Global Automaker Uses Remote Access Cybersecurity to Maintain Safety at its Manufacturing Production Zones

In the world of manufacturing, an unplanned outage typically requires technicians to be onsite to troubleshoot problems. But these experts usually work for partner companies and may take more than 24 hours to arrive onsite, leading to costly outages and production delays.

To address the problem, one of the world's largest automakers, widely considered one of the most technologically forward-looking organizations in all of manufacturing, asked Bayshore Networks and its partners to design and build secure remote access to its factory production cell zones.

Due to the IT department's strict security guidelines, the partners, which provide engineering solutions such as robots and electronic controllers for assembly line conveyor belt motors, were typically only allowed to remotely access cell zones during emergencies. During these emergencies, they were granted access over VPNs. The IT department would open several ports and manually allow users to enter. Of course, the open VPN ports did not enable the IT department to maintain its typically high standard of granular access. Access was provided on an exception basis, crippling the department's ability to establish persistent postures for cybersecurity and safety.

The manufacturer required a solution that safely provided secure remote access with transaction control while ensuring zero downtime and higher availability of production systems.



The Bayshore IT/OT Gateway enables secure remote access to cell zones while providing granular access control and meeting the IT Department's zero downtime requirements.

The automaker asked its engineering partners to work with Bayshore Networks to design a solution that provided secure remote access that adhered to the company's safety and cybersecurity guidelines. The resulting solution ensured that remote users would have line-of-sight access to assembly line robots to ensure they were managed safely. At the same time, the solution prevented potentially downtime-impacting actions that would have been allowed in the emergency VPN scenario, such as accidentally writing commands to robots. Thanks to Bayshore's IT/OT Gateway software technology, engineers at partner companies can remotely troubleshoot problems safely and securely from smart devices.

Summary

New cyber security threats targeting IIoT in the manufacturing sector are emerging every day, risking public and employee safety, operational disruptions and plant downtime, and costly physical damage to plants, machines, and products, in addition to loss of intellectual property via espionage on the corporate network. Identifying and protecting against cyber threats is a mandatory first step before connecting plant processes, networks, and applications.

Bayshore inspects machine-specific industrial protocol traffic, which eliminates cyber threats before they reach critical equipment, protecting OT applications, networks, machines, workers, and the environment. Additionally, Bayshore's Managed Remote Access solution allows manufacturers to grant tightly controlled access to third parties, such as equipment vendors, for maintenance and troubleshooting.

Next Steps

For more information on the Bayshore Industrial Cyber Protection platform, visit **www.bayshorenetworks.com/platform.**

About Bayshore Networks, Inc.

Bayshore Networks® is the leading provider of industrial cyber protection. The Company's award-winning technology unlocks the power of the Industrial Internet of Things (IIoT), providing enterprises with unprecedented visibility into their Operational Technology infrastructure while safely and securely protecting ICS systems, industrial applications, networks, machines, and workers from cyber threats. Bayshore's strategic partners include among others Arista, AT&T, BAE, Cisco, Dell, SAP, VMware, and Yokogawa. Bayshore is a privately held company headquartered in Washington, DC and backed by Trident Capital Cybersecurity, Yokogawa, Samsung Next, and BGV Capital. For more information, visit **www.bayshorenetworks.com.**

BAYSHORE

BAYSHORE

www.bayshorenetworks.com