# Table of Contents

**Improving Operational Resiliency for Manufacturers Through ICS Visibility and Cyber Security** ............................................................ 1

1. **Top Manufacturing Industry Challenges** ........................................... 2  
   - I. Maintaining Operational Resiliency and Uptime ... 2  
   - II. Employing a Cyber Security Framework and Best Practices ... 3  
   - III. Achieving Visibility into (and Protecting) ICS Networks ... 4  
   - IV. Integrating IT and OT Systems to Close Security Gaps ... 4

2. **The Nozomi Networks Solution** ....................................................... 5  
   - I. How the Nozomi Networks Solution Improves Operational Resiliency ... 5  
   - II. Sample Deployment Architecture ... 6

3. **Improving Network and Operational Visibility** ................................. 7  
   - I. Use Case: Effectively Monitoring the Industrial Control System (ICS) Network ... 7  
   - II. Use Case: Keeping Production Lines Running ... 9

4. **Detecting Cyber Risks and Improving Cyber Resiliency** ..................... 11  
   - I. Use Case: Integrating IT/OT Security Efforts ... 11  
   - II. Use Case: Applying Cyber Security Best Practices ... 13

5. **Conclusion** ...................................................................................... 15  
   - I. Operational Visibility and Cyber Security Boost Manufacturing Resiliency ... 15

What to Look for in a Real-time ICS Visibility and Cyber Security Solution ... 16

See the Nozomi Networks Solution in Action ... 16

Additional Resources ... 16

References ... 17
INTRODUCTION

Improving Operational Resiliency for Manufacturers Through ICS Visibility and Cyber Security

Even after years of declining growth, manufacturers continue to face headwinds from consumers, channels and competition. Innovation and automation are key to unlocking growth potential, but the new technologies driving digitization also increase exposure to cyber threats that can disrupt operations.

Fortunately, advanced solutions that provide real-time visibility and cyber security for industrial networks significantly reduce risk and build production resiliency.

Small, nimble competitors entering the manufacturing space increase the pressure on established players to deliver on millennial consumer expectations. To compete, companies must deploy new technology to take advantage of interconnected systems and supply chains, artificial intelligence for predictive maintenance, and mass customization trends.

Compounding the challenge is a cyber security labor crisis. While automation can reduce the number of low-skilled roles and increase operational productivity, more plant floor connectivity opens the network to threats that require a new set of IT/OT (operational technology) skills.

From a cyber security standpoint, manufacturers have traditionally flown under the radar. Threat actors initially targeted critical infrastructure, such as energy and transportation, and industry and governmental security oversight followed.

But, according to the 2018 Cyber Security for Manufacturing report, manufacturing is now the third most targeted industry, behind only government systems and finance. And nation-state sponsored and other malicious hackers are taking full advantage of the opportunity. According to the Verizon’s 2019 Data Breach Investigations Report, intentional attacks on manufacturing by outsiders accounted for 70% of all breaches reported.

External threats, however, aren’t the only risks that keep company leaders awake at night—accidental and unintentional cyber incidents caused by employees or suppliers can impact productivity as well. Given the large number of vulnerable devices and insecure processes, the risk of some type of breach is very real. And, despite a historic lack of industry oversight, guidelines and regulations are coming.

THE ROAD TO MANUFACTURING RESILIENCY

Read this paper to learn how easy it is to gain operational visibility, reliability and cyber security using a real-time ICS (industrial control systems) monitoring and threat detection solution.

Manufacturers, including the food and beverage, chemical, pharma and automotive sectors, need to get ahead of the curve. The first step is to adopt a cyber security framework that IT and OT can collaborate on. Armed with cyber security best practices and the right technology, companies can protect their production, people and reputation, while preserving the bottom line.
Top Manufacturing Industry Challenges

As manufacturers automate and digitize, they face the following challenges that, if not properly addressed, leave them exposed to significant business risks.

1. Maintaining Operational Resiliency and Uptime

Interconnectivity between enterprise and operational networks opens the door for cyberattacks. So does external connectivity spurred by Industry 4.0 and the Industrial Internet of Things (IIoT). That means that if a production line goes down, companies can lose millions within minutes.

While that’s a worst-case scenario, manufacturers are hyper-aware of the potential financial impact of downtime. For this industry, maintaining 24/7 uptime is business-critical.

In 2017, for example, British consumer goods company Reckitt Benckiser Group suffered an estimated $117 million loss after a NotPetya attack. The malware caused widespread business disruption, information loss, revenue loss and equipment damage across multiple markets. Dubbed by many to be the most devastating cyberattack in history, NotPetya cost Reckitt Benckiser 1% of its annual sales—and inflicted $10 billion in damages across industries globally.

Due to the impact downtime can have on manufacturers’ ability to deliver product to market, many opt to keep additional inventory on hand as a risk mitigation tactic. Producing and storing extra inventory for days or even weeks at a time is an expensive proposition. It also takes manufacturers away from just-in-time (JIT) manufacturing—an ideal inventory control method that increases productivity while lowering costs. Instead, companies have been forced to delay their inventory turnover due to fear of cyber incidents that could disrupt operations.

To protect production lines, manufacturers can take advantage of OT risk detection and mitigation solutions that don’t compromise uptime.

THE HEAVY BURDEN OF OPERATIONAL DOWNTIME

For the manufacturing industry, maintaining 24/7 uptime is business critical. In 2017, British consumer goods company Reckitt Benckiser Group suffered an estimated $117 million loss after a NotPetya attack.
II. Employing a Cyber Security Framework and Best Practices

Devastating and costly cyberattacks dominate the news media, leaving manufacturers to consider, “What would happen if an attack hit our organization?” From NotPetya to WannaCry to Dragonfly 2, these malware attacks wreak havoc on manufacturers’ ability to operate, and ultimately cause massive financial hits to the bottom line.

As companies look at their security posture and practices, executive leadership and Boards of Directors fear that while IT functions appear to be well covered, no visibility or protection is in place for operations. OT teams are feeling the pressure from the CIO, or Chief Information Security Officer (CISO), to ensure that company IP, technology and production processes are adequately protected.

Top manufacturers are researching and selecting a cyber security framework to follow, such as IEC 62443 NIST, or NIS. These frameworks offer guidelines for cyber security best practices and tools for facilitating their implementation.

BEING PROACTIVE IS BEST PRACTICE

While the manufacturing sector has largely flown under the radar, cyber regulations are now being developed for nearly every industrial sector. With a trusted framework selected, manufacturers can identify the right people, processes and tools required for robust cyber security hygiene. From an accurate asset inventory to identifying potential threats, manufacturers can follow industry guidelines and best practices to attain next-level cyber security resiliency.
III. Achieving Visibility into (and Protecting) ICS Networks

For decades, automation manufacturers defined their own proprietary networking protocols. In recent years, however, the industry has come to appreciate the benefits of common networking platforms to ensure compatibility across devices and properly protect their systems.

As the industry transitions, navigating a blend of new and old infrastructure can prove challenging. Between legacy OT systems and new IIoT devices being added without documentation, many teams don’t have an accurate view of what’s on their network. It’s not uncommon for manufacturers to think that they have 5,000 devices, when the number is more like 10,000. This lack of visibility makes it nearly impossible to secure and monitor industrial networks, leaving many manufacturers unsure of where to start.

To transform the system architecture and achieve the required visibility, manufacturers need to employ the latest technology and best practices. This starts with inventorying all assets on the network. If the IT/OT team doesn’t know what they have, they can’t protect their assets or segment the network for better resiliency.

Visibility also enables operational efficiencies and potential cost savings. For example, an inefficient network link with unusually high bandwidth usage can be easily identified. And once the full network is visible, it can be monitored on an ongoing basis for deviations. Manufacturers can then easily spot vulnerable areas and assets in need of protection – and oversee an efficient, resilient system.

IV. Integrating IT and OT Systems to Close Security Gaps

Manufacturing executives are putting pressure on their CISOs and Operational VPs to 1) protect the company from risk and 2) transform plant operations by improving operational effectiveness. This transformation can only be accomplished with IT and OT working together.

With divergent priorities, bringing OT and IT teams and systems together can feel like an uphill battle. And as more systems converge, the vulnerability points and potential risks only continue to increase. Teams need to balance their dueling priorities and tap into each other’s unique expertise.

IT can advise on cyber security issues and processes. OT keeps production systems running and prevents downtime. Together, these functions make holistic threat monitoring and secure data flows possible, to reduce blind spots and minimize security risks.

The insights derived from IT/OT convergence can optimize factory operations, enhance equipment utilization, enable predictive maintenance, and improve cyber security. And the impact doesn’t end there. These insights create a more scalable system, ready to tackle new logistical challenges.

THE VALUE OF IT/OTCOLLABORATION

The insights derived from IT/OT convergence can optimize factory operations, enhance equipment utilization, enable predictive maintenance, and improve cyber security.

In fact, a factory’s path to digital transformation reaches across the entire value chain, from product development to distribution (and beyond). With comprehensive, real-time operational visibility, plants can increase productivity and close security gaps.
The Nozomi Networks Solution

I. How the Nozomi Networks Solution Improves Operational Resiliency

Nozomi Networks helps manufacturers accelerate the pace of digital transformation by pioneering innovation for industrial cyber security and operational control. We make it possible for organizations to tackle escalating cyber risks to operational networks while modernizing their businesses to succeed in the future.

Nozomi Networks delivers OT visibility, threat detection and insight to thousands of the largest industrial sites around the world. Through the innovative use of artificial intelligence (AI), our solution automates the hard work of inventorying, visualizing and monitoring industrial control networks.

Manufacturers benefit from the real-time visibility and threat detection needed to ensure high cyber resiliency and reliability.

Guardian™ provides complete visibility and cyber security for ICS environments by combining asset discovery, vulnerability assessment, threat detection, and anomaly detection in a single, unified solution.

Central Management Console™ (CMC) enables centralized security visibility and management for multi-tier, distributed OT deployments across the world.

OT ThreatFeed™ delivers up-to-date threat intelligence to effectively detect threats and identify vulnerabilities in ICS environments.
II. Sample Deployment Architecture

Shown above is a general example of how the Nozomi Networks solution can be deployed.

A wide variety of appliances, a flexible architecture, and integrations with other systems allow us to provide a solution tailored to meet the needs of your organization.

Additionally, Remote Collectors™ can be added to Guardian appliances to capture data from remote and offsite locations.
3 Improving Network and Operational Visibility

I. Use Case: Effectively Monitoring the Industrial Control System (ICS) Network

In the world of manufacturing, one small change or networking issue can have a significant effect – on product quality, production uptime and even plant safety. Staying on top of what’s happening in the industrial control network, and responding to changes fast, is mission critical.

But industrial operators can’t monitor and manage what isn’t visible and documented. For example, during a recent Proof of Concept, a manufacturing company stated that they had 3,000 devices on their network. When the Nozomi Networks solution was deployed, 15,000 appeared! And while working with a wholesaler, Guardian uncovered devices that were thought to be decommissioned, former contractors who still had system access, and other surprising insights.

Do you really know what types of devices are on your network, and how many there are? Which ones are actively communicating and what protocols they’re using? Would you know if someone intentionally or accidentally changed the configuration on a PLC, or deleted a log file?

To spot and troubleshoot networking and communication issues that threaten reliability, you need real-time visibility into your assets, connections, communications, protocols and more.
The Challenge

• Staying on top of network status and changes

The Solution: Using Real-time ICS Visibility to Improve Situational Awareness

• The Nozomi Networks solution analyzes network traffic, using the data to build a live, interactive visualization of the system, often revealing unknown aspects of the ICS.

• Manufacturers can efficiently monitor industrial networks and easily troubleshoot problems before they impact operations.

Results

• Network-wide situational awareness
• Faster troubleshooting of system changes and issues
• Better oversight of vulnerabilities and risks
• Higher operational reliability

Nozomi Networks Solution: Network Visualization Graph

Within minutes of deployment, Guardian visualizes the nodes of the manufacturing network, often revealing aspects operators weren’t previously aware of.
II. Use Case: Keeping Production Lines Running

Unplanned downtime happens for multiple reasons—a component breaks down from operating 24/7, a networking change impacts production lines, or a cyber incident disrupts communication.

Not only does it take time to understand and address the problem, valuable production capacity is lost. To mitigate risks like this, some manufacturers carry extra inventory just to cover potential downtime.

But in the manufacturing business, time is money, so planned and unplanned downtime, and excess inventory, can hit the bottom line hard. According to Gartner, the cost of downtime clocks in at somewhere between $300k–500k an hour. Let’s take a look at the impact of downtime:

In 2019, Norsk Hydro, a multinational manufacturer headquartered in Norway and one of the world’s largest aluminum producers, reported that it was hit by a ransomware that affected its production and IT systems. The Extruded Solutions unit, which makes components for car manufacturing, construction and other industries, reduced its output by 50%.

Administrative systems, such as reporting, billing and invoicing, suffered delays. It took Norsk Hydro several weeks to bring operations back to normal. Lost margins and low production volumes were estimated to cost up to $70 million. Can you imagine the benefits of proactively identifying potential equipment problems, cyber threats, and bringing your stock on hand down by 50% or more?
Nozomi Networks Solution: Process Variable Alert and Graph
Abnormal device or manufacturing process behavior automatically generates alerts (left screen shot) that provide information on anomalies (right screen shot). Operators can take action before operational disruption and costly downtime occur.

The Challenge
- Preventing loss of production capacity

The Solution: Using Anomaly Detection to Identify At-Risk Equipment Before It Fails
- The Nozomi Networks solution monitors the network, detects anomalies as compared to the baselines it observes, and alerts operators to deviations.
- Operators spend less time troubleshooting issues and can take quick action before equipment failures occur.

Results
- Proactive detection of potential equipment failure
- Reduced troubleshooting and forensics
- Faster problem resolution
- Maximized production line uptime
Detecting Cyber Risks and Improving Cyber Resiliency

I. Use Case: Integrating IT/OT Security Efforts

OT knows how to meet production targets and keep the plant running. IT has the expertise to address networking and cyber security issues that are unfamiliar to ICS staff. Wouldn’t it be great if the OT and IT teams worked together to build operational resiliency?

Unfortunately, oversight of OT security can be quite fragmented. A report by Automation World found that less than eight percent of companies surveyed had combined the two departments, while twenty-four percent saw almost no interaction between them.8

Sometimes OT security is managed by the engineering technology group, in other cases by a plant manager. Sometimes, an IT team member has moved across to OT to handle it, other times, there is little to no interaction between IT and OT.

Yet collaboration between IT and OT is critical to reducing the blind spots and security risks surrounding highly connected industrial control systems. As “smart” factories leverage more IIoT technology, and OT networks become more connected to business networks and the cloud, the IT/OT divide puts business at risk.
Nozomi Networks Solution: Easy IT/OT Integration
Built-in support for many asset and identity management systems, firewalls, SIEMs and more makes it easy to integrate and share ICS information (like that shown in the left screen shot) across IT/OT environments (right screen shot).

The Challenge

• Leveraging IT expertise with OT production know-how to improve resiliency

The Solution: Aligning IT and OT With a Single Solution

• The Nozomi Networks no-risk solution provides IT and OT with deep visibility into ICS assets and continuous monitoring for risks that could impact reliability or cyber security. It provides a common platform to drive IT/OT convergence.

• Manufacturers can easily integrate real-time OT monitoring into overall security infrastructure for improved operational resiliency and reliability.

Results

• Reduction of OT security blind spots

• Continuous monitoring for better oversight of threats, violations and risks

• Faster troubleshooting

• OT threat monitoring that is fully integrated into the overall security mandate
II. Use Case: Applying Cyber Security Best Practices

Operational risk comes from multiple sources including people, processes and technology. According to the Verizon 2019 Data Breach Investigations Report, intentional attacks on manufacturing by outsiders accounted for 70% of all breaches reported.²

But while malware and other high profile cyberattacks get a lot attention, the SANS Institute reports that 28% of ICS professionals rank insider (and often accidental) incidents as a top threat vector. The organization’s recently released OT/ICS Cybersecurity Survey found that 62% of respondents rated “people” as the riskiest pillar for compromise, well behind technology and processes.³

Examples of human-generated operational risk include device configuration errors, open ports, the use of weak passwords, and forgetting to remove a contractor’s access after they’ve left the organization.

Given the significant risk to operations, it’s not surprising that OT leaders want to up their security game. But how do you implement a cyber security framework, and take cyber resiliency to the next level?
The Challenge
• Building organization-wide security maturity

The Solution: Pairing a Trusted Security Framework with Advanced Monitoring and Risk Identification
• The Nozomi Networks solution makes it easy to understand and adopt cyber security best practices, such as those outlined by the NIST Cybersecurity Framework Manufacturing Profile, IEC 62443 and ISO 27000.

For example, NIST outlines five security framework functions – identify, protect, detect, respond and recover, that should be incorporated into your operational processes to address cyber risk. Identification includes asset management and risk assessment, while detection includes continuous monitoring and insight into anomalies and events, among other functions.

• With the adoption of an OT visibility solution, manufacturers can automate the creation of an asset inventory, and continuously monitor their network and ICS. They can also rapidly identify vulnerabilities and proactively identify threats to the security of their industrial control systems.

Nozomi Networks Solution: Automated Asset Inventory Provides Essential ICS Information
The Nozomi Networks solution makes it easy for manufacturers to understand and adopt cyber security best practices, such as those outlined in the functions and categories of the NIST Cybersecurity Framework for Manufacturing.¹⁰

Results
• Adoption of cyber security frameworks and best practices
• Proactive identification and mitigation of operational risks
• Improved operational resiliency
CONCLUSION

Operational Visibility and Cyber Security Boost Manufacturing Resiliency

Manufacturers are embracing digital transformation to find efficiencies and grow revenue. In doing so, they’ll inevitably need to address common operational challenges – such as gaining visibility into their ICS networks and closing security gaps.

Without ICS visibility, it’s difficult to stay on top of what’s happening on the network. One small change or networking issue can impact product quality, production uptime, plant safety, and revenue. While a fast response to anomalies is critical, spotting issues requires real-time visibility into plant assets, connections, communications and more. Unfortunately, these are capabilities that many manufacturers lack.

Security gaps related to people, processes and technology can have a big impact on operational resiliency too. For example, the separation of IT and OT, combined with increasingly connected industrial control systems, can lead to cyber security blind spots. But with the right technology and a focus on best practices, manufacturers can improve their operational resiliency.

In fact, with the Nozomi Networks solution, visibility and cyber security are easy to achieve. It delivers improved ICS visibility by automatically creating an up-to-date inventory of all assets on the network. It then monitors their behavior for anomalies and alerts operators to changes that could indicate potential problems. The solution also provides advanced vulnerability and threat detection, along with detailed insights that lead to faster prioritization and remediation.

Tailored to meet the unique challenges of manufacturing, the Nozomi Networks solution helps operators gain deeper operational visibility, apply security best practices and align IT and OT.

FIND OUT MORE

Manufacturers can benefit greatly from investing in a network visibility, monitoring and security solution. Find out for yourself how quickly the Nozomi Networks solution boosts resiliency for industrial facilities.
What to Look for in a Real-time ICS Visibility and Cyber Security Solution

While increasing cyber threats dominate the news, there is good reason to be optimistic.

The Nozomi Networks Solution, for example, is easy and safe to deploy. It dramatically improves OT visibility and cyber security, and integrates seamlessly with IT infrastructure.

When choosing a cyber security solution and vendor for your organization, make sure they have the advantages shown here.

- Accurate OT Operational Visibility
- Advanced ICS Threat Detection
- Proven, Large-scale Global Installations
- Swift Deployment Across Many Sites
- Easy IT/OT Integration
- Global Partner Ecosystem
- Passion for Customer Success

See the Nozomi Networks Solution in Action

If you would like to see our solution in action, and experience how easy it is to work with Nozomi Networks, please contact us at nozominetworks.com/contact

Additional Resources

SOLUTION BRIEF
Real-time Cyber Security for Industrial Control Networks
DOWNLOAD

WEBPAGE
Solution: Manufacturing
VISIT

EXECUTIVE BRIEF
Integrating OT into IT/OT SOCs
DOWNLOAD

EXECUTIVE BRIEF
The Cost of OT Cyber Security Incidents and How to Reduce Risk
DOWNLOAD
References

7. Norsk Hydro First Quarter 2019 Report

About Nozomi Networks

Nozomi Networks is accelerating the pace of digital transformation by pioneering innovation for industrial cyber security and operational control. Leading the industry, we make it possible to tackle escalating cyber risks to operational networks. In a single solution, Nozomi Networks delivers OT visibility, threat detection and insight to thousands of the largest critical infrastructure, energy, manufacturing, mining, transportation and other industrial sites around the world.
For detailed information about our products, visit

www.nozominetworks.com

#thosewhoknowpicknozomi