Whitepaper

# DEFENDING THE INDUSTRIAL ETHERNET

## How to Secure Your ICS Environment

GARLAND TECHNOLOGY

See every bit, byte, and packet®

# **Industrial Ethernet** | Table of Contents

# Introduction

The Industrial network has evolved rapidly over the past 30 years. Industrial Ethernet has overtaken traditional fieldbus technology in new node installations, while Industry 4.0, Industrial Internet of Things (IIoT), Industrial control system (ICS), virtualization and advancements in software-defined networks (SDNs), hybrid clouds, and artificial intelligence (AI) are all having a major impact on industrial network development.

While data center virtualization may be coming into the mainstream, the Industry 4.0 movement is still both new and unfamiliar to many. The adoption of Ethernet in Industrial control system (ICS) applications has been imperative for this evolution, as many companies look to future-proof their systems, with an eye towards Industry 4.0 and the Industrial Internet of Things (IIoT), while maintaining today's demands.

Unlike in IT settings, OT leaders can't afford even minor data inconsistencies or downtime. With protocols like PROFINET, EtherNet/IP, and EtherCAT, you can ensure messages sent from IIoT end-devices across the network are transmitted with 100% reliability. Without these protocols, you would need multiple translation solutions and communication switches throughout the industrial infrastructure to make peer-to-peer connection possible.

But thanks to standardized Ethernet protocols, you can lay the groundwork for successful IIoT projects utilizing the benefit of Industrial Ethernet, like increased speeds, up from 9.6 kbit/s with RS-232 to 1 and 10 Gbit/s, as well as the option to use optical fiber for increased distance and the ability to incorporate standard networking appliances.

# Defending The Industrial Ethernet

Fieldbus, serial bus and legacy equipment have long been the bedrock of industrial infrastructure. Legacy equipment has persisted for decades because of its superior abilities to maintain the safety and security of critical infrastructure. But increasing demands to bridge IT capabilities and OT processes cause problems with maintaining them.

Ethernet isn't new technology. Networks of all sizes have made the move to Ethernet connections to keep up with variable Internet traffic demands. Factory settings and production cells, on the other hand, have lagged behind Ethernet innovation due to different circumstances in industrial environments.

Many industrial networks are still running at either 10M or 100M with 100BaseFX or 100BaseTX cabling and are known to run older operating systems such as Windows 95 and Windows XP due to security concerns—even after the operating systems are no longer supported. Because the static production traffic is heavily regulated, any changes to the machine environment requires total recertification and calibration of the industrial operation, which is both time consuming and costly.

Despite these challenges, the industrial sector can no longer overlook the benefits of Ethernet connectivity. Ethernet's simple and effective design combined with the relatively low cost of Ethernet hardware, have made it an attractive network design in industrial networks. Manufacturers and managers of critical infrastructure such as energy, communication and healthcare are just now making the shift to Ethernet protocols with rugged connectors and modifications—spurring the rise of Industrial Ethernet innovation.

The Industrial Ethernet will undoubtedly bring benefits to manufacturing automation and critical infrastructures—but only if it is deployed and maintained correctly. Securing the Industrial Ethernet will be a major hurdle for the industrial sector as manufacturers move from their proprietary serial port-to-port infrastructures to Ethernet protocols.

# Architecting Visibility for Industrial Control System (ICS) Environments

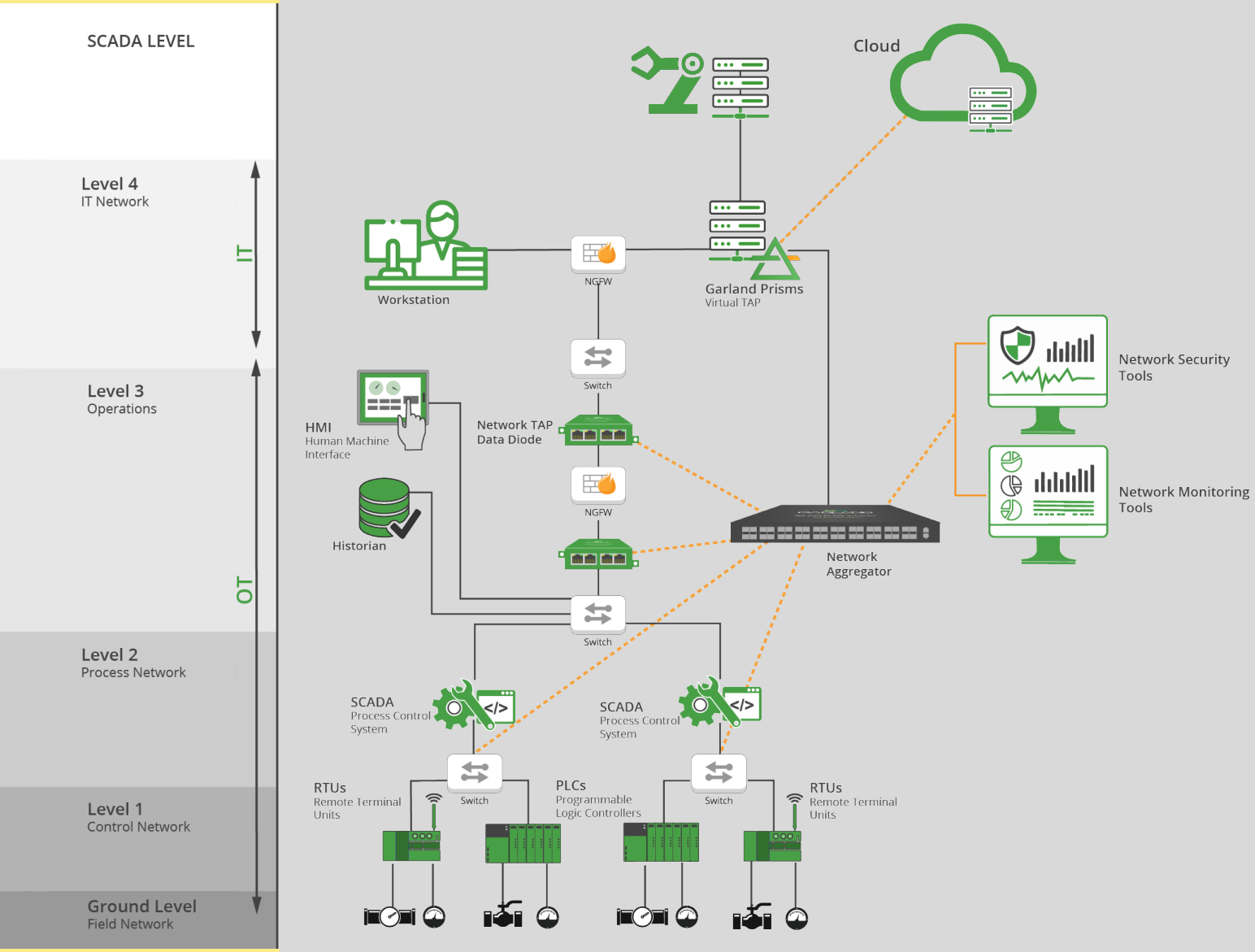
Industrial control system (ICS) infrastructure and the convergence of Operational Technology (OT) with Information Technology (IT), have exposed many challenges for the industry, including increased vulnerability to cyber attacks and network blindspots. Many companies do not have the visibility into their OT systems, like they may with their IT infrastructure.

Industrial control system (ICS) describes the critical infrastructure network connectivity of hardware and software integration in industrial environments. ICS includes supervisory control and data acquisition (SCADA) and distributed control systems (DCS), industrial automation and control systems (IACS), programmable logic controllers (PLCs), programmable automation controllers (PACs), remote terminal units (RTUs), control servers, intelligent electronic devices (IEDs) and sensors. Local operations are often controlled by Field Devices that receive supervisory commands from remote stations. ICS systems are extensively used in industries such as chemical processing, manufacturing, power generation, oil and gas processing, and telecommunications.

In these ICS environments, the availability of data within industrial automation is critical. Optimized security and performance starts with 100% visibility into network traffic including both virtual and physical environments. And visibility starts with the packet. A network visibility fabric that includes network TAPs and packet brokers, providing complete network visibility and link optimization, can reduce network complexity, enable easier infrastructure upgrades, help meet specific regulations, facilitate traffic growth and improve the effectiveness of tool and network performance.

# ICS Visibility Architecture

Most industrial security and network monitoring tools are packet based. Getting access to network traffic in the form of packets is critical. There are some inherent challenges within this infrastructure though. SPAN ports are available on OT switches but are prone to drop packets, duplications, or may already be in use. Even some older legacy switches, may not even have SPAN port options.




This diagram illustrates how a visibility fabric of network TAPs and SPAN traffic delivering full visibility for layers 2-4, aggregated with network packet brokers, filtering and sharing the traffic with the security and network monitoring tools, may be integrated within an ICS system.

# Network visibility provides many benefits for your industrial infrastructure:

- **Improved Network Security**: Advanced attackers thrive on network blind spots. They create threat vectors capable of slipping through your defenses by blending in with your normal traffic. When you can't see every bit, byte, and packet, you risk missing malicious activity. Maximizing network visibility ensures your security tools see all the data necessary to alert you about potential threats.

- **More Efficient Performance**: Even minor delays in application performance can significantly impact employee productivity and your bottom line. Your ability to prevent these delays hinges on proactively addressing performance anomalies. Without proper network visibility, you may not see an issue until it's already impacted the workforce. Proper network visibility increases the efficiency of your monitoring tools so you can be more proactive in network management.

- **Increase Tool Utilization**: Network visibility includes your ability to load balance traffic effectively. This means making filtering traffic based on the data that security and monitoring tools truly need. When you have total visibility, you can ensure no bandwidth is wasted and that your security and monitoring tools are fully utilized.

- **Minimize Mean Time to Resolution**: Knowing there's a network issue to troubleshoot is only half the battle. Minimizing the mean time to resolution is critical to business performance. When you have network visibility into 100% of data packets, you can take advantage of log data to quickly identify root causes of issues and troubleshoot efficiently.

Architecting network monitoring and security, while managing the performance of ICS applications is much the same with a traditional network visibility fabric. Tapping points of interest throughout the assembly line application and factory network, enhances monitoring and diagnostic capabilities. This foundation requires some thoughtful consideration on connectivity, environment and security.

# Connectivity

## Laying the Industrial Ethernet Framework

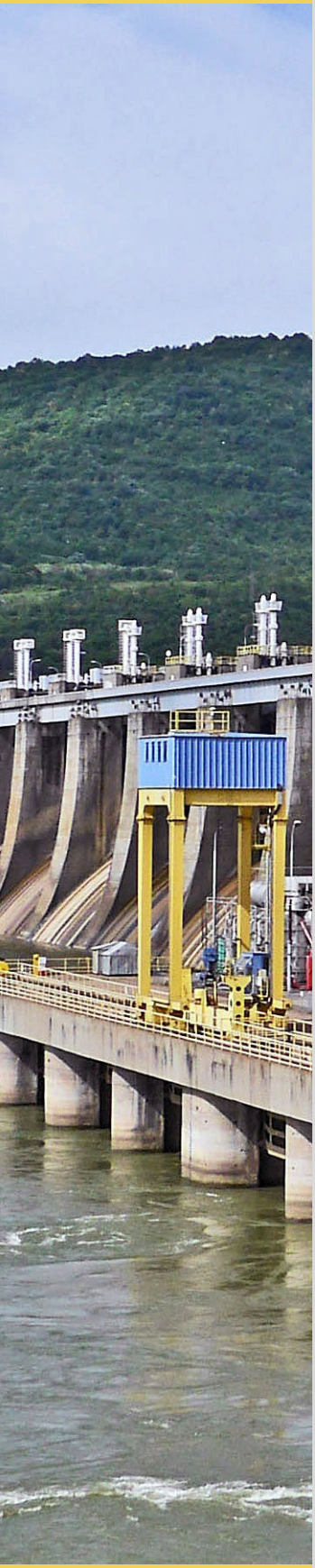
Securing the Industrial Ethernet begins with the right procurement and deployment processes. Putting the right framework in place beforehand can help mitigate cyber attacks in the future. In terms of basic equipment, deploying Industrial Ethernet requires the right cables and connectors.

It's easy to get ahead of ourselves when we talk about the Industrial Ethernet. You look at the ever-growing reality of the Industrial Internet of Things and the longstanding concerns for security in these networks and you start to take this level of connectivity for granted.

As you upgrade your network, choosing the right framework will be critical to ensure you don't disrupt traffic in the process. Choosing cables, connectors and mounting for standard settings can be hard enough—but when you're upgrading to Ethernet in an industrial setting, keep these 7 points in mind:

### 1) What are your data rate demands?

When making the switch to Ethernet protocols, industrial companies must adhere to IEEE 802.3 standards. The biggest contention companies must deal with is restrictions on cabling lengths. While copper and fiber are both supported, copper device-to-device connections cannot exceed 100 meters. Fiber connections are much more accommodating with a 2,000-meter limit—but fiber isn't always an option depending on the environment. Keep these restrictions in mind when sitting down to design a new Industrial Ethernet deployment.



**Determine Application Data Rate**: Your networking needs could be 100M Ethernet all the way through 1G, 10G and beyond. This is the point where you weigh your fiber/copper options and consider various cable categories (Cat 5e for 100M or 1G, up to Cat 7 for 10G). One best practice is to avoid mixing and matching cable types—choose the right cable for the environment and deploy it as universally as possible.

**2-Pair vs. 4-Pair Cables**: If only common 10/100BaseT applications are required, 2-pair cables are acceptable. However, when industrial environments are moving up to gigabit, 10G and beyond, 4-pair cabling is far more efficient. Four-pair cabling also supports more powerful "Power over Ethernet (PoE)" functionality.

## 2) How harsh is your environment?

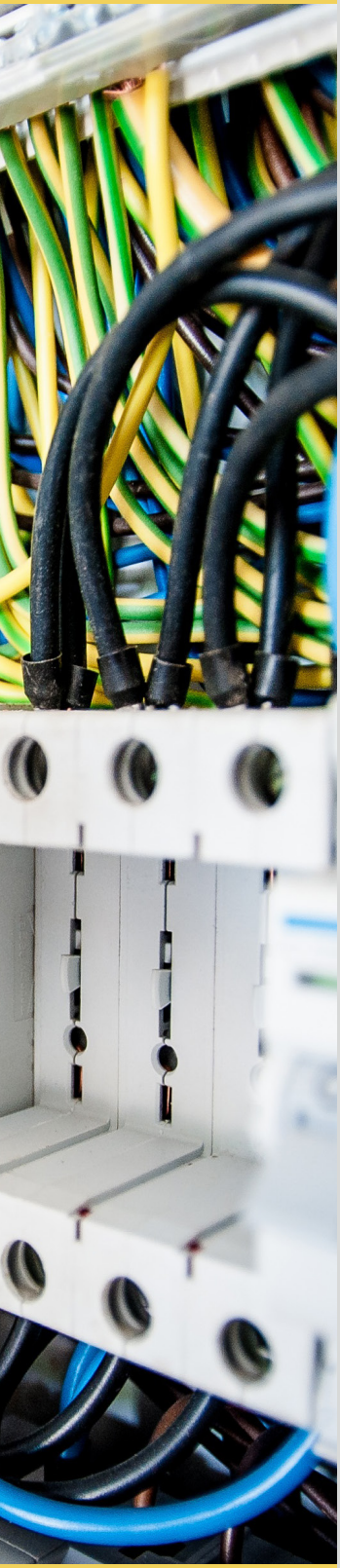
In a standard IT network, you can choose cables based on business application needs. But when you're talking about a factory floor's OT network, the environment is everything.

Many of your considerations come down to the ruggedness of specific cable choices. Regardless of the cables you assess for your environment, you need to understand performance in all of the following categories:

- Abrasion
- Cold blend
- Cold impact
- Crushing
- Cut through
- High temperatures
- Oil resistance
- UV exposure
- Water immersion

Consider the level of vibration that cables will have to withstand. Will you keep cables protected in a specific control room? In this case you might not need to find such a flexible cable because vibration will be minimized.

However, if your cables are exposed to oil, moderate vibration, chemicals and more on the factory floor, you'll need a more durable option. And at the extreme end, any cables that exist on your machines will need the highest levels of flexibility due to increased corrosion and vibration.



## 3) The Right Jacket

After considering your environment, you'll want to make a decision on the right jacket protection for the cables in your network. There are 4 main options to consider:

- PVC: The jack-of-all-trades jacket works well for most situations at an affordable price.
- Flame Retardant Non-Corrosive (FRNC): If fire is a key concern for your environment, paying a bit more for this jacket could be your best bet.
- Thermoplastic Elastomer (TPE): This combination of plastic and rubber offers the best performance in cooling situations and also offers excellent flexibility. However, the higher performance comes at a higher price than FRNC or PVC.
- Polyurethane (PUR): Extreme durability for high-abrasion situations or environments where cables are exposed to chemicals, oils and other solvents.

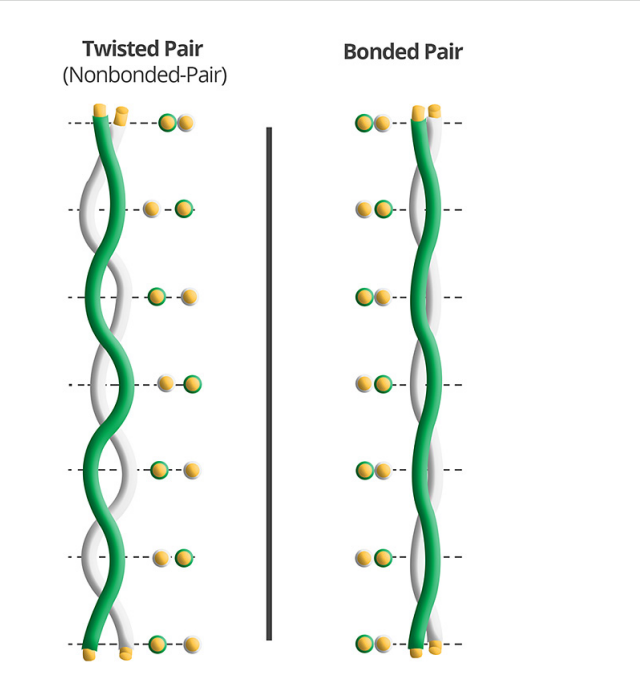
## 4) To Shield Or Not To Shield

Many environments are safe to use unshielded twisted cables, but some industrial deployments require more protection. If cables are exposed to noise from valves or other machining elements, shielded cables could be necessary.


## 5) Twisting vs. Bonding Through Vibration

When you don't have to worry about vibration in your environment, solid conductors will work just fine. However, you face a choice between twisted or bonded-pair options when vibration challenges call for stranded conductors.

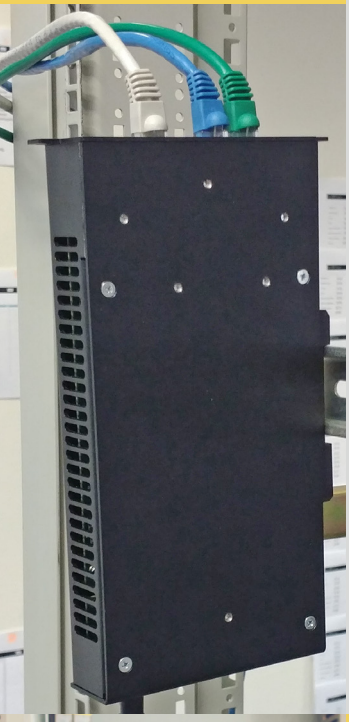
Twisted conductors might save you some money, but they are susceptible to damage during implementation and can cause greater challenges with network mismatching. Bonded-pair conductors are more suited for rigorous manufacturing environments.




## 6) Industrial Ethernet Connectors

Industrial Ethernet designers must select the proper connectors for their specific environment. Contaminants and disruptions are common in industrial networks, but the correct connector can safeguard cables from potential problems. While sealed connectors keep cables safe from dust and chemicals, screw-type connectors provide better protection against vibration. The Industrial Ethernet connector decision often comes down to two options - RJ45 and M12.

- **RJ45 Connectors**: These connectors are often found in standard office environments, but variations exist for Industrial Ethernet. The locking mechanism and 8-pin component layout supports Cat5 and Cat6 cabling. However, these large connectors can often cause design issues.
- **M12 Connectors**: As network architects trend toward more compact designs, M12 connectors find their niche. M12 connectors are smaller than RJ45, but offer a similar level of robust protection from harsh conditions.



## 7) DIN Rails - Mounting in an Industrial Environment

Instead of the standard 19-inch racks engineers may see in a data center environment, many industrial networks use industrial control panels with DIN Rails mounts. DIN Rails are a mounting system used to secure or install electrical devices to the network. The goal in this environment is to have as few moving parts as possible to minimize the risk of a cable coming unplugged or disrupting the network.

In order to secure electrical components such as routers, switches, firewalls and monitoring appliances to a din rail, the component itself has to have a DIN rail mount.

# Overcoming Connectivity Challenges in Industrial Ethernet

With so many connectivity options, regulations and operating systems, as well as combining legacy equipment with security and performance monitoring tools, many engineers run into challenges. How do you connect various connector or media types? What do you do if your network analyzer runs copper gigabit, and you need to connect a 100Base-FX link? There is no 100Base-FX NIC card for your security or performance monitoring device.

When architecting your visibility fabric, specialized network TAPs, like those offered by Garland Technology provide media conversion to solve those issues while providing full-duplex copies of the traffic through 100BASE-FX/LX, LC, ST fiber connections.

Garland Technology also has an assortment of industrial based TAP accessories, including DIN rail mounts for network TAPs, DC-DC power converters and screw power lock connectors provide extra assurance power supplies that stay connected to help overcome the connectivity and environmental challenges you may face.

When the Industrial Ethernet framework is in place, companies must prepare the network for the litany of security challenges that accompany the shift from serial to Ethernet. If the right security measures are taken, cyber attack concerns don't have to be so daunting.

# Securing the Industrial Ethernet

Cyber attacks against critical infrastructure are at a much higher stake than typical IT networks. This is why operational technology teams are so cautious with technology. But you can't run closed networks on legacy operating systems forever.

Critical infrastructure security is of the utmost importance, and with high profile attacks up in recent years, The World Economic Forum is sounding the alarm. Their Global Risks Report 2020 highlights, "Cyberattacks on critical infrastructure—rated the fifth top risk in 2020 by our expert network—have become the new normal across sectors such as energy, healthcare, and transportation.[1]"

With an estimated 21 billion IoT devices worldwide, which will double by 2025, The Global Risks Report acknowledges, "Attacks on IoT devices increased by more than 300% in the first half of 2019, while in September 2019, IoTs were used to take down Wikipedia through classic distributed denial of service (DDoS) attacks, and the risk of IoT devices being used as intermediaries is expected to increase. In 2021, cybercrime damages might reach US$6 trillion— what would be equivalent to the GDP of the world's third largest economy.[2]"

# The Need for Better Security Assessments

One of the most concerning statistics in a recent SANS State of ICS Security Survey[3] is the majority of respondents who believe 75% of their network connections are undocumented. As IT and OT converge, lacking network awareness will only increase the vulnerabilities of Incident Command Systems ( ICS) to dangerous cyber attacks.

To help improve the state of awareness, there is a suggested six-fold approach to security assessments for critical infrastructure companies:

- **Asset Inventory**: Discover any undocumented devices
- **Network Traffic Baselining**: The closed loop of ICS traffic means having a baseline for your traffic makes it easier to identify malicious anomalies
- **Security Breach Detection**: Attackers can persist in networks for weeks, months or even years—regular security assessments can help you recognize a breach
- **Vulnerability Identification**: Stay up to date on the latest security threats so you can find where your own vulnerabilities lie
- **Confirmation of Remediation**: You should document each vulnerability you've addressed and how you hardened your ICS
- **Security Posture Insight**: Proper documentation allows analysis that gives executives the necessary metrics to approve resource allocation

All of these steps can help ICS security professionals get on the right path to improved critical infrastructure security. However, defending the Industrial Ethernet will require more than just security assessments.

Implementing a foundation of visibility accelerates security incident detection with improved uptime and service performance, reducing security incidents and breaches.

# Six Tips For Better Industrial Security

In many cases, securing the Industrial Ethernet doesn't look so different from securing the standard network. However, this is a new world for the industrial sector and all potential problems must be covered by comprehensive security preparation. Here are a few standard industrial security practices to consider.

## 1 Securing the Physical Network

Traffic in industrial environments cannot be tampered with. Network architects cannot take any chances when it comes to unauthorized access and must implement port security to prevent traffic manipulation. Another precaution to take is to disable unused ports, eliminating the chance for unauthorized users to manipulate traffic.

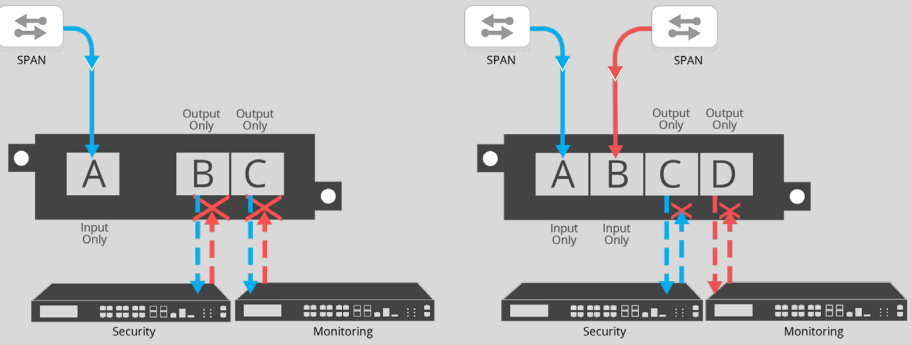
Port-based MAC address management can help prevent unauthorized access. Access control lists can be created by system administrators, allowing only configured MAC hardware addresses to connect to the network. These lists should be kept short and limited only to those who must connect their workstations for business critical applications.

# 2 Unidirectional Gateways

For specific industries, new regulations enforce physical unidirectionality coupled with software that replicates databases and emulates protocol servers to handle bi-directional communication and contains a broad range of cybersecurity features like, secure boot, certificate management, data integrity, forward error correction (FEC), and secure communication via TLS.

According to ANSSI's Cybersecurity for Industrial Control Systems on Management Information Systems, "The interconnection shall be unidirectional towards the corporate network. The unidirectionality shall be guaranteed physically (e.g. with a data diode). Certified devices should be used for the interconnection.[4]"

In these network deployments, using SPAN simply is not acceptable. SPAN or port mirroring from a network switch are bi-directional, which creates an opportunity for hacking by deploying a device for monitoring or security. A Data Diode offers a unidirectional connection, providing the security needed.




These diagrams show a single and dual option for providing a data diode solution for undirectional gateways.

Data diodes are a network appliance or device, similar to a network TAP, that allows raw data to travel only in one direction, used in guaranteeing information security or protection of critical digital systems, such as industrial control systems, from inbound cyber attacks. Garland Technology's Data Diode TAPs offer "no injection" tap aggregation for 10/100/1000M copper networks. These will help you create unidirectional monitoring solutions that capture every bit, byte, and packet and ensure copied packets don't go back in and disrupt the industrial network—all in a package that's purpose-built and unhackable.

## 3 Passive, Listen-Only TAP Brings Legacy into Industrial Ethernet

Legacy equipment wasn't designed to communicate beyond its isolated system. When you start to push legacy equipment to transfer data outside of these proprietary systems, you open the industrial network to security vulnerabilities.

The need for passive, real-time monitoring is stronger than ever in an Industrial Ethernet environment saddled with legacy equipment. Passive network TAPs are an essential connectivity solution in Industrial Ethernet settings, and are available in passive fiber and passive 10/100M copper. Security and monitoring appliances must receive 100% of the traffic without introducing new or manipulated traffic to the stream.

## 4 Airgapping the Network

Air-gapping physically isolates devices and applications from outside networks and the internet, to ensure attackers cannot penetrate or compromise key components of your IT/OT infrastructure. With performance demands and the rise of innovative Industry 4.0 use cases for IoT devices, artificial intelligence, and virtualization, adding an air-gapped solution becomes critical and equally challenging. Garland Prisms provides air-gapped traffic mirroring and TLS decryption in cloud environments, enabling your virtualization migration.

## 5 Standard Security Measures Still Apply

Defending the Industrial Ethernet still requires the standard security appliances that exist in typical data center and IT settings.

Out-of-band security analysis tools like intrusion detection and network detection and response are all necessary when Ethernet is introduced to the industrial sector. Packets are delivered to out-of-band solutions by either Network TAPs or SPAN, which can then be coupled with Network packet brokers (NPBs) to aggregate and groom packet data for out-of-band solutions.

Inline security appliances—next-gen firewalls, intrusion prevention systems, and data leakage protection can also be utilized in industrial IT infrastructure. With inline appliances placed within the inbound and outbound traffic, ensuring that a failure does not cause downtime is critical. While some security appliances may have internal bypass functionality, the reliability and performance of an external bypass device are considered best practice, making bypass TAPs essential to inline security.

A main difference between these appliances in an industrial setting and in a typical environment is that production traffic is standardized. While data centers deal with variable traffic demands from external users, production traffic is set to run through the same exact loops repeatedly. Any variations in these traffic patterns introduced by security appliances can wreak havoc on the network and cause major security holes.

## 6 Visibility is Essential for Securing the Industrial Ethernet

The last and arguably most important tip for securing your Industrial environment is network visibility. Putting expensive security and monitoring appliances in place and investing millions in employee training won't help defend the Industrial Ethernet if the network isn't designed with visibility in mind. When critical infrastructures are involved, companies can't afford blindspots, drop packets, traffic bottlenecks or suffer network downtime. Deploying network TAPs throughout the Industrial Ethernet framework ensures uptime and eliminates the packet delivery issues that SPAN/Mirror ports inevitably introduce.

According to SANS 2019 State of OT/ICS Cybersecurity Survey "Visibility is critical for managing OT/ICS systems. According to survey respondents, increased visibility into control system cyber assets and configurations is the top initiative organizations are budgeting for in the next 18 months.[5] "

Garland Technology has developed a line of network TAP specifically designed for Industrial Ethernet connectivity, as we know defending the Industrial Ethernet requires 100% traffic visibility without manipulating or introducing new packets.

# Setting Yourself Up for Industrial Network Visibility Success

If you want to learn more about bridging the gap between your legacy equipment and the shift to Industrial Ethernet and IIoT, we'd love to help. Contact us today for more information about the importance of visibility for your industrial ethernet.

Book a free Design-IT consultation and one of our engineers will work directly with you on designing your network connectivity strategy. No obligation.

Garland Technology is an industry leader delivering network products and solutions for enterprise, service providers, and government agencies worldwide. Since 2011, Garland Technology has developed the industry's most reliable test access points (TAPs), network packet brokers (NPB), and cloud visibility solutions, enabling data centers to address IT challenges and gain complete network visibility. For help identifying the right visibility solution for projects large and small, visit GarlandTechnology.com or @GarlandTech.

## Contact

sales@garlandtechnology.com

GARLAND TECHNOLOGY
See every bit, byte, and packet®


**1/2-The World Economic Forum - The Global Risks Report 2020**
http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
**3-SANS State of ICS Security Survey**
https://www.sans.org/reading-room/whitepapers/analyst/membership/37067
**4-ANSSI - Cybersecurity for Industrial Control Systems**
https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf
**5-SANS 2019 State of OT/ICS Cybersecurity Survey**
https://www.sans.org/reading-room/whitepapers/analyst/2019-state-ot-ics-cybersecurity-survey-38995