This report explores how industrial networks defend against cyber threats, using the Purdue and Zero Trust models as a framework. It combines theoretical understanding with practical insights gained during my internship at Pringles, where I worked on ICS traffic diagnostics. The goal is to highlight both the challenges and evolving strategies shaping industrial cybersecurity.

Introduction

In today's world, industrial facilities are no longer isolated islands of machinery. Modern factories rely on complex networks of controllers, sensors, and software to keep production running smoothly. This interconnectedness brings unprecedented efficiency and visibility—but it also opens the door to new risks.

Industrial Control Systems (ICS) are the backbone of these operations. They include PLCs, HMIs, SCADA systems, and field devices that control everything from conveyor belts to chemical reactors. When these systems are disrupted—whether by accident or cyberattack—the consequences can be severe: production losses, equipment damage, safety incidents, or even environmental harm.

Cybersecurity in ICS is not just an IT problem; it is a matter of safety, reliability, and business continuity. Unlike corporate IT networks, industrial environments have unique challenges: legacy devices with no built-in security, networks designed for uptime rather than protection, and the growing integration of IT and OT systems. These factors make ICS environments both critical and vulnerable.

During my internship in a real factory environment, I experienced firsthand how these systems are structured, where vulnerabilities emerge, and what measures are in place to protect them. This report reflects what I learned:

- how factories structure their networks to stay secure,
- what lessons can be drawn from past ICS cyberattacks,
- which defense strategies and standards are most effective, and
- how the industry is adapting to new threats.

Using the well-known **Purdue Model** as a guide, I aim to bridge theory with practice and better understand how industrial networks defend against hostile digital landscape.

The Purdue Model and Zero Trust

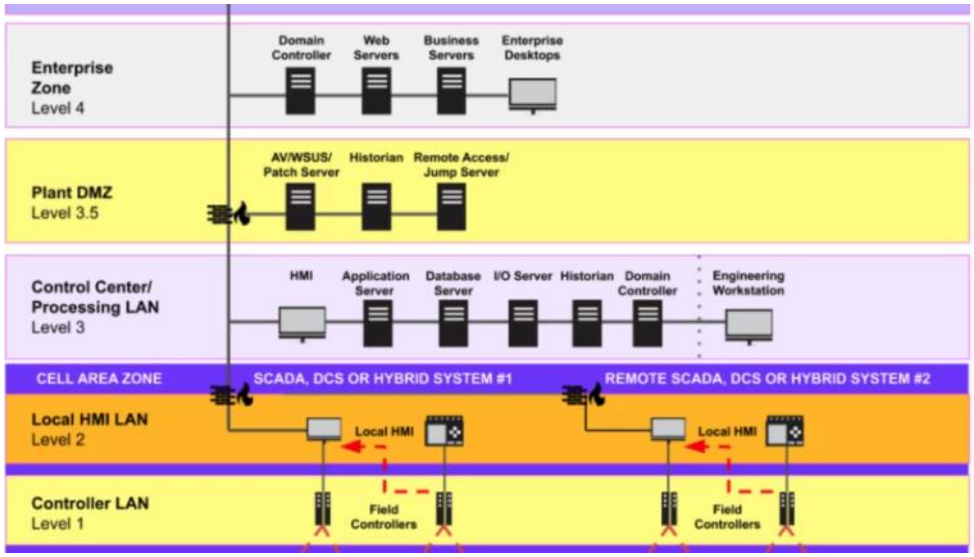
The **Purdue Model** is the traditional framework for securing industrial networks. It separates **Operational Technology (OT)**—the systems controlling physical processes—

from **Information Technology (IT)**—the systems managing data and business operations.

- **Levels 1–3** cover OT: field I/O devices, local controllers, HMIs, and PLCs.
- **Levels 4–5** cover IT: corporate servers, business applications, and external connectivity.

The key principle is segmentation: only controlled, authenticated pathways connect these layers, reducing the chance of threats spreading from IT to OT.

Today, many organizations are going beyond Purdue by adopting the **Zero Trust Model**. This approach assumes no part of the network is inherently safe. Instead of a single barrier between IT and OT, every system—even individual production lines or machines—requires its own authentication. For example, in a factory with six production lines, access to each line would require separate credentials, limiting the impact of a potential breach.



OT vs IT Security: Why They Differ

While IT security focuses on protecting data, OT security safeguards physical processes and the devices that control them. This difference shapes everything:

- **IT systems** manage and process information, so breaches often result in data theft or service disruption.
- **OT systems** control industrial processes; attacks can disable safety mechanisms, halt production, or even cause physical harm.

OT hardware was never designed to be connected to external networks, and many devices still run decades-old operating systems. Security features have only recently

begun to appear in new industrial products. Because industrial equipment often stays in service for 20–30 years, **network segmentation remains the most reliable protective measure**.

In short: while IT breaches can cost money and reputation, OT breaches can cost lives.

Historical Attacks and Weak Points

High-profile cyberattacks have demonstrated the risks of insecure industrial networks. Incidents like **NotPetya** showed how ransomware targeting IT can spill into OT, causing billions in damages. Globally, OT-specific cyber incidents have cost corporations an estimated **$7 billion**.

Common vulnerabilities exploited in these attacks include:

- **Hardcoded passwords** in PLCs and HMIs
- **Flat network architectures** without segmentation
- **Outdated operating systems** (e.g., Windows 98) with unpatched zero-day exploits

These weaknesses highlight why a layered defense is essential.

Defense Strategies for ICS

Protecting ICS requires a combination of technical measures, policies, and standards. Key strategies include:

- **Network Segmentation** – Isolating IT from OT, and applying Zero Trust principles for internal divisions.
- **Patch Management and Asset Inventory** – Keeping systems updated, even when downtime is inconvenient, and knowing exactly what devices are on the network.
- **Anomaly Detection** – Monitoring ICS traffic to detect suspicious activity. During my internship, I contributed to this effort by building an **IP diagnostics tool** to help visualize network traffic and identify irregularities.
- **Adherence to Standards** – Following frameworks such as **IEC 62443** and **NIST SP 800-82**, which provide best practices for securing industrial networks.

When these strategies are combined, they greatly reduce the attack surface of an industrial facility.

The Future of IIoT Cybersecurity

The industrial world is rapidly embracing the **Industrial Internet of Things (IIoT)**, connecting more devices than ever before. This convergence of IT and OT boosts efficiency and lowers costs—but it also increases exposure to cyber threats.

As manufacturers adopt more secure protocols and hardware, they must also ensure that older devices and legacy systems remain protected. The industry's challenge will be to maintain the high reliability expected of OT while integrating the connectivity demanded by modern operations.

Looking ahead, cybersecurity will not be a one-time effort but a continuous process of **monitoring, updating, and adapting**. The lessons from past incidents, combined with evolving standards and technologies, will guide factories toward safer, more resilient networks.

Conclusion

Industrial cybersecurity is no longer a theoretical concern—it is a frontline issue that directly affects safety, productivity, and even the environment. Through my time working in a real factory setting, I witnessed how complex and interconnected these systems have become, and how even small oversights can create significant vulnerabilities.

What stood out most is that **effective defense is not about one tool or one policy—it's about layers of protection**: segmentation, constant monitoring, strict access control, and adherence to standards. The Purdue Model and Zero Trust approach remain critical because they translate these principles into practical network design.

As IT and OT continue to converge, the challenges will only grow. Legacy devices, evolving threats, and the pressure to stay online will keep this field dynamic for years to come. But with the right mindset—balancing innovation with security—factories can remain both efficient and resilient.

For me, this project was not just about learning theory; it was about understanding how cybersecurity decisions are made under real-world constraints. It reinforced the idea that **cybersecurity in industrial environments is as much about people and processes as it is about technology**.

I look forward to building on these insights and contributing to a future where industrial networks are not only smarter—but also safer.

Key Takeaways

- **ICS cybersecurity is about safety, not just data.** Attacks on OT systems can have physical consequences far beyond financial losses.

- **Segmentation is still king.** The Purdue Model and Zero Trust remain foundational defenses, even as technology evolves.
- **Legacy systems are the weakest link.** Outdated devices without built-in security require additional layers of protection.
- **Standards matter.** Following IEC 62443 and NIST SP 800-82 significantly reduces risk.
- **Continuous vigilance is essential.** Cybersecurity in industrial environments is not a one-off task but an ongoing process of monitoring, patching, and adapting.

This report was created during my internship at Pringles where I worked on ICS traffic monitoring and diagnostics. My goal is to continue exploring cybersecurity for industrial environments and contribute to safer, more resilient systems.

https://claroty.com/blog/it-and-ot-cybersecurity-key-differences

https://claroty.com/blog/ics-security-the-purdue-model