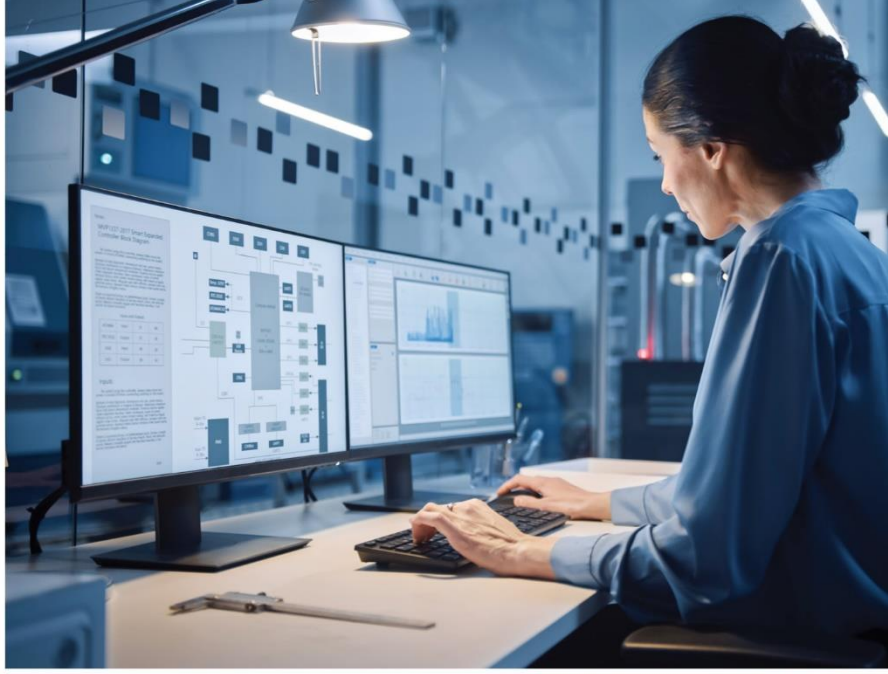

Top 25 Vulnerabilities of Industrial Automation and Control Systems

antaira®

making connectivity simple...

Industrial control systems (ICS) have been of incredible value to industrial industries. The ability to control the production and manufacturing process of goods and services has been a major milestone in our modernized world. However, everything comes with risks. Malicious actors, attackers, and hackers all are terms used to describe the individuals who try to intentionally cause harm through both virtual and physical means to systems responsible for our modern life styles. These attacks can cause serious harm or even death to individuals or even whole communities by destroying water purification systems, disabling power plants, prolonging critical system outages, on top of bad press, and even government fines.

Antaira Technologies provides industrial networking solutions with advanced security feature sets to protect critical systems against would-be actors or malicious activity. Our portfolio of industrial Ethernet switches, media converters, industrial wireless devices, and serial communication devices will securely keep your data moving without falling prey to common vulnerabilities.

Crossing Cybersecurity Boundaries

Cybersecurity attacks, vulnerability exploits, and digital espionage have crossed the boundaries into what was once considered off limit targets. Hacking and cyber-attacks have always been considered a "Dark Art", primarily focused on taking small systems offline, stealing data, and holding information for ransom. But times have changed. Cybersecurity attacks have evolved and become weaponized with the capabilities of destroying critical infrastructure systems that support everyday life. An example of such a cyber weapon was the STUXNET worm that infected Siemens Industrial Systems and caused heavy damage to Iran's nuclear program. [1]

It is essential to work with an experienced company that can help you select the proper hardware and software and assist with a design to protect your vital equipment and ensure your networks are adequately secured.

Understanding Common Networking Vulnerabilities

A common question that is often asked is '**Is Cybersecurity Hard?**'. The answer to that is no, but it does take time and experience to understand how attackers gain access into networks, exploited vulnerabilities, and the sources that generate them.

There is no straight forward method that will provide 100% protection against cyber-attacks. Instead, the list below should be a small element of a broader toolbelt used as part of the cybersecurity lifecycle.

1. **Lack of Employee Training -** ICS Engineers often find themselves dealing with IIoT (Industrial Internet of Things) devices that need advanced configurations and 3rd party support. In many cases, engineers have limited access to the necessary resources for stable configurations. Instead, engineers with only a basic understanding of IT systems

takes it upon themselves to manually configure devices and place them in their networks. Due to no formal training on networking, IT security policies, protocols, and cybersecurity, devices are often misconfigured and riddled with security holes and vulnerabilities.

2. **Misconfigurations** – Systems that have been misconfigured present major security vulnerabilities. For instance, poorly configured security settings may be able to limit different types of traffic on an interface but leave commonly used ports open for intruders to exploit.

3. **Insider Threats-** Insiders are often responsible for cybersecurity breaches, both inadvertently and deliberately. A disgruntled employee may “shoulder surf” his lax employees and steal passwords as they are entered. This gives the disgruntled employees access to systems that they might not normally have access to, and their knowledge of plant workings means that they can wreak havoc. [2]

4. **Unnecessary User Access** – Granting unqualified users permissions to access commands and other programming features of devices is a common vulnerability. Users who don’t fully understand company security policies, the complexity of how a device interacts with each other, or the ramifications of how a misconfiguration can impact a network should not be allowed to configure or make changes to important systems or critical devices.

5. **Asset Disposal** – Disposing of old equipment that used to be a part of a company network has to be done carefully by sanitizing any remanence of the network. Any data captured from expired assets can be used to provide reconnaissance of the network.

6. **3rd Party Outsourcing -** Contractors, vendors, and outside consultants provide guidance and subject matter expertise to manufacturers as well as other companies who require their assistance. So having outside personnel accessing critical systems from remote locations is a typical daily occurrence that often gets overlooked by busy admin and engineers. While the initial person they hired might be properly vetted, the contractor might then turn around and hand menial tasks to someone who is careless, hasn’t had the proper security clearance, or is not qualified to have accessibility to the network.

7. **Legacy Hardware / Software -** Legacy hardware and technologies operating inside of industrial systems is a common practice we still see today. Many companies who are

operating legacy systems due not have the finical resource to make the necessary upgrades, instead choosing to patch and replace components as needed. However, this type of operational model opens the door to security vulnerabilities that can easily be exploited by a seasoned hacker due to outdated systems having little no manufacturing support in terms of cyber security, while patches and system updates are none existent.

8. **Inadequate Hardware** – Companies often try to save money by purchasing inadequate hardware that's not designed for a specific application. Purchasing cheaper products and "making them work" typically leads to misconfigurations, workarounds and rouge programming which opens the door to security gaps and vulnerability exploitation.

9. **Hardware Design Flaws** – Industrial control systems interact with a wide variety of devices that are designed with limited cybersecurity features. For instance, power analyzers or liquid flow control sensors may be considered smart because they communicate with a centralized management system but may be susceptible to simple programming errors and software code that can easily be overwritten, making them ideal takes for malicious code execution.

10. **No Backups -** Not having secure copies of local backup configurations for critical systems can lead to a wide range of vulnerabilities. Often is the case where a critical system or piece of equipment has failed and urgently needs to be replaced. When no working backups exist, complex configurations that must adhere to company security policies are misconfigured and present security gaps for intruders to exploit.

11. **Software Updates -** Not having the latest version of software for a device can lead to security and vulnerability issues. When manufacturers release software updates, it's typically to resolve known security and functionality issues and add functionality that can prevent future issues from occurring.

12. **Memory Overload –** Memory overload takes place when an attacker gains unauthorized access to a device. At which point, the attacker can execute simple code to input more data than the device can hold, overloading stored memory and causing the device to crash, reboot, or provide entry to low-level commands which can be reprogramed to point toward malicious code that can be executed later.

13. **No Download Validation** – Downloading software for applications and security patches can sometimes lead unsuspecting users to a look-a-like website that offers what looks

like legitimate software. Not having any mechanisms to validate software can lead to a wide range of security holes and vulnerabilities that can cripple a network.

14. **Poor Network Design** – Operational networks have become just as complicated and robust as their IT counterparts, often requiring segmented isolation for various functions and processes through virtual LANs or firewalls. Poor network designs don't provide isolated needed for security, instead are configured as one large network that, when accessed, provides an attacker access to everything inside the network.

15. **Network Assessments** – Fully functional networks, more often than not, are left alone and with minimal monitoring and system reporting tools operating in the background. It's rare that admins take the extra step of assessing the network for security flaws, vulnerabilities and operational readiness. These types of extra measures are needed to ensure that OT networks are fully protected and updated with the latest vulnerability patches, security updates and optimal configurations.

16. **Limited Network Visibility** – Admins and engineers responsible of managing OT networks typically have monitoring tools that can track the availability of hardware devices and, in some cases, track applications running on the network. However, in today's complicated networks with multiple network segmentation and remote access capabilities, admins need to be more vigilant with the way they monitor traffic. Having secondary firewalls that can monitor traffic at a packet level, ensuring no unknown data packets are traversing the network, mapping out destinations and hardware signatures for later use as a planned attack on the network.

17. **Lack of Documentation** – Not having updated documentation on your network, connected devices, security policies and operational procedures can lead to a wide range of security vulnerabilities. For example, incorrectly configured security features, unpatched software holes, incorrectly segmented networks, open access and availability that should be secured.

18. **Telecommuting –** Over the past two years we've seen a significant increase in remote workers and telecommunicating positions. In many cases, these employees need access to internal company resources for work purposes. Companies that do provide remote access capabilities to remote and telecommuters typically use a VPN or other remote connection software to provide an additional layer of security for the remote connection. However, companies are finding out that remote employees have basic to little security on their home networks and have security holes that can easily be compromised. Once a company computer or laptop connects to the local home network,

it's attacked and, through malicious code, can be taken over at a later time. Once the machine is connected to the company network through a VPN, the attacker can then gain access to a company's resources.

19. **Remote Applications –** Having remote applications for company resource access, tech support, and real-time monitoring and alerting can be extremely beneficial. However, these types of applications present a major security risk and vulnerabilities to their adherent nature. An attacker who can steal credentials for these types of applications can wreak havoc on an OT network. Be sure to enforce strict password policies and two factor authentication to ensure that only granted users can access these types of applications on the network.

20. **Phishing** – Phishing and email scams have always been a major source of vulnerability exploits and malicious code execution. The process is simple and highly effective. Unsuspecting users download a file from what looks like a trusted source or click on a weblink. The process downloads a small malicious piece of code that can be used at a later time to download a secondary piece of code or software and allows attackers access into systems.

21. **Two-Factor Authentication Workarounds -** Two-factor authentication is an excellent way to reduce the likelihood that the wrong person gains access to information, but it can be defeated if a hacker takes control of the computer *after* the two-factor authentication has taken place. A remote industrial automation control system technician may log in from their home network, thinking that the information in transit is safe thanks to their VPN. But a virus or RAT that they accidentally installed earlier may be activated by the presence of the VPN, and access may be unknowingly granted—in much the same way as in the last entry—by offering an innocuous message saying that their first login failed and they need to try again.

22. **Unsecured Data Sockets** – Using default or commonly known data sockets or communication ports for applications within an OT network presents huge vulnerabilities. Attackers are aware of the common port settings and write malicious code directly targeting these ports.

23. **Unnecessary Services** - Running all default services on applications that are not needed can leave security gaps in your OT network. You should find out what services are necessary to run your hardware and applications and shutoff everything else.

24. **Weak firewall Rules** – Firewalls are an intricate part of enterprise networks. However, in the case of OT networks, many firewalls are not configured as thoroughly and instead configured with only basic parameters for functionality. In these types of scenarios, firewalls can easily be bypassed and the lightly secured network can be accessed.

25. **Authentication Bypass** – Users often tire of logging into systems for small minimal changes especially if long complicated passwords are required for authentication. In many cases users will disable authentication unknowingly exposing their system to attackers.

Addressing most of these vulnerabilities requires a holistic approach, addressing every link in the chain. This includes people involved with those systems on every level, and not just the tools they work with. Reach out to Antaira today to help your company meet the challenges of closing breaches and security holes that have made government agencies increasingly security-conscious.

References:

[1] https://www.sciencedirect.com/science/article/pii/S1877050921012709

[2] https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/wp-top-20-cyberattacks.pdf