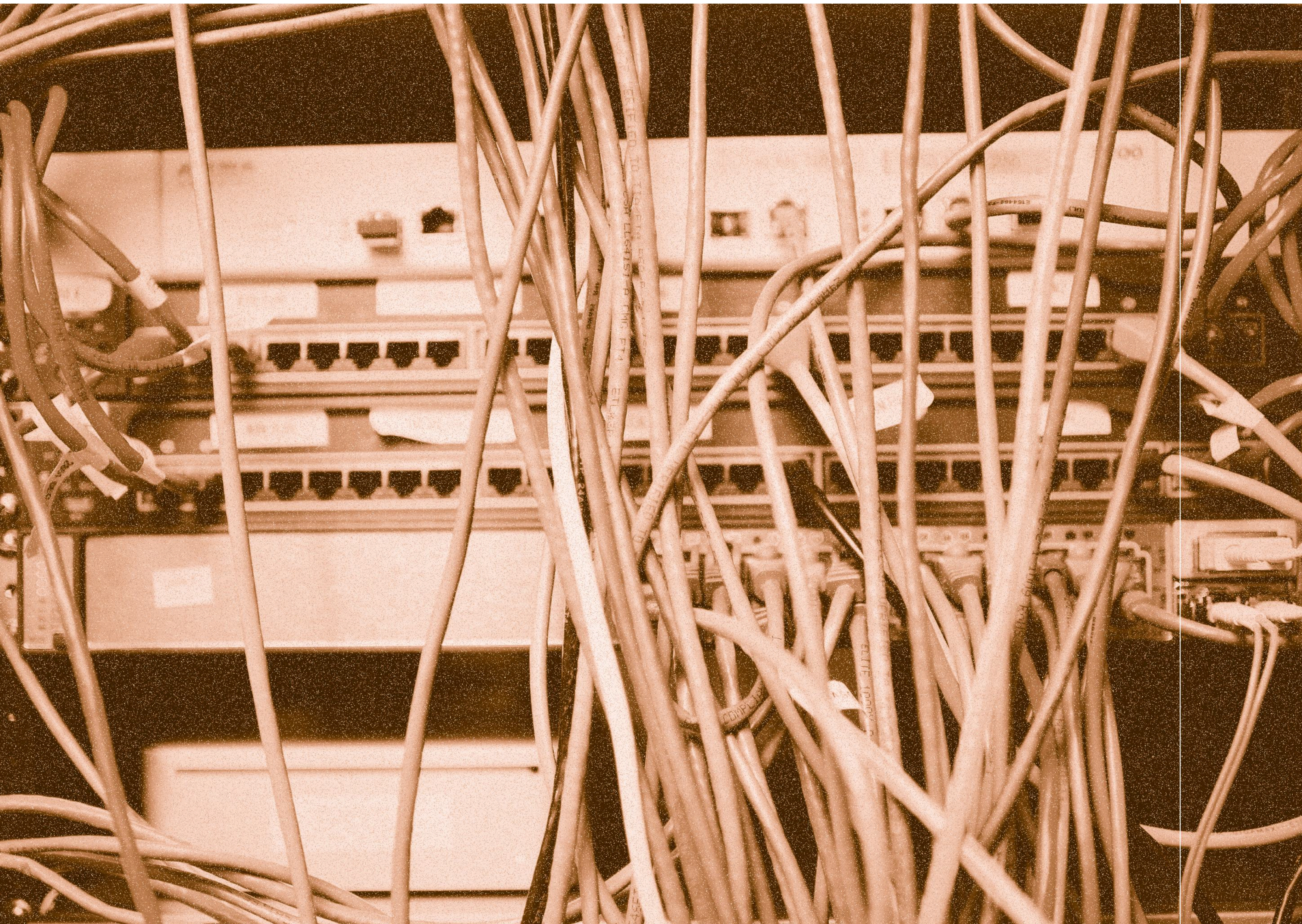
Trout

# “Forever-Day” Vulnerabilities in ICS/OT environment



# Executive Summary

This report will focus on what we call a “Forever day” vulnerability or bug. and their context and importance in industrial environments.

- **Introduction**

1. What is a “Forever-Day” Vulnerability ?
2. Why is it particularly common and critical in industrial environments ?

- **Different types of “Forever-Day” vulnerabilities**

1. Legacy Protocols and Standards
2. Unsupported Operating Systems
3. End-of-Life (EOL) Products.
4. “Forever-Day” Vulnerabilities in ICS/OT environment 1Poor infrastructure design

- **Impact and examples of “Forever-Day” targeted attacks**
- **Mitre ATT&CK Mapping and Cyber Kill Chain**
- **Mitigations**

# Introduction

What is a “Forever-Day” Vulnerability? To add a little bit of context we going to explain every types of XXXX-day vulnerabilities here.

## Zero-day vulnerability

Let’s talk about zero day vulnerability first,

A zero-day vulnerability is a vulnerability in a system or device that has been disclosed but is not yet patched. It’s been found by a researcher but it still unknown to the vendor, and where there is no patch, mitigation, or fix available to address it. The term “zero-day” refers to the amount of time vendors have to address the flaw before hackers can exploit it.

In the field of cybersecurity, we often hear about the discovery of a zero-day vulnerability, certainly because it can be so lucrative for the researcher since a white-hat who discover zero-day vulnerabilities are usually rewarded financially by the vendor. It's seen as a great achievement for ethical hackers to find one.

For black-hat in the other hand they often sell zero-day vulnerabilities to another hacking groups and nation-state threat actors. Once acquired, zero-day vulnerabilities are highly coveted and usually only deployed by a single threat actor against a limited number of high-value targets to lessen the chance the zero-day vulnerability is discovered.

## One day/N day vulnerability :

We also have One-day vulnerability,

One-day vulnerabilities are known vulnerabilities for which a patch or mitigation is available but hasn’t yet been applied. The “one day” term refers to the period between when the vulnerability is disclosed and when affected systems are patched.

Sometimes these vulnerabilities are referred to as “n-day” vulnerabilities since the period is often much longer than one day, as the average mean time to patch (MTTP) is between 60 and 150 days.

Unfortunately, the exploitation of one-day vulnerabilities is often accelerated by the release of Proof-of-Concept (PoC) exploit code before affected users have adequate time to patch their systems. This practice seems to have gotten worse in recent months as cybersecurity vendors and researchers attempt to flex their technical skills, despite the damage it causes.

While more sophisticated threat actors will reverse-engineer a patch to figure out what issue it was meant to fix and then develop their own exploits based on their findings, less technical actors will adopt the publicly available PoC code. This allows the vulnerability to be leveraged by less sophisticated actors who otherwise would not have had this capability without external assistance.

A recent, relevant example of one-day vulnerabilities are CVE-2024-1708, an authentication bypass flaw, and CVE-2024-1709, a path traversal flaw, in ConnectWise’s ScreenConnect servers. (Field Effect)

## Forever-Day vulnerability :

"Forever day is a play on "zero day"

Also called iDays, or "infinite days" by some researchers. A “forever-day” vulnerability is one where the vendor won’t fix the vulnerability. This usually happens because the vendor or original author is no longer maintaining the product. They may no longer be in business or the author may have moved on and abandoned the project.

You can avoid ending up with Forever Day vulnerabilities in your systems by stop using old technologies and start using device or software that is actively maintained.

We could also talk about insecure-by-design vulnerabilities resulting from non-adherence to security best practices during the design process, but in some cases insecure-by-design vulnerabilities can be secured by the implementation of a mitigation, when it’s not possible we can talk about forever day vulnerability.

## Why is it particularly common and critical in industrial environments ?

Industrial control systems (ICS) and operational technologies (OT) often have life cycles spanning decades. In sectors such as manufacturing, energy, and critical infrastructure, equipment is designed to operate reliably for extended periods, often far exceeding typical software life spans.

These systems are challenging and expensive to upgrade or replace. Once deployed, the cost, time, and operational disruptions associated with updates or replacements make it difficult to maintain compliance with evolving safety standards and security patches.

In many industrial environments, security is often treated as an afterthought—or not considered at all —by engineers or IT personnel. The next section will explore examples of outdated components commonly found in ICS/OT environments.

- Communication protocols and standard (like Modbus for example)
- Operating Systems (like DOS OS or old Windows version)
- End-Of-Life Product as PLCs, HMIs and other legacy devices, like printers (which could be an entry point in the network) and old ventilation fan (which could create a overheating situation if hacked)
- Software aside (like the buzz around the ABB WebWare Server for example)
- Simply by some security vulnerabilities in how the infrastructure was studied and build (flat network and lack of vigilance)

# Different types of “Forever-Day” vulnerabilities

## Legacy Protocols and Standards

SCADA/ICS systems are differentiated from traditional information systems in a number of ways. Probably the most important differentiation are the many communication protocols. Unlike traditional IT systems with their standardized TCP/IP protocols, SCADA/ICS systems are marked by significant variation in their communication protocols. They could use Modbus or DNP3 or others communications protocols (like you could see in our PLC report). But we going to talk about the most famous one for the example :

**Modbus**

Modbus is an open-source communication protocol positioned at level 7 of the OSI model initially developed in 1979 by Modicon (now Schneider Electric) for industrial automation systems. It's primarily used to connect supervisory control and data acquisition (SCADA) systems with programmable logic controllers (PLCs) and other devices, facilitating communication in industrial environments. Modbus operates on a client-server model and is simple, making it popular in energy management, manufacturing, and other industrial settings.

**Security Concerns**

The original Modbus protocol was designed without security in mind, as it was intended for closed, isolated industrial environments. This results in several vulnerabilities:

- **Lack of Authentication:** Modbus does not include any form of authentication. An attacker only needs to create a packet with a valid address, function code and any associated data.
- **No Encryption:** All communication over Modbus is done in cleartext. An attacker can sniff the communication between the master and slaves and discern the configuration and use.
- **Susceptibility to Replay Attacks:** Because there’s no encryption or message integrity, Modbus is highly vulnerable to replay attacks. An attacker could capture legitimate Modbus commands and replay them to disrupt processes or operations.

- **No Checksum:** Although Modbus RTU uses a message checksum, when Modbus is implemented in TCP/IP, the checksum is generated in the transport layer, not the application layer, enabling the attacker to spoof Modbus packets.

- **Broadcast Control Risks:** The protocol doesn't have safeguards for preventing or limiting broadcast commands, meaning a single command can affect multiple devices simultaneously. An attacker exploiting this could disrupt large parts of an industrial system.

## DNP3 (Distributed Network Protocol)

DNP3 was developed in the 1990s by Westronic, Inc. to improve interoperability in SCADA systems and was later standardized by IEEE. It's commonly used in the utilities sector, especially for water and electricity systems, to control equipment over long distances. DNP3 is more complex and reliable than Modbus and includes features for error detection, timestamping, and event-driven reporting.

**Security Concerns:**
DNP3 was also developed without built-in security, as it assumed isolated environments. This leads to similar vulnerabilities:

- **No Native Encryption:** Although the protocol includes error-checking, it does not encrypt data, making it vulnerable to interception and eavesdropping.

- **Lack of Authentication in Basic DNP3:** Basic DNP3 lacks mechanisms for authenticating messages, leaving it vulnerable to spoofing and unauthorized commands. An attacker could inject malicious commands that disrupt system operations.

- **Advanced DNP3 with Secure Authentication (DNP3-SA):** Later, DNP3 was extended to include secure authentication (DNP3-SA) under IEEE 1815-2012. However, adoption of this secure version is inconsistent, and many legacy systems still use the insecure version.

- **Vulnerability to Denial-of-Service (DoS) Attacks:** Due to the lack of strong access control, DNP3 systems can be targeted by DoS attacks, overwhelming the system and disrupting communications.

## Unsupported Operating Systems

Outdated and unsupported operating systems are still present and they still pose a serious risk in many industrial organizations, according to a new report from industrial cybersecurity firm CyberX.(1) Some individuals might still rely on Disk Operating System (DOS), while others might have made a partial transition to Windows 3.1, Windows 2000, or Windows XP or even old Linux version.

**DOS**

MS-DOS acronym for Microsoft Disk Operating System, also known as Microsoft DOS) is an operating system for x86-based personal computers mostly developed by Microsoft. Collectively, MS-DOS, its rebranding as IBM PC DOS, and a few operating systems attempting to be compatible with MS-DOS, are sometimes referred to as "DOS" (which is also the generic acronym for disk operating system). MS-DOS was the main operating system for IBM PC compatibles during the 1980s, from which point it was gradually superseded by operating systems offering a graphical user interface (GUI), in various generations of the graphical Microsoft Windows operating system.

”Some older hardware and software systems may still rely on MS-DOS for operation, particularly in industrial or embedded systems.”

MS-DOS is very vulnerable due to several reasons, like :

- It as no concept of user accounts, privileges, or access controls.
- Any program running in MS-DOS has full control over the entire system, including memory, files, and hardware
- MS-DOS was not originally designed for networking. When network functionalities were added through extensions or third-party tools, no robust security mechanisms (e.g., encryption, authentication) were integrated which give the opportunity to eavesdropping, unauthorized access, and man-in-the- middle attacks.
- It is highly susceptible to viruses and malware, especially boot sector viruses and file-infecting viruses : Michelangelo Virus (boot sector) and Cascade Virus (file-infecting) are classic example.
- The File Allocation Table (FAT) file system used by MS-DOS lacks any security features like file permissions or encryption. Any user or program can read, modify, or delete files without restriction.

**Window**

Windows XP is still used in some industrial environments. It died in April 8 2014, when support for Windows XP ended. Above that, XP simply lacks a ton of security features that make newer versions of Windows “Forever-Day” Vulnerabilities in ICS/OT environment 7safer. In fact, Windows 11 already has a few new features that theoretically make the system safer than Windows 10, and we're talking about 20 years of changes between Windows 11 and Windows XP.

For example, most operating systems use techniques such as Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) to protect against memory-based attacks. ASLR randomizes the memory addresses used by system and application processes, making it harder for attackers to predict where their malicious code will be executed. DEP, on the other hand, prevents code from running in areas of memory that are intended to store data, further thwarting attempts to exploit vulnerabilities. Windows XP never had ASLR, and DEP was only added in SP2.

To go a step further, features like Secure Boot, added with Windows 8 in 2011, ensures that only trusted software that has been verified by the system’s firmware is allowed to run during the boot process. This is something else noticeably absent from Windows XP. Windows XP, even if it were end of life but had those features, would be significantly more secure as a result.(xda)

In Windows XP users by default receive an administrator account that provides unrestricted access to the underpinnings of the system. If the administrator's account is compromised, there is no limit to the control that can be asserted over the PC. Windows XP Home Edition also lacks the ability to administer security policies and denies access to the Local Users and Groups utility. (wikipedia)

A lot of CVEs and tutorial of exploits are present on Windows XP allowing code execution, overflow, memory leak...etc

## End-of-Life (EOL) Products.

In a factory, some devices are here since the beginning, that can be the case for PLCs/HMIs, SCADA, HVAC, lightning control systems, Industrial Network Devices like switchs or routers, robotic systems, power units, printers, CCTVs... Everything in a factory can become obsolete, creating security and cybersecurity problems, even things like HVAC or printers can have terrible repercussions, such as overheating of the systems or a lateral movement from the printers impacting the systems.

**The PLC-5 Allen-Bradley (Rockwell Automation)**

This PLC is a perfect example it was a very popular model and widely used in the manufacturing industry but unfortunately the model is not maintained anymore which leave the place for vulnerabilities to persist in the environment who still use it.

Allen-Bradley PLC-5 Family PLCs uses DF1 Full Duplex protocol. The DF1 protocol does not provide encryption or authentication mechanisms, making it vulnerable to unauthorized access and data interception over the Internet.

Old PLC and HMI, (not necessarily this one) default credentials are easy to find or to bruteforce. If someone got access to the PLC remotely or physically it would be easy for him to manipulate the device to give it the required parameters (if not already present) for attacks.

Exemple : the CVE-2012-4690 allow remote attackers to cause a denial of service via messages that trigger modification of status bits.

**Printers vulnerabilities**

Multifunction printers (MFPs) play a fundamental role in offices worldwide. But they could also be an entry gates to the network if not secured enough, not so long ago a hacker attacked 150 000 printers accidentally left accessible via the web to show his skill and to raise awareness over the threat of remote access. That could be an entry gates, but also a way to simply steal sensitive information that was printed.

**HVAC**

There have been several instances where HVAC (Heating, Ventilation, and Air Conditioning) systems have been targeted in cyberattacks, highlighting the vulnerabilities of critical infrastructure in buildings and industrial settings.

An article from HVAC&R News in Australia highlights a 2020 report from Forescout in which HVAC systems are listed as #2 on the list of 10 riskiest IoT devices. The reason to target HVAC could be : access point, stop it to create overheating and additional chaos to an attack situation...

## Software too

There is not only Operation-system and physical device that can be not maintained and vulnerable, but also software.

That the case for example of the ABB WebWare Server which is a remote supervision and management software solution that will not be fixed even though it provides the means to remotely execute malicious code on computers that run the application (Sonatype).

## Cybersecurity risk from poor infrastructure design

And to finish, we gonna talk about the fact that the major security in a network is the fact of being flat or to have crazy easy entry-point like a public WiFi connected to the inside-network or worse.

### Flat Network

A flat network is a type of network architecture where all the devices in the data center can reach each other without having to go through intermediary devices like routers. In a flat network, all devices are linked to a single switch, meaning that all the workstations connected to the flat network are part of the same network segment. Since all devices are connected to a single switch, it becomes one of the easiest network designs to manage. It is also very cost-effective.

But of course it pose significant risks ! A flat network typically lacks internal boundaries like subnets or VLANs. While this setup is simple and easy to manage, it's vulnerable to security threats, including unrestricted lateral movement, which can expose sensitive data across the entire network.

You need to adopt segmented network and add strict access control or your network would be an easy target to any attackers.

### Crazy easy entry-point

In addition it would be terrible if you had entry point like internet accessible device or a public WiFi linked to your internal network.

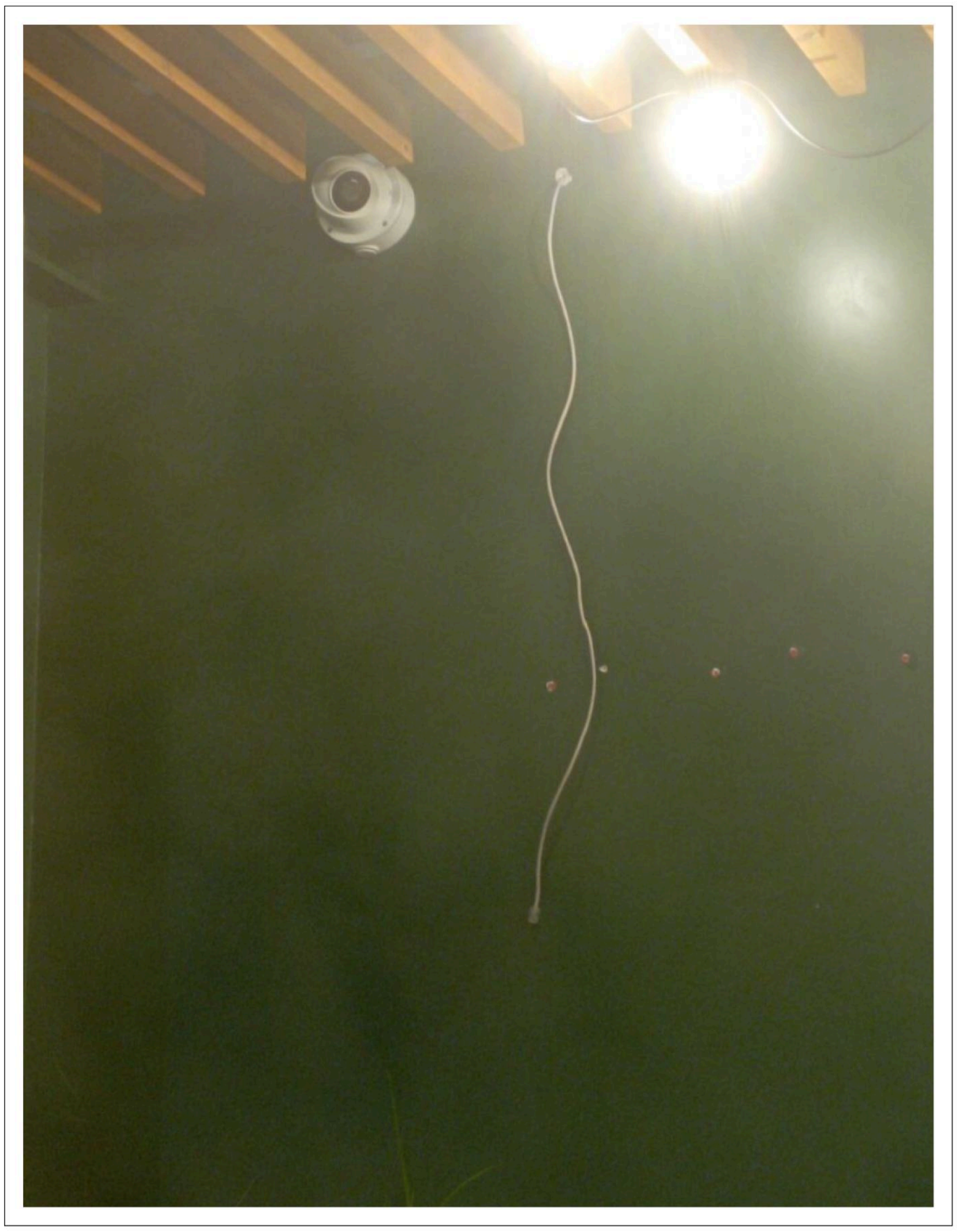


*Figure 1: Real pic of an Ethernet cable leaved in a public area of a plant.*

# MITRE ATT&CK Mapping and Cyber Kill Chain Analysis

## Tactics and Techniques

| Tactic | Technique ID | Technique Name | Context |
|---|---|---|---|
| Initial Access | T0883 | Internet Accessible Device | Device like printers, CCTV, or HMI which are accessible from the internet is a terrible flaw that can make an attacker attack your entire network if flat and unprotected. |
| Initial Access | T0819 | Exploit Public-Facing Application | Same here, if a device have open ports and services that can be leverage to permit an attacker to move into the ICS network, it's critical. |
| Initial Access | T0817 | Drive-by Compromise | Legacy devices or systems with open, unsecured connections (e.g., Internet-facing devices or printers) could be exploited. |
| Initial Access | T0847 | Replication Through Removable Media | Old and un-patched device such as PLCs or computer with old OS are more vulnerable to an attack using USB (for example) to get access to the network. |

| Tactic | Technique ID | Technique Name | Context |
|---|---|---|---|
| Initial Access | T0848 | Rogue Master | Legacy systems that use insecure communication protocols like Modbus or DNP3, or systems with default credentials, can allow unauthorized access or manipulation of system processes (e.g., PLC or SCADA manipulation). |
| Privilege Escalation | T0890 | Exploitation for Privilege Escalation | Adversaries may exploit software vulnerabilities in an attempt to elevate privileges.<br>A rogue master in a system could execute commands or manipulate the operational flow by exploiting privilege escalation techniques. |
| Initial Access / Lateral Movement | T0866 | Exploitation of Remote Services | Vulnerabilities in outdated protocols or systems that don't support encryption or authentication could lead to Exploitation of Remote Services |

| Tactic | Technique ID | Technique Name | Context |
|---|---|---|---|
| Lateral Movement / Persistence | T0812 / T0891 | Default Credentials / Hardcoded Credentials | Old PLCs and devices are more likely to have unchanged default credentials or to come with hardcoded credentials often never updated, allowing attackers to bypass security. |
| Credential Access | T1110 | Brute Force | Old Device are more likely vulnerable to Brut-force technique to gain credentials. |
| Discovery / Collection | T0842 / T0830 | Network Sniffing / Adversary-in-the-middle | Unencrypted communication protocols are vulnerable to network sniffing and MitM attacks. |
| Inhibit Response Function | T0814 | Denial of Service | Vulnerabilities in communication protocols, devices, or services could allow attackers to launch denial-of-service attacks, interrupting industrial operations. |

# Mitigations

**Update and upgrade**

Prioritize upgrading your systems, even though it's challenging. While it may seem like a daunting task, allocating time and resources to update security policies and modernize devices is far more manageable than recovering from a ransomware attack. With the average cost of ransomware recovery nearing $2 million, proactive measures are a critical investment.

**Network segmentation**

The cornerstone of securing industrial environment is avoiding a flat network design. Effective segmentation requires isolating critical assets at Layer 3 with routed networks rather than relying on VLANs, which can create a false sense of security, add unnecessary complexity, and often fail to prevent lateral movement due to inter-VLAN routing. Protocols like 802.1x, though widely known, are expensive to implement and maintain and may not provide sufficient modern security. True segmentation should create secure, isolated environments for critical systems, with controlled access.

**Perform Audits**

Utilize industry frameworks such as ISO 27001, NIS2, and NIST 800 to evaluate your organization's security posture against established standards. "Forever-Day" Vulnerabilities in ICS/OT environment 13Use these assessments to create actionable plans to bolster defenses. If your organization lacks in-house cybersecurity expertise, consider engaging external services to perform comprehensive audits.

## Why Trout and SecurityHub could help you

- **Demilitarized LAN** (Software-Defined Air-Gap Subnetworks): Trout products enables the creation of isolated, secure network segments to protect critical infrastructure.

- **Comprehensive Network Monitoring:** SecurityHub provides advanced tools to monitor and identify malicious access attempts in real time.

- **Threat Behavior Rules:** Utilize built-in rules to detect and mitigate known threats based on behavioral patterns.

- **Guided Best Practices:** SecurityHub offers dedicated playbooks to help maintain strong security protocols and stay aligned with industry standards.

# In Summary

The landscape of vulnerabilities in industrial control systems (ICS) and operational technologies (OT) underscores the critical need for proactive cybersecurity measures. From outdated protocols and end-of-life devices to poor network design, these vulnerabilities represent significant risks to operations, safety, and data integrity.

Addressing these challenges requires a multi-faceted approach: updating legacy systems, implementing robust network segmentation, conducting regular security audits, and adopting forward-looking security solutions. While upgrading decades-old systems is a complex and resource-intensive process, the cost of inaction — whether through downtime, safety incidents, or ransomware attacks — is far greater.

Protecting the future of industrial operations starts with securing the systems of today. Let's build a safer, more resilient foundation together.

Trout