# An Empirical approach towards discovering hidden vulnerabilities in Industrial Control System (ICS) Networks

Himanshu Goyal
Georgia Institute of Technology
*hgoyal33@gatech.edu*

## Abstract

Industrial control systems (ICS) are used to automate and monitor processes and equipment in various industries, such as energy, transportation, and manufacturing. These systems provide many benefits, but they can also be vulnerable to security threats if not properly protected. Most ICS networks use protocols designed for controlled environments and do not have built-in security mechanisms. However, the increasing connectivity of ICS devices to networks and the internet creates opportunities for malicious actors to cause disruptions and malfunctions. In this study, we employed an empirical methodology to assess the potential vulnerabilities in existing ICS networks. Using network scanning techniques, we identified vulnerable ICS devices according to the Purdue model, which considers the hierarchical structure of ICS networks and the different services that devices run on. Our evaluation showed that this method could effectively identify high-risk devices and prioritize them for security measures.

## 1 Introduction

Industrial control devices are essential for many industries, including manufacturing, energy, and critical infrastructure. These devices enable remote control and monitoring of industrial processes, making them crucial for modern industry. However, the security of ICS networks is often neglected, putting vital infrastructure at risk. ICSs are vulnerable to cyberattacks [6], which can have serious consequences. For example, a cyberattack on the Maroochy Water Services [33] in Australia in 2010 led to the leaking of almost one million gallons of untreated sewage into the environment. Another example is the Stuxnet virus [18], which disrupted the industrial control systems of Iranian nuclear plants and caused damage. Recently, the NSA also discovered malware [1] before it was distributed. It is seen that this malware is developed by a state-level actor and is capable of taking full control of the underlying ICS network. These examples depict the potential dangers of neglecting the security of ICS networks and the importance of implementing proper security measures to protect them against cyberattacks.

To enable remote control and monitoring of industrial processes, industrial control systems (ICSs) employ a number of communication protocols. These protocols are desired to offer reliable and efficient communication between various ICS devices and connecting systems. For instance, Modbus is a widely recognized standard for industrial communication used in ICSs. Modbus is a simple and adaptable protocol that can communicate with various device types, such as programmable logic controllers (PLCs), sensors, and actuators. DNP3, specifically developed for communication between distributed devices in large-scale systems, is another extensively used protocol in ICSs. In general, ICSs use a variety of generalized and custom communication protocols to provide the necessary communication within ICSs, and are essential for the proper functioning of these systems.

On the other hand, many existing ICS protocols are vulnerable to cyberattacks for various reasons. Many ICS standards were established and deployed before cybersecurity was a major concern. As a result, they lack built-in security measures and have ineffective authentication mechanisms. It facilitates attackers gaining access to the system and exploiting flaws. Another difficulty is that many ICS protocols are proprietary, which means outside parties cannot audit them. This can make identifying and addressing vulnerabilities in these protocols difficult for security researchers. Furthermore, proprietary protocols may be poorly described, making it difficult for enterprises to apply effective security measures. Another reason that makes ICS protocols vulnerable to threats is their widespread use in vital infrastructures, such as power plants and water treatment plants. For attackers, these systems are highly valuable targets, and the repercussions of a successful attack can be catastrophic. Therefore, to mitigate these risks, organizations must install strong security measures and update and maintain their ICS protocols on a regular basis.

In this work, we aim to investigate the security flaws associated with hosts employing industrial control systems (ICS) communication protocols. Our method is empirical for identifying and analyzing risks connected with enterprises that operate their infrastructure with automation devices. In the future, we expect it will provide insights and suggestions for enhancing the security of industrial control networks.

# 2 Related works

In order to streamline manufacturing processes, virtually all businesses today use remote SCADA (Supervisory Control and Data Acquisition) systems [34]. One or more remote field sites with control servers, communication links, and field devices in a centralized control room make up a typical SCADA network. Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs) are a few examples of the field sensors used by SCADA systems at remote sites to continually monitor a wide variety of parameters related to electromechanical devices (IEDs). The automation industry has traditionally been considered safe and secure due to well-configured machines and human oversight. However, as the industry has evolved and more devices have been introduced that can be remotely monitored and modified, it has become vulnerable to attack. Malicious actors can use the same methods used in traditional networking domains to disrupt industrial infrastructure, leading to potentially catastrophic results. Integrating remote monitoring and control capabilities into the automation industry has led to several notable real-world attacks [6] with significant economic loss, the potential to damage physical equipment, and the possibility of causing harm to human life. An extensive survey of SCADA network security can be found in [20, 30], where the authors describe the communication architecture and classify potential threats and attacks.

ICS operations are typically mission-critical and require real-time performance. Examples of these systems include nuclear power plants and smart grids. Industrial standards recommend using antivirus software and firewalls to protect these networks, but implementing these measures can slow down the underlying process and cause the loss of crucial message packets, reducing the efficiency of the SCADA system. In some cases, operators may disable these protections to avoid such delays, leaving the network vulnerable to attack [27]. The National Infrastructure Security Co-ordinator Center has summarized firewall setup, vulnerabilities, and best practices for SCADA architecture. Still, poor firewall rules due to a lack of network competence can result in bypassing security mechanisms [31].

Establishing clear rules for SCADA communication protocols is essential to prevent vulnerabilities such as IP spoofing and man-in-the-middle attacks. These are common in TCP/IP protocols and can also affect SCADA systems that use open standard protocols over TCP/IP without additional protection measures [20, 30]. ICS organizations generally allow SQL traffic for data historian servers. Therefore, SCADA communication protocols such as HTTP, OPC/DCOM, FTP, TFTP, and MODBUS/TCP are vulnerable to the Slammer worm, a threat vector for SQL data. Chen et al. [11] have also shown that it is possible to inject crafted packets into an ongoing MODBUS session, causing slave industrial devices to respond to these illegal functions. Darwish et al. [14] have demonstrated that man-in-the-middle attacks can be launched against critical infrastructures, such as smart grids, using the DNP3 protocol. In general, attackers have exploited these underlying communications protocols to launch internal and external attacks, denial of service attacks, virus and worm infiltrations, remote access attacks, and other cyber incidents that have harmed process environments.

Most attacks in this domain can be linked to the Internet accessibility of these SCADA devices. It provides a route for launching remote attacks. Multiple ICS communication protocols function in a master-slave architecture; hence, the master's visibility makes it even more dangerous. Using network scanning techniques tools such as Censys [2, 15] and Shodan [5], researchers [12, 17, 26, 38] discovered that several ICS devices were inadvertently accessible through the public Internet. In addition, authors noticed that bulletproof hosting providers affiliated with bad actors conduct extensive network scans to identify potentially vulnerable ICS systems. However, the work is limited to horizontal scans that provide little insight into the entire deployment issues associated with organizations. In addition, Giovanni et al. [8] have presented a method for evaluating the visibility of ICS-protocol-based SCADA devices via IXP network traffic. The authors found their proposed technique superior to the widely used network scanner Shodan [5]. However, gaining IXP data is subject to several legal concerns if one wants to understand worldwide ICS networks. Therefore, In this study, we employ network scanning techniques to precisely categorize the deployment issues associated with adopting SCADA devices in industrial automation networks. We believe it will assist in identifying the most to least vulnerable ICS devices in a typical organization's network.

# 3 Background

## 3.1 Purdue Model

The Purdue model [13, 19, 28] is a framework for developing and deploying secure industrial networks. It is also known as the Purdue enterprise reference architecture. This model incorporates a number of essential components that are geared at ensuring the safety of industrial networks. It also places emphasis on the use of a multilayered approach, as shown in Figure 1, to the architecture of a network, with each layer offering certain services and different levels of protection being provided in between. The overall network can be mainly categorized into two parts: Information Technology (IT) and Operations Technology (OT).

The fine-grained separation among the networks is as follows:

1) Enterprise Zone, or IT network, contains the standard IT devices and systems such as the logistic business systems and the enterprise network.

2) The Demilitarized Zone (DMZ) regulates the data transmission between the Control Zone and the Enterprise Zone. It helps in maintaining the connection between the IT and the OT networks in a secure fashion.

3) Control Zone, sometimes called OT network, encompasses systems and equipment for monitoring, controlling, and maintaining the automated functioning of the logistic and physical processes. It consists of four sub-levels:

- **Level 0** includes physical sensors and actuators that act directly on the physical process.
- **Level 1** includes intelligent devices such as Programming Logic Controllers (PLC), Intelligent Electronic Devices (IED), and Remote Terminal Units (RTU).
- **Level 2** includes control systems such as Human Machine Interfaces (HMI), alarms, and control room workstations;
- **Level 3** includes manufacturing operation systems that frequently manage control plant operations to produce the desired end product. Through the DMZ, Level 2 and Level 3 devices can communicate with the Enterprise Zone.

4) Safety Zone consists of equipment and systems for controlling ICS security by monitoring for anomalies and preventing catastrophic failures.

Firewalls, intrusion detection systems, and access control systems are only some of the various security measures that are included for each network layer in the Purdue model. These procedures protect against potential security concerns, such as distant attacks or dangers from employees within the firm. The Purdue model also argues for assigning various roles and responsibilities to individuals or groups inside the network. It helps to prevent unwanted access and ensures the preservation of essential functions. Overall, the Purdue model provides a comprehensive framework for implementing secure industrial networks. By following this model and implementing its security measures, organizations can protect their critical infrastructure and ensure the smooth operation of their industrial processes.

## 3.2 ICS Protocols Overview

Communication protocols are necessary for the efficiency, dependability, and precision of real-time activities in industrial automation and control. However, these protocols prioritize functionality over security, making consumers susceptible to vulnerabilities. The convergence of protocols on IP networks has spawned new security vulnerabilities to accommodate changing business requirements. Organizations must emphasize safety in their protocols and apply strong security measures to safeguard their networks and systems from these vulnerabilities. In this work, we mainly focussed on five popular ICS communication protocols. Below we provide a brief overview of these protocols and their security features.

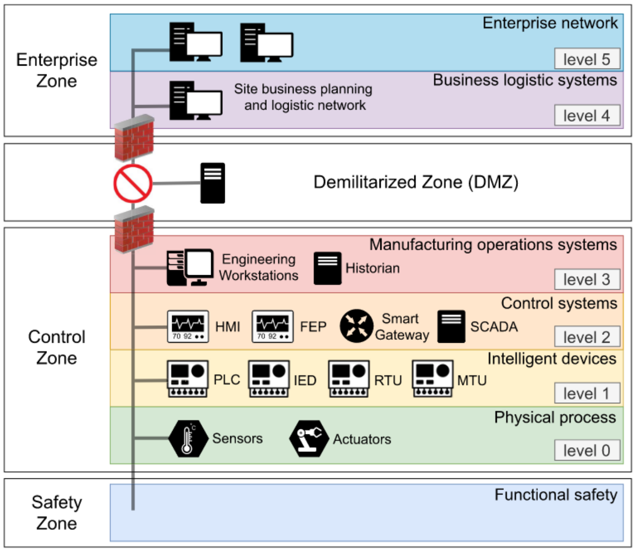

Figure 1: Standard architecture of an ICS network according to a Purdue Model [13]

**1. Modbus (TCP/502):** Modbus [35] is a widely-used communication protocol in industrial control systems (ICSs). It is an open standard, meaning it is not proprietary and is available to anyone. Modbus was designed for usage in Internet-isolated environments with regard to application layer security. Modbus uses a client-server architecture, with a master device sending requests to one or more slave devices. The protocol defines a range of function codes that specify the request type, such as reading or writing data. One key advantage of Modbus is its broad support among different devices, including programmable logic controllers (PLCs), sensors, and actuators. This makes it easy to integrate Modbus into existing ICSs and allows communication between various devices. Despite being widely popular for industrial automation and control, it does not include any built-in security features. As a result, attackers can easily intercept and manipulate communication over the network. To improve security, it is important to use a secure variant of Modbus, such as Modbus TLS or Modbus over HTTPS, and to implement good security practices, such as regular patching and updates, network segmentation, and user access controls. Several researchers [10, 32] have also developed out-of-band covert-channel-based mechanisms to provide confidentiality and authentication.

**2. Siemens S7 (TCP/102):** Siemens S7 is a proprietary industrial protocol [22] used for communication between programmable logic controllers (PLCs) and human-machine interfaces (HMIs) in automation systems. It is based on the ISO transport protocol and uses a client-server architecture for communication. S7 supports multiple data types, including integers, floating-point numbers, and Boolean values, and provides functions for reading and writing data from PLC memory. S7 also includes support for function blocks, which are reusable blocks of logic that can be used to perform common tasks, such as math operations or data processing. As with any communication protocol, Siemens S7 is vulnerable to various cyber-attacks. It does not include built-in encryption for data transmitted over the network. Moreover, it does not provide any mechanism for authenticating devices or users on the network. This makes it easy for attackers to impersonate legitimate devices and gain access to sensitive data or control systems. The system is vulnerable to replay attacks [24]. Stuxnet exploited the security vulnerabilities in S7Comm to compromise an Iranian Nuclear Power Plant in 2010. Siemens has developed S7CommPlus, a new version of the protocol with protection against replay attacks, in response to this incident. It has also been demonstrated that this version is vulnerable to reverse debugging techniques [24]. However, a secure variant of Siemens S7, such as Siemens S7-SSL or Siemens S7-TLS, can provide additional security for communication.

**3. DNP3 (TCP/20000, UDP/20000):** DNP3(Distributed Network Protocol) [16] is another communication protocol used in industrial control and automation systems. It is designed to allow various devices and systems within a control network to communicate with each other and exchange information in a reliable and consistent manner. DNP3 uses a combination of TCP and UDP as transport protocols and can operate over various physical media, including serial links, radio, and Ethernet. It is commonly used in the electric power industry for substation automation and distribution management applications. However, it also doesn't provide sufficient security guarantees. It does not provide any encryption for data transmitted over the network, leaving it vulnerable to interception and tampering. DNP3 provides basic authentication mechanisms, but attackers can bypass them. Moreover, it is susceptible to buffer overflow attacks, which could allow attackers to execute arbitrary code on vulnerable devices. It is important to implement robust security measures and controls within DNP3-based systems to address these security vulnerabilities. To protect confidentiality and integrity, some solutions such as end-to-end encryption [25] and VPN for ICS Networks [7] have been proposed.

**4. BACnet (UDP/47808):** BACnet (Building Automation and Control Networks) is a communication protocol used in building automation and control systems. It is designed to allow various devices and systems within a building, such as heating and cooling systems, lighting, and security systems, to communicate with each other and exchange information in a standard and interoperable manner. BACnet is based on the OSI (Open Systems Interconnection) model and uses a combination of TCP and UDP as its transport protocols. It is widely used in the building automation industry and is the most widely-used protocol in the North American market. BACnet includes a wide range of object types that can represent data and functions within building automation and control systems. It also provides support for multiple services and functions, including device discovery, data read and write, and alarm reporting. The protocol specification includes security features, but Kaur et al. [21]found that manufacturers do not implement these. Moreover, it has other security vulnerabilities [37] that potential attackers can leverage to get access to the underlying network. These vulnerabilities include a lack of encryption for data transmitted over the network, weak authentication mechanisms that can be easily bypassed, and susceptibility to denial-of-service attacks. In addition, BACnet is potentially vulnerable to buffer overflow attacks and is not actively maintained or updated, so there may be unknown vulnerabilities.

**5. Tridium FOX (TCP/1911):** The Tridium Fox protocol [4] uses a publish-subscribe model for communication, where clients can subscribe to data streams from servers and receive updates whenever the data changes. This allows for efficient communication and data exchange in building automation systems. It is widely used in building automation, energy management, and other industrial applications. It is a popular choice for connecting and managing devices and systems in IoT environments, as it allows for efficient and secure communication and data exchange. Regarding network security, the Fox protocol is designed to be secure and reliable. It uses encryption and authentication to protect the data transmitted over the network and has support for various data types and encoding schemes. However, sometimes industrial operators do not incorporate sufficient security features leaving the network vulnerable to potential security threats.

The security of industrial protocols, such as Modbus, Siemens S7, DNP3, BACnet, and Tridium Fox, varies depending on the specific protocol and implementation. In general, these protocols were designed and developed when security was not a major concern, so they may not include built-in encryption or authentication. Moreover, some of the common vulnerabilities common to all of these protocols are *lack of encryption*, *lack of authentication*, *lack of access controls*, and *lack of regular updates*. As a result, the ICS networks having these outdated protocols are prone to attacks. Therefore, it is important to implement additional security measures, such as network segmentation and virtual private networks (VPNs), to protect against cyber attacks.

To address some of these security concerns, a number of industrial standards [23] have been developed, including ANSI/ISA99 and IEC 62443.02. These standards, similar to the Purdue Model [13], recommend dividing industrial networks into distinct zones to improve security. However, According to [36], 80% of the routers that connect the zones in an industrial network are vulnerable to cyberattacks due to insufficient security settings. These vulnerabilities could allow attackers to access control-related traffic on an enterprise's network and abuse the operational network. Moreover, the authors emphasize that inadequately specified security perimeters and inadequate security interfaces (zones) can result in exploitable system vulnerabilities.

## 3.3 Network Scanning

Network scanning [29] is a technique for discovering and mapping network devices, services, and vulnerabilities. This process involves sending probe requests to multiple network devices of the target service and analyzing the results to obtain information about the network and its security status. Manual or automated network scanning is often used with other security tools and techniques to detect and mitigate potential security threats and vulnerabilities. Standard network scanning techniques include port scanning, vulnerability scanning, and network discovery. Consequently, the collected information can provide critical insight and knowledge to protect networks from potential attacks. There are several benefits of network scanning for industrial networks, including:

- **Hidden vulnerabilities detection:** By sending requests and probes to various network devices and services, specialized software such as NMap may detect and map potential security vulnerabilities such as open ports and out-of-date software. This data could be helpful in prioritizing and deploying security solutions to protect against these vulnerabilities and reduce the risk of unauthorized access or attacks.

- **Better organisational functioning:** Network scanning can assist in improving the effectiveness and reliability of industrial networks by locating and fixing potential points of vulnerability. This may ultimately result in increased production and decreased downtime, both of which are important factors from the organization's point of view.

- **Adherence to safety standards:** To maintain lawful and secure operations, a variety of industries, including the energy and transportation sectors, must adhere to specific security requirements. By regularly scanning their networks, businesses may ensure compliance with these requirements and avoid fines and penalties.

Finally, network scanning is also crucial to a comprehensive industrial network security strategy. Organizations that execute these inspections regularly and consistently can defend themselves against potential security threats, boost operational efficiency, and comply with industry laws.

### 3.3.1 Censys overview

Censys [2] is an industry-standard search engine that allows organizations and individuals to ask questions about the devices and networks that make up the Internet. It was developed by a team of researchers at the University of Michigan and is currently a commercial product. However, it is believed that Censys is built on top of ZMap [15] and ZGrab [3], which are open-source projects. ZMap is a single packet network scanner used to perform transport layer scans, and ZGrab is a stateful application-layer scanner that works with ZMap. Security researchers widely use these tools for their efficiency, reliability, and faster convergence time for internet-wide scans than other standard tools like Nmap. These scanners have played a central role in discovering or analyzing some of the most significant internet-scale vulnerabilities, including FREAK, Logjam, DROWN, Heartbleed, and the Mirai botnet.

# 4 Experimentation

In this work, we use the dataset obtained by the Censys scanner for the corresponding five services: Modbus, Siemens S7, BACnet, Tridium FOX, and DNP3. Censys performs weekly scans for each of these services, and we believe the resulting data is valuable in answering interesting questions. The only limitation of Censys is that it can only identify devices running Modbus on any port. Therefore, it cannot recognize the remaining services on ports other than their respective standard ports. We provide a brief description of the Censys dataset below.

```
host_identifier ## IP-address of the scanned device
    ipv4
    ipv6
services ## service-level information
snapshot_date ## Date of scan
ipv4_int ## IPv4 address in Integer notation
ipv6_int ## IPv6 address in Integer notation
location ## geographical details about the host
autonomous system ## Network provider information
ports_list ## ports associated with services
service_names_list ## services running on the host
```

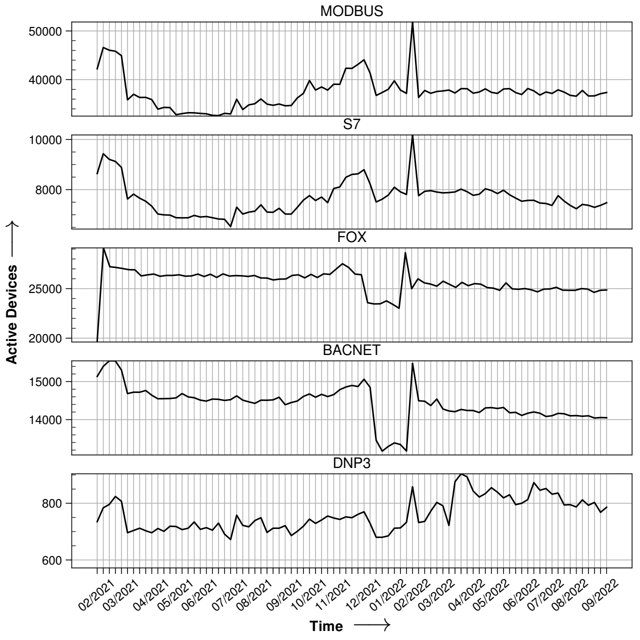

Figure 2: Number of active SCADA devices running ICS communication protocols

## 4.1 Distribution of active devices

In this section, we present an analysis of the weekly data collected from February 2021 to September 2022 regarding the number of active devices on each of our targeted ICS communication protocols. Our measurement results are shown in Figure 2. The count of active devices exhibits a consistent behavior with some deviations during certain time periods. Interestingly, the behavior appears to be similar across all protocols. Our analysis also revealed that the number of device IPs with open ports for these ICS services is significantly larger than the number of devices that actually run these services on the open ports. Therefore, we report only the number of devices that participated in protocol handshakes. As of Sep 2022, we observed approximately 37,000 Modbus devices, 7,500 S7 devices, 14,000 BACnet devices, 25,000 Tridium FOX devices, and 800 DNP3 devices. To facilitate a better understanding of our results, we compare them to the statistics reported in [26]. Our analysis reveals that the number of vulnerable hosts for services like Modbus, S7, and DNP3 has increased significantly. In contrast, we observed a decline in the number of vulnerable hosts for the remaining two services. We hypothesize that devices have migrated from their original communication protocols to alternative ones. The overall change in the number of vulnerable SCADA devices from 2016 to 2022 can be better understood from Table 1.

**Reason for a sudden increase in vulnerable hosts:**

In Figure 2, from December 2021 through February 2022, we observed a strange behavior in the number of vulnerable hosts for all communication protocols. Initially, we suspected that the Russia-Ukraine crisis may have been the cause, so we analyzed the variation in the number of active devices in both countries during this time frame, as shown in Figure 3. However, our analysis revealed that the contribution of both countries to this strange behavior was negligible. Therefore, we investigated it further by analyzing autonomous systems (ASes). Consequently, we grouped the vulnerable hosts based on their ASN. To better understand the behavior, we examined the data from two different perspectives. First, we fixed the top 10 ASes contributing to the final count on Nov 9, 2021, and observed how the device count varied in these ASes during this time interval. Second, we looked at the top 10 ASes on each day of our measurement. In the first perspective, we found that most ASes exhibited consistent behavior, with the exception on February 1, 2022, when the top contributing AS experienced an increase in active device count, although several other ASes also showed a reduction in active devices. Overall, we observed that these ASes did not contribute much to the sudden increase. In the second perspective, we also noticed that most of the ASes were the same as the earlier top 10 set, and the new ASes did not significantly contribute to the overall count. However, we did observe a substantial increase in the overall number of active ASes (highlighted on top of each bar) on February 1, 2022, compared to other measurement dates. These incoming

| Protocol | March 2016 [26] | Sep 2022 | Percentage Change |
|---|---|---|---|
| BACnet | 16,813 | 14,000 | -16.7% |
| DNP3 | 429 | 780 | 81.8% |
| Modbus | 23,120 | 37,485 | 62.1% |
| S7 | 2,798 | 7,489 | 167.7% |
| Fox | 26,299 | 25,000 | -4.9% |

Table 1: Change in total number of vulnerable IPv4 ICS hosts in comparison to [26]

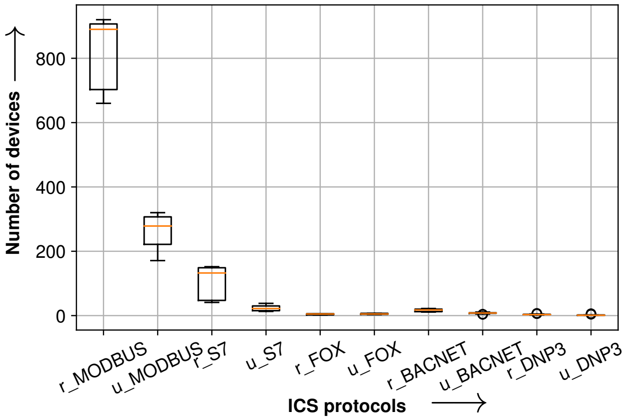

Figure 3: Variation in vulnerable active devices in Russia(r) and Ukraine(u) during Dec 2021 to Feb 2022

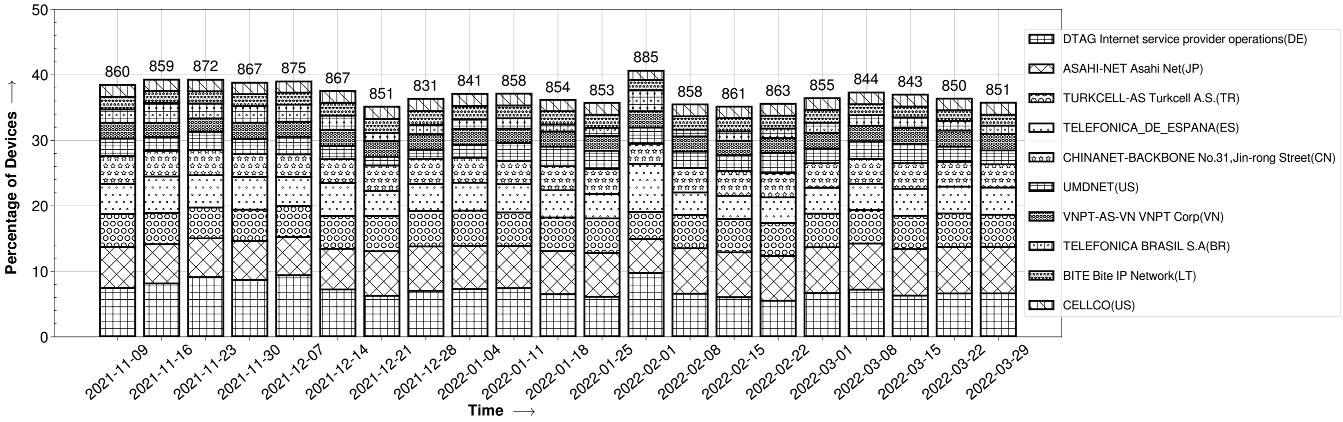

Figure 4: **Siemens S7:** Variation in the number of vulnerable hosts in top 10 ASes starting Nov 9, 2021

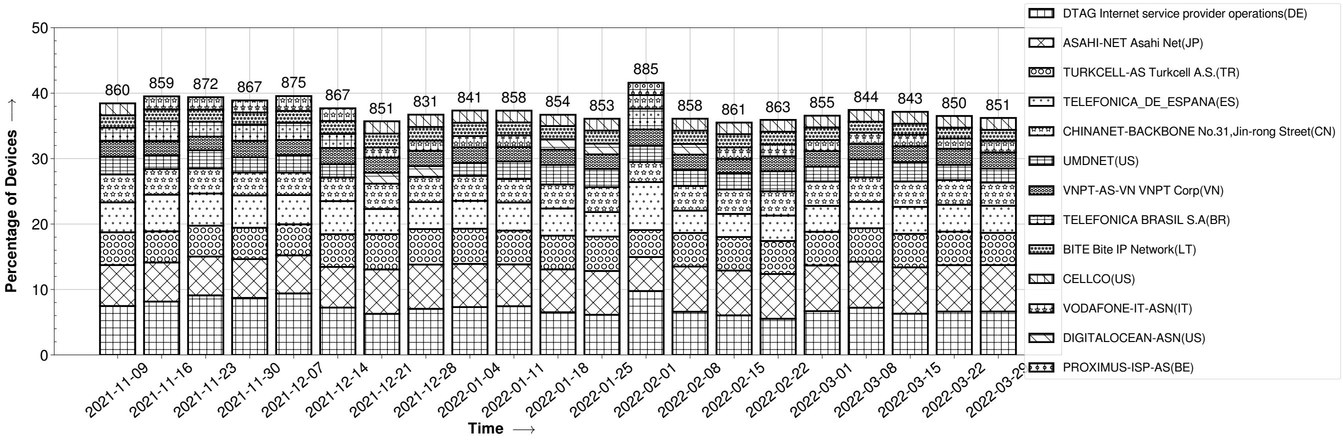

Figure 5: **Siemens S7:** Top 10 contributing ASes on each week starting Nov 9, 2021

ASes stayed for a short time and contributed very little to the overall count. Nevertheless, we ultimately found that there was a substantial increase in the number of vulnerable hosts in several existing ASes, resulting in an overall increase. We present our findings for the Siemens S7 protocol in Figure 4 and Figure 5. We observed similar behavior for all other services as well. We do not know the exact reason behind this abnormal behavior.

**Vulnerable host population in /24 subnets:** Based on September 2022 scan data, we categorized vulnerable devices based on their /24 subnets and found the following number of /24 subnets for each of the five ICS services: 21609 for Modbus, 864 for DNP3, 5267 for S7, 17482 for FOX, and 10724 for BACnet, as shown in Figure 6. We observed that for all of these services, around 80% of /24 subnets contained at most 1-2 devices. Additionally, the maximum number of devices seen in a /24 subnet was about 85 for Modbus service. This suggests that /24 subnets for ICS services are not densely populated with only those services. It aligns with the Purdue model, which assumes that devices in the control zone mostly run these services. The device count for /24 subnets would have been higher if enterprise zone devices were included in the analysis.

## 4.2 Geographical distribution

In this, we aim to study the geographic distribution of vulnerable hosts for target ICS services. To do so, we employ geo-location techniques to determine the locations of these hosts for each ICS service. The top 20 countries hosting vulnerable devices for each service are presented in Figure 7 as of September 2022. Our analysis reveals that the United States has the highest concentration of vulnerable devices, particularly concerning FOX, BACnet, and DNP3 services. However, the data also suggest that other countries hosting significant numbers of vulnerable devices for Modbus and S7 services are also vulnerable to potential attacks.

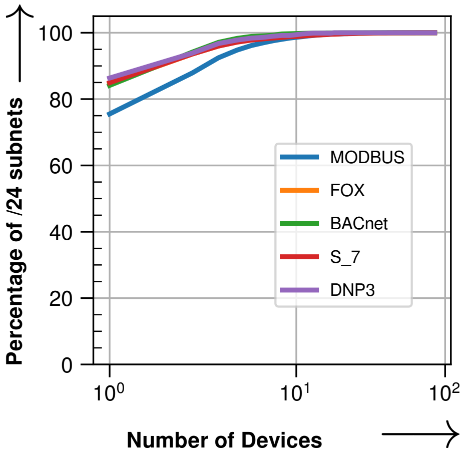

Figure 6: **Device distribution in /24 subnets**: <*y-axis*>: percentage of /24 subnets with the atmost <*x-axis*> number of devices

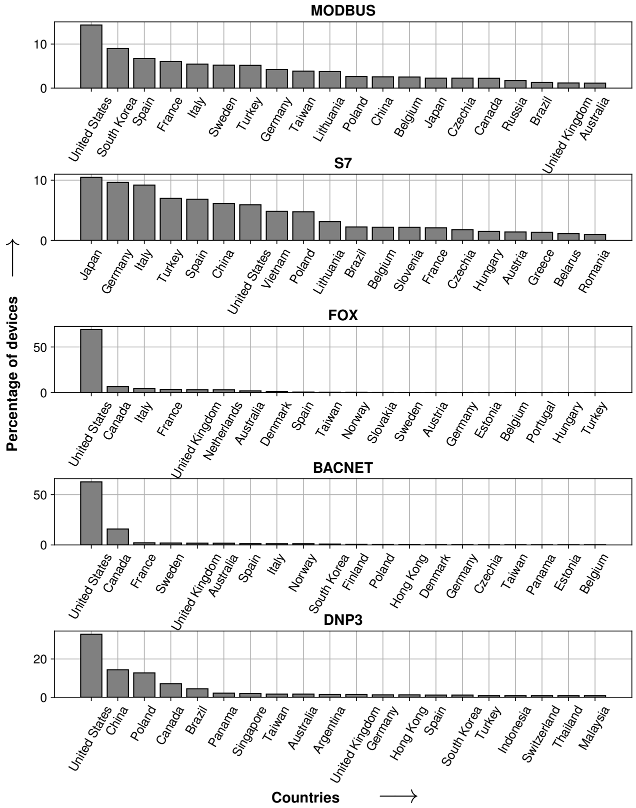

Figure 7: Geographical distribution of vulnerable hosts running ICS communication protocols

## 4.3 Port Distribution

In this section, we aim to provide the distribution of ports used by ICS devices. We first pivot the devices that use a particular ICS communication protocol and then check the ports on each device that run some services. It should be noted that we do not look for open ports but rather consider ports that respond to handshake requests. For each service, we aggregate the number of devices using each port. We consider the top 20 ports for each ICS protocol and report it in Figure 8. Additionally, to better understand the co-location of ICS services, we also report the count for ports corresponding to targeted service ports separately if they are not among the top 20. We notice several devices run some other service on ports corresponding to ICS services.

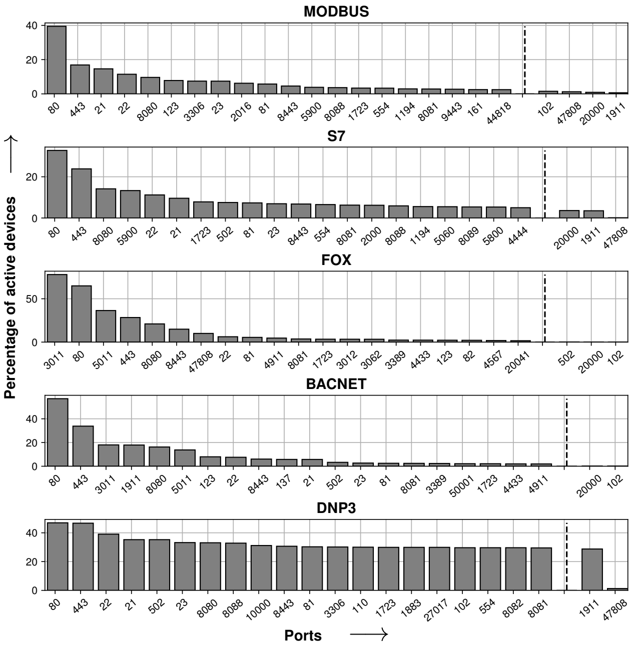

Figure 8: Port distribution of SCADA devices

For better understanding, we took the most common top 200 ports for each service and found that only 59 ports were common among them, with a union of 456 ports among the top 200 of each service. To further understand the distribution, we looked at whether or not different ports consistently host the same services across all responding devices. However, we found that the same port is often used to host different services across devices. We report the measurement results for each service in Table 2.

It can be seen that a significant number of ports run different services across different devices. It shows heterogeneity in the device configuration.

# 5 Future Work

1. **Better classification of vulnerable devices according to Purdue Model:** Currently, we have identified all the vulnerable devices running these ICS protocols. How-

| Services | Modbus | S7 | BACnet | FOX | DNP3 |
|---|---|---|---|---|---|
| 1 | 88.6% | 25.2% | 93.1% | 88.2% | 72.19% |
| 2 | 8.49% | 55.1% | 5.8% | 10.4% | 22.41% |
| 3 | 2.3% | 18.6% | 0.8% | 1.14% | 4.3% |
| 4 | 0.4% | 1.1% | 0.2% | 0.19% | 1.02% |
| 5 | 0.1% | 0.02% | 0.04% | 0.02% | 0.01% |
| 6 | 0.04% | 0.006% | 0.03% | - | 0.003% |
| 7 | 0.01% | - | - | - | - |
| 8 | 0.01% | - | - | - | - |

Table 2: Number of services vs Percentage of ports

ever, this does not provide sufficient information about the hierarchical structure of a typical network. Previous attacks have demonstrated that gaining access to higher-level devices can have much more severe consequences than accessing lower-level ones, due to the master-slave architecture of these underlying communication protocols. As part of our preliminary results, we have identified several services that these devices run on simultaneously with ICS services, which we believe can be used to perform this classification. We provide brief details about some services that could be helpful in doing this classification as follows:

| Port | IANA assigned service |
|---|---|
| 88 | Kerberos |
| 2077 | Old Tivoli Storage Manager |
| 1270 | Microsoft Operations Manager |
| 7443 | Oracle Application Server |
| 8800 | Sun Web Server Admin Service |
| 9008 | Open Grid Services Server |
| 12345 | italk chat system |
| 16000 | Administration server access |
| 19998 | IEC 60870-5-104 process control |
| 16003 | Automation and Control by REGULANE.ORG |
| 9001 | ETL Service Manager |
| 8230 | RexecJ Server |
| 3306 | MYSQL |
| 2455 | WAGO-IO-SYSTEM |
| 2078 | IBM Total Productivity Center Server |

Table 3: Suspicious services for a better breakdown of devices in layers

2. **Variability among scanners:** In this work, we have used the Censys scanner for our experimentation. However, we believe that it would be beneficial to compare our current measurement results with those of other well-known scanners such as Shodan. This would not only help us evaluate these scanners, but also provide better insights into Industrial Control Systems (ICS). Previous research, such as [9], has shown that these scanners operate differently and have different scanning strategies.

3. **Identifying the scanning agents:** As shown in [26], several public, private, and malicious agents also periodically scan for Industrial Control System (ICS) services, in addition to traditional network scanners. The authors [26] showed this scanning behavior for 2016. However, we believe that the situation has changed since then, as more ICS devices are now in operation, which has increased the scope of potential threats. Therefore, we want to understand the current scenario of potential scanners for ICS services.

# 6 Conclusion

Industrial control systems (ICS) are critical infrastructure components that are responsible for the automation and control of industrial processes. However, these systems are often vulnerable to attacks, which can have severe consequences such as the disruption of critical services and the loss of sensitive data. In this work, we broadly identify vulnerable hosts corresponding to five well-known ICS communication protocols. These protocols lack basic security features such as authentication, encryption, etc. Overall, our research provides important insights into the vulnerability of ICS networks and highlights the need for improved security measures to protect against potential attacks. We believe that our work can help to raise awareness of these issues and inform the development of effective countermeasures for securing ICS networks.

# 7 Acknowledgements

The authors would like to express their gratitude to the entire Censys team [2] for generously providing access to their scanning database for our research. The data and insights obtained from Censys were essential for our study, and we are grateful for their support and cooperation. We would also like to thank Saman Zonouz, Paul Pearce, and Abhishek Vasisht Bhaskar for their helpful feedback. Their expertise, guidance, and resources were invaluable for this project.

# References

[1] Apt cyber tools targeting ics/scada devices. `https://www.cisa.gov/uscert/ncas/alerts/aa22-103a`. Accessed: 2022-12-13.

[2] Censys. `https://www.shodan.io/`. Accessed: 2022-12-13.

[3] Censys. `https://github.com/zmap/zgrab2`. Accessed: 2022-12-13.

[4] Niagaraax networking and it guide. `https://www.lynxspring.com/documents/AX_Networking_IT_Guide.pdf`. Accessed: 2022-12-13.

[5] Shodan search engine. `https://www.shodan.io/`. Accessed: 2022-12-13.

[6] Alladi, T., Chamola, V., and Zeadally, S. Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications 155* (2020), 1–8.

[7] Bagaria, S., Prabhakar, S. B., and Saquib, Z. Flexi-dnp3: Flexible distributed network protocol version 3 (dnp3) for scada security. In *2011 International Conference on Recent Trends in Information Systems* (2011), IEEE, pp. 293–296.

[8] Barbieri, G., Conti, M., Tippenhauer, N. O., and Turrin, F. Assessing the use of insecure ics protocols via ixp network traffic analysis. In *2021 International Conference on Computer Communications and Networks (ICCCN)* (2021), IEEE, pp. 1–9.

[9] Bennett, C., Abdou, A., and van Oorschot, P. C. Empirical scanning analysis of censys and shodan. In *apresentado na Workshop on Measurements, Attacks, and Defenses for the Web, Virtual* (2021).

[10] Bernieri, G., Cecconello, S., Conti, M., and Lain, G. Tambus: A novel authentication method through covert channels for securing industrial networks. *Computer Networks 183* (2020), 107583.

[11] Chen, B., Pattanaik, N., Goulart, A., Butler-Purry, K. L., and Kundur, D. Implementing attacks for modbus/tcp protocol in a real-time cyber physical system test bed. In *2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)* (2015), IEEE, pp. 1–6.

[12] Chen, Y., Lian, X., Yu, D., Lv, S., Hao, S., and Ma, Y. Exploring shodan from the perspective of industrial control systems. *IEEE Access 8* (2020), 75359–75369.

[13] Conti, M., Donadel, D., and Turrin, F. A survey on industrial control system testbeds and datasets for security research. *IEEE Communications Surveys & Tutorials 23*, 4 (2021), 2248–2294.

[14] Darwish, I., and Saadawi, T. Attack detection and mitigation techniques in industrial control system-smart grid dnp3. In *2018 1st International Conference on Data Intelligence and Security (ICDIS)* (2018), IEEE, pp. 131–134.

[15] Durumeric, Z., Adrian, D., Mirian, A., Bailey, M., and Halderman, J. A. A search engine backed by internet-wide scanning. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (2015), pp. 542–553.

[16] East, S., Butts, J., Papa, M., and Shenoi, S. A taxonomy of attacks on the dnp3 protocol. In *International Conference on Critical Infrastructure Protection* (2009), Springer, pp. 67–81.

[17] Erkek, I., and Irmak, E. Cyber security of internet connected ics/scada devices and services. In *2021 International Conference on Information Security and Cryptology (ISCTURKEY)* (2021), pp. 75–80.

[18] Farwell, J. P., and Rohozinski, R. Stuxnet and the future of cyber war. *Survival 53*, 1 (2011), 23–40.

[19] Geng, Y., Wang, Y., Liu, W., Wei, Q., Liu, K., and Wu, H. A survey of industrial control system testbeds. In *IOP Conference Series: Materials Science and Engineering* (2019), vol. 569, IOP Publishing, p. 042030.

[20] Ghosh, S., and Sampalli, S. A survey of security in scada networks: Current issues and future challenges. *IEEE Access 7* (2019), 135812–135831.

[21] Kaur, J., Tonejc, J., Wendzel, S., and Meier, M. Securing bacnet's pitfalls. In *IFIP International Information Security and Privacy Conference* (2015), Springer, pp. 616–629.

[22] Kleinman, A., and Wool, A. Accurate modeling of the siemens s7 scada protocol for intrusion detection and digital forensics. *The Journal of Digital Forensics, Security and Law: JDFSL 9*, 2 (2014), 37.

[23] Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., and Halgand, Y. A survey of approaches combining safety and security for industrial control systems. *Reliability engineering & system safety 139* (2015), 156–178.

[24] Lei, C., Donghong, L., and Liang, M. The spear to break the security wall of s7commplus. *Blackhat USA* (2017).

[25] Majdalawieh, M., Parisi-Presicce, F., and Wijesekera, D. Dnpsec: Distributed network protocol version 3 (dnp3) security framework. In *Advances in Computer, Information, and Systems Sciences, and Engineering*. Springer, 2007, pp. 227–234.

[26] Mirian, A., Ma, Z., Adrian, D., Tischer, M., Chuenchujit, T., Yardley, T., Berthier, R., Mason, J., Durumeric, Z., Halderman, J. A., et al. An internet-wide view of ics devices. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)* (2016), IEEE, pp. 96–103.

[27] Nicholson, A., Webber, S., Dyer, S., Patel, T., and Janicke, H. Scada security in the light of cyber-warfare. *Computers & Security 31*, 4 (2012), 418–436.

[28] Obregon, L. Sans institute information security reading room secure architecture for industrial control systems.

[29] Orebaugh, A., and Pinkard, B. *Nmap in the enterprise: your guide to network scanning*. Elsevier, 2011.

[30] Pliatsios, D., Sarigiannidis, P., Lagkas, T., and Sarigiannidis, A. G. A survey on scada systems: secure protocols, incidents, threats and tactics. *IEEE Communications Surveys & Tutorials 22*, 3 (2020), 1942–1976.

[31] Ranathunga, D., Roughan, M., Nguyen, H., Kernick, P., and Falkner, N. Case studies of scada firewall configurations and the implications for best practices. *IEEE Transactions on Network and Service Management 13*, 4 (2016), 871–884.

[32] Shahzad, A., Lee, M., Lee, Y.-K., Kim, S., Xiong, N., Choi, J.-Y., and Cho, Y. Real time modbus transmissions and cryptography security designs and enhancements of protocol sensitive information. *Symmetry 7*, 3 (2015), 1176–1210.

[33] Slay, J., and Miller, M. Lessons learned from the maroochy water breach. In *International conference on critical infrastructure protection* (2007), Springer, pp. 73–82.

[34] Stouffer, K., Falco, J., Scarfone, K., et al. Guide to industrial control systems (ics) security. *NIST special publication 800*, 82 (2011), 16–16.

[35] Swales, A., et al. Open modbus/tcp specification. *Schneider Electric 29* (1999), 3–19.

[36] Upadhyay, D., and Sampalli, S. Scada (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security 89* (2020), 101666.

[37] Wendzel, S., Tonejc, J., Kaur, J., Kobekova, A., Song, H., Fink, G., and Jeschke, S. *Cyber security of smart buildings*. Wiley, 2017.

[38] Xu, W., Tao, Y., and Guan, X. The landscape of industrial control systems (ics) devices on the internet. In *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* (2018), pp. 1–8.