KTH ROYAL INSTITUTE
OF TECHNOLOGY

Degree Project in Computer Science and Engineering

First cycle 15 credits

Vulnerabilities in Swedish Industrial Control Systems

An examination and classification of remotely discoverable ICS devices in Sweden, and an assessment of their vulnerability to cyber attacks

NILS ODIN

ANDRÉ ÖSTERLUND

Stockholm, Sweden 2022

Vulnerabilities in Swedish Industrial Control Systems

An examination and classification of remotely discoverable ICS devices in Sweden, and an assessment of their vulnerability to cyber attacks

ANDRÉ ÖSTERLUND

NILS ODIN

Degree Project in Computer Science and Engineering, First Cycle 15 credits
Date: June 8, 2022
Supervisor: Robert Lagerström
Examiner: Pawel Herman
Swedish title: Sårbarheter i svenska industriella styrsystem
School of Electrical Engineering and Computer Science

Abstract

Over the last couple of years, more and more industrial control systems (ICS) have been designed to be connected to the internet to allow for remote control and monitoring of industrial processes. This have opened a possibility for hackers to exploit weaknesses in such systems remotely through the internet. Such exploits could allow an attacker to steal sensitive information, make the system inaccessible, or even take control of critical infrastructure. It is therefore of great importance to know how easily these systems can be found on the internet and how vulnerable found devices would be to remote attacks. Learning these things have been the goal of this report.

To accomplish this goal, we have sorted through every Swedish IP address on the IPv4 internet for services that run on ports and through protocols associated with known ICS devices. We fetched data about these IP addresses via the Shodan project and examined that data to determine how many ICS devices are in operation in Sweden, as well as the device models and manufacturers. Lastly, we cross-checked our list of found devices with the CVE database of publicly disclosed software vulnerabilities to learn how many of the devices had known exploits that could be used in an attack.

Our findings are that there exist 2,237 Swedish ICS devices that can be easily found through the internet. Out of these, 244 devices had at least one known vulnerability. Most vulnerable devices had more than one known vulnerability, and about 77% had at least one exploit that was of medium, high, or critical severity as per the Common Vulnerability Scoring System. The oldest critical vulnerability found was publicly disclosed in 2011, meaning that some ICS devices in Sweden has been running with critical vulnerabilities for over 12 years.

Our research shows that a significant number of Swedish industrial control systems run with unpatched vulnerabilities. This means that even an inexperienced attacker could perform targeted attacks against vulnerable Swedish systems from anywhere on the globe. Since we were unable to determine what kind of industrial processes are controlled by these ICS devices, we don’t know how damaging such an attack would be. However, since these devices can be part of the operation of critical infrastructure it is crucial that effort is made to minimize the vulnerabilities in these systems.

We hope that our research motivates ICS operators and manufacturers to assess how vulnerable their systems are to these kinds of attacks, and that they implement strategies to minimize that vulnerability.

Sammanfattning

Under de senaste åren har allt fler industriella styrsystem (eng. Industrial Control System eller ICS) designats för att anslutas till internet i syfte att möjliggöra fjärrstyrning samt fjärrövervakning av industriella processer. Detta har dock öppnat upp en möjlighet för hackare att utnyttja svagheter i sådana system via internet. Sådana utnyttjanden kan tillåta en angripare att stjäla känslig information, göra systemet otillgängligt eller till och med ta kontroll över kritisk infrastruktur. Det är därför av stor vikt att veta hur lätt dessa system kan hittas på internet och hur sårbara dessa enheter skulle vara för fjärrattacker. Att utreda detta har varit målet med denna rapport.

För att uppnå detta mål har vi undersökt varje svensk IP-adress på IPv4-internet för tjänster som körs på portar och genom protokoll kopplade till kända ICS-enheter. Vi hämtade data om dessa IP-adresser via Shodan-projektet och undersökte denna data för att fastställa hur många ICS-enheter som är i drift i Sverige, samt specifika enhetsmodeller och tillverkare. Slutligen jämförde vi vår lista över hittade enheter med CVE-databasen som tillhandahåller offentligt kända mjukvarusårbarheter för att ta reda på hur många av enheterna som hade kända sårbarheter som kunde användas i en attack.

Våra resultat visar att det finns 2 237 svenska ICS-enheter som lätt kan hittas via internet. Av dessa hade 244 enheter minst en känd sårbarhet. De sårbara enheterna hade oftast mer än en känd sårbarhet, och cirka 77 % hade minst en sårbarhet som var av medelhög, hög eller kritisk svårighetsgrad enligt branschstandarden Common Vulnerability Scoring System. Den äldsta kritiska sårbarheten som hittades offentliggjordes 2011, vilket innebär att vissa ICS-enheter i Sverige har körts med kritiska sårbarheter i över 12 år.

Vår forskning visar att ett betydande antal svenska industriella styrsystem i dagsläget körs med offentligt kända sårbarheter. Det betyder att även en oerfaren angripare skulle kunna utföra riktade attacker mot sårbara svenska system från var som helst i världen. Eftersom vi inte kunde avgöra vilken typ av industriella processer som styrs av dessa ICS-enheter, vet vi heller inte hur skadlig en sådan attack skulle vara. Men eftersom dessa enheter kan vara en del av driften av kritisk infrastruktur är det mycket viktigt att ansträngningar görs för att minimera sårbarheterna i dessa system.

Vi hoppas att vår forskning motiverar ICS-operatörer samt tillverkare att granska hur sårbara deras system är för den här typen av attacker och att de implementerar strategier för att minimera skadan eventuella angrepp kan medföra.

Contents

1 Introduction **6**

1.1 Research motivation 6

1.2 Background 7

1.3 Problem Statement 8

1.4 Report Structure 9

1.5 Delimitations 9

2 Literature Study for Internet Scanning **11**

2.1 Different Scanning Tools 11

2.2 Search Methodology 14

2.3 Device Metadata 15

3 IP Fetching and Device Classification **16**

3.1 Method of Classifying ICS Devices 16

3.2 Example of Shodan Metadata 16

3.3 Findings 18

3.3.1 Found ICS Products 18

3.3.2 Found ICS manufacturers 19

3.3.3 Organizations Operating ICS Devices 19

4 Assessing ICS Device Vulnerabilities **21**

4.1 Vulnerabilities Background 21

4.2 Classification of Device Vulnerabilities 22

4.3 Findings 22

4.4 Found CVEs 27

5 Conclusions and Discussion **33**

5.1 Conclusions 33

5.2 Measures for Protection 33

5.3 Further Research 34

***6* Appendices** **36**

6.1 Appendix A – Port Numbers and Protocols 36

6.2 Appendix B - Classified Products 37

6.3 Appendix C - Classified Manufacturers 40

6.4 Appendix D - Autonomous Systems 42

1 Introduction

1.1 Research motivation

ICS (Industrial Control System) devices are a kind of dedicated control units that manage or oversee many kinds of industrial systems and processes. An example could be a machine that controls the flow valves of a sewage processing facility, or a machine that controls the ventilation systems of a factory. Such devices exist to allow engineers to easily monitor and control complex systems, which makes industry safer and more effective. Over the last years, more and more of these devices have been designed to be connected to the internet to allow remote monitoring and control of their operation. This is especially useful for industry that is far from where humans are, such as wind turbines placed in oceans. However, when ICS devices are connected to the internet, then anyone on the internet can attempt to connect to that device. This means that these ICS devices need to be secure to stop hackers or unauthorized users from connecting and steal information or take control of infrastructure. Figure 1.1 shows this evolution from early ICS devices controlled directly by engineers to the modern internet-connected devices which opens for hackers to connect as well.

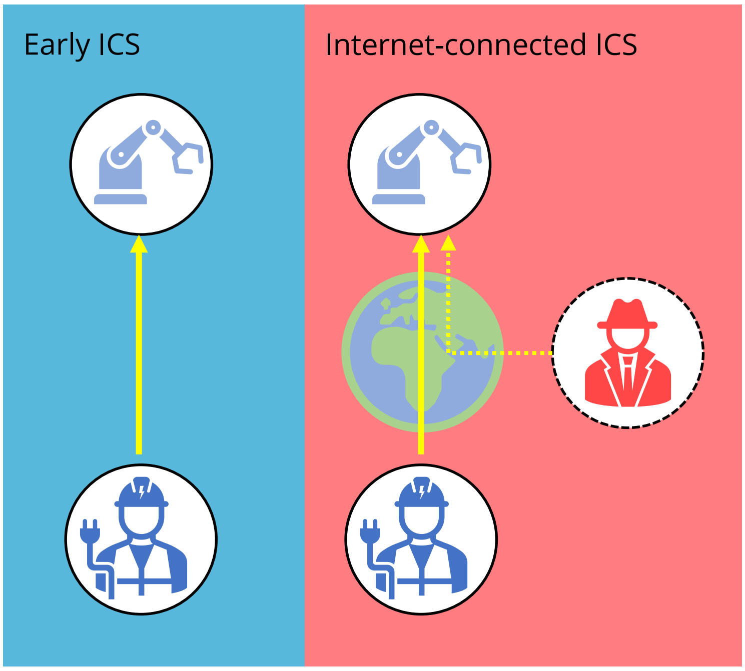


Figure 1.1: Evolution of how ICS devices are controlled and the risks of internet attacks

Because ICS devices control all kinds of infrastructural processes, attacks against these devices could lead to damage or unavailability of infrastructure that is needed to keep society functioning. For example, disruption of powerplants could lead to both huge economic damage but also loss of human lives.

Making sure that ICS devices are kept as secure as possible is therefore very important, and thus the motivation for this research. The goal of the report is to find all Swedish ICS devices that can easily be found on the internet and assess how vulnerable they would be to attacks through the internet.

1.2 Background

Operational technology (OT) is a collective term which commonly refers to "hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events." [1] OTs were initially disconnected both logically and physically from other operations, but in our connected world of today, it is hard to find OTs which are not connected to the internet in some way, since a major benefit of using them is the capability to remotely control the associated systems. However, there is an obvious risk in having essential infrastructures connected to the internet, namely different kind of cyberattacks. A large subset of OT consists of Industrial Control Systems (ICS), which are generally systems that control and oversee industrial processes. In turn, SCADA (Supervisory Control and Data Acquisition) devices is a subset of ICS, whose main purpose is supervision of systems traversing larger geographical areas, for example in nationwide gas pipelines in contrast to ICS devices placed in a single plant or factory, with local supervision in mind. ICS devices have a wide range of use, and control much of the critical infrastructure that regular people depend on every day, such as:

- Power plants and power distribution
- Water treatment and sewage facilities
- Factories and manufacturing facilities
- Transportation infrastructure
- Communication infrastructure

Disruptions in these systems may cause serious consequences, both in terms of material loss but also in terms of human loss. It is therefore highly important that ICS devices are set up in such a way that the chance of partial or complete failure is minimized. The isolated nature of older ICS devices naturally made general cyber security a non-issue, since there was no way for an attacker to gain remote access to the system. This is certainly not true today, with recent research indicating that close to 40% of worldwide ICS devices has been targeted with malicious intents in 2021 alone [2]. The main source of the threats was unsurprisingly through internet connected devices, which further highlights the importance of cyber security, especially since many ICS devices are connected to such critical infrastructure.

Some recent noteworthy examples of times where security has been insufficient includes a 2021 ransomware attack on the Colonial Pipeline, the largest pipeline system for petroleum in the United States, which halted operations for almost a week until the system could be restarted and required payment of a ransom of $4.4 million paid in Bitcoin [3]. Later that month, the world's largest meat processing company, Brazilian JBS S.A., disabled all servers supporting OT after another ransomware attack, and practically shut down beef production across North America for three days. Even though the outage only lasted a couple days, the disruption significantly impacted the supply chain and meat industry overall [4].

Another example was a 2015 attack on the Ukraine power grid attributed to a Russian hacking group, which left hundreds of thousands of people without electricity for up to six hours [5].

Although these examples may not appear to have been directly life threatening, it is not hard to imagine what severe consequences may arise if food, water, or electricity supply were to be completely cut off for an extended period of time, for a society largely dependent on these automated services.

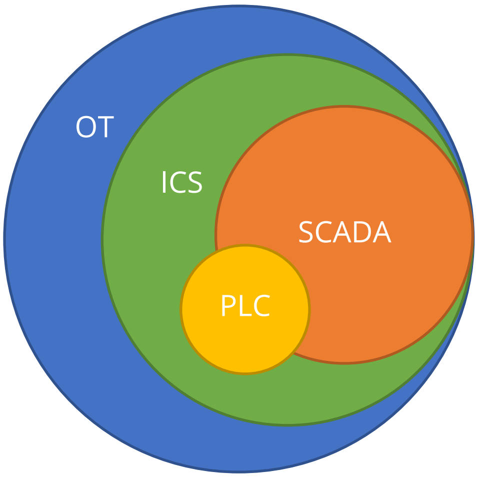


Figure 1.2: How different operational technology terms relate to each other

1.3 Problem Statement

While departments of the Swedish government have acknowledged the need for increased security of ICS devices in public documents [6], we could find no previous research that aimed to chart the number and types of ICS devices in Sweden. We were also unable to find assessments of how vulnerable Swedish ICS devices would be to cyber-attacks. In fact, such research has been hard to find even when looking internationally. One major study has been made in the Netherlands [7], but we were unable to find studies for other European countries. Because no data exists on which ICS devices are present in Sweden and on how vulnerable they are, this report aims to answer these questions using the following problem statements:

- **How many ICS devices located in Sweden can be easily found online by potential attackers?**
- **How many of these devices are potentially vulnerable to cyber-attacks?**

1.4 Report Structure

Because no previous data existed that charted Swedish ICS devices, the report needed to be conducted in several steps. First a literature study was conducted to find ICS device identifiers, such as most used ports and protocols, as well as which existing tools could be used to collect information about IP addresses with these identifiers. Then, data about IP addresses matching these features was collected. After that, the data was parsed to separate ICS devices from other services that merely operated using the same features, as well as classified to specific models and manufacturers. Lastly, the found ICS devices was examined for known vulnerabilities. Each of these steps are explained in detail in their appropriate chapter, both regarding methodology and results. We conclude the report with a chapter discussing our findings. An illustration of this report structure is found in Figure 1.3.

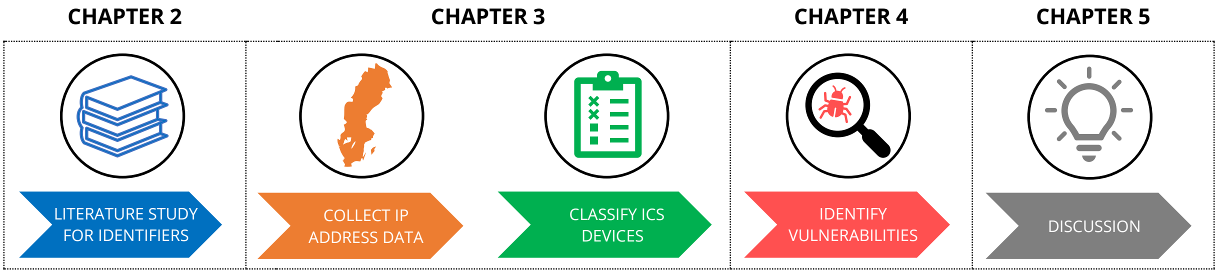


Figure 1.3: Report structure

1.5 Delimitations

Because the subject of ICS security is so broad and complex, and because our research had limited time and resources, we had to be selective with what we examined. This section highlights some aspects that are not covered by this report because they proved to be difficult from a technical, ethical, or legal standpoint.

- We chose to not perform port scanning of IP addresses ourselves. The main reason for this is that several established port scanning projects already exists, and our results is not dependent on us conducting the port scanning ourselves. In addition to this, even basic port scanning on a system without the explicit consent of the system's owner might be considered as an attack and have potential legal implications. Very simplified, it could be somewhat comparable to surveying physical street addresses by looking for unlocked doors. There is also an ethical consideration in that some ICS devices respond to an attempted port connection by rebooting which could lead to disruption of service on critical systems, such as those controlling hospital equipment. The implication of this decision is that our results are dependent on the validity of the dataset we have acquired from an already existing port scanning project.

- We chose to not consider ICS devices located on the IP address version 6 (IPv6) network. As far as we can tell, there currently exists no effective way of scanning the entire IPv6 address space within a reasonable timeframe. The IPv6 network has roughly 340 trillion trillion trillion unique addresses (2^{128}), which is about one million billion times more than the estimated number of stars that exist in the universe. Scanning that many IP addresses would take more than twenty-five billion billion centuries, which is beyond the scope of this report. Since there may be ICS devices operating on IPv6, this means that there could exist devices out of reach for our research.

- When determining potential vulnerabilities of the found devices, we used a public list of known vulnerabilities and exposures provided by The National Institute of Standards and Technology. To the best of our knowledge, this is the world's most complete and accurate list of known vulnerabilities in devices and software. However, there can still exist exploits not yet known or catalogued, such as zero-day exploits. Also, since The National Institute of Standards and Technology is an organization belonging to the United States Department of Commerce there is a possibility that data related to American devices take higher priority, and thus is more extensive and/or of higher quality than data about European devices. The implication of this is that there may exist more vulnerabilities in European made devices than those presented in this report.

2 Literature Study for Internet Scanning

2.1 Different Scanning Tools

An IPv4 address consists of thirty-two bits, i.e. 32 ones or zeroes. This means that there are 2^{32} IPv4 addresses, which amounts to roughly 4.3 billion unique addresses. Therefore, we need to use automated tools to scan the internet for connected ICS devices. There are several tools available, with three the most well-known listed in Table 2.1.

	Scanning tool	**Internet wide scan time**	**Reference**
1	Nmap	A few weeks	Lyon [21]
2	Zmap	Around one hour	Durumeric et al [22]
3	Masscan	Around 5 minutes	Graham [23]

Table 2.1: Common port scanning tools

One of the most well-known port scanning tools is Nmap (short for *Network Mapper*) which was released in 1997 and can scan the entire internet in a few weeks. While Nmap is the most well-known and established port scanning tool, its primary use is for thorough analysis of short ranges of IP addresses. Zmap was built by researchers at the University of Michigan in 2013 and used less overhead by using a stateless scanning method, improving its speed by more than 1,000 times compared to Nmap. This lets Zmap scan the entire IPv4 address space in about an hour, if only a single port is targeted. Masscan claims to be able to scan the entire internet in under five minutes from a single computer, given that it has sufficiently large bandwidth.

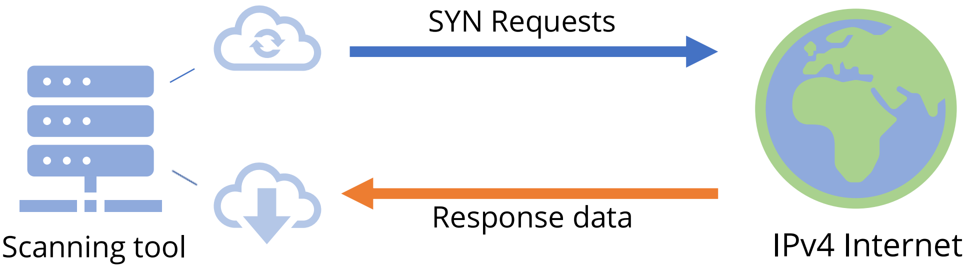


Figure 2.1: Example of full IPv4 network scan

For this project we decided to not use any port scanning tool ourselves. The reason for this is that there already exist several projects that scan the entire internet on a weekly basis. This was done to avoid the ethical gray area of generating unnecessary network traffic to potentially vulnerable devices [24] as well as the potential legal issues that may arise since port scanning without the owner's explicit consent can sometimes be considered an attempt of a cyberattack.

Three of the most established port scanning projects are Shodan, Censys, and ZoomEye. According to Shodan's website, Shodan is the world's first search engine for internet connected devices. The port scanning project examines all internet connected devices for information, and stores it on their servers, enabling users to query the database based on criteria's such as geo-location, the ISP provider, user provided key words, port numbers et cetera.
Censys is a very similar port scanning project, which regularly probes all public IP addresses and stores the metadata in a searchable database.
ZoomEye describes themselves as "the leader of global cyberspace mapping, China's first and world-renowned cyberspace search engine ... Through a large number of global surveying and mapping nodes, according to the global IPv4, IPv6 address and website domain name databases, it can continuously scan and identify multiple service port and protocols 24 hours a day, and finally map the whole or local cyberspace." [25]

When deciding what port scanning project or combination of different projects would best suit our needs, we conducted a brief literature study to examine the functionality and extent of different search engines, primarily with regards to results geo-located in Sweden. Since the three aforementioned projects appeared to be the most widespread implementations, we directed our focus to them. ZoomEye returned the most results overall with 15.8 million hits, compared to 2.5 million and 1.3 million for Shodan and Censys respectively. However, since we are only interested in some specific type of devices, the total number of search results is not necessarily of great interest for us. Further, ZoomEye sometimes returned historical data as well, leading to duplicate results which made it unclear what results were relevant. ZoomEye did not offer any student accounts or free pricing tiers that allowed downloading the results. Since we lacked funding, this ultimately made ZoomEye infeasible for this report.

We investigated support of some of the most common protocols related to ICS and SCADA devices from Shodan and Censys and compiled the result in Table 2.2. The results are based on protocols explicitly stated as supported by Censys [18], and by manual labor on Shodan, since Shodan seemingly do not provide a complete list of supported protocols covered by their search engine [19].

Protocol	*Shodan*	*Censys*
ATG		Yes
BACnet	Yes	Yes
CITRIX		Yes
CODESYS	Yes	Yes
DIGI	Yes	Yes
DNP3	Yes	Yes
EtherNet/IP	Yes	Yes
GE-SRTP	Yes	Yes
HART	Yes	Yes
IEC 60870-5-104	Yes	Yes
MELSEC-Q	Yes	
Modbus	Yes	Yes
OMRON FINS	Yes	Yes
PCWorx	Yes	Yes
ProConOS	Yes	Yes
Red Lion	Yes	
Siemens S7	Yes	Yes
Tridium Fox	Yes	Yes
WDBRPC		Yes

Table 2.2: Comparison of ICS protocol support provided by Shodan versus Censys

As shown, both services support a similar number of relevant protocols, with arguably the most important protocols supported by both. We also sampled the quality of results by querying a subset of our list of search terms and found that the set of relevant results from Shodan was a superset of the results from Censys. This in combination with that the total search results geo-located in Sweden was almost doubled from Shodan compared to Censys, helped us deem Shodan the best tool for our purposes.

A disadvantage with Shodan was their priced tiers of access. Ideally, we would have preferred an enterprise subscription that would give us an unlimited number of searches, but that was outside the budget for this report. This subscription would have made it possible to download data for every single searchable internet connected device located in Sweden to filter possible ICS devices from. With our accounts, we were limited to downloading around 100,000 search results for the duration of this project. However, previous studies imply that there are less than 5,000 ICS devices in Sweden [10], making it possible to gather data from an overwhelming majority of the available devices with well manufactured search terms.

2.2 Search Methodology

Due to the sheer volume of IP addresses assigned in Sweden, which exceeds 30 million [8], some sort of automated tool was necessary to help us gather our desired data. In the forthcoming sections we explain our decisions more in-depth, but the main source of our data was collected with the help of Shodan [9], a port scanning project which includes a search engine for internet connected devices.

To discern potential ICS devices from other devices and services connected to the internet, we needed to gather comprehensive data regarding as many ICS models as possible, with widely used devices and manufacturers taking priority. The information most valued to us at this stage was primarily which protocols were used, and the default port initiated by the manufacturer. Although some devices allow the default port to be changed, others do not give that option, and many devices do not require the default port to be changed. For this reason, using only default ports and protocols may not be collectively exhaustive for finding every ICS device. However, it should provide us with a sufficient baseline of results to further investigate.

Our literature study of ICS identifiers consisted of several segments. We searched for relevant existing works published on Google Scholar, with keywords including combinations of the terms "ICS", "SCADA", "protocols", "port", "scan", and "discovery" [7] [11] [12] [13] [14] [15] [16] [17]. In addition to this, we referred to the manuals of some of the most common ICS devices. We also referred to lists of protocols and ports tagged as ICS-related by Censys and Shodan [18, 19], two of the most predominant IP scanning projects. We also used a list put together by the Austrian Energy CERT for the Austrian energy industry, containing search terms for Shodan specifically designed to find ICS and/or IoT devices [20].

Due to our limited time and budget, it was important to carefully select what search terms we used to make our data be as inclusive as possible while minimizing the amount of manual effort needed to sort through the dataset we were collecting.
Our complete list of search terms was a combination of the list made by the Austrian Energy CERT together with the port numbers/protocols found in the literature study. A complete list of these port numbers and protocols can be found in Appendix A.

Because any number of protocols can be running on a single port, and because a single protocol can be running on any number of ports, we cannot consider port numbers alone enough to exhaustively classify ICS devices, and thus, we decided to also investigate the collected metadata available from the active service processes on the devices in question.

2.3 Device Metadata

When an IP address is successfully connected to over the internet, the device or service located on that address sends a response message. This response message usually signals what kind of device is responding, what kind of services it provides, what software it is running, what protocols it supports, and some form of welcome message. This information provided in this response is what we call metadata. Typically, devices and services have a default response but can be changed by a system administrator. The default response is usually verbose and can contain sensitive information, such as a login screen, which can help a hacker target that system. If the system administrator has configured the device with a custom response, it can be either limited, obfuscated, or intentionally provide misinformation to make attacks harder.

In our report, we make use of this metadata in part by matching known default responses of ICS devices. The metadata available for a search result varies, and in some cases, it was possible to accurately classify a device from other given information, such as active running software, manufacturer, or simply the product name.

3 IP Fetching and Device Classification

3.1 Method of Classifying ICS Devices

Our method of classifying ICS devices contains several steps.

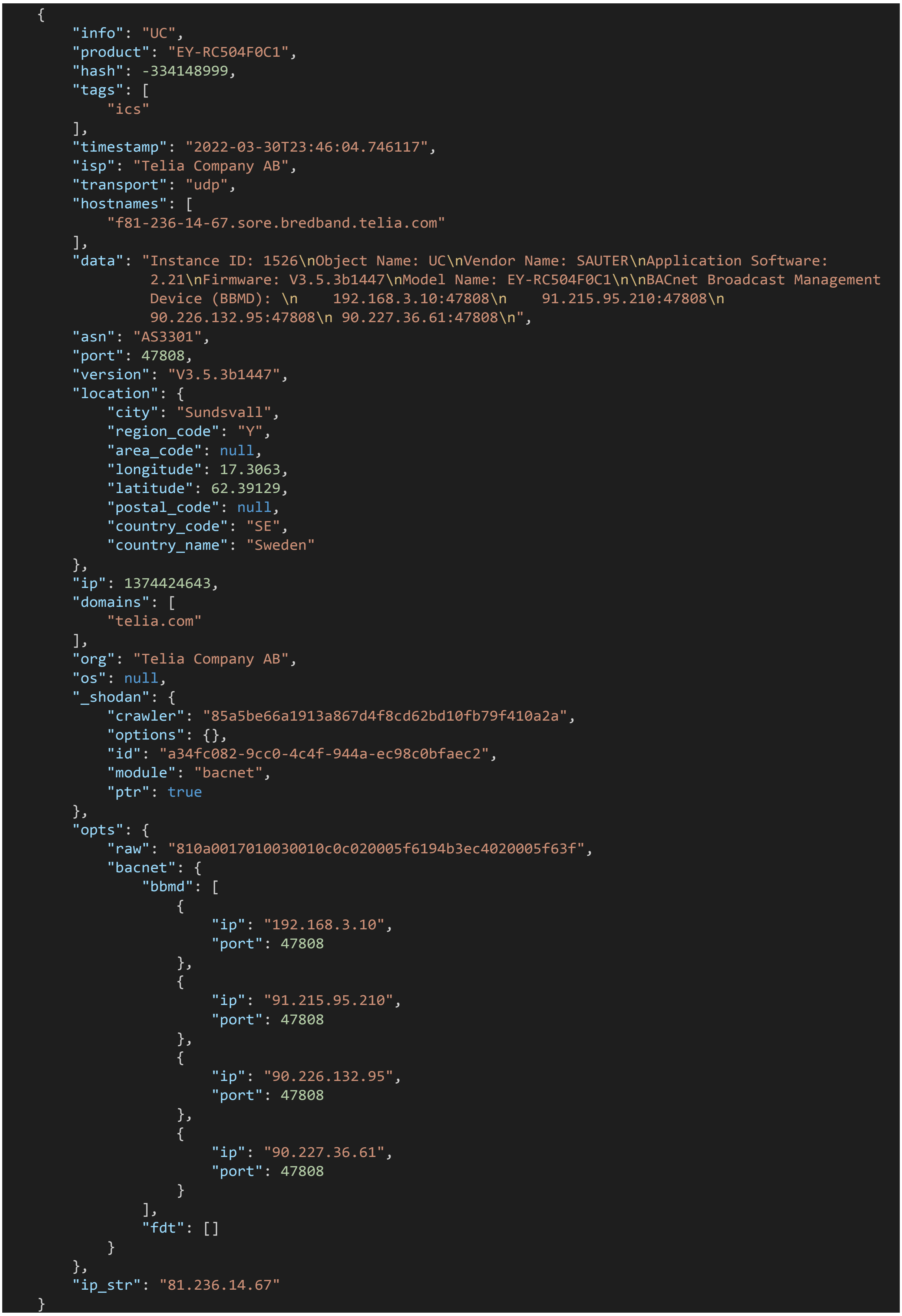
First, we use the search terms mentioned in Section 2.2 to download the metadata for all IP addresses that could contain ICS devices from Shodan. Our dataset was retrieved between the dates March 28 and March 31, 2022. In total, we downloaded information from 19,784 IP addresses located in Sweden for further analysis. Since our dataset contained some duplicate data, we removed any duplicate combinations of IP addresses and port numbers.

Second, we analyzed the Shodan metadata to find how the data from each IP address was formatted. Because each entry in our dataset was not guaranteed to contain the same banners (fields of information), we had to parse the data in a way that still gave us meaningful classifications even when entries lacked certain banners. For this problem, we ended up creating a data parser that filtered our dataset by every type of banner available to us in each entry. This meant that we could classify our results on an entry-by-entry basis. For example, if one entry had product information stored in a banner called "product", and the other had it in a banner called "data", we could still find that product information either way.

Third, we used our data parser to filter every entry in our dataset that contained either a well-known ICS protocol, a well-known ICS port number or a well-known product identifier. This left us with a list of data entries that was likely running some form of ICS device. From this list, we manually inspected each entry to determine what specific model it was. If we were unable to determine the model, we classified it as "Unknown".

3.2 Example of Shodan Metadata

The data retrieved from Shodan was in the form of Gzipped JSON-files where each row contains metadata about the retrieved IP address. The metadata is sorted into key-value pairs using banners, which each hold specific information about an aspect of the IP address. For example, the "location" banner contains information about the geographical location of IP address, while the "timestamp" banner contains information about when the data was retrieved. Some banners are always available, such as the "_shodan" banner which contains information about how Shodan found the IP address. Others, like the "mac" banner is only available if information about the mac-address of the IP addresses is available. An example of retrieved data from a single IP can be seen in Figure 3.1.



```
{
    "info": "UC",
    "product": "EY-RC504F0C1",
    "hash": -334148999,
    "tags": [
        "ics"
    ],
    "timestamp": "2022-03-30T23:46:04.746117",
    "isp": "Telia Company AB",
    "transport": "udp",
    "hostnames": [
        "f81-236-14-67.sore.bredband.telia.com"
    ],
    "data": "Instance ID: 1526\nObject Name: UC\nVendor Name: SAUTER\nApplication Software:
             2.21\nFirmware: V3.5.3b1447\nModel Name: EY-RC504F0C1\n\nBACnet Broadcast Management
             Device (BBMD): \n     192.168.3.10:47808\n     91.215.95.210:47808\n
             90.226.132.95:47808\n 90.227.36.61:47808\n",
    "asn": "AS3301",
    "port": 47808,
    "version": "V3.5.3b1447",
    "location": {
        "city": "Sundsvall",
        "region_code": "Y",
        "area_code": null,
        "longitude": 17.3063,
        "latitude": 62.39129,
        "postal_code": null,
        "country_code": "SE",
        "country_name": "Sweden"
    },
    "ip": 1374424643,
    "domains": [
        "telia.com"
    ],
    "org": "Telia Company AB",
    "os": null,
    "_shodan": {
        "crawler": "85a5be66a1913a867d4f8cd62bd10fb79f410a2a",
        "options": {},
        "id": "a34fc082-9cc0-4c4f-944a-ec98c0bfaec2",
        "module": "bacnet",
        "ptr": true
    },
    "opts": {
        "raw": "810a0017010030010c0c020005f6194b3ec4020005f63f",
        "bacnet": {
            "bbmd": [
                {
                    "ip": "192.168.3.10",
                    "port": 47808
                },
                {
                    "ip": "91.215.95.210",
                    "port": 47808
                },
                {
                    "ip": "90.226.132.95",
                    "port": 47808
                },
                {
                    "ip": "90.227.36.61",
                    "port": 47808
                }
            ],
            "fdt": []
        }
    },
    "ip_str": "81.236.14.67"
}
```

Figure 3.1: A pretty-printed data entry of a Sauter EY-RC 504 ICS device

3.3 Findings

3.3.1 Found ICS Products

Through Shodan, we found over 2.45 million IP addresses located in Sweden reachable via 4,595 Autonomous Systems (AS). Out of these 2.45 million devices, we found 19,784 IP addresses with metadata matching the search terms we found in our literature study.

Out of these 19,784 IP addresses, we classified 2,237 as ICS devices (see Section 3.1). In total, we found 93 different ICS models, made by 36 different manufacturers. In Figure 3.2 we show the ten most common ICS products in Sweden. A complete list with all 93 identified ICS models can be found in Appendix B.

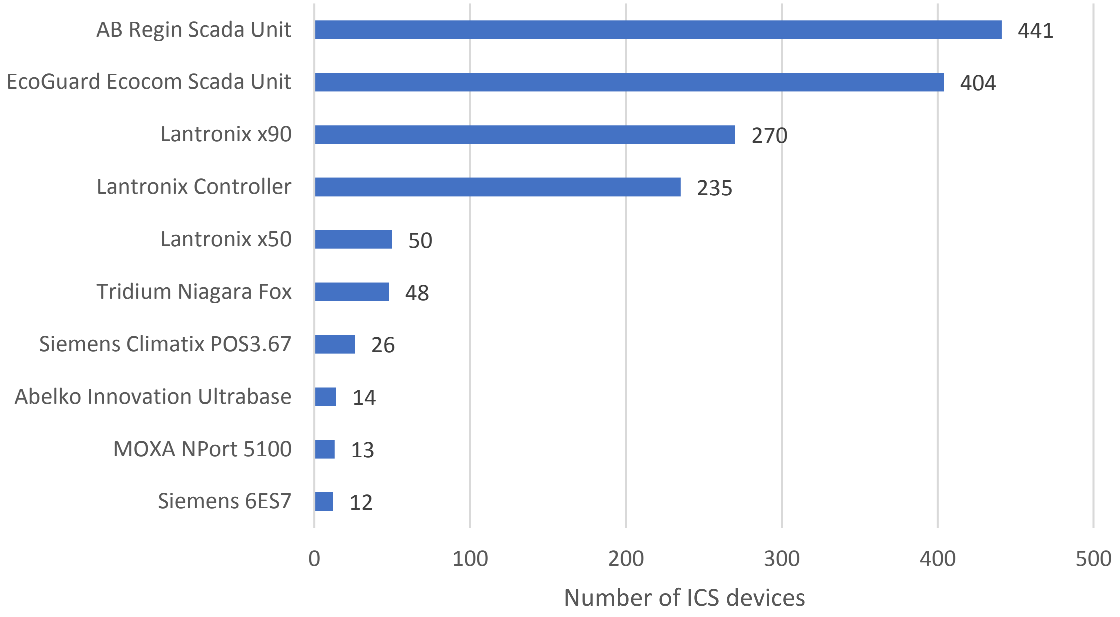


Figure 3.2: Top 10 most common ICS products in Sweden

The most found ICS product in Sweden is Scada control units manufactured by Swedish companies AB Regin and EcoGuard. These devices are often used for automating and regulating heating and ventilation of buildings. Other common products are those made by Lantronix, an American company specializing in multi-function automation and control of industrial complexes.

3.3.2 Found ICS manufacturers

In total, we identified 36 different manufacturers of ICS devices that had their devices in operation in Sweden. In Figure 3.3 we show the ten most prevalent manufacturers by number of ICS devices that are in operation in Sweden. A complete list with all the 36 identified manufacturers can be found in Appendix C.

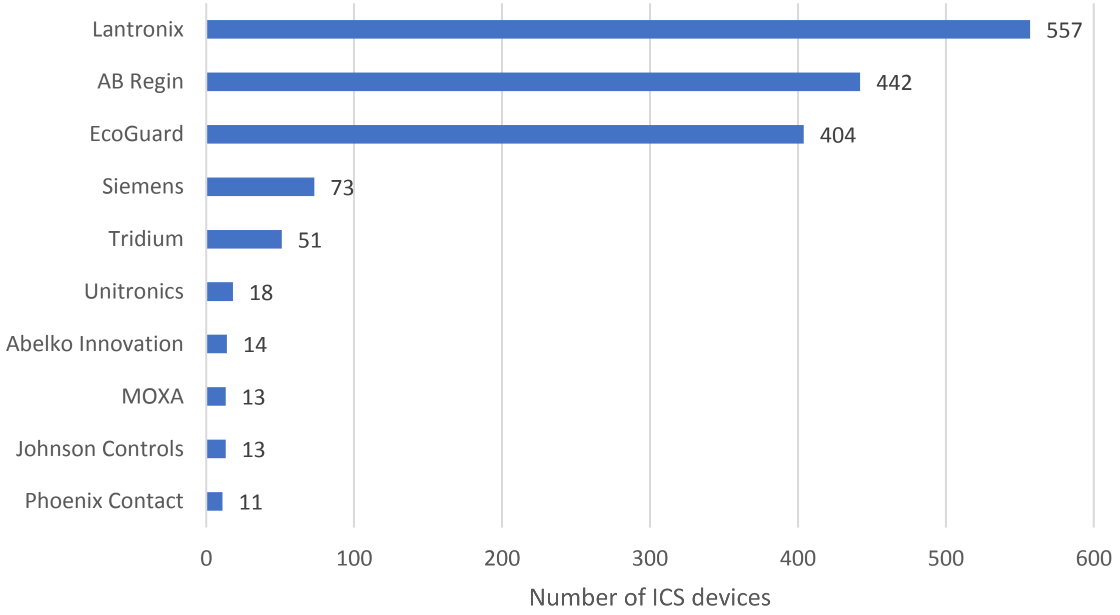


Figure 3.3: Top 10 ICS manufacturers in Sweden

3.3.3 Organizations Operating ICS Devices

We would have liked to do a mapping between the ICS devices found and the organizations that operate these devices, since we believe that this would be helpful to assess how damaging attacks against Swedish ICS devices would be. However, mapping IP addresses with physical organizations is difficult from both an ethical, as well as a legal aspect. Since organizational information is not available in Shodan, we would need to do further investigations into the IP addresses we found. Doing this kind of probing might make certain ICS devices restart or stop operation, which would functionally be very close to performing an attack on the device. There is also an issue with complying with GDPR which considers IP addresses as personal data, meaning that mapping individual IP addresses to specific organizations is most likely illegal (albeit there are some differences in between how countries interpret these laws).

While mapping individual IP addresses to organizations is something we refrained from doing, we *can* still map sets of related IP addresses to organizations. Such sets are called Autonomous Systems (AS) and exist for routing purposes, i.e., all IP addresses within an AS shares the same route to and from other ASs on the internet. Additionally, Shodan collects information about which AS every IP address is part of. This allows us to still make some assessment as to which organizations operate the ICS devices located in Sweden.

Using the AS numbers gathered from the “asn” banner in the data from Shodan, we identified 70 autonomous systems which controlled one or more ICS devices in Sweden with the help of the AS Number lookup provided by BigDataCloud [26]. A full list of every autonomous system identified can be found in Appendix D. The top 10 ASs which connected the most ICS devices in Sweden can be found in Figure 3.4.

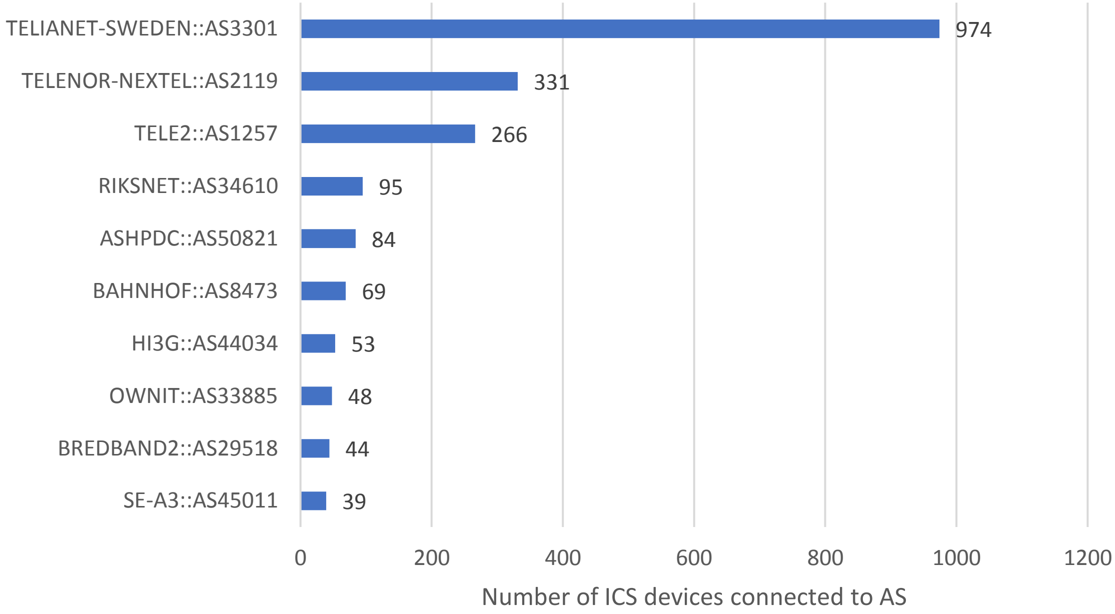


Figure 3.4: Top 10 autonomous systems which connects the most ICS devices in Sweden

All the top 10 ASs found was those of internet service providers (ISPs). The most common ISP was Telia Company AB, which controls both AS3301 (TELIANET-SWEDEN) and AS34610 (RIKSNET). In fact, out of all the ASs identified nearly all belonged to ISPs. This means that organizations operating ICS devices deploy them through ISP rather than through their own networks, which effectively masks which organizations are really controlling the ICS devices. An interesting side effect of this is that blackouts of ISP services would also result in unavailability of all ICS devices deployed throughout that ISP.

4 Assessing ICS Device Vulnerabilities

4.1 Vulnerabilities Background

The National Cybersecurity FFRDC (Federally Funded Research and Development Center), operated by the MITRE Corporation, maintains a system named the Common Vulnerabilities and Exposures, referred to as CVE [27]. The goal of the CVE system is to uniquely name, define, and catalog publicly known cybersecurity vulnerabilities and exposures, thus creating a standardized naming convention to ensure that organizations or software tools refers to the same vulnerability or exposure [28].

CVE defines a vulnerability as "A flaw in software, firmware, hardware, or service component resulting from a weakness that can be exploited, causing a negative impact to the confidentiality, integrity, or availability of an impacted component or components." [29]

The National Vulnerability Database, henceforth referred to as NVD, is "the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics." [30] The NVD project is hosted by The National Institute of Standards and Technology, NIST, a part of the U.S. Department of Commerce.

When assigning degree of severity for the vulnerabilities, we referred to a system as recommended by NIST, called the Common Vulnerability Scoring System, CVSS. The CVSS is provided and maintained by FIRST [31], a U.S.-based non-profit organization which aims to connect a wide assortment of security and incident response team from around the world. When rating a severity, the CVSS accounts for several metrics including but not limited to the complexity and difficulty level, which technical means and privileges are required to exploit a vulnerability, and the direct consequences of a successful attack. The latest standard, CVSS v3.1 [32], provides quality severity ratings on the scale shown in Table 4.1.

Rating	*Score Range*
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Table 4.1: CVSS v3.1 Severity rating and score range.

4.2 Classification of Device Vulnerabilities

For this report, we have used the database provided by NVD to cross reference our downloaded search results from Shodan. Our methodology consisted of extracting relevant metadata, when available, for each result. As mentioned in Chapter 3, the content of the metadata did not follow any standard convention, and which banners contained which information was somewhat arbitrary. Disregarding the inconsistency, the banners of most value for our research were "Product", "Version", and "Data". In the cases where both the "Product" and "Version" banners contained useful data, the task of cross referencing our downloaded results with the NVD was trivial, as CVE identifiers incorporates both product names and software version numbers affected by the vulnerability. However, in the cases were said banners were empty or inconclusive, manual extraction of metadata was required. In the cases where there was no relevant identifiable metadata available, we did not further attempt to perform a device vulnerability classification and is simply listed as unknown. For the remaining devices, the "Data" banner was carefully examined to see if we could conclusively identify the manufacturer and device, e.g., by comparing services being ran at the point of data collection. Again, since the metadata provided did not conform to any standard, we were required to adapt our exact methodology on a case-by-case basis.

4.3 Findings

Out of the 2,237 ICS devices we identified in Chapter 3, we found that 244 devices had at least one known CVE vulnerability. Out of the devices with at least one CVE vulnerability, 183 had vulnerabilities that could be exploited remotely from anywhere in the world over the internet. Many devices had more than one CVE vulnerability, and some had been left unpatched since as far back as 2011. Table 4.2 shows a full reference to every CVE vulnerability found.

Since our source data was unstructured and manually processed, there might be more known CVE vulnerabilities than those presented here. It is also worth noting that even when an ICS device does not have any known CVE vulnerability, they could still be susceptible to zero-day exploits that are yet unknown to the public. There is also the inherent risk of being connected to the internet at all. For example, any ICS device available on the internet would be susceptible to attacks such as DDOS where an attacker sends massive amounts of requests until the device is unable to handle them all and stops working.

Manufacturer	Models	CVE	#	Score	Type
Unitronics	Various	CVE-2015-7939	18	9.3	Remote
Unitronics	Various	CVE-2015-7905	18	7.5	Remote
Unitronics	Various	CVE-2016-4519	18	7.5	Remote
Unitronics	Various	CVE-2015-6478	18	6.8	Remote
Tridium	Niagara Fox	CVE-2017-16748	48	7.5	Remote
Tridium	Niagara Fox	CVE-2017-16744	48	6.5	Remote
Tridium	Niagara Fox	CVE-2018-18985	48	3.5	Remote
Tridium	Niagara Fox	CVE-2020-14483	48	3.3	Local
Siemens	Climatix Bacnet	CVE-2015-4174	27	4.3	Remote
Schneider Electric	TSXETY4103	CVE-2011-4859	1	10.0	Remote
Rockwell Automation	1756-ENBT	CVE-2012-6437	1	10.0	Remote
Rockwell Automation	1756-ENBT	CVE-2012-6440	1	9.3	Remote
Rockwell Automation	1756-ENBT	CVE-2012-6439	1	8.5	Remote
Rockwell Automation	1756-ENBT	CVE-2012-6435	1	7.8	Remote
Rockwell Automation	1756-ENBT	CVE-2012-6436	1	7.8	Remote
Rockwell Automation	1756-ENBT	CVE-2012-6438	1	7.8	Remote
Rockwell Automation	1756-ENBT	CVE-2012-6441	1	5.0	Remote
Rockwell Automation	1763-L16BWA B	CVE-2016-9334	1	5.0	Remote
Rockwell Automation	1763-L16BWA B	CVE-2016-9338	1	4.0	Remote
Red Lion Controls	Crimson	CVE-2020-27279	8	7.8	Remote
Red Lion Controls	Crimson	CVE-2019-10978	8	6.8	Remote
Red Lion Controls	Crimson	CVE-2019-10984	8	6.8	Remote
Red Lion Controls	Crimson	CVE-2019-10996	8	6.8	Remote
Red Lion Controls	Crimson	CVE-2020-27285	8	6.4	Remote
Red Lion Controls	Crimson	CVE-2020-27283	8	5.0	Remote
Red Lion Controls	Crimson	CVE-2019-10990	8	4.3	Remote
Omron	CJ2M PLC, CJ2H PLC	CVE-2015-0987	6	5.0	Remote
Omron	CJ2M PLC, CJ2H PLC	CVE-2015-1015	6	2.1	Local
IV Produkt	AHU	CVE-2020-7574	1	4.3	Remote
Fläktgrupp	eQ	CVE-2020-7574	2	4.3	Remote
Automated Logic	Various	CVE-2016-5795	7	7.5	Remote
Automated Logic	Various	CVE-2017-9644	7	6.9	Local
Automated Logic	Various	CVE-2017-9640	7	6.5	Remote
Automated Logic	Various	CVE-2022-1019	7	5.8	Remote
Automated Logic	Various	CVE-2017-9650	7	4.6	Local
Automated Logic	Various	CVE-2021-31682	7	4.3	Remote
3S-Smart	CODESYS	CVE-2012-6069	8	10.0	Remote
3S-Smart	CODESYS	CVE-2012-6068	8	10.0	Remote
3S-Smart	CODESYS	CVE-2018-5440	1	7.5	Remote
3S-Smart	CODESYS	CVE-2015-6482	8	5.0	Remote

Table 4.2: All found CVE vulnerabilities

In Figure 4.1, the pie-chart on the left shows the distribution of devices with or without CVE vulnerabilities. The graph on the right shows how the device could be exploited. The fact that we found 1,460 ICS devices without any unpatched vulnerabilities suggests that many of the organizations that deploy ICS devices do put in effort to keep their security up to date, there is still over 10% of ICS devices in Sweden that are vulnerable to exploits that could leak sensitive information or let the attacker take unauthorized control of Swedish infrastructure.

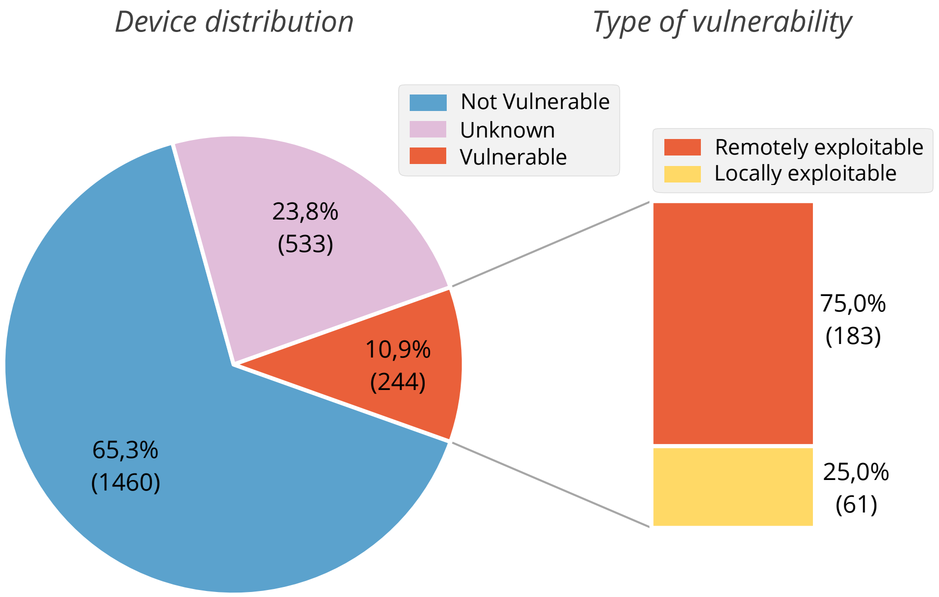


Figure 4.1: Percentage of vulnerable devices and how they could be exploited

Many of the devices had more than one vulnerability. In fact, some devices had up to 7 unpatched CVEs at the time of our research. In total, 40 different CVEs was found. To assess how severe these vulnerabilities would be, the CVSS severity rating presented in Section 4.1 was used to sum the number of devices each vulnerability affected, making a distribution of vulnerability severity. Our findings were that 77% of devices had a vulnerability with Medium, High, or Critical severity which in theory could lead to an attacker taking complete control over the affected ICS device. This distribution is presented in Figure 4.2.

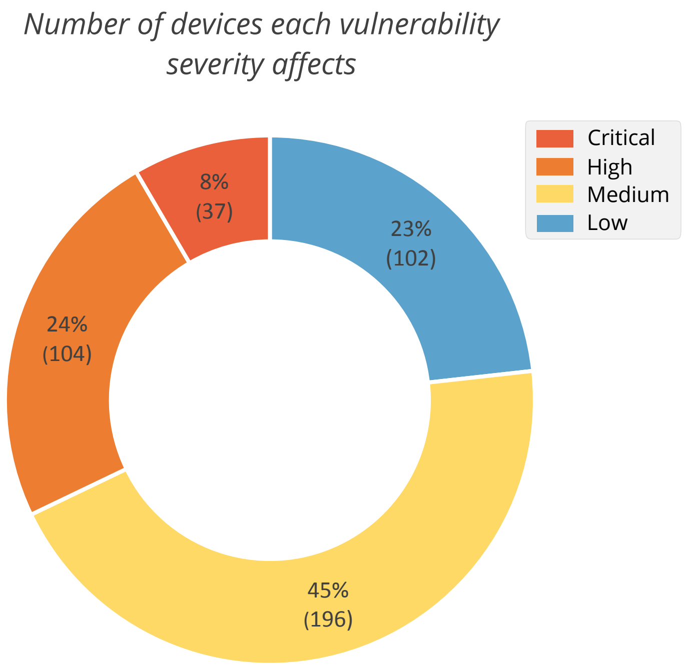


Figure 4.2: Distribution of severity of found vulnerabilities

In total, devices from 11 different manufacturers were found to have unpatched CVEs. The manufacturer with the most affected devices was Tridium. Their Niagara Fox model was susceptible to four different CVEs and there are 48 such devices in use in Sweden. All top three manufacturers with most devices in Sweden (Lantronix, AB Regin, and EcoGuard) had no CVEs publicly listed, but this might be because all these devices were hard to classify to a specific model or piece of software. This means that an attacker that performed more aggressive attempts at data fetching could reveal additional device information that let them find more CVEs. It could also be the case that vulnerabilities of AB Regin and EcoGuard devices are not updated as often in the CVE database since both manufacturers are Swedish. Table 4.3 shows the number of unique devices with at least one CVE for each manufacturers found.

Out of the devices made by the ten most common manufacturers, only devices by Siemens, Tridium, and Unitronics were shown to have known vulnerabilities. These three manufacturers were responsible for 93 different vulnerable ICS devices, almost half of all the vulnerable devices in Sweden. These findings are presented in Table 4.4 and Table 4.5.

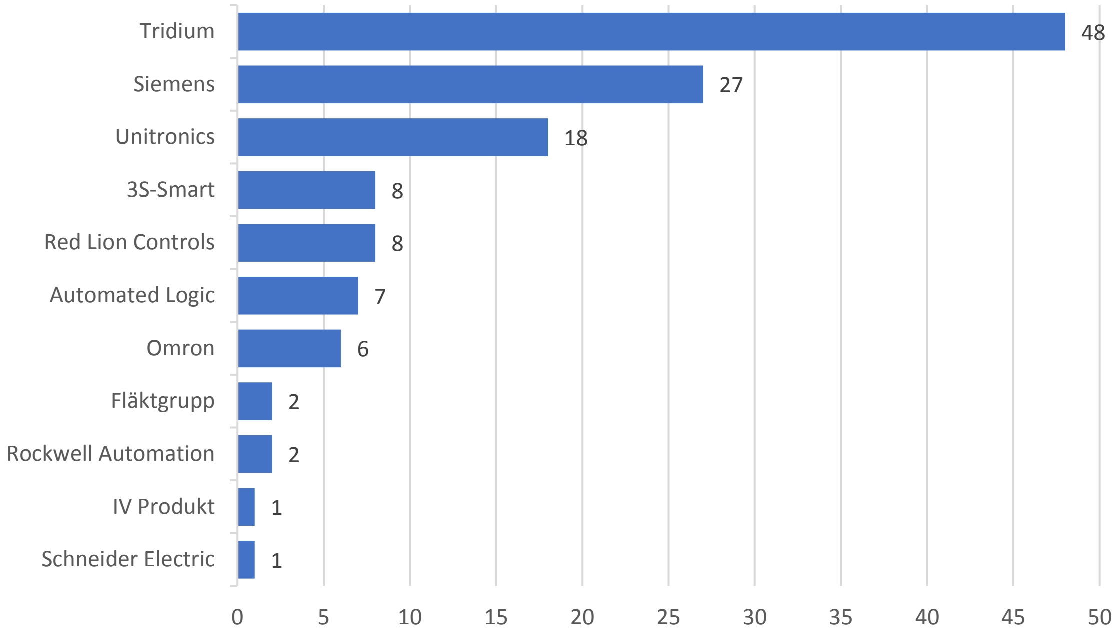
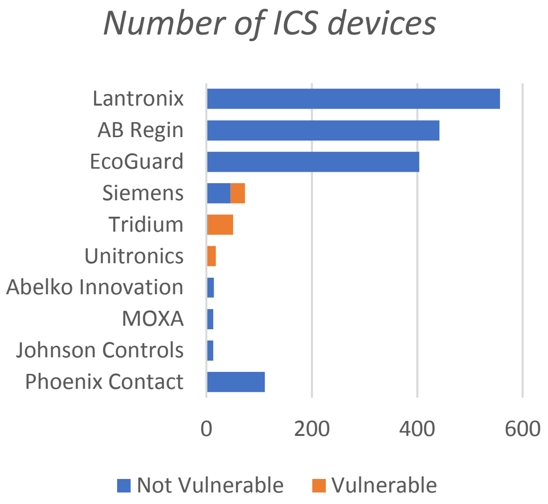


Table 4.3: Number of vulnerable devices per manufacturer



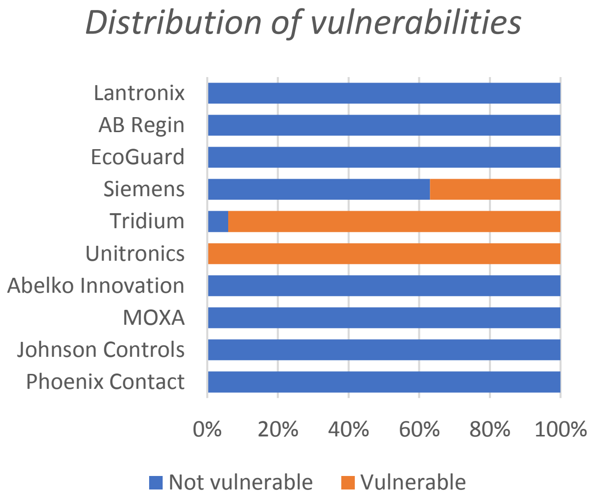


Table 4.4: Number of ICS devices with vulnerabilities made by the top 10 most common manufacturers

Table 4.5: Distribution of vulnerable ICS devices made by the top 10 most common manufacturers

4.4 Found CVEs

In total, we found 40 CVEs that affected at least one ICS device in Sweden. In this section we list every found vulnerability, along with the description of the vulnerability as provided by the CVE database.

- **CVE-2015-0987** - Omron CX-One CX-Programmer before 9.6, CJ2M PLC devices before 2.1, and CJ2H PLC devices before 1.5 rely on cleartext password transmission, which allows remote attackers to obtain sensitive information by sniffing the network during a PLC unlock request.

- **CVE-2015-1015** - Omron CX-One CX-Programmer before 9.6, CJ2M PLC devices before 2.1, and CJ2H PLC devices before 1.5 use a reversible format for password storage in object files on Compact Flash cards, which makes it easier for local users to obtain sensitive information by reading a file.

- **CVE-2012-6435 -** Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allow remote attackers to cause a denial of service (control and communication outage) via a CIP message that specifies a logic-execution stop and fault.

- **CVE-2012-6436** - Buffer overflow in Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allows remote attackers to cause a denial of service (CPU crash and communication outage) via a malformed CIP packet.

- **CVE-2012-6437** - Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 do not properly perform authentication for Ethernet firmware updates, which allows remote attackers to execute arbitrary code via a Trojan horse update image.

- **CVE-2012-6438** - Buffer overflow in Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allows remote attackers to cause a denial of service (NIC crash and communication outage) via a malformed CIP packet.

- **CVE-2012-6439** - Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allow remote attackers to cause a denial of service (control and communication outage) via a CIP message that modifies the (1) configuration or (2) network parameters.

- **CVE-2012-6440 -** The web-server password-authentication functionality in Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allows man-in-the-middle attackers to conduct replay attacks via HTTP traffic.

- **CVE-2012-6441** - Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allow remote attackers to obtain sensitive information via a crafted CIP packet.

- **CVE-2016-9334 -** An issue was discovered in Rockwell Automation Allen-Bradley MicroLogix 1100 controller 1763-L16AWA, Series A and B, Version 14.000 and prior versions; 1763-L16BBB, Series A and B, Version 14.000 and prior versions; 1763-L16BWA, Series A and B, Version 14.000 and prior versions; and 1763-L16DWD, Series A and B, Version 14.000 and prior versions. User credentials are sent to the web server in clear text, which may allow an attacker to discover the credentials if they are able to observe traffic between the web browser and the server.

- **CVE-2016-9338 -** An issue was discovered in Rockwell Automation Allen-Bradley MicroLogix 1100 controller 1763-L16AWA, Series A and B, Version 14.000 and prior versions; 1763-L16BBB, Series A and B, Version 14.000 and prior versions; 1763-L16BWA, Series A and B, Version 14.000 and prior versions; and 1763-L16DWD, Series A and B, Version 14.000 and prior versions. Because of an Incorrect Permission Assignment for Critical Resource, users with administrator privileges may be able to remove all administrative users requiring a factory reset to restore ancillary web server function. Exploitation of this vulnerability will still allow the affected device to function in its capacity as a controller.

- **CVE-2015-4174** - Cross-site scripting (XSS) vulnerability in the integrated web server on the Siemens Climatix BACnet/IP communication module with firmware before 10.34 allows remote attackers to inject arbitrary web script or HTML via a crafted URL.

- **CVE-2011-4859** - The Schneider Electric Quantum Ethernet Module, as used in the Quantum 140NOE771* and 140CPU65* modules, the Premium TSXETY* and TSXP57* modules, the M340 BMXNOE01* and BMXP3420* modules, and the STB DIO STBNIC2212 and STBNIP2* modules, uses hardcoded passwords for the (1) AUTCSE, (2) AUT_CSE, (3) fdrusers, (4) ftpuser, (5) loader, (6) nic2212, (7) nimrohs2212, (8) nip2212, (9) noe77111_v500, (10) ntpupdate, (11) pcfactory, (12) sysdiag, (13) target, (14) test, (15) USER, and (16) webserver accounts, which makes it easier for remote attackers to obtain access via the (a) TELNET, (b) Windriver Debug, or (c) FTP port.

- **CVE-2018-5440** - A Stack-based Buffer Overflow issue was discovered in 3S-Smart CODESYS Web Server. Specifically: all Microsoft Windows (also WinCE) based CODESYS web servers running stand-alone Version 2.3, or as part of the CODESYS runtime system running prior to Version V1.1.9.19. A crafted request may cause a buffer overflow and could therefore execute arbitrary code on the web server or lead to a denial-of-service condition due to a crash in the web server.

- **CVE-2015-6482** - Runtime Toolkit before 2.4.7.48 in 3S-Smart CODESYS before 2.3.9.48 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted request.

- **CVE-2012-6069** - Directory traversal vulnerability in the Runtime Toolkit in CODESYS Runtime System 2.3.x and 2.4.x allows remote attackers to read, overwrite, or create arbitrary files via a .. (dot dot) in a request to the TCP listener service.

- **CVE-2012-6068** - The Runtime Toolkit in CODESYS Runtime System 2.3.x and 2.4.x does not require authentication, which allows remote attackers to (1) execute commands via the command-line interface in the TCP listener service or (2) transfer files via requests to the TCP listener service.

- **CVE-2016-5795 -** An XXE issue was discovered in Automated Logic Corporation (ALC) Liebert SiteScan Web Version 6.5 and prior, ALC WebCTRL Version 6.5 and prior, and Carrier i-Vu Version 6.5 and prior. An attacker could enter malicious input to WebCTRL, i-Vu, or SiteScan Web through a weakly configured XML parser causing the application to execute arbitrary code or disclose file contents from a server or connected network.

- **CVE-2017-9640 -** A Path Traversal issue was discovered in Automated Logic Corporation (ALC) ALC WebCTRL, i-Vu, SiteScan Web prior to 6.5; ALC WebCTRL, SiteScan Web 6.1 and prior; ALC WebCTRL, i-Vu 6.0 and prior; ALC WebCTRL, i-Vu, SiteScan Web 5.5 and prior; and ALC WebCTRL, i-Vu, SiteScan Web 5.2 and prior. An authenticated attacker may be able to overwrite files that are used to execute code. This vulnerability does not affect version 6.5 of the software.

- **CVE-2017-9644 -** An Unquoted Search Path or Element issue was discovered in Automated Logic Corporation (ALC) ALC WebCTRL, i-Vu, SiteScan Web 6.5 and prior; ALC WebCTRL, SiteScan Web 6.1 and prior; ALC WebCTRL, i-Vu 6.0 and prior; ALC WebCTRL, i-Vu, SiteScan Web 5.5 and prior; and ALC WebCTRL, i-Vu, SiteScan Web 5.2 and prior. An unquoted search path vulnerability may allow a non-privileged local attacker to change files in the installation directory and execute arbitrary code with elevated privileges.

- **CVE-2017-9650 -** An Unrestricted Upload of File with Dangerous Type issue was discovered in Automated Logic Corporation (ALC) ALC WebCTRL, i-Vu, SiteScan Web 6.5 and prior; ALC WebCTRL, SiteScan Web 6.1 and prior; ALC WebCTRL, i-Vu 6.0 and prior; ALC WebCTRL, i-Vu, SiteScan Web 5.5 and prior; and ALC WebCTRL, i-Vu, SiteScan Web 5.2 and prior. An authenticated attacker may be able to upload a malicious file allowing the execution of arbitrary code.

- **CVE-2021-31682 -** The login portal for the Automated Logic WebCTRL/WebCTRL OEM web application contains a vulnerability that allows for reflected XSS attacks due to the operatorlocale GET parameter not being sanitized. This issue impacts versions 6.5 and below. This issue works by passing in a basic XSS payload to a vulnerable GET parameter that is reflected in the output without sanitization.

- **CVE-2022-1019** - Automated Logic's WebCtrl Server Version 6.1 'Help' index pages are vulnerable to open redirection. The vulnerability allows an attacker to send a maliciously crafted URL which could result in redirecting the user to a malicious webpage or downloading a malicious file.

- **CVE-2019-10978 -** Red Lion Controls Crimson, version 3.0 and prior and version 3.1 prior to release 3112.00, allow multiple vulnerabilities to be exploited when a valid user opens a specially crafted, malicious input file that operates outside of the designated memory area.

- **CVE-2019-10984 -** Red Lion Controls Crimson, version 3.0 and prior and version 3.1 prior to release 3112.00, allow multiple vulnerabilities to be exploited when a valid user opens a specially crafted, malicious input file that causes the program to mishandle pointers.

- **CVE-2019-10990** - Red Lion Controls Crimson, version 3.0 and prior and version 3.1 prior to release 3112.00, uses a hard-coded password to encrypt protected files in transit and at rest, which may allow an attacker to access configuration files.

- **CVE-2019-10996 -** Red Lion Controls Crimson, version 3.0 and prior and version 3.1 prior to release 3112.00, allow multiple vulnerabilities to be exploited when a valid user opens a specially crafted, malicious input file that can reference memory after it has been freed.

- **CVE-2020-27279 -** A NULL pointer deference vulnerability has been identified in the protocol converter. An attacker could send a specially crafted packet that could reboot the device running Crimson 3.1 (Build versions prior to 3119.001).

- **CVE-2020-27283 -** An attacker could send a specially crafted message to Crimson 3.1 (Build versions prior to 3119.001) that could leak arbitrary memory locations.

- **CVE-2020-27285 -** The default configuration of Crimson 3.1 (Build versions prior to 3119.001) allows a user to be able to read and modify the database without authentication.

- **CVE-2015-6478 -** Unitronics VisiLogic OPLC IDE before 9.8.02 does not properly restrict access to ActiveX controls, which allows remote attackers to have an unspecified impact via a crafted web site.

- **CVE-2015-7905 -** Unitronics VisiLogic OPLC IDE before 9.8.02 allows remote attackers to execute unspecified code via unknown vectors.

- **CVE-2015-7939 -** Heap-based buffer overflow in Unitronics VisiLogic OPLC IDE before 9.8.09 allows remote attackers to execute arbitrary code via a long vlp filename.

- **CVE-2016-4519 -** Stack-based buffer overflow in Unitronics VisiLogic OPLC IDE before 9.8.30 allows remote attackers to execute arbitrary code via a crafted filename in a ZIP archive in a vlp file.

- **CVE-2017-16744 -** A path traversal vulnerability in Tridium Niagara AX Versions 3.8 and prior and Niagara 4 systems Versions 4.4 and prior installed on Microsoft Windows Systems can be exploited by leveraging valid platform (administrator) credentials.

- **CVE-2017-16748 -** An attacker can log into the local Niagara platform (Niagara AX Framework Versions 3.8 and prior or Niagara 4 Framework Versions 4.4 and prior) using a disabled account name and a blank password, granting the attacker administrator access to the Niagara system.

- **CVE-2018-18985 -** Tridium Niagara Enterprise Security 2.3u1, all versions prior to 2.3.118.6, Niagara AX 3.8u4, all versions prior to 3.8.401.1, Niagara 4.4u2, all versions prior to 4.4.93.40.2, and Niagara 4.6, all versions prior to 4.6.96.28.4 a cross-site scripting vulnerability has been identified that may allow a remote attacker to inject code to some web pages affecting confidentiality.

- **CVE-2020-14483 -** A timeout during a TLS handshake can result in the connection failing to terminate. This can result in a Niagara thread hanging and requires a manual restart of Niagara (Versions 4.6.96.28, 4.7.109.20, 4.7.110.32, 4.8.0.110) and Niagara Enterprise Security (Versions 2.4.31, 2.4.45, 4.8.0.35) to correct.

5 Conclusions and Discussion

5.1 Conclusions

As indicated by the problem statement for this report, we only take easily findable ICS devices into consideration, and we discovered 2,237 devices by using tools freely available online. This implies that anyone with or without malicious intent, as long as they possess at least some technical proficiency, is able to discover these devices and access the associated metadata. The ease of finding these devices may raise some concerns regarding security since we assume that, for example, hacker groups with real intentions of disrupting infrastructure possesses more advanced methods of both finding and exploiting ICS devices. While we made the decision to not attempt a mapping of the device owners, an attacker could be more inclined to pursue this option in search of a suitable target. However, for an institution or a company operating ICS devices connected to critical infrastructure, it is reasonable to assume that the cyber security of said devices is of utmost importance. With this in mind, it seems likely that there exists ICS devices hidden from search engines such as the one provided by Shodan.

With the restrictions imposed for this report, we are not able to positively conclude whether any of the devices control critical infrastructure, and in turn what potential consequences targeted attacks may have. This makes it difficult to assess the general state of Swedish infrastructure from a cyber security point of view as 188 of the 244 vulnerable devices were rated with a medium, high, or critical severity rating and theoretically could lead to critical failure if exploited by an attacker. However, as shown in our results, roughly 90% of the devices we found were not affected by any CVE. With the presumption that there exist more devices hidden from common search engines such as Shodan, it is clear that at least some effort is made to protect the integrity of ICS devices in Sweden, yet the 188 vulnerable devices indicates there is still room for improvement.

5.2 Measures for Protection

From our findings in Assessing Chapter 4, we have identified a few protective measures that could help improve the security of operations involving ICS devices. The first measure is to assure that all firmware is kept up to date. The first four digits in a CVE identifier represents the year the vulnerability or exploit was added to the database, and while examining the CVEs we found in Section 4.4, it is clear that many of the vulnerabilities have been around for many years at the time of writing. Many of the CVEs we discovered only apply to a specific firmware version, or a range of versions, which in practice implies that these issues could be resolved by a firmware update, especially for the older CVEs.

Another measure is to limit which devices has access to critical infrastructure, and whether they are connected to the Internet or not. As briefly mentioned in the introduction, ICS devices has over time gotten more and more connected. With the obvious benefits of availability comes the risk of an unrelated third party getting easier access to the system. As shown in Chapter 4, we found that in 75% of the relevant CVEs, the device in question was susceptible to remote attacks. Therefore, it could be worth to investigate some sort of trade-off where the most critical or vulnerable devices are to be taken offline and thus only reachable locally. This could help to both reduce the number of individuals able to perform an attack, as well as mitigate potential consequences of such an attack.

A significant part of the methodology used in this report consisted of investigating TCP and UDP ports well known to host services and protocols commonly associated with ICS devices. Changing which ports are used for communication would make it significantly harder to discover these devices, although not impossible. Further, many of the ICS devices identified in this study was classified with the help of their associated metadata. Again, removal of this metadata, or at least an attempt to conceal critical information such as what software and which version is running would make it more difficult to positively identify a device as an ICS device, which in turn would make targeted attacks much harder to execute.

Finally, a general preventive measure could simply be acknowledging the operational risk of connected ICS devices and keep well-informed about news in the field of cybersecurity. Part of this could be to at a minimum maintain a list of devices connected to the system, and regularly cross reference vulnerability databases such as the NVD for newly discovered vulnerabilities or exploits related to devices or software being used by the organization, preferably using some automated process.

5.3 Further Research

It is important to take into consideration that the findings of this project simply represent a snapshot of the current situation as was during the data collecting process. An interesting extension would be to extend the duration of the project, noting any disparity in the number of discovered devices, and in the relative number of found vulnerabilities to investigate if and how ICS device operators take actions to newly found vulnerabilities or exploits. Naturally, the research could also easily be extended to include additional countries or regions for either a comparison or simply an extended reach.

As previously discussed, an adequate scanning method of the IPv6 address space could lead to an increase in found devices. With time, it is safe to assume that more and more ICS devices will be migrated to IPv6, as the general rate of adoption of the newer protocol increases, in addition to the benefits to ICS device functionality it would bring, as shown by previous research [33].

Regarding the number of discovered devices, a more complete result could potentially be achieved by using a priced tier of access to Shodan, allowing for an unlimited number or searches. A comparison between different port scanning projects could also be of interest, even though our preliminary investigation showed that Shodan provided the best result for the scope of this report. Alternatively, researchers could conduct their own port scanning using tools such as Nmap or MASSCAN, if disregarding or working around the ethical and legal reasons not to, instead of relying on existing projects.

Finally, determining which organizations operate the ICS devices and how they are being used in practice would lead to a much more conclusive assessment of the risk associated with potential vulnerabilities, especially regarding what consequences a potential attack would bring.

6 Appendices

6.1 Appendix A – Port Numbers and Protocols

Below are all port numbers and associated device or protocol found in the literature study.

Port numbers	Associated protocol/device
23	Beckhoff CX5020 PLC
102	Siemens S7, ICCP-TASE.2, IEC 61850
161	Beckhoff CX5020 PLC UDP snmp
789	Crimson, Red Lion Crimson V3
987	Beckhoff CX5020 PLC TCP Unknown Service
1153	ANSI C12.22
1900	Beckhoff CX5020 PLC UDP upnp
1911	Tridium Niagara Non-Secure Fox Port
1926	PCWorx
2222	CSPV4
2455	Codesys
3011	Tridium Niagara Non-Secure Platform Port
4911	Tridium Niagara Secure FOX Port
5011	Tridium Niagara Secure Platform Port
5094	HART IP
9600	OMRON FINS
10001	Automatic Tank Gauge, ATG
20547	ProConOS
34980	EtherCAT
48898	Beckhoff CX5020 PLC TCP Unknown service
48899	Beckhoff CX5020 PLC UDP Unknown service
1089-1091	FF HSE
11754-11755	Zigbee IP
18245, 18246	GE-SRTP
1883, 8883	MQTT
19999, 20000	DNP3
2221, 2222, 44818	Ethernet/IP
2404, 19998	IEC608070-5-104
34962-34964	PROFINET
47808-47823	BACnet
4840, 4843	OPC UA
5006, 5007	MELSEC-Q
502, 802	Modbus
55000-55003	FL-net
5671, 5672	AMQP
5683, 5684	CoAP

6.2 Appendix B - Classified Products

Below is the full list of ICS products classified.

	Device name	Devices found	Percentage
1	AB Regin Scada Unit	441	19.714%
2	EcoGuard Ecocom Scada Unit	404	18.060%
3	Lantronix x90	270	12.070%
4	Lantronix Controller	235	10.505%
5	Lantronix x50	50	2.235%
6	Tridium Niagara Fox	48	2.146%
7	Siemens Climatix POS3.67	26	1.162%
8	Abelko Innovation Ultrabase	14	0.626%
9	MOXA NPort 5100	13	0.581%
10	Siemens 6ES7	12	0.536%
11	Siemens PXG3.L	10	0.447%
12	Unitronics Vision V570-57-T20	9	0.402%
13	IEC 61131-3 PLC	8	0.358%
14	Red Lion Controls Crimson	8	0.358%
15	Rego 5200 Controller	7	0.313%
16	Delta Electronics PLC	6	0.268%
17	Phoenix Contact ILC 170 ETH 2TX	6	0.268%
18	SmartX AS-P Controller	5	0.224%
19	Phoenix Contact ILC 171 ETH 2TX	5	0.224%
20	Johnson controls MS-NCE2500-0	5	0.224%
21	OPTO 22 PLC	5	0.224%
22	SE Electronic E-DDC3.3 S	4	0.179%
23	Unitronics Vision V700-T20BJ	4	0.179%
24	Schneider Electric BMXNOE0100	3	0.134%
25	OMRON CJ2M-CPU31	3	0.134%
26	Sauter EY-RC 504 f0c1	3	0.134%
27	Swegon Gold E/F	3	0.134%
28	Automated Logic LGR250	3	0.134%
29	Johnson controls MS-NCE2560-0	3	0.134%
30	Tridium Niagara 4	3	0.134%
31	Siemens PXC36 E-D v3.02	3	0.134%
32	Rego 5200 Controller	3	0.134%
33	Rockwell Automation Allen-Bradley PLC	3	0.134%
34	Siemens SIMATIC 300 PLC	3	0.134%
35	OMRON CJ2H-CPU65-EIP	2	0.089%
36	Distech Controls ECY-S1000	2	0.089%
37	Sauter EY-AS 525 f001	2	0.089%
38	Sauter EY-AS 525 f005	2	0.089%
39	Sauter EY6AS80f021	2	0.089%
40	Fläktgrupp eQ Prime	2	0.089%
41	Keiback & Peter DDC4000 System	2	0.089%

42	Automated Logic ME812u Controller	2	0.089%
43	Johnson Controls MS-NAE3510-2	2	0.089%
44	OMRON Controller	2	0.089%
45	Siemens PXC22 E-D v11.01	2	0.089%
46	Siemens PXG3.W100	2	0.089%
47	Siemens PXG3.W100-1	2	0.089%
48	Siemens PXG3.W200-1	2	0.089%
49	Schnieder Electric TSXETY4103	2	0.089%
50	Solare Datensysteme GmbH Scada device	2	0.089%
51	Unitronics Vision 1210 PLC	2	0.089%
52	ABB AC500 34 V2.5.1	1	0.045%
53	ABB AC500 42 V2.4.2	1	0.045%
54	SmartX AS-B-24 Controller	1	0.045%
55	Schneider Electric BMXP342020	1	0.045%
56	OMRON CJ2M-CPU33	1	0.045%
57	Siemens Climatix POL908.00/STD	1	0.045%
58	OMRON CP1L-EM30DR-D	1	0.045%
59	Siemens UC CPU 315-2	1	0.045%
60	Crouzet Automation Em4 Logic Controller	1	0.045%
61	Datakom DPR-145	1	0.045%
62	Regin Controllers E281DW-3	1	0.045%
63	Distech Controls ECY-PTU208	1	0.045%
64	Sauter EY-RC 504 f001	1	0.045%
65	General Electric SRTP PLC	1	0.045%
66	Swegon Gold C/D	1	0.045%
67	Swegon Gold E	1	0.045%
68	HMS Industrial Networks Anybus	1	0.045%
69	IV Produkt AHU	1	0.045%
70	Lantronix 3d$	1	0.045%
71	Lantronix x55	1	0.045%
72	Automated Logic LGR1000	1	0.045%
73	Automated Logic LGR25	1	0.045%
74	Johnson Controls M4-SNC16120-0	1	0.045%
75	Johnson Controls MS-NAE5510-2	1	0.045%
76	Johnson Controls MS-NCE2510-0	1	0.045%
77	Saia Burgess Controls PCD7.D443	1	0.045%
78	Siemens PXC100 E-D PXA40-W0 v1.00	1	0.045%
79	Siemens PXC100 E-D PXA40-W2 v3.00	1	0.045%
80	Siemens PXC100 E-D PXA40-W0 v3.00	1	0.045%
81	Siemens PXC100 E-D PXA40-W0 v1.00	1	0.045%
82	Siemens PXC100 E-D PXA40-W2 v1.00	1	0.045%
83	Siemens PXC22 E-D v8.01	1	0.045%
84	Siemens PXC36 E-D v5.02	1	0.045%
85	Siemens PXG3.L-1	1	0.045%
86	Eaton PXGMS UPS	1	0.045%
87	Siemens PXM30.E	1	0.045%

88	Samba OPLC SM35-J-R20 PLC	1	0.045%
89	Swegon SuperWISE II	1	0.045%
90	Schneider Electric TM221CE24R PLC	1	0.045%
91	Schneider Electric TM241CE24T PLC	1	0.045%
92	Unitronics Vision V350-35-T38	1	0.045%
93	Unitronics Vision V350-35-TU24	1	0.045%
	Unknown	533	23.826%
	TOTAL DEVICES FOUND	2237	100%

6.3 Appendix C - Classified Manufacturers

Below is the full list of manufacturers classified.

	Manufacturer	Devices found	Percentage
1	Lantronix	557	24.898%
2	AB Regin	442	19.759%
3	EcoGuard	404	18.060%
4	Siemens	73	3.263%
5	Tridium	51	2.280%
6	Unitronics	18	0.805%
7	Abelko Innovation	14	0.626%
8	MOXA	13	0.581%
9	Johnson Controls	13	0.581%
10	Phoenix Contact	11	0.492%
11	Rego	10	0.447%
12	Sauter	10	0.447%
13	OMRON	9	0.402%
14	3s-smart	8	0.358%
15	Red Lion Controls	8	0.358%
16	Automated Logic	7	0.313%
17	Delta Electronics	6	0.268%
18	SmartX	6	0.268%
19	Schneider Electric	6	0.268%
20	Swegon	6	0.268%
21	OPTO	5	0.224%
22	SE Electronic	4	0.179%
23	Rockwell Automation	3	0.134%
24	Distech Controls	3	0.134%
25	Fläktgrupp	2	0.089%
26	Keiback & Peter	2	0.089%
27	Schnieder Electric	2	0.089%
28	Solare Datensysteme GmbH	2	0.089%
29	ABB	2	0.089%
30	Crouzet Automation	1	0.045%
31	Datakom	1	0.045%
32	General Electric	1	0.045%
33	HMS Industrial Networks	1	0.045%
34	IV Produkt	1	0.045%
35	Saia Burgess Controls	1	0.045%
36	Eaton	1	0.045%
	Devices not classified	533	23.826%
	TOTAL DEVICES FOUND	**2237**	**100%**

6.4 Appendix D - Autonomous Systems

Below is the full list of autonomous systems classified. In total we found 70 Autonomous Systems that our classified ICS devices were connected to. The first column to the name linked with the AS. The second column is the AS number, which is a form of identifier. The third column refers to how many of our identified ICS devices were linked to that AS. Lastly, we present what percentage of our identified ICS devices were connected to this AS.

	AS name	AS number	Devices	Percentage
1	TELIANET-SWEDEN	AS3301	974	43.54%
2	TELENOR-NEXTEL	AS2119	331	14.796%
3	TELE2	AS1257	266	11.891%
4	RIKSNET	AS34610	95	4.247%
5	ASHPDC	AS50821	84	3.755%
6	BAHNHOF	AS8473	69	3.084%
7	HI3G	AS44034	53	2.369%
8	OWNIT	AS33885	48	2.146%
9	BREDBAND2	AS29518	44	1.967%
10	SE-A3	AS45011	39	1.743%
11	FOUREDGE-AS	AS48220	35	1.565%
12	AFFV-AS	AS34686	31	1.386%
13	AC-NET	AS25176	28	1.252%
14	ASN-TM-	AS213195	14	0.626%
15	IPO-EU	AS12552	13	0.581%
16	NAO	AS35706	7	0.313%
17	VIAE-AS	AS47155	7	0.313%
18	SITABINFRA-NORDIC-AS	AS50989	6	0.268%
19	INFRACOM	AS29468	5	0.224%
20	GASTABUD-	AS43012	5	0.224%
21	FREPPA-AS	AS43853	5	0.224%
22	SE-SAPPA	AS35790	4	0.179%
23	CSB	AS48514	4	0.179%
24	Qavat AB - Sweden	AS51546	4	0.179%
25	LIDERO Lidero Network	AS13189	3	0.134%
26	SUNET	AS1653	3	0.134%
27	SE-TEKNIKPARK	AS28847	3	0.134%
28	OBE-NET	AS3399	3	0.134%
29	TELESERVICE	AS34244	3	0.134%
30	CHALMERS	AS2841	2	0.089%
31	WetterNet-AS	AS34946	2	0.089%
32	SVENSKA-AS	AS41340	2	0.089%
33	FASTBIT-AS	AS42318	2	0.089%
34	BORNET	AS44743	2	0.089%
35	GRIFFEL	AS47467	2	0.089%
36	MEDIATEKNIK	AS48803	2	0.089%

37	IP-OSTERAKER	AS57131	2	0.089%
38	N62-AS	AS61146	2	0.089%
39	NORDICOM	AS62183	2	0.089%
40	VODAFONE_ES	AS12430	1	0.045%
41	GOTANET	AS12597	1	0.045%
42	EQUINIX	AS15830	1	0.045%
43	DNA	AS16086	1	0.045%
44	GAVLENET	AS16117	1	0.045%
45	KOPINGS-KABEL-TV	AS197623	1	0.045%
46	WEKUDATA	AS198612	1	0.045%
47	LYSSNA-NJUT-AB	AS200701	1	0.045%
48	MICROGROUP	AS202296	1	0.045%
49	ADVANIA-AS	AS202780	1	0.045%
50	BITCOM	AS205199	1	0.045%
51	HOFORS	AS206114	1	0.045%
52	LJUSNET-AS	AS25417	1	0.045%
53	UUNET	AS2834	1	0.045%
54	GSIX	AS2840	1	0.045%
55	HIGHLANDNET-SWEDEN	AS28854	1	0.045%
56	NEZ-AS	AS30795	1	0.045%
57	SERVANET-AS	AS31507	1	0.045%
58	VARNAMO-ENERGI	AS31642	1	0.045%
59	TELIANET-DENMARK	AS3308	1	0.045%
60	BIKAB-AS	AS34622	1	0.045%
61	DT-AS	AS39889	1	0.045%
62	PORTLANE	AS42708	1	0.045%
63	ITCONNECT-AS	AS43770	1	0.045%
64	BOSNET	AS44769	1	0.045%
65	CANDIDATOR-AB	AS49419	1	0.045%
66	SE-ACON-AS	AS50904	1	0.045%
67	ARKADEN	AS51132	1	0.045%
68	TEKNIKBYRAN	AS51815	1	0.045%
69	ELISA-AS	AS719	1	0.045%
70	TELENOR_DANMARK_AS	AS9158	1	0.045%

References

1. Gartner.com. *Operational Technology (OT)*. [cited 2022 05-17]; Available from: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot.

2. Kaspersky. *Threat landscape for industrial automation systems*. [cited 2022 03-03]; Available from: https://ics-cert.kaspersky.com/publications/reports/2022/03/03/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2021/.

3. Reuters.com. *Colonial Pipeline Halts All Pipeline Operations After Cybersecurity Attack*. [cited 2022 06-07]; Available from: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/.

4. Reuters.com. *Cyber attack hits JBS meat works in Australia, North America*. [cited 2022 06-07]; Available from: https://www.reuters.com/technology/cyber-attack-hits-jbs-meat-works-australia-north-america-2021-05-31/.

5. Reuters.com. *Ukraine's power outage was a cyber attack: Ukrenergo*. [cited 2022 06-07]; Available from: https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA.

6. Myndigheten för Samhällsskydd och Beredskap, *Guide to Increased Security in Industrial Control Systems*. 2014.

7. J.M. Ceron, J.J.C., J.J.C. Santanna, A. Pras, *Online Discoverability and Vulnerabilities of ICS/SCADA Devices in the Netherlands.* 2019.

8. IP2Location.com. *Sweden IP address ranges*. [cited 2022 05-17]; Available from: https://lite.ip2location.com/sweden-ip-address-ranges.

9. Shodan.io. *Homepage*. [cited 2022 05-17]; Available from: https://www.shodan.io/.

10. Oxana Andreeva, S.G., Gleb Gritsai, Olga Kochetova, and S.I.S. Evgeniya Potseluevskaya, Alexander A. Timorin, *Industrial Control Systems and Their Online Availability*. Kaspersky Labs.

11. Gregor Bonney, H.H., Benedikt Paffen, Marko Schuba, *ICS/SCADA Security - Analysis of a Beckhoff CX5020 PLC.* Proceedings of the 1st International Conference on Information Systems Security and Privacy: p. 137-142.

12. Marcin Nawrocki, T.C.S., Matthias Wählisch, *Uncovering Vulnerable Industrial Control Systems from the Internet Core.* NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium: p. 1-9.

13. Markus Dahlmanns, J.L., Jan Pennekamp, Jörn Bodenhausen, Klaus Wehrle, Martin Henze, *Missed Opportunities: Measuring the Untapped TLS Support in the Industrial Internet of Things.* Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security: p. 252–266.

14. Eric D. Vugrin, J.C., Christian Reedy, Thomas Tarman, Ali Pinar, *Cyber threat modeling and validation: port scanning and detection.* HotSoS '20: Proceedings of the 7th Symposium on Hot Topics in the Science of Security: p. 1-10.

15. W. Xu, Y.T., X. Guan, *The Landscape of Industrial Control Systems (ICS) Devices on the Internet.* IEEE 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment: p. 1-8.

16. Ismail Erkek, E.I., *Cyber Security of Internet Connected ICS/SCADA Devices and Services.* 2021 International Conference on Information Security and Cryptology: p. 75-80.

17. Marcin Nawrocki, T.C.S., Matthias Wählisch, *Industrial control protocols in the Internet core: Dismantling operational practices.* International Journal of Network Managment. **32**(1): p. 32-52.

18. Censys.io. *Internet Scanning Information*. [cited 2022 05-17]; Available from: https://support.censys.io/hc/en-us/articles/360059603231.

19. Shodan.io. *Industrial Control Systems*. [cited 2022 05-17]; Available from: https://www.shodan.io/explore/category/industrial-control-systems.

20. Austrian Energy CERT. *ICS Search Dorks*. [cited 2022 06-07]; Available from: https://github.com/AustrianEnergyCERT/ICS_IoT_Shodan_Dorks/blob/master/AEC_ICS_IOT_Shodan_dorks.CSV.

21. Lyon, G.F., *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. 2009, Insecure: Insecure.

22. Durumeric, Z., E. Wustrow, and J. Halderman, *ZMap: fast internet-wide scanning and its security applications*. 2013. 605-620.

23. Graham, R. *MASSCAN: Mass IP port scanner*. 2014; Available from: https://github.com/robertdavidgraham/masscan.

24. Partridge, C. and M. Allman, *Ethical considerations in network measurement papers.* Communications of the ACM, 2016. **59**: p. 58-64.

25. Zoomeye.org. *About*. [cited 2022 05-17]; Available from: https://www.zoomeye.org/about.

26. BigDataCloud.com. *AS Number Lookup*. [cited 2022 05-22]; Available from: https://www.bigdatacloud.com/asn-lookup.

27. CVE.org. *FAQs*. [cited 2022 06-07]; Available from: https://www.cve.org/ResourcesSupport/FAQs.

28. CVE.org. *Overview*. [cited 2022 06-07]; Available from: https://www.cve.org/About/Overview.

29. CVE.org. *Vulnerability definition*. [cited 2022 05-17]; Available from: https://www.cve.org/ResourcesSupport/Glossary?activeTerm=glossaryVulnerability.

30. nvd.nist.gov. *Homepage*. [cited 2022 05-17]; Available from: https://nvd.nist.gov/.

31. FIRST.org. *About*. [cited 2022 05-17]; Available from: https://www.first.org/about/.

32. FIRST.org. *Common Vulnerability Scoring System v3.1: Specification Document*. [cited 2022 05-17]; Available from: https://www.first.org/cvss/v3.1/specification-document.

33. Leeuwen, B.V., *Impacts of IPv6 on Infrastructure Control Systems* US Department of Energy, 2007: p. 19-24.

TRITA-EECS-EX-2022:515