Identifying Vulnerabilities on ICS Devices Connected to the Internet Using Shodan

Filip Polbratt
filpo653@student.liu.se

Christopher Peters
chrpe104@student.liu.se

***Abstract*—Standardized protocols operate on ICS- and BAC-devices. These devices are susceptible to vulnerabilities if their software is not maintained properly and some are completely lacking in security features. This investigation aims to quantify vulnerable devices across the Nordic countries, as well as compare and analyze the results using Shodan and CVE-search. The most popular protocols overall were identified by repeatedly querying Shodan over a period of time. Modbus and MQTT are examples of popular protocols across the Nordic countries, while are also shown to be operated on devices with vulnerable software versions. Our results show that more ICS- and BAC-devices are vulnerable than not in the Nordic countries.**

I. Introduction

There will be an expected 30 billion devices connected to the Internet in 2020, according to Cisco [1]. The Internet service provider Telia Company stated that on average, there were 16.9 connected devices per household in Sweden, in 2018 [2]. A portion of these connected devices is Industrial Control Systems (ICS) and Building Automation and Control (BAC) which may or may not be access points to significant hardware. These ICS devices are set up to use standard protocols and are totally transparent to the public using the Internet scanner tool, Shodan [3].

These ICS devices were originally intended for use on private networks in physically secure locations and often have little or no protection from malicious entities [4]. This paper aims to compare the devices in the Nordic countries as well as analyze the data gathered for potential vulnerabilities using CVE-search.

This paper will be structured as follows. Section II will provide background information and introduced concepts. Section III explains the methodology used in this paper. In section IV, the results are presented. In Section V, other, similar works are discussed. Section VI brings the paper to a close.

II. Background

This section describes the concepts and tools that are of interest in this project report. The purpose of this section is for the reader to gain an overall understanding of these topics.

A. Industrial Control System

Internet of Things (IoT) is a term for physical devices that operates primarily with little human interaction while communicating with other, similar devices over the Internet [5]. Supervisory Control and Data Acquisition (SCADA) is a scheme for controlling a system of distributed devices interacting with the physical world. These devices are connected to a network where the devices are controlled by a control center. This SCADA-network is a type of ICS which is a more general term for systems that control an industrial process [4].

B. Shodan.io

Shodan is a search engine for the devices on the Internet. Compared to the search engine Google, which searches the World Wide Web for hosts, Shodan detects all devices directly connected to the Internet. This is a powerful tool for engineers and developers. It allows for precise queries with the purpose of finding out how many, what type, and in what way devices are connected to the Internet. For instance, if a new exploit was trending, one could use Shodan to find devices that are vulnerable to that exploit [6].

C. Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) is a common standard for giving vulnerabilities and exposures unique identifiers for interoperability between security products and software. Being a common standard, new threats and discovered vulnerabilities are being collectively gathered and entered by engineers and representatives across the world [7].

D. CVE-search

Computer Incident Response Center Luxembourg (CIRCL) hosts a web interface and REST API to a CVE-search database. CVE-search fuses several feeds regarding security vulnerabilities into a single database that is free and open source and can be queried for security vulnerabilities in both hardware and software. Feeds that are fused in the CVE-search database at CIRCL are NIST National Vulnerability Database, Common Platform Enumeration, Common Weakness Enumeration, toolswatch/vFeed, and CIRCL's own statistics [8].

E. Protocols

Network protocols have specific port numbers reserved for their services. Knowing what protocol to investigate, its network standard specifies what ports to scan. The ICS device-related protocols which were of greater interest in this project, are the following.

1) Modbus: Modbus is a serial communications protocol for ICS devices, standardized by Modicon in 1979. Modbus uses port 502 [9]. Modbus does not have any security features in its original guise.

2) Message Queue Telemetry Transport (MQTT): MQTT is a lightweight machine-to-machine protocol that uses publish/subscribe messaging transport on port 1883 [10].
3) Emerson/Fisher ROC: Emerson Remote Operations Controllers and other Emerson devices communicate to a ROC Polling Server using the Emerson ROC protocol on port 4000 [11].
4) EtherNet/IP: EtherNet/IP converts common control device messages into EtherNet packets so that it can be transmitted through a network. EtherNet/IP uses TCP on port 44818 for explicit messaging and UDP on port 2222 for implicit messaging [12].
5) Niagara Fox: Niagara Fox is a proprietary protocol used on the ports 1911 and 4911 on Tridium platforms. Niagara^{AX} is Tridium's original platform for IoT devices to be network connected and controlled. Niagara 4 is its successor and allows for more complex features such as advanced visualization, security and navigation tools.

III. Methodology

This section describes the process of this project. It is meant to express how the result is achieved. The main methods for this project were the use of public APIs and analysis based on information from external authorities.

A. Identifying popular protocols

Shodan has several account-tiers which grant access to different features of Shodan's API, e.g. filters, and in different amounts. Each account tier has a monthly refreshing amount of query credits attached to it. These credits are used to get the following pages of results when there are more than 100 results to a query. However, it is possible to use a query that only returns the total number of results. We used this type of query to determine which protocols were popular.

For this project to be able to contribute useful results, the scope of research was limited to the five most popular protocols for ICS devices in each Nordic country. These were found by querying Shodan's API. Using Shodan's API has multiple benefits. Repeating extensive groups of queries is simplified compared to manually inputting each query to Shodan. It allows for easier analysis of data since the data is delivered in JSON-format.

The most established protocols along with appropriate filters were preemptively gathered in order to make queries to Shodan on an hourly basis during the time period of seven days. This occurred automatically and the quantities were put into a local database for later assessment. After the mentioned time period, the average of each protocol in each country was calculated and finally, the top five protocols for each country was extracted. The initial list of protocols and their default ports were based on [13]. The list of protocols and filters used can be found in Appendix A.

B. Analysis of selected protocols

For further analysis of ICS and BAC protocols in the Nordic countries, the field of additional data Shodan provides in a query response will be used. From the previous phase of querying Shodan, it became apparent that a Freelancer account at Shodan would be necessary to gather all results due to the amount of found hosts. To keep this task manageable we restricted this to only the most popular protocols. To make sure that protocols of interest in all the Nordic countries are analyzed, the five top-five protocols of each country were selected for analysis. The same filters were used in querying Shodan as when the popularity of protocols was determined.

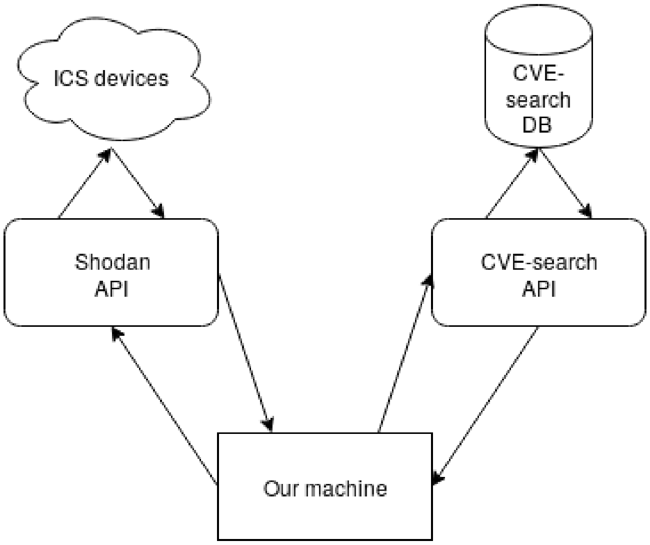

Fig. 1. Process
The process of acquiring device- and vulnerability data.

Following the gathering of data, it was subject to analysis. In order to identify what devices were vulnerable, CVE-search provided complete sets of vulnerabilities of products which could be queried using CIRCL's API. By identifying what product a device was specified as, and querying the vulnerabilities for that product, vulnerable software versions could be mapped back and compared to the software version running on the device. Figure 1 illustrates the process.

The atomic distinction of the vulnerability analysis is that there are only two possible outcomes when classifying a device as being vulnerable or not.

- If a device has at least one vulnerability, it is identified as vulnerable.
- In any other case, it is identified as without known vulnerabilities.

Furthermore, since the Modbus protocol does not implement security features, every identified Modbus device was considered vulnerable. Additionally, the data provided by Shodan is not always detailed enough to identify versions of software or even the name of the software being run on a device, in this case, the device cannot be considered vulnerable.

Protocols were investigated based on what information Shodan had retrieved and how vulnerabilities were recorded in the CVE-search database. For each protocol, the approach was the following:

1) Siemens S7: Devices that use the Siemens S7 protocol are standardized and can be categorized within families. Vulnerabilities inhabiting specific software versions could be identified, by mapping each device's family.
2) Niagara Fox: The software which is run on the Niagara platform are Niagara^{AX} and Niagara 4. The data field only expressed software versions for the former software, which could be analyzed for vulnerability. However, if a device was running Niagara 4 it was not possible to identify versions with known vulnerabilities since they only return their platform version as ”Niagara 4”.
3) MQTT: Identifying what connection code a device returned to Shodan determined the accessibility to the device. If the connection code was equal to ”0”, this means anyone can access the device without authentication which grants the user administrative privileges. This is what was looked for. Furthermore, if the device returned connection code ”0” it was possible to analyze the server software. If the device was running a Mosquitto server, it was investigated whether or not the device had any more vulnerabilities.
4) Emerson/Fisher ROC: The data Shodan received from devices running on port 4000 was unidentifiable as part of the Emerson/Fisher ROC protocol. There was no way to detect vulnerabilities.
5) EtherNet/IP: A large majority of devices running on EtherNet/IP protocol are Rockwell Automation/Allen-Bradley devices. These devices can be categorized into families and for each family, vulnerable software versions are available on the vulnerability lists that CVE-search supplies. Additionally, devices from Schneider Electric and WTW were analyzed. Together the three have manufactured roughly 90% of all EtherNet/IP devices that were identified.
6) Modbus: Has Shodan detected a device running on Modbus, it is vulnerable by default. In October of 2018, the Modbus Organization announced a new secure version of Modbus which will be running on port 802 and products should start to enter the market in 2019 [14].

IV. Result

Shodan was queried for data in two campaigns. First, the most popular ICS and BAC protocols in the Nordic countries were determined by querying Shodan every hour for two days starting on the first of April. This was used to determine what protocols to focus on the second time data was gathered in late April. The results from both phases are presented below.

A. Popularity of protocols

The Nordic countries are quite homogeneous in what protocols they use for ICS and BAC. In Table I the commonly used protocols in Sweden are listed in order of popularity. Similarly, Table II lists the protocols popular in Denmark, Table III the protocols in Norway, Table IV the protocols in Finland and Table V the popular protocols in Iceland. In the five top-fives, only six unique protocols feature. These six are the protocols that were studied in more detail and data from Shodan analyzed for vulnerabilities.

Modbus	1084
MQTT	627
Emerson/Fisher ROC	210
EtherNet/IP	166
Niagara Fox	137

TABLE I
Top five most popular ICS protocols in Sweden.

Niagara Fox	275
Modbus	153
EtherNet/IP	141
MQTT	136
Siemens S7	30

TABLE II
Top five most popular ICS protocols in Denmark.

B. Vulnerabilities of devices

For each protocol and country, vulnerabilities in devices will be illustrated. The distinction of devices running on EtherNet/IP was made since Rockwell Automation/Allen-Bradley devices were an overwhelming majority of EtherNet/IP devices discovered. Furthermore, devices running the MQTT protocol that also have a Mosquitto server up and running were more closely investigated. Figure 2 below illustrates the portion of vulnerable devices relative to devices where no vulnerabilities could be identified.

In Figure 3 all vulnerable devices detected per protocol and country are presented.

Figure 4 illustrates the proportion of devices communicating over Niagara Fox in each Nordic country which are vulnerable to the total amount of Niagara Fox using devices in each country. In Figure 5 the same type of proportional illustration is made for devices communicating over Siemens S7.

Rockwell Automation/Allen-Bradley devices are a majority of identified EtherNet/IP devices and are illustrated alongside the vulnerable and total identified EtherNet/IP devices in Figure 6. All devices identified as vulnerable were from Rockwell Automation/Allen-Bradley.

Niagara Fox	360
MQTT	198
Emerson/Fisher ROC	156
EtherNet/IP	130
Modbus	98

TABLE III
Top five most popular ICS protocols in Norway.

MQTT	274
EtherNet/IP	269
Niagara Fox	137
Modbus	100
Emerson/Fisher ROC	31

TABLE IV
Top five most popular ICS protocols in Finland.

EtherNet/IP	48
MQTT	14
Siemens S7	7
Modbus	1
Emerson/Fisher ROC	1

TABLE V
TOP FIVE MOST POPULAR ICS PROTOCOLS IN ICELAND.

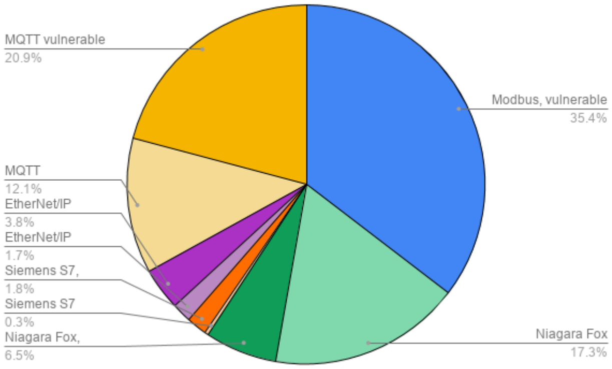

Fig. 2. Proportions of vulnerable protocols out of all protocols

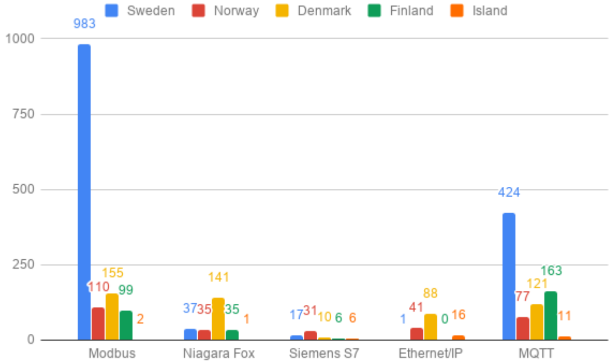

Fig. 3. Vulnerabilities over protocols and countries

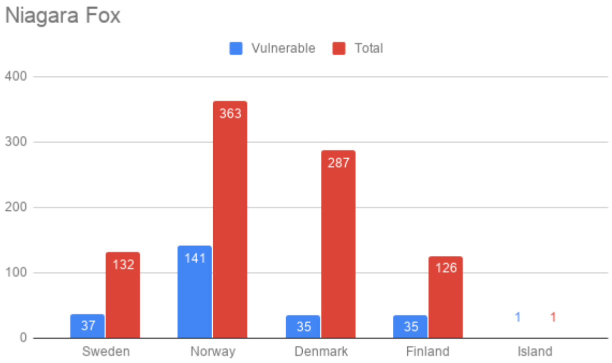

Fig. 4. Niagara Fox

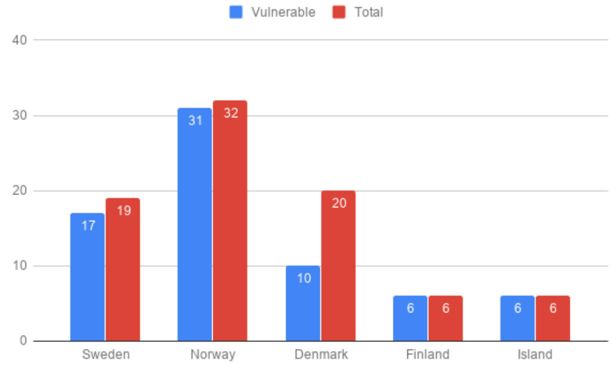

Fig. 5. Siemens S7

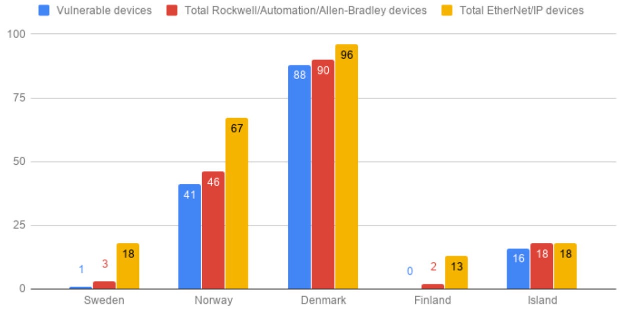

Fig. 6. EtherNet/IP with proportion of Rockwell Automation/Allen-Bradley manufactured devices.

Figure 7 illustrates the proportions of MQTT devices that do not require authentication to access.

For the MQTT protocol, a large portion (587 of 796) of the devices without authentication were running Eclipse Mosquitto, an open source message broker for the MQTT protocol. Mosquitto is a common tool to connect IoT devices. The default configuration for Mosquitto is to run without authentication [15]. When this is the case, Shodan can identify the version of Mosquitto running on the device. Figure 8

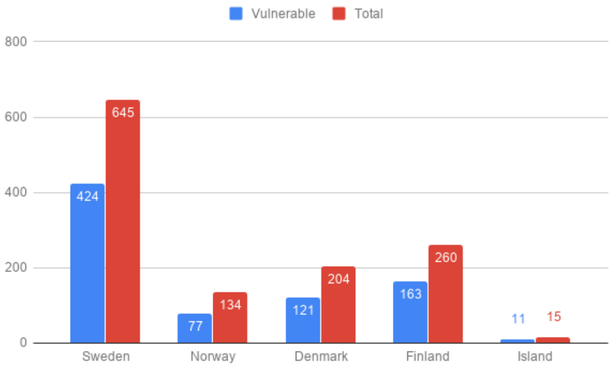

Fig. 7. MQTT

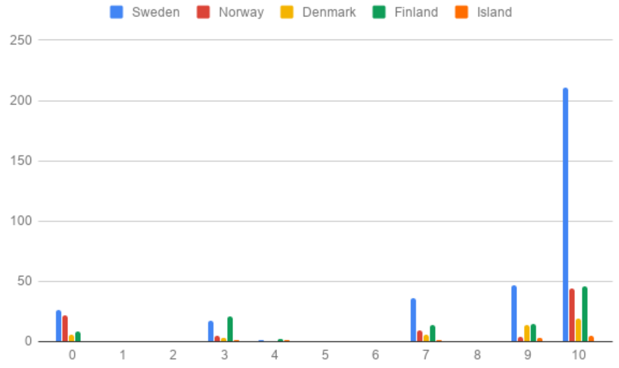

Fig. 8. Vulnerabilities on Mosquitto brokers

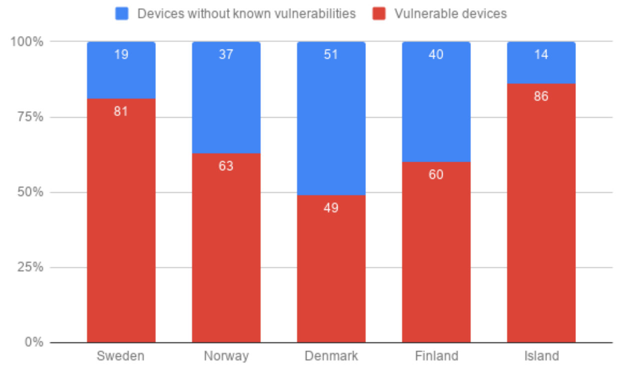

Fig. 9. Proportion of devices per country that are vulnerable

illustrates the number of vulnerabilities per device running Mosquitto per country.

The proportion of ICS and BAC devices that were found to be vulnerable are illustrated per country in Figure 9.

V. Related Work

This project was partially inspired by the work of Hasson et al. However the scope of this project was expanded across the Nordic countries and a different type of analysis was made [16]. Their scope was limited to devices in Sweden and a direct comparison between our results are the number of devices running MQTT, EtherNet/IP, Modbus and Niagara Fox protocol. This is shown in Table VI.

VI. Conclusion

Overall, a large portion of ICS devices is operated on vulnerable software, as can be seen in Figure 2 and in Figure 9. We were not able to investigate the protocol Emerson/Fisher ROC as Shodan did not return results that provide information about what hardware and software they were using. As for the other five protocols: Siemens S7, Niagara Fox, MQTT, EtherNet/IP, Modbus, the following conclusions can be made.

Year	2018	2019	Change
MQTT	341	627	84%
EtherNet/IP	269	166	-38%
Niagara Fox	120	137	14%
Modbus	894	1084	21%

TABLE VI
A QUANTITY COMPARISON OF DEVICES RUNNING ON PROTOCOLS IN SWEDEN

1) Siemens S7: Most devices in most Nordic countries were identified to have some vulnerability. Only Denmark stood out were half the devices had no known vulnerability. Overall, Siemens S7 devices found by Shodan are vulnerable and Shodan can provide very specific information about devices communicating on Siemens S7.
2) Niagara Fox: Shodan is very capable of identifying and providing information about devices running Niagara^{AX}, but not for the more modern Niagara 4. This causes some issues with determining if a Niagara 4 device uses an application version with known vulnerabilities.
3) MQTT: The number of MQTT devices have grown explosively in Sweden since [16]. It is a very popular protocol in all Nordic countries, if slightly less so in Denmark. It is fair to claim that this protocol is very vulnerable due to the most popular server having a default configuration that does not require any authentication. The percentage devices that do not use authentication is roughly similar among the Nordic countries at around 60% with Iceland as the exception at 73%.
4) EtherNet/IP: At the time of measurement, EtherNet/IP was by far the most popular protocol used in Iceland, representing slightly more than two-thirds of all devices. The absolute majority of devices (in all Nordic countries) using the EtherNet/IP protocol are manufactured by Rockwell Automation/Allen-Bradley. Most of these were run on vulnerable firmware versions. Detailed figures can be seen in Figure 6.
5) Modbus: This protocol is vastly more popular in Sweden than in the other Nordic countries, almost three times the others combined. It is also interesting to note that the number of Modbus devices in Sweden has increased by 21% since [16] investigated ICS devices in Sweden.

As shown in Figure 8, there are large quantities of devices running Mosquitto servers which inherently represent a large number of IoT-devices being connected to the Internet. In total, more devices are vulnerable than not in the Nordic countries. The only exception to this is Denmark in which 51% of devices do not have known vulnerabilities.

VII. Acknowledgment

Our mentor for this project, Andrei Gurtov, supported this project by providing a freelance account for Shodan so that we were able to gather extensive amounts of data.

References

[1] T. Stack, *Internet of things (iot) data continues to explode exponentially. who is using that data and how?* Feb. 2018. [Online]. Available: https://blogs.cisco.com/datacenter/internet-of-things-iot-data-continues-to-explode-exponentially-who-is-using-that-data-and-how.

[2] *Explosive growth of connected devices in sweden in 2018*, Jan. 2019. [Online]. Available: https://www.teliacompany.com/en/news/news-articles/2019/connected-devices-2018/.

[3] [Online]. Available: https://www.shodan.io/.

[4] K. A. Stouffer, J. A. Falco, and K. A. Scarfone, "Sp 800-82. guide to industrial control systems (ics) security: Supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc)," Tech. Rep., 2011.

[5] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," *arXiv preprint arXiv:1807.10438*, 2018.

[6] [Online]. Available: https://help.shodan.io/the-basics/what-is-shodan.

[7] [Online]. Available: https://cve.mitre.org/about/index.html.

[8] [Online]. Available: https://www.circl.lu/services/cve-search/.

[9] Apr. 2004. [Online]. Available: http://www.modbus.org/docs/ProtocolTransfer0404.pdf.

[10] [Online]. Available: http://mqtt.org/.

[11] [Online]. Available: https://www.emerson.com/documents/automation/manual-roc-polling-services-user-manual-en-133774.pdf.

[12] [Online]. Available: https://www.odva.org/Technology-Standards/EtherNet-IP/Overview.

[13] [Online]. Available: https://web.archive.org/web/20111203052654/http://www.digitalbond.com/tools/the-rack/control-system-port-list.

[14] [Online]. Available: http://www.modbus.org/docs/Modbus-SecurityPR-10-2018.pdf.

[15] [Online]. Available: https://mosquitto.org/man/mosquitto-conf-5.html.

[16] A. Hansson, M. Khodari, and A. Gurtov, "Analyzing internet-connected industrial equipment," in *2018 International Conference on Signals and Systems (ICSigSys)*, IEEE, 2018, pp. 29–35.

Appendix A

Following is a table of terms used to find ICSs using Shodan's API. Prefixing a term with '-' is equivalent to a logical NOT and '+' is an explicit logical AND.

Protocol	Port	Filter terms
S7	102	"Basic Hardware"+"Module" "+Basic Firmware"
Modbus	502	Unit ID
Red Lion	789	"Red Lion Controls"
Foundation Fieldbus HSE	1089,1090,1091	-DHT -NetBIOS -Ubiquiti
Foxboro DCS Informix	1541	-DHT
MQTT	1883	MQTT
Niagara Fox	1911,4911	"^fox a 0"
PCWorx	1962	PLC
EtherNet/IP	2222,44818	-SSH -HTTP -FTP -220 -TeamSpeak -Agent -html -Yoshi -Verlihub
IEC 60870-5-104	2404	asdu address
CODESYS	2455	operating system
Emerson/Fisher ROC	4000	-HTTP -SSH -ERROR
OPC UA	4849	DisplayName
Project/SCADA	4592, 14592	-DHT -SIP
MELSEC-Q	5006,5007	product:mitsubishi
HART IP	5094	HART-IP
Telvent OASyS DNA	5050,5051,5052,5065, 12135,12136,12137, 56001 to 56099	-HTTP -SSH
OSIsoft	5450	-DHT -HTTP
OMRON-FINS	9600	response code
Automated Tank Guage	10001	I20100
ABB Ranger 2003	10307,10311,10364, 10365,10407,10409, 10410,10412,10414, 10415,10428,10431, 10432,10447,10449, 10450,12316,12645, 12647,12648,13722, 13724,13782,13783, 38589,38593,38600, 38971,39129,39278	-DHT -Ubiquiti -HTTP
Metasys N1	11001	-DHT -Ubiquiti -HTTP
Genesis32 GenBroker	18000	-DHT -HTTP
GE-SRTP	18245,18246	product:"general electric"
DNP3	20000	source address
ProConOS	20547	PLC
PROFINET	34962,34963,34964	-DHT -Ubiquiti -SIP
EtherCAT	34980	-DHT -Ubiquiti -SIP
SNC GENe	38000,38001,38011, 38012,38014,38015, 38200,38210,38301, 38400,38700,62900, 62911,62924,62930, 62938,62956,62957, 62963,62981,62982, 62985,62992,63012, 63041,63075,63079, 63082,63088,63094, 63027 to 63036 and 65443	-DHT -HTTP -Ubiquiti -SIP
Foxboro DCS AIMAPI	45678	-DHT -HTTP -Ubiquiti -SIP
Spectrum Power TG	50001 to 50016, 50018,50019,50020, 50021,50025,50026, 50027,50028,50110, 50111	
BACnet/IP	47808	"Instance ID","BACnet"
FL-net	55000,55001,55002, 55003	-DHT -HTTP -Ubiquiti -SIP