Finding and analyzing ICS devices in the Nordic Countries

Isak Toivanen
Linköping university
Linköping, Sweden
isato760@student.liu.se

Samuel Knutsson
Linköping university
Linköping, Sweden
samkn228@student.liu.se

***Abstract*—More and more protocols are connected to the internet every day, but some devices that are connected totally lack security features which makes them very vulnerable. This report tries to map how many devices in the Nordic countries that are currently connected to the internet with vulnerable protocols. The result differs very much between the different countries and there also seems to be a correlation with the number of ICS devices and the GDP in the analyzed countries.**

I. Introduction

Around the world there are an increasing amount of devices that can connect to the internet. The thing that is often forgotten is the security in these devices. 30.9 billion[1] devices are connected as the project is being performed and a portion of these are Industrial Control Devices (ICS). What makes ICS devices stand out is the fact that the protocols that often are used in the devices have known vulnerabilities[2]. This project is aimed to find these devices that are openly connected to the internet and could possibly be harmful if the wrong person finds them. ICS devices were not connected openly from the beginning, the ICS devices then were often connected in small closed networks and did not have any security features. The project will compare how many ICS devices that are connected in different countries and what protocols they are using. The project will also cover how the results differ in countries based on their GDP to find if there is any correlation.

II. Background

A. General information

1) shodan.io: Shodan.io is a search engine for finding devices connected to the internet. Shodan.io is different from ordinary search engines like firefox in the fact that firefox searches on www sites while shodan will search the whole internet [1]. By finding devices connected to the internet it is easy to find current vulnerabilities and unexpected exposures. These devices that are found by Shodan can be hidden if security implementations are made. An example of an method used to hide a device from Shodan is port knocking [2]. This project will use shodan.io to scavenge the internet for ICS devices that are potentially vulnerable and compare results based on different factors like protocols and country. Shodan.io will be the main source of information in the project.

2) ICS: ICS means Industrial Controls System and is a collective concept that is used to describe devices that are used to either monitor or automate certain processes [3]. This includes webcams and sensors that are connected to the internet to monitor industrial processes. The problem with some of these devices are that they, from the beginning, were only used in local environments so the security features did not have to be developed. The problem therefore comes now more than ever since more and more of unsecured ICS devices are connected to the internet directly, even with known security flaws. These are the kind of ICS devices that this report will target.

B. Different protocols used on the ICS-devices

1) Modbus: Modbus is a client-server communication protocol that is used among different devices and was invented in 1979. The thing that makes Modbus widely used is the fact that it is truly open and has a de facto standard. The protocol provides an easy access to a control system without requiring any authentication [4]. Modbus uses serial communication and only uses port 502 when sending data. The lack of authentication with the Modbus protocol allows for a known exploit that starts and stops the ICS device's processes by sending function code 90 to the device.

2) MQTT: MQTT (Message Queuing Telemetry Transport) is a transport protocol with Client-Server architecture that uses publish/subscribe messaging to communicate. The protocol has been published as an official OASIS standard meaning that it is also open source [5]. MQTT is lightweight with low complexity, being energy efficient and has low overhead. The protocol requires a TCP/IP connection with port 1883 but can also use TLS/SSL with port 8883. A MQTT client can either be a publisher or a subscriber to a specific topic. A central server called broker uses these subscriptions to forward information to interested clients [6]. MQTT cannot be connected directly to other clients and can only communicate with a broker.

3) BACnet: BACnet (Building Automation and Control networks) is a communication protocol designed for building automation and control systems. Examples of modern building automation and control networks are heating, air-conditioning and lighting. BACnet comes with an optional security architecture that is not always used within the building automation industry because it has been deemed unnecessary with extra network security [7]. The protocol communicates with two different techniques request-response and event-based communication. Both cases of communication use client-server principle [8]. The client is the building device and the server is the control unit that oversees the devices. The most common communication made between client and server is Read-Property and Write-Property. BACnet uses port 47808 for communication.

4) Emerson/Fisher ROC: Emerson/Fisher ROC (Remote Operations Controller) is a protocol used by Emerson devices to communicate to a ROC server. It uses Electronic Flow Monitoring to track flow data at remote sites [9]. ROC devices are most commonly found at industrial automations. The device collects data from measurements for example gas measurements and uses the protocol to send this data to the ROC server. The protocol communicates through port 4000.

5) Niagara fox: With the Niagara Framework comes a proprietary protocol Fox which is used for communication between different stations and workbench-to-station. Fox sits on top of a TCP connection and functions as a multiplexed peer to peer protocol [10]. Niagara Fox can be seen as a predecessor to Niagara 4. With Niagara 4 came a lot of security features not present in Niagara Fox. A security feature that the protocol uses is the security model of users with permissions [4]. The default communication port for Niagara Fox is 1911.

6) DNP3: DNP3 is a request-response protocol that is commonly used in automated systems. Communication with the protocol DNP3 is between a device and outstations that are servers [11]. When communicating between a device and outstation DNP3 uses Secure Authentication (DNP3-SA). Secure Authentication authenticates messages between device and outstation [12]. An ICS-device using DNP3 monitors relevant data with the help of different sensors and sends status-updates to the outstations. The protocol is constructed in the following four layers: Application layer, Pseudo Transport Layer, Data Link layer and Physical layer [13]. DNP3 has port 20000 as default.

7) EtherNet/IP: EtherNet/IP is a protocol that makes use of the CIP protocol. The CIP protocol stands for Control and Information Protocol and uses objects for sending packets when communicating. There are different objects that can be sent in a packet but the required ones are identification objects, connection objects and message routing objects [14]. The EtherNet/IP architecture follows a producer and consumer model where producer is a device sending data and the consumer receives the data. The producer can send data which is obtained by multiple consumers simultaneously through the network. CIP provides multiple ways of communication. This results in EtherNet/IP using port 2222 for UDP traffic and port 44818 for TCP traffic [15].

8) S7: S7 is a Siemens owned communication protocol that is used between PLCs and a S7 device where PLC stands for programmable logic controller. A device using S7 can use the communication protocol as a tool for programming the PLC's, accessing PLC data and exchange data between PLCs [16]. S7 runs on port 102.

III. Method

The method will consist of two major parts. Part one is identifying different protocols used for ICS devices. This will be done by research. The second part is to use shodan to query results. This project will not target only IPv6 devices so the results are based on both IPv6 and IPv4 devices. Also, this project will not investigate devices on a closer level but merely look at the statistics as a whole. This project will therefore not include any specific pictures of devices.

- Number of ICS devices in the nordic countries
- Top 5 most used protocols in the each of the nordic countries
- Has the number of ICS devices decreased or increased in the Nordic Countries.

IV. Results and collected data

Much of the information we gather will be numbers so we will then create graphs and tables to be able to compare results. The results will cover the questions raised in the section above.

A. Top protocols in Sweden

From the results from shodan.io the top 5 protocols used in sweden. Down below are the number of devices used by each of the protocols and the percent of the total protocols.

1) Modbus: 1410

2) MQTT: 1394

3) Ethernet/IP: 273

4) Niagara Fox: 187

5) BACnet: 31

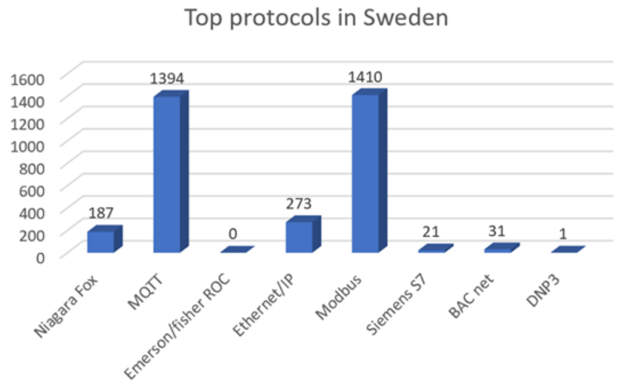


Fig. 1. Top protocols in Sweden

B. Top protocols in Finland

From the results from shodan.io the top 5 protocols used in Finland. Down below are the number of devices used by each of the protocols and the percent of the total protocols.

1) MQTT: 805

2) Ethernet/IP: 254

3) Modbus: 166

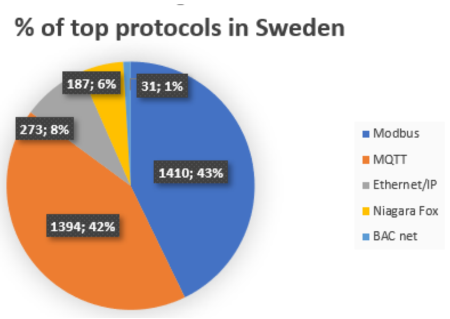


Fig. 2. % of top protocols in Sweden

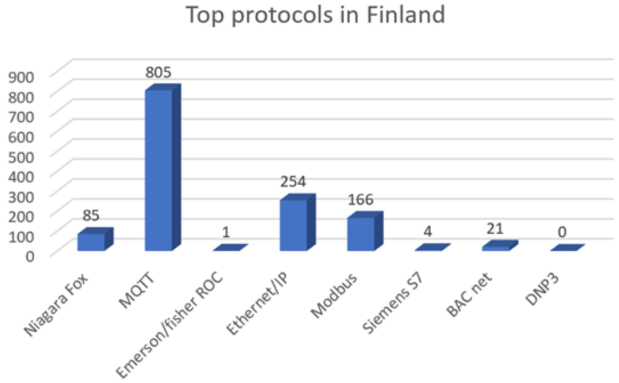


Fig. 3. Top protocols in Finland

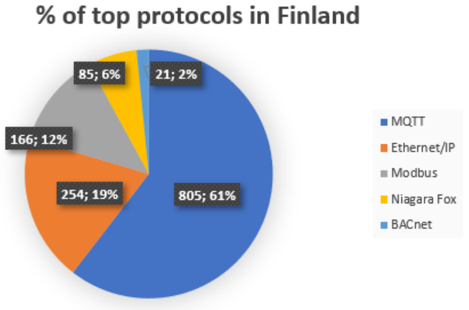


Fig. 4. % of top protocols in Finland

4) *Niagara Fox:* 85
5) *BACnet:* 21

C. Top protocols in Denmark

From the results from shodan.io the top 5 protocols used in Denmark. Down below are the number of devices used by each of the protocols and the percent of the total protocols.

1) *Niagara Fox:* 466
2) *Modbus:* 270
3) *MQTT:* 194
4) *Ethernet/IP:* 179
5) *BACnet:* 30

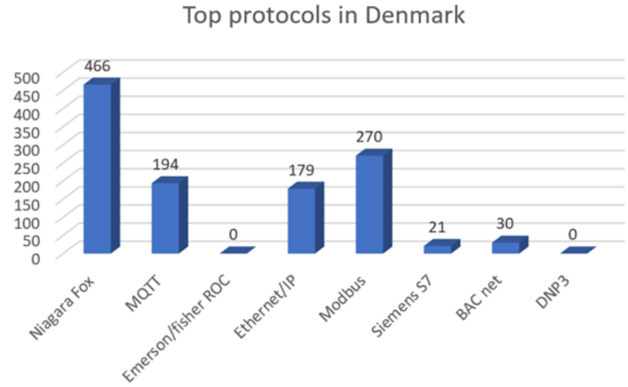


Fig. 5. Top protocols in Denmark

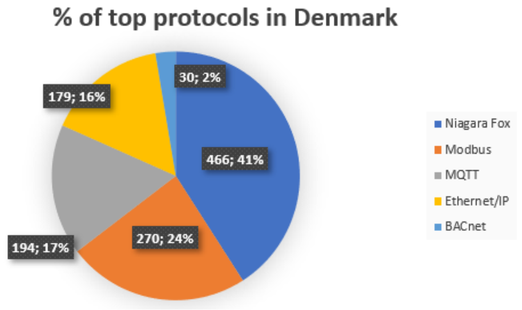


Fig. 6. % of top protocols in Denmark

D. Top protocols in Norway

From the results from shodan.io the top 5 protocols used in Norway. Down below are the number of devices used by each of the protocols and the percent of the total protocols.

1) *Ethernet/IP:* 789
2) *MQTT:* 281
3) *Niagara Fox:* 239
4) *Modbus:* 144
5) *Siemens s7 and BACnet:* 12

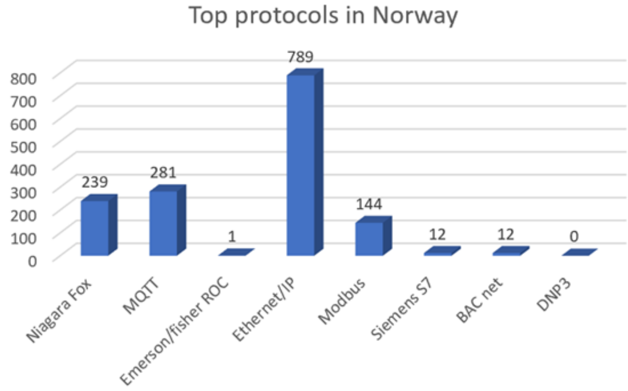


Fig. 7. Top protocols in Norway

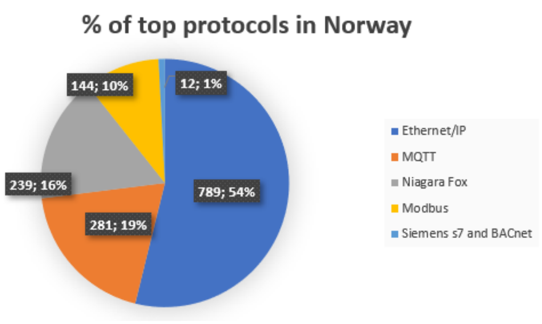


Fig. 8. % of top protocols in Norway

E. Top protocols in Iceland

From the results from shodan.io the top 5 protocols used in Island. Down below are the number of devices used by each of the protocols and the percent of the total protocols.

1) *Ethernet/IP:* 61
2) *MQTT:* 22
3) *Modbus:* 7
4) *Siemens S7:* 3

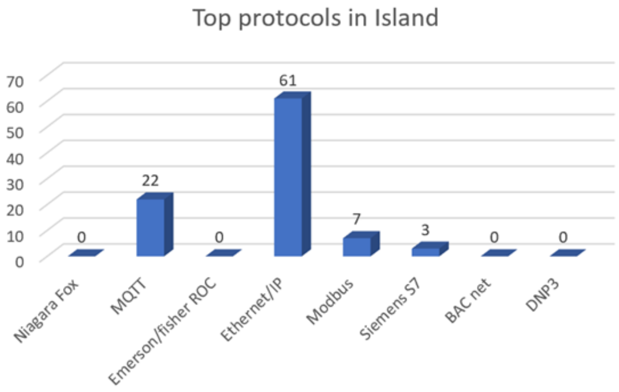


Fig. 9. Top protocols in Iceland

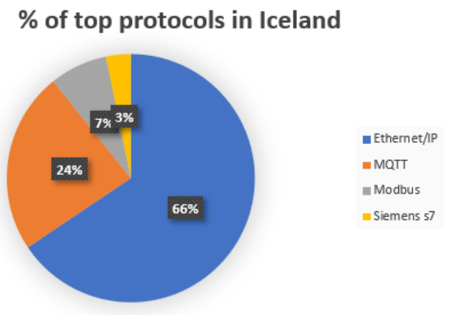


Fig. 10. % of top protocols in Iceland

F. GDP in the different countries

- GDP in Sweden is 537,6 Billion USD.
- GDP in Denmark is 355,2 Billion USD.
- GDP in Norway 362 Billion USD.
- GDP in Finland is 271,2 Billion.
- GDP in Iceland 21,71 Billion USD.

As we can see when comparing GDP in the analyzed countries, Sweden has highest BNP followed by Norway, Denmark, Finland and Iceland.

G. Estimate of Total amount of ICS per country

To make a good estimation we will add the number of the top 5 protocols for every country since it will give a good estimation of the number of ICS devices in that country.

1) *Sweden:* 3295
2) *Finland:* 1331
3) *Denmark:* 1139
4) *Norway:* 1465
5) *Iceland:* 93

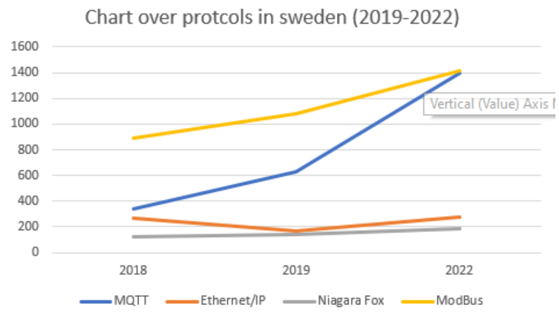
H. Earlier years results regarding increase and decrease of ICS devices connected to the internet

From this article [17] we have gathered very relevant data that we can use to compare our results. This article is from an earlier year of the course and we sincerely hope that we can use some of the results stated in this paper.

1) *Number of ICS devices earlier years in Sweden:*

protocol	2018	2019	2022
MQTT	341	627	1394
Ethernet/IP	269	166	273
Niagara Fox	120	137	187
ModBus	894	1084	1410

TABLE I
NUMBER OF PROTOCOLS EARLIER YEARS IN SWEDEN



As the result states from earlier years there has been an great increase in both MQTT and ModBus while Ethernet/IP and Niagara Fox has not changed so much. To make results more clear, no information from 2020 and 2021 was found so the results stated above may not be exact in that time frame.

2) *Trends in ICS devices in Finland:*

protocol	2019	2022	difference
MQTT	274	805	194%
Ethernet/IP	269	254	-5.6%
Modbus	100	166	66%
Niagara Fox	137	85	-38%
BACnet	NaN	21	NaN%

TABLE II
NUMBER OF PROTOCOLS EARLIER YEARS IN FINLAND

3) *Trends in ICS devices in Norway:*

protocol	2019	2022	difference
Ethernet/IP	269	789	193%
MQTT	274	281	3%
Niagara Fox	NaN	239	NaN%
Modbus	98	144	47%
Siemens s7	NaN	12	NaN%

TABLE III
NUMBER OF PROTOCOLS EARLIER YEARS IN NORWAY

4) *Trends in ICS devices in Denmark:*

protocol	2019	2022	difference
Niagara Fox	275	466	69%
Modbus	153	270	76%
MQTT	136	194	43%
Ethernet/IP	141	179	27%
BACnet	NaN	30	NaN%

TABLE IV
NUMBER OF PROTOCOLS EARLIER YEARS IN DENMARK

5) *Trends in ICS devices in Iceland:*

protocol	2019	2022	difference
Ethernet/IP	48	61	27%
MQTT	14	22	57%
Modbus	1	1	0%
Siemens S7	7	3	-57%

TABLE V
NUMBER OF PROTOCOLS EARLIER YEARS IN ICELAND

V. DISCUSSION

In this section we will compare different protocols and talk more about interesting finding about ICS devices and correlation to the GDP. A subsection for each of the protocols exist where discussion relating to that specific protocol exists.

A. Results compared to GDP

Number of ICS devices compared to GDP.

Country	GDP[USD]	Number of ICS devices
Sweden	536.6 Billion	3295
Norway	362 Billion	1465
Denmark	355.2 Billion	1139
Finland	271.1 Billion	1331
Iceland	21.71 Billion	93

TABLE VI
GDP COMPARED TO NUMBER OF ICS DEVICES

From the results that we gathered there is clear that there is some kind of correlation between the GDP in the country compared to the number of ICS devices. This could be due to the fact that GDP has a correlation to how wealthy a country is and more wealthy countries therefore could have more usage of ICS devices. The number of ICS devices could therefore be used to get a estimate picture of the economy of the studied country. This result is similar to result stated by an article [18] that did a comparison on a bigger scale and that came to the same conclusion that there definitely could be a correlation between the two. Both our study and the comparing study are not getting exact results so it cannot be trusted to exactly determine the number of ICS devices. In our small scale study Denmark and Finland should change places to make the result more exact but there is still a trend that is very promising. This result is also somewhat expected since a country with better economy is expected to have more advanced technology and more possibilities. Therefore the result is not surprising in any way but still very interesting to acknowledge.

As stated before, the result would have been more exact if Denmark and Finland swapped places with each other and that could be misleading. This result could correspond not only to the total number of devices but also the type of devices that the country has. If we compare Denmark with Finland we can see that the top protocol in Finland is MQTT and the top Protocol in Denmark is Niagara Fox. MQTT are more used from machine to machine (M2M) communication on an industrial scale while Niagara Fox is more specific and is used between Niagara systems by Tridium. Since Tridium is a very big company and has a great amount of these devices in Denmark, that could indicate on great industry and therefore greater GDP.

B. Expected result

The expected result is close when approximating the number of ICS devices since it is obvious that bigger countries are supposed to have more ICS devices. The thing that was most surprising was that there was such a big difference what protocols that were used. Since all the analyzed countries were Nordic countries and very close to each other geographically, we would suspect that the same protocols would dominate on the market. But our results proves the theory very wrong and this outcome can have many explanations. Down below in our report will try to explain the result and what the difference could depend on.

C. Niagara Fox

Niagara Fox can be found in all Nordic countries except Iceland. In Iceland the total number of protocols could be considered so small and be the main reason why Niagara Fox is not present. When comparing the percentage of vulnerable devices using Niagara Fox with the total amount of vulnerable ICS devices found for a specific country we get the following numbers. Denmark (41%), Norway (16%), Finland (6%), Sweden (6%) and Iceland (0%). Sweden, Finland and Norway all have percentages that can be expected since they all are somewhat similar. Denmark on the other hand has a large share of the ICS devices using Niagara Fox. The reason for Denmarks large share of Niagara Fox is that two companies, TDC A/S and Hi3G Access AB, together have 260 devices with the protocol within their IP ranges. TDC A/S is a danish company that only operates in Denmark while Hi3G Access AB is a Swedish company. Something interesting about Hi3G is that there are approximately 130000 devices in Sweden and 85000 in Denmark. Even though the total number of devices are in Sweden's favor the amount of vulnerable devices using Niagara Fox is higher in Denmark with 466 compared to Sweden's 187.

D. MQTT

MQTT is found in all researched countries at a high percentage. Since the MQTT protocol is an OASIS standard it is most likely commonly used by companies and Internet of Things related projects. As an OASIS standard it is developed to be a safe protocol regardless of that the amount of MQTT devices that are found in Shodan and can be considered vulnerable is the highest combined number out of all protocols. The reason for the high amount of vulnerable devices could be connected to the high popularity of the protocol. Even with the high amount of vulnerable devices it could be a fraction of the total amount of devices that are not deemed vulnerable. Another interesting point is that MQTT is a commonly used protocol for private home automation systems. An example of this could be an automatic system for light dimming. Systems like these that use MQTT for communication could potentially not be secure against vulnerabilities because the user does not have the knowledge of the vulnerabilities.

E. Emerson/Fisher ROC

For Emerson/Fisher ROC there were only two vulnerable ICS devices found, one in Finland and one in Norway. The reason for the low amount of vulnerable devices is most likely connected to the fact that the protocol is used by devices sold by a company called Emerson/Fisher. The company sells devices that makes use of their own protocol ROC. This also means that Emerson are responsible for the security of the devices and protocol. For this reason the amount of vulnerable devices should be low and this is most likely why only two devices were found. If ROC was a more publicly used protocol the number of vulnerable devices would be expected to increase.

F. EtherNet/IP

EtherNet/IP has a high vulnerable presence in all countries. The percentage of vulnerable devices that use EtherNet/IP is very diverse between the different countries. Iceland (66%), Norway (54%), Finland (19%), Denmark (16%), Sweden (8%). As EtherNet/IP is a commonly used protocol that has a more general use case and is not targeted towards a specific industry it can be expected to have vulnerable devices. Since EtherNet/IP could be seen as one of the go-to's for noncommercial reasons the user may not always be up to date or aware about the possible vulnerabilities of the protocol. This could lead to the high amount of vulnerable devices.

G. Modbus

Modbus appears in all reported countries but Sweden has the most vulnerable Modbus devices (1410) by a large margin. Modbus is a de facto standard and also open source leading it to be used by many manufacturers and industries for communication between electronic devices and monitoring software. Since Modbus is open source manufacturers of ICS-devices using Modbus can use different solutions which makes interoperability harder and be a potential reason for vulnerable ICS devices with Modbus communication. As previously mentioned, Modbus was created back in 1979 when the Internet was not yet widely used and the concern for security is not yet seen as a problem. This means that organizations themselves have to add a layer of security for the device to be protected.

H. Siemens S7

S7 is a Siemens owned communication protocol that is used for programmable logic controllers. With such a specific target-area for the company and the fact that the protocol is corporate owned it is no surprise that the amount of vulnerable devices is not higher. Siemens also sell their own devices that make use of their protocol which would decrease the chance of vulnerabilities since Siemens them self are responsible for the ICS devices security.

I. BACnet

In the Nordic countries the amount of vulnerable ICS devices using BACnet is rather low with an average of 1% of the vulnerable devices. The highest amount of vulnerable BACnet devices can be found in Sweden with 31 devices. BACnet has an optional security architecture that comes with the protocol. Previously, this security architecture has been overlooked and seen as unnecessary for the building automation industry but lately the concern and awareness of network security has increased. This could be the cause for the low number of vulnerable BACnet ICS devices. With the same logic the vulnerable BACnet devices found could be used without the security architecture active.

J. DNP3

In the Nordic countries there was only one ICS device using DNP3 that was deemed vulnerable. DNP3 comes with the security function Secure Authentication (SA) which protects from unauthenticated users to access the data. By having this security feature most vulnerabilities are handled and contributes to Shodan only being able to detect a single ICS device unsecured.

VI. Conclusion

Conclusion of the result is that there definitely could be a correlation between number of ICS devices connected to the internet and the GDP. This is stated by our small result that we made about the Nordic countries but also of research papers that has came to the same conclusion. The number of

ICS devices is not a waterproof method to calculate the GDP since it is not backed by science, but by looking at the number of ICS devices one can have a good estimate of the GDP in the country.

As we stated above from the result the different kinds of protocols differ very much in the Nordic countries even though they are very close to each other. The conclusion of the differences in protocols was hard to single out to a specific reason, usage and use cases seems to have great impact.

VII. Acknoledgement

We sincerly would like to thank Andrei Gurtov as our mentor. Andrei Gurtov provided alot of useful feedback and also a shodan.io account that made this research paper possible.

References

[1] Wikipedia, “shodan,” @miscS7, author = Wireshark, title = S7 Communication (S7comm), howpublished = https://wiki.wireshark.org/S7comm, note = Accessed: 2022-03-11 , accessed: 2022-03-11.

[2] D. Hasselquist, A. Rawat, and A. Gurtov, “Trends and detection avoidance of internet-connected industrial control systems,” *IEEE Access*, vol. 7, pp. 155 504–155 512, 2019.

[3] T. MICRO, “Industrial control system,” https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system, accessed: 2022-04-01.

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

[5] D. Eridani and E. D. Widianto, “Performance of sensors monitoring system using raspberry pi through mqtt protocol,” in *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2018, pp. 587–590.

[6] O. Sadio, I. Ngom, and C. Lishou, “Lightweight security scheme for mqtt/mqtt-sn protocol,” in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 2019, pp. 119–123.

[7] Q. Liu and P. Ren, “Study on the congestion control arithmetic of bacnet routers,” in *2008 3rd IEEE Conference on Industrial Electronics and Applications*, 2008, pp. 2284–2287.

[8] M. Nast, B. Butzin, F. Golatowski, and D. Timmermann, “Performance analysis of a secured bacnet/ip network,” in *2019 15th IEEE International Workshop on Factory Communication Systems (WFCS)*, 2019, pp. 1–8.

[9] “Emerson roc/floboss,” https://autosoln.com/protocols/emerson-fisher-floboss-roc/, accessed: 2022-04-9.

[10] Tridium, “NiagaraAX networking and it guide,” https://www.lynxspring.com/documents/AX_Networking_IT_Guide.pdf, accessed: 2022-04-14.

[11] I.-J. Shin, D.-S. Eom, and B.-K. Song, “The coap-based m2m gateway for distribution automation system using dnp3.0 in smart grid environment,” in *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2015, pp. 713–718.

[12] R. Amoah, S. Camtepe, and E. Foo, “Securing dnp3 broadcast communications in scada systems,” *IEEE Transactions on Industrial Informatics*, vol. 12, no. 4, pp. 1474–1485, 2016.

[13] A. Richard and P. Appiah-Kubi, “Design and performance of a split protocol architecture on distributed network protocol 3 (dnp3),” in *2017 IEEE International Conference on Electro Information Technology (EIT)*, 2017, pp. 249–253.

[14] D. Junfeng, R. Xiang, Y. Shuohang, and W. Lipeng, “Design of mine-used combination switch gateway based on ethernet/ip,” in *2020 5th International Conference on Power and Renewable Energy (ICPRE)*, 2020, pp. 382–386.

[15] C. Zaiping, S. Xia, J. Chao, and N. Jianyun, “Implementation of embedded system for ethernet/ip protocol,” in *ICCAS 2010*, 2010, pp. 2409–2412.

[16] Wireshark, “S7 communication (s7comm),” https://wiki.wireshark.org/S7comm, accessed: 2022-04-11.

[17] C. P. Filip Polbratt, “Identifying vulnerabilities on ics devices connected to the internet using shodan,” https://www.ida.liu.se TDDD17oldprojects 2019TDDD17_project_report_filpo653_chrpe104_final.pdf, accessed: 2022-03-21.

[18] Q. Li, X. Feng, H. Wang, and L. Sun, “Understanding the usage of industrial control system devices on the internet,” *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2178–2189, 2018.

VIII. Appendix A

TABLE VII
THE TABLE BELOW IS ABOUT THE QUERIES USED IN SHOODAN TO FIND THE REQUESTED DATA.

Protocol	**Country**	**Query**
Niagara Fox	Sweden	country:SE port:1911,4911 ”fox a 0”
MQTT	Sweden	country:SE port:1883 MQTT
Emerson Fisher ROC	Sweden	country:SE port:4000 -HTTP -SSH -ERROR
Ethernet/IP	Sweden	country:SE port:2222 ,44818 -SSH -HTTP -FTP -220 -TeamSpeak -Agent -html -Yoshi -Verlihub
Modbus	Sweden	country:SE port:502 UNIT ID
Siemens S7	Sweden	country:SE port:102 ”Basic Hardware” + ”Module” + ”Basic Firmware”
BACnet	Sweden	country:SE port:47808 ”Instance ID”,”BACnet”
DNP3	Sweden	country:SE port:20000 source address
Niagara Fox	Finland	country:FI port:1911,4911 ”fox a 0”
MQTT	Finland	country:FI port:1883 MQTT
Emerson Fisher ROC	Finland	country:FI port:4000 -HTTP -SSH -ERROR
Ethernet/IP	Finland	country:FI port:2222,44818 -SSH -HTTP -FTP -220 -TeamSpeak -Agent -html -Yoshi -Verlihub
Modbus	Finland	country:FI port:502 UNIT ID
Siemens S7	Finland	country:FI port:102 ”Basic Hardware” + ”Module” + ”Basic Firmware”
BACnet	Finland	country:FI port:47808 ”Instance ID”,”BACnet”
DNP3	Finland	country:FI port:20000 source address
Niagara Fox	Denmark	country:DK port:1911,4911 ”fox a 0”
MQTT	Denmark	country:DK port:1883 MQTT
Emerson Fisher ROC	Denmark	country:DK port:4000 -HTTP -SSH -ERROR
Ethernet/IP	Denmark	country:DK port:2222,44818 -SSH -HTTP -FTP -220 -TeamSpeak -Agent -html -Yoshi -Verlihub
Modbus	Denmark	country:DK port:502 UNIT ID
Siemens S7	Denmark	country:DK port:102 ”Basic Hardware” + ”Module” + ”Basic Firmware”
BACnet	Denmark	country:DK port:47808 ”Instance ID”,”BACnet”
DNP3	Denmark	country:DK port:20000 source address
Niagara Fox	Norway	country:NO port:1911,4911 ”fox a 0”
MQTT	Norway	country:NO port:1883 MQTT
Emerson Fisher ROC	Norway	country:NO port:4000 -HTTP -SSH -ERROR
Ethernet/IP	Norway	country:NO port:2222,44818 -SSH -HTTP -FTP -220 -TeamSpeak -Agent -html -Yoshi -Verlihub
Modbus	Norway	country:NO port:502 UNIT ID
Siemens S7	Norway	country:NO port:102 ”Basic Hardware” + ”Module” + ”Basic Firmware”
BACnet	Norway	country:NO port:47808 ”Instance ID”,”BACnet”
DNP3	Norway	country:NO port:20000 source address
Niagara Fox	Iceland	country:IS port:1911,4911 ”fox a 0”
MQTT	Iceland	country:IS port:1883 MQTT
Emerson Fisher ROC	Iceland	country:IS port:4000 -HTTP -SSH -ERROR
Ethernet/IP	Iceland	country:IS port:2222,44818 -SSH -HTTP -FTP -220 -TeamSpeak -Agent -html -Yoshi -Verlihub
Modbus	Iceland	country:IS port:502 UNIT ID
Siemens S7	Iceland	country:IS port:102 ”Basic Hardware” + ”Module” + ”Basic Firmware”
BACnet	Iceland	country:IS port:47808 ”Instance ID”,”BACnet”
DNP3	Iceland	country:IS port:20000 source address