Possibilities of the Search Engine Shodan in Relation to SCADA

Jan Vávra, Martin Hromada
The Department of Security Engineering
Tomas Bata University in Zlín
Zlín, Czech Republic
e-mail: {jvavra, hromada}@*fai.utb.cz*

Abstract— **Recently isolated Industrial Control System (ICS) became accessible and interconnected with Information and Communication Technology (ICT). Nowadays, the ICS is considered as the target of a considerable number of cyber-attacks. Moreover, the contemporary development of the ICS indicates its growing availability over the Internet. There are a few methodologies how to find Internet-connected devices. However, there is one well-known search engine for Internet-connected devices. The Shodan is a widely used tool that provides an enormous capability for targeting Internet-connected devices. In this article, we examine the current state of the ICS availability via the Internet. Therefore, we evaluate the possibility of exposing the vulnerable ICS systems in order to specify their relations to SCADA cyber security. Finally, we identify 974 vulnerable SCADA devices via the Shodan.**

Keywords-Shodan; Cyber Security; Industrial Control System; Vulnerability; Supervisory Control and Data Acquisition.

I. Introduction

An enormous number of the cyber-attacks relating to the ICS and its main subgroup Supervisory Control and Data Acquisition (SCADA) systems have the eminent influence on the SCADA cyber security. Moreover, the disruption of the SCADA services could have a significant impact on the population, environment or the state itself.

The SCADA was designed as an isolated system. However, the recently isolated system has become more interconnected with external technologies like Information and Communication Technologies (ICT). The evolution of the SCADA has led to a production of new vulnerabilities, which are significant threats to SCADA. Furthermore, Pollet [8] predicted an increasing dependency of the SCADA systems on IT; therefore, the percentage of industrial companies utilizing cyber security solutions will rapidly grow.

There is a considerable number of search engines for Internet-connected devices. Patton et al. [9] have investigated some of the emerging vulnerabilities that exist. Moreover, they give us examples on how dangerous Shodan[3] can be even with a small subset of devices. Markowsky et al. [10] demonstrated how simple can the Internet of Things (IoT) be reachable via Shodan. In addition, Bodenheim et al. [11] investigated the capabilities of the Shodan in relation to SCADA. The authors conclude that Shodan should be categorized as a threat to Internet-facing SCADA.

The Shodan project is highly interested in searching for SCADA devices. Therefore, the ICS radar was created in order to present the results to the public. However, the previous research has not fully addressed all cyber security aspects, especially vulnerable SCADA devices. Moreover, the cyber security of SCADA communication protocols is discussed in the article.

The rest of the article is organized as follows. Section II presents basic information about SCADA systems. The search engine for Internet-connected devices Shodan is analyzed in Section III. Section IV gives an overview of Industrial Control Systems Cyber Emergency Response Team. In Section V, the industrial communication protocols are described. The next Sections (VI and VII) include methods and results. Finally, Section VIII provides the discussion of the article.

II. Supervisory Control and Data Acquisition System

SCADA is a main subgroup of the ICS. Moreover, it can be described as data gathering, remote and centralized system. It is also used for monitoring, management and control of industrial processes. Therefore, the public and private organizations use them as a means to improve efficiency of the industrial system. Moreover, the SCADA is an internal part of the Critical Information Infrastructure (CII) [12]. Nowadays, the CII has enormous influence in almost every sector of the critical infrastructure (transportation systems, power plants, dams, water treatment, oil production, chemicals, gas distribution, etc.). Therefore, every cyber-attack on the CII systems must be considered as a critical threat, which can result in a fatal impact on the environment, population or a country [12].

The SCADA have a positive influence on contemporary society; nevertheless, these systems are under increasing pressure to improve connectivity via the Internet [12]. Thus, the recently isolated systems are becoming more dependent on interconnection with external technologies [1]. This recent evolution of industrial systems resulted in productions of new vulnerabilities. Thus, the protected system becomes more vulnerable to new cyber-attacks.

III. Shodan

Shodan is a robust search engine for Internet connected devices. The engine was developed by John Matherly. Moreover, he launched it in 2009. Shodan has capabilities to find and collect important information about Internet-connected devices. The main source of information comes from banners. The engine uses a banner grabbing technique in order to find specific devices like servers, routers, printers, ICS, etc. Shodan is continuously searching for the technology accessible from the Internet. Furthermore, it is able to index the devices and investigate available services. This information is collected and stored in the main Shodan database. As a result, there is a highly valuable database with thousands of the records. The database is free to use, moreover, there are no restrictions for users. They can easily use one of the filters in order to find valuable information. The basic filters are focused on these fields:

- Product name
- Product version
- Port
- Operating system
- Country or city
- Specific IP address

Shodan is able to track most of the Internet-connected devices. Moreover, it includes SCADA. The SCADA systems are based on specialized technology and protocols. The uniqueness of the SCADA creates new opportunities for the attackers. Shodan provides unique ability to find and scan industrial devices. The representation of SCADA devices connected to the Internet can be seen in Figure 1. Thus, they are accessible around the World especially in the United States of America and Europe. As a result, there are a considerable number of vulnerable devices connected to the Internet.

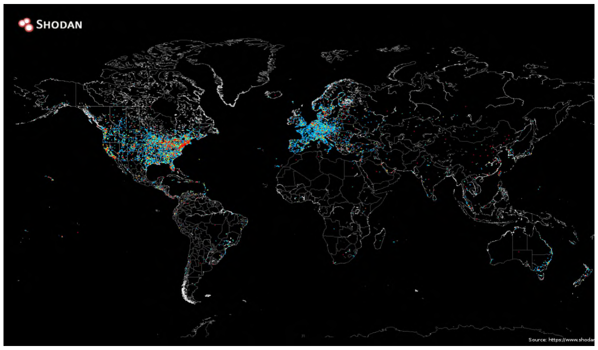


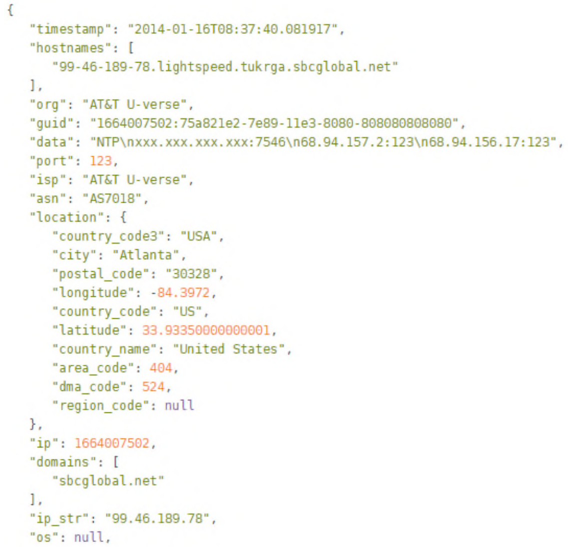
Figure 1. The SCADA map created by Shodan. (adapted from [3])

Reconnaissance and data gathering is the first step of every cyber-attack. Moreover, the attacker can focus on important information about the targeted organization. They are looking for vulnerable elements of the system which can be exploited. For example: the information about SCADA assets, ICT assets, partners, services, protective measures and even employees themselves [2].

A. Banner Specification

The banners are metadata about the system. They are highly useful for administrators to manage and categorize their networks. However, the banners are the main type of information for Shodan. Besides, there is the technique called banner grabbing. It is used to identify the information like services, operating system, open ports, communication protocol name or information about product and its version in order to find a vulnerable system [4]. A partial example of the banner is shown in Figure 2. This is real example acquired from the Shodan. There is a lot of information about the system; however, only some information is really important. The important information includes: port, longitude, latitude, area_code, dma_code, and ip.

- **Port** – This segment represents the end point of network communication. Furthermore, it has close relationship with IP address and communication protocol. Each port is developed for different services.
- **Longitude** – The longitude is a geographic coordinate. Moreover, it defines east-west geolocation of the device.
- **Latitude** – The latitude is a geographic coordinate. Moreover, it defines north–south geolocation of the device.
- **Area_code** – The area code is a special identifier for the location where the device is located. However, it is only available in the USA [3].
- **Dma_code** – The DMA code is an acronym for designated market area code. It is a specific group of counties covered by television stations.
- **IP** – It is designed as a unique identifier for every device connected to a global or local network.



```
{
   "timestamp": "2014-01-16T08:37:40.081917",
   "hostnames": [
      "99-46-189-78.lightspeed.tukrga.sbcglobal.net"
   ],
   "org": "AT&T U-verse",
   "guid": "1664007502:75a821e2-7e89-11e3-8080-808080808080",
   "data": "NTP\nxxx.xxx.xxx.xxx:7546\n68.94.157.2:123\n68.94.156.17:123",
   "port": 123,
   "isp": "AT&T U-verse",
   "asn": "AS7018",
   "location": {
      "country_code3": "USA",
      "city": "Atlanta",
      "postal_code": "30328",
      "longitude": -84.3972,
      "country_code": "US",
      "latitude": 33.93350000000001,
      "country_name": "United States",
      "area_code": 404,
      "dma_code": 524,
      "region_code": null
   },
   "ip": 1664007502,
   "domains": [
      "sbcglobal.net"
   ],
   "ip_str": "99.46.189.78",
   "os": null,
```

Figure 2. The real example of the banner. (adapted from [3])

Figure 2 shows the other important information such as organization name, Internet Service Provider (ISP), country code or city. The information extracted from the banners is very useful for administrators. However, it is also helpful to hackers.

IV. Industrial Control Systems Cyber Emergency Response Team

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is a division of the Department of Homeland Security. The objective of the ICS-CERT is to create a reliable system for one main purpose. The ICS-CERT designed a complex system in order to manage the risk of the ICS. The database of ICS vulnerabilities was developed. Furthermore, the ICS-CERT provides important services for ICS cyber security [5]. Figure 3 illustrates the essential ICS-CERT services.

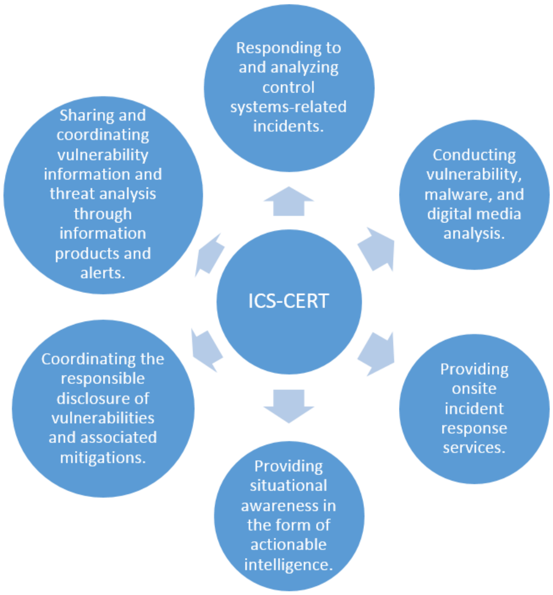

ICS-CERT
Responding to and analyzing control systems-related incidents.
Conducting vulnerability, malware, and digital media analysis.
Providing onsite incident response services.
Providing situational awareness in the form of actionable intelligence.
Coordinating the responsible disclosure of vulnerabilities and associated mitigations.
Sharing and coordinating vulnerability information and threat analysis through information products and alerts.

Figure 3. The essential ICS-CERT services. (adapted from [5])

The information published by ICS-CERT has significant influence in risk reduction in relation to the SCADA system. Nevertheless, it has a high value for the attackers. The database of ICS vulnerabilities can be used for targeting and exploiting of the vulnerable system. Furthermore, the SCADA has enormous problems with the updates. The updates implementation is a time consuming process because of testing. The time gap between publication of the vulnerability and updating of the system is the target for the attacker.

V. Industrial Communication Network Protocols

Industrial networking is essential for every SCADA system. Moreover, it is responsible for establishing and maintaining industrial communication between controls, supervisory or even business devices. This section is designed as a theoretical basis which describes industrial communication network protocols.

A. Modbus

It is one of the most widely used industrial communication protocol. It can be described as a serial communication protocol which is robust, open and simple. It was designed in 1979 by Modicon [2]. This communication protocol commonly uses port 502 in order establish communication.

B. DNP3

Distributed Network Protocol (DNP3) is an extensively used industrial communication protocol which is designed to establish traffic between master station and slave stations. In addition, it is widely used in the water and electric sectors of the critical infrastructure [2]. It is common knowledge that DNP3 uses port 20000 for communication.

C. IEC-104

This standard for industrial communication was created by the International Electrotechnical Commission (IEC). The whole name of the standard is IEC 60870-5-104. Moreover, the standard enables communication between control station and remote sites via TCP/IP [6]. The standard usually uses port 2404.

D. EtherNet/IP

This application layer protocol is based on Ethernet technologies and Common Industrial Protocol [6]. The protocol can be used for information exchange or controlling of processes. It was developed by Rockwell Automation [6]. In addition, it is mostly used in the USA. EtherNet/IP establishes the communication based on port 44818.

E. EtherCAT

This Ethernet based Fieldbus was invented by Beckhoff Automation. This protocol excels in short time cycle, low jitter and low hardware costs. The EtherCat is applicable for hard and soft real-time requirements in automation technology; it was introduced in 2003 [7]. This communication protocol commonly uses 34980 port in order establish communication.

VI. Methods

The research presented in this paper is entirely focused on a process of identification of the SCADA via the Internet. Therefore, the search engine for Internet-connected devices Shodan was used. This research can be divided into two main parts.

The first objective of the research is to evaluate the current state of vulnerable SCADA devices which are accessible via the Internet. To fulfill this goal of the research we used Shodan and ICS-CERT database of vulnerabilities. Our primary aim is the time gap between publication of the vulnerability and updating of the system in order to eliminate

ISBN: 978-1-61208-493-0

the vulnerability. The SCADA updates cannot be implemented on a daily basis due to updates testing. Therefore, every update can be considered as critical. Thus, this interval is extensive in case of SCADA. We used ICS-CERT database in order to identify potential vulnerable devices. Moreover, we focused especially on devices which must not be accessible via the Internet due to the mitigation strategies. Thus, the research is concentrated on the product name and its version in order to detect vulnerable systems. Furthermore, the product name and version is collected as a result of banner grabbing technique. Thereafter, we identify and uncover vulnerable devices via Shodan. A considerable number of devices were collected. The total sample consists of almost one thousand devices which were collected in the first three months of 2016. In the follow-up phase of the study, we evaluated the data in order to obtain crucial information for the purpose of the article. In addition, each device was evaluated and classified.

The second goal of the research is to specify the current state of cyber security in relation to industrial communication protocols. Five industrial communication protocols were chosen. They are main representatives of the industrial protocols. Furthermore, we identified their commonly used communication ports. As a result of this knowledge, we were able to find these devices via Shodan. Moreover, the operating system of each device was tested in order to find devices based on industrial communication protocol with vulnerable operating system like Windows XP.

TABLE I. SCADA PORTS

Industrial Communication Protocol	Port
Modbus	502
DNP3	20000
IEC-104	2404
EtherNet/IP	44818
EtherCAT	34980

Table 1 presents the tested industrial communication protocols with their ports. In the interest of determining the relationship between industrial communication protocols and operating systems, a quantitative data analysis was used. Each rule was evaluated and classified.

VII. RESULTS

The aim of the article is the evaluation of the cyber threats in relation to the SCADA systems. In order to evaluate the SCADA cyber security, we determined two main objectives. The first objective of the research was to evaluate the data in term of vulnerability distribution and the influence on the countries. The second objective focused on the cyber security in relation to industrial communication protocols. The cyber security specification of industrial communication protocols and their vulnerabilities was developed.

The first goal of the research can be divided into two main parts. The first of them is aimed on a specific group of vulnerabilities. They are published by ICS-CERT. Therefore, they are considered as a serious threat. Moreover, all the collected vulnerabilities cannot be accessible via the Internet due to mitigation strategies. However, we found 974 devices with vulnerability registered in ICS-CERT database. The distribution of the devices collected via Shodan is shown in Figure 4.

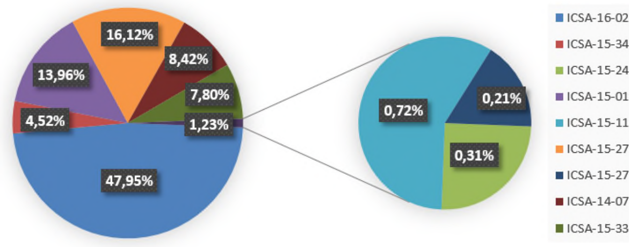


Figure 4. Vulnerable devices collected via Shodan.

As can be seen, the largest percentage of cases represents vulnerability with name ICSA-16-026-02 with almost 48% of all cases; following ICSA-15-274-01 with 16,12% and ICSA-15-013-03 with 13,96% of all cases.

The second part of the first objective is based on the previous part. Furthermore, we wanted to find the answer to the question: “Which country is the most affected by the vulnerabilities from the previous section.” The result can be seen in Figures 5 and 6.

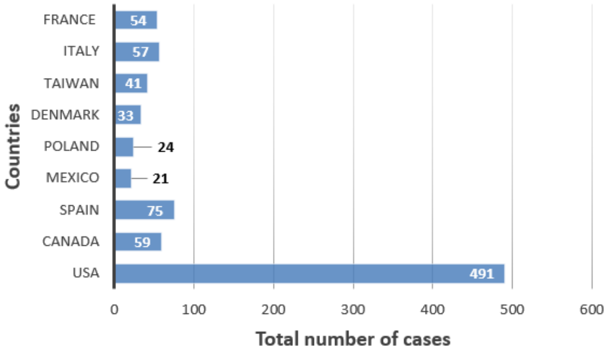


Figure 5. Affected countries due to the vulnerabilities - high impact.

Due to a considerable number of affected countries, the sample was divided into Figure 5 and Figure 6. As can be seen in Figure 5 the most affected country is the USA with almost 50% of all affected devices. On the other hand, we cannot omit Spain with 75 affected devices and Canada with

ISBN: 978-1-61208-493-0

59 affected devices. In addition, even in the case of Europe, there are only 291 affected devices in comparison with the USA.

Figure 6 shows us the countries which were affected less than the countries in Figure 5. However, Figure 5 shows us that even relatively small countries like Lithuania, Netherlands or Austria were affected by the vulnerabilities.

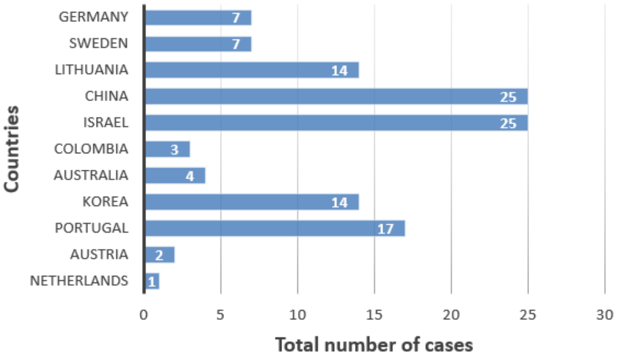


Figure 6. Affected countries due to the vulnerabilities - low impact.

The second objective of the research was to evaluate the current state of industrial communication protocols. Five industrial control protocols were evaluated. The main idea of the research was to find and identify vulnerable points in relation to industrial communication protocols. Therefore, we focus on an operating system of the devices. Thus, the SCADA devices were identified via an industrial communication protocol; moreover, the sample was classified by operating system due to find vulnerable devices. We consider Windows XP as vulnerable against cyber-attacks. Therefore, every system running on Windows XP is not reliable compared to others operating systems.

According to the research, we examined 317 891 Internet-connected SCADA devices. The distribution of the devices is shown in Figure 7.

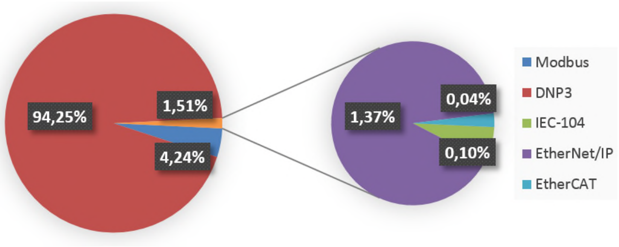


Figure 7. The distribution of the Internet connected SCADA devices.

This considerable number of the Internet-connected SCADA devices is mostly represented by the devices with the DNP3 communication protocol (94.25% of all devices). It is noticeable that the other SCADA protocols contain only 5.75% of all devices. They consist of 18 275 devices.

The second part of the objective was to evaluate the SCADA devices according to their operating system. For the purpose of the research; the data from the previous section were used. We added a new query which led to information selection. The results can be seen in Figure 8.

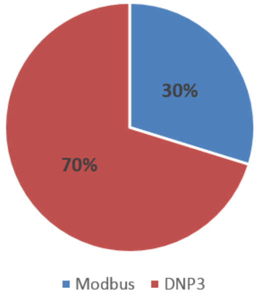


Figure 8. The distribution of the internet connected SCADA devices based on Windows XP.

The total number of affected devices was 188. In addition, it is important to notice that only devices based on Modbus (30% of all devices) and DNP3 (70% of all devices) communication protocol use Windows XP as an operating system. As a consequence, there are 56 potentially vulnerable Modbus devices in the USA. Furthermore, there are 132 potentially vulnerable DNP3 devices divided between the USA, Serbia, Croatia, the United Kingdom and the Russian Federation.

VIII. DISCUSSION

The objective of the article was to evaluate the SCADA cyber security. Therefore, this case study was based on search engine Shodan and ICS-CERT database. The results are in relation with earlier studies conducted with Shodan (Patton et al. [9]; Markowsky et al. [10]; Bodenheim et al. [11]. However, the results indicate the enormous number of vulnerable devices accessible via Shodan.

Contemporary trends show us the imminent interest in identifying of Internet connected devices like IoT or SCADA. However, the results show us that there is a group of potentially vulnerable devices. Moreover, there must be noted that every SCADA vulnerability can be considered as a critical threat.

Our research is concentrated primarily on a time gap between publication of the vulnerability and updating of the system in order to eliminate the vulnerability. Once the information about vulnerabilities is published, every attacker may exploit it for cyber-attack.

The first objective of the research showed us that 974 SCADA devices can be accessible via the Internet although it is not allowed. Furthermore, almost 50% of all devices were affected by the ICSA-16-026-02 vulnerability. In addition, the most affected country was the USA with 491 devices. It is 50% of all affected devices due to the highest density of SCADA devices. Furthermore, it is noticeable that all of the affected countries are considered technically advanced with the relatively high density of SCADA devices.

The second objective of the research showed the cyber security comparison between industrial communication protocols. Thus, five protocols were tested. Almost 320 000 devices were collected. 94% of all collected devices operated via the DNP3 communication protocol.

Even though DNP3 is one of the most widely used communication protocols, the current state of the DNP3 devices density does not match the results of this research. Therefore, we can conclude that devices communicating via DNP3 are vulnerable against search engines like Shodan.

In addition, we used the collected data in order to find SCADA systems operating with Windows XP, which is not considered as a trustworthy operating system. It should be noted that 188 devices were affected. 70% of all devices operate with the DNP3 protocol and the rest with the Modbus protocol. The collected SCADA devices can be vulnerable against cyber-attacks focused on the exploitation of the operating system. Furthermore, the rest of protocols seem to be secured against banner grabbing technique.

It should be noted that this study has been primarily concerned with SCADA-specific devices. Although we examined an enormous amount of SCADA devices, we must consider that only a few of them can be exploited. However, we tried to make the sample as accurate and credible as possible. Thus, the necessary extension of the state of the art was fulfilled. Nonetheless, more research is required in this area in order to determine the reliable cyber defense of the critical information infrastructure.

ACKNOWLEDGMENT

This work was funded by the Internal Grant Agency (IGA/FAI/2016/014) and supported by the project ev. no. VI20152019049 "RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems", supported by the Ministry of the Interior of the Czech Republic in the years 2015-2019. Moreover, this work was supported by the Ministry of Education, Youth and Sports of the Czech Republic within the National Sustainability Program project No. LO1303 (MSMT-7778/2014) and also by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

REFERENCES

[1] K. Stouffer, J. Falco, and K. Scarfone, Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology, 2011.

[2] E. Knapp, Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems. Waltham, 2011.

[3] Shodan: The search engine. [Online]. Available from: https://www.shodan.io/ 2016.03.01

[4] T. S. Kondo and L. J. Mselle, “Penetration Testing With Banner Grabbers and Packet Sniffers,” Journal of Emerging Trends in Computing and Information Sciences, vol. 5, no. 4, Apr. 2014, pp. 321-327.

[5] Industrial Control Systems Cyber Emergency Response Team. ICS-CERT. [Online]. Available from: https://ics-cert.us-cert.gov 2016.03.16

[6] B. Galloway and G. P. Hancke, “Introduction to industrial control networks,” Communications Surveys & Tutorials, vol. 15, no. 2, Jul 2013, pp. 860-880.

[7] EtherCat: Technology Group. [Online]. Available from: https://www.ethercat.org/en/technology.html 2016.03.18

[8] J. Pollet, SCADA 2017: The Future of SCADA Security. [Online]. Available from: https://files.sans.org/summit/euscada12/PDFs/RedTigerSecurity_SCADA_2017.pdf 2016.03.15

[9] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, and H. Chen, “Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT),” IEEE Joint, Intelligence and Security Informatics Conference (JISIC 2014), Sept. 2014, pp. 232-235, doi: 10.1109/JISIC.2014.43.

[10] L. Markowsky and G. Markowsky, “Scanning for vulnerable devices in the Internet of Things,” Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS 2015), Sept. 2015, pp. 463-467, doi: 10.1109/IDAACS.2015.7340779.

[11] R. Bodenheim, J. Butts, S. Dunlap, and B. Mullins, “Evaluation of the ability of the shodan search engine to identify internet-facing industrial control devices,” International Journal of Critical Infrastructure Protection, vol. 7, no. 2, Jun. 2014, pp. 114-123.

[12] J. Vávra and M. Hromada, “Comparison of the intrusion detection system rules in relation with the SCADA systems,” 5th Computer Science On-line Conference (CSOC 2016), vol. 465, Apr. 2016, pp. 159-169, doi: 10.1007/978-3-319-33622-0_15.