The Attack Vector on the Critical Information Infrastructure of the Fuel and Energy Complex Ecosystem

Nikolai Korneev [1,2,3]

[1] National University of Oil and Gas Gubkin University, 65 Leninsky Prospekt, Moscow, 119991, Russia
[2] Financial University under the Government of the Russian Federation, 49 Leningradsky Prospekt, Moscow, 125993, Russia
[3] All-Russian Research Institute for Civil Defence of the EMERCOM of Russia, 7 Davydkovskaya Street, Moscow, 121352, Russia

Abstract

There was carried out a comprehensive analysis and determined digital transformation tasks of the existing infrastructure for the fuel and energy market participants. Considering digital transformations of the existing infrastructure there were proposed ecosystem components for major participants of the fuel and energy market. A new concept of the attack vector on the infrastructure (in particular, the critical information infrastructure) was formulated on the basis of the information and energy approach and there was shown its relevance in the information security field of Automated Process Control System (APCS) and SCADA. Practical examples demonstrated how to get an attack vector on the infrastructure using the classical testing theory on the example of Web-Applications and Modbus serial communication protocol. The OWASP Web-Application Security Testing Guide was used as a guideline. It was proposed to deliberately limit the space of the attack vector on the infrastructure by the Descartes basis of information leaks and digital footprints. Separate Google Dorks have been developed for each manufacturer of embedded systems for APCS and SCADA. Penetration testing was performed as an example of APCS and SCADA on port 502 of the modbus protocol using Nmap.

Keywords

Complex security, APCS, SCADA, digital trace, digital transformation, industry 5.0, cyberattack, society 5.0, OWASP, Nmap, Google Dorks, ecosystem

1. Introduction

The structure of information processing systems changes fundamentally which is now based on distributed information-computing networks, connected to global data networks, convergent, hyper-converged, neuromorphic and quantum computing systems. At the same time, regulatory requirements are toughen, especially, in terms of complex object security: physical, economic, fire, informational, psychological, intellectual property security, technogenic, security against terrorism, ecological safety and power security.

For the fuel and energy complex (FEC) – this is first and foremost Energy security doctrine of the Russian Federation (Decree of the President of the Russian Federation 13.05.2019 № 216), new version of the information security Doctrine (Decree of the President of the Russian Federation 05.12.2016 № 646), Federal law July 26, 2017 № 187-FL "On the Security of the Russian Federation Critical Data Infrastructure, Federal law July 21, 2011 № 256-FL "On the safety of fuel and energy complex facilities", Federal law July 27, 2006 № 149-FL "About information, information technology and data security ". In these documents, the priority is given to the fuel and energy complex facilities safety, including through continuous monitoring of object operation threats [1, 2].

BIT-2021: XI International Scientific and Technical Conference on Secure Information Technologies, April 6-7, 2021, Moscow, Russia
EMAIL: niccyper@mail.ru
ORCID: 0000-0002-0254-1121

Considering the National Strategy for the development of artificial intelligence for the period up to 2030 (Decree of the President of the Russian Federation No. 490 of 10.10.2019), security issues of critical facilities of the fuel and energy complex should be solved using data mining, where the digitalization of business processes of the fuel and energy complex plays a central role.

In this regard, all fuel and energy market participants have to solve digital transformation problems of the existing infrastructure.

Experience shows that such an approach leads to the creation of its own artificial ecosystems that can solve a whole range of problems, including the safety of fuel and energy complex facilities. The example of such a system is the Sberbank ecosystem, where the services integration is achieved by the effective use of digital technologies, taking into account financial and economic goals of digital transformation. Major fuel and energy market players will have to similarly solve their digital transformation tasks of the existing infrastructure.

2. The materials and approach

As ecosystem components for major players of the fuel and energy market, considering digital transformations of the existing infrastructure, we can distinguish the following transformation tasks:

- digital means of labor, for example, digital birthplaces, digital seismic reflection, unmanned aerial vehicles, etc.;
- digital tools, such as digital oil refineries;
- smart employees who use the ecosystem to perform their job responsibilities effectively.

Due to the dynamic development of the facility and its environment, the components composition is not limited to the above.

Modern or large automated process control systems (APCS) are not possible without supervisory dispatch control and data acquisition (SCADA) systems. APCS examples can be such critical information infrastructures (CII) as: transport management systems and networks, power supply management systems and networks, heat supply management systems and networks, fuel and energy complex (FEC) management systems and networks, nuclear power plant management systems and networks, etc. On the one hand, all these modern systems and networks are based on automatic control principles [3] and use digital data in APCS and SCADA [4]. On the other hand, they are represented as an information processing system [5] that is vulnerable to the corresponding destabilizing factors [4, 5, 6] according to the ISO/IEC 27002 standard, including cyber attacks, malware, such as "Triton" [7], "Irongate" [8] and modules for frameworks, such as "Autosploit" [9], "ICSSPLOIT", "Metasploit", "Core Impact", and "Immunity Canvas".

3. Results

There are several communication protocols that are used in APCS and SCADA. Unlike Ethernet or Internet Protocols (IP), automated control system uses several protocols that are often unique to the PLC-controller manufacturer. The most popular are Modbus, dnp, dnp3, fieldbus, Ethernet/IP, EtherCAT and profinet.

Primarily, such a wide specification determines the need to form a unique vector to directly display the object and the environment state [10], based on diagnostic information on the object and the most complete information of the environment state – available for APCS and SCADA. Further, we will call such diagnostic information – an attack vector on the infrastructure, for example, CII.

At the same time, we cannot assume that this information is identical to the equation given in the work [3, 10], for this reason:

$$\tilde{X}[\mathrm{k}+1] = \tilde{\Phi}\big(\tilde{X}, U, \tilde{F}, t\big)\tilde{X}[k] + \tilde{\Gamma}[t]U[k] + \tilde{G}[t]\tilde{F}[k]\tilde{X}[k+1], \tag{1}$$

where $\tilde{X}[\mathrm{k}+1], \tilde{X}[k]$ – the most accurate possible vectors evaluations of the object state and environment; $\tilde{\Phi}\big(\tilde{X}, U, \tilde{F}, t\big)$ – state transition function determined by the most accurately known parameters of the object state and environment; $\tilde{F}[k]$ – vector evaluation of direct environmental impacts; $\tilde{\Gamma}[t]U[k], \tilde{G}[t]\tilde{F}[k]$ – integral transformations of the most accurately represented controlling and disturbing influences.

Secondly, given specification of unique PLC-controllers for the manufacturer requires adequate "unique" methods of information security (corresponding to the APCS and SCADA) from destabilizing factors [4, 5, 11, 12, 13, 14] (cyberattack, malware), which consider the specified attack vector on the infrastructure, for example, on the basis of the integrated security core [10].

Finally, it is necessary to implement proposed information security methods in the projects on information and integrated security of CII. Methodological basis of this approach was set out in [3, 5, 10, 11, 12]. In this article we will demonstrate how to practically get such an attack vector on the infrastructure, using the classical testing theory on the example of Web-applications and the Modbus serial communication protocol. For this purpose, we will develop separate Google Dorks for each manufacturer of embedded systems for APCS. In order to form the attack vector on the infrastructure, we will conduct penetration testing for APCS and SCADA using Nmap.

Modbus – is a serial communication protocol originally published by Modicon (now Schneider Electric) in 1979 to be used with its PLC-controllers. In fact, Modbus became a standard communication protocol in APCS/SCADA.

As a methodological guide we use the OWASP Web-application security testing guide [15, 16, 17, 18], paragraphs 4.1.1. "Search engines usage for information leaks", 4.1.2. (4.1.9) "Web-server fingerprints (application)". Thus, we will deliberately limit the space of the attack vector on the infrastructure [10] by the Descartes basis of information leaks and digital footprints.

To form the information leaks basis we use the Shodan search engine which allows to identify banners and information or parameters that they disclose [19]. Since Modbus works on port 502, in the search box we write "port:502" (Figure 1).

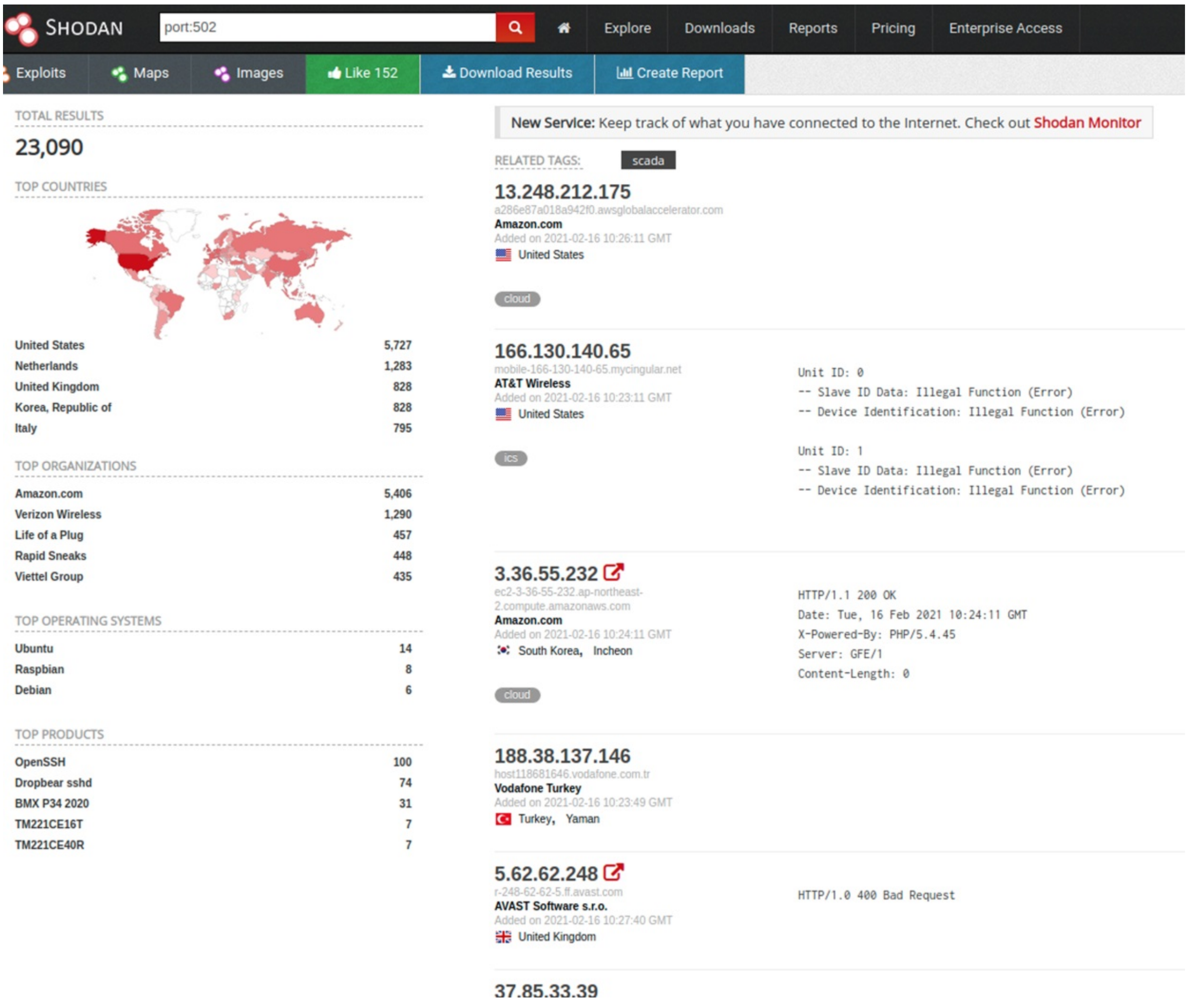

Figure 1: Search result of devices that use Modbus

Although there is no guarantee that all these IP-addresses work with Modbus, but most of them do, because 502 is a popular port, but not the only for Modbus. The protocol can be also identified by "Modbus Bridge", "ModbusGW", "HMS AnyBus-S WebServer", "title:'Carel pCOWeb Home Page'". However, SCADA systems are mostly used in the global Internet. They can be determined not only by the port, but also by the manufacturer. The "SCADA" query gives 2.925 results, but you can find 27 Schneider Electric servers with the "ClearSCADA" query.

Also, queries that can find APCS or SCADA have the following format: "port:2404 asdu address", "I20100 port:10001", «"port:789 product:""Red Lion Controls"""», "ISC SCADA Service HTTPserv:00001", «port:4800 'Moxa Nport'», "Reliance 4 Control Server", "Welcome to the Windows CE Telnet Service on HMI_Panel", "Schneider Electric EGX300", etc.

To form the basis of digital footprints we use Google dorks. It is well known that Google stores and indexes the information which finds on websites. However, Google has its own language to extract the information [20] which we used to form Google dorks.

As an example we use Google Dork for PLC-controllers Siemens S7. It is almost the same generation of controllers that was the target of the Stuxnet attack on Iran's uranium enrichment plants in 2010, and probably, is the most complex attack on APCS in history [21]. Google Dork for this controller: «inurl:/Portal/Portal.mwsl». Figure 2 shows an example of the query.

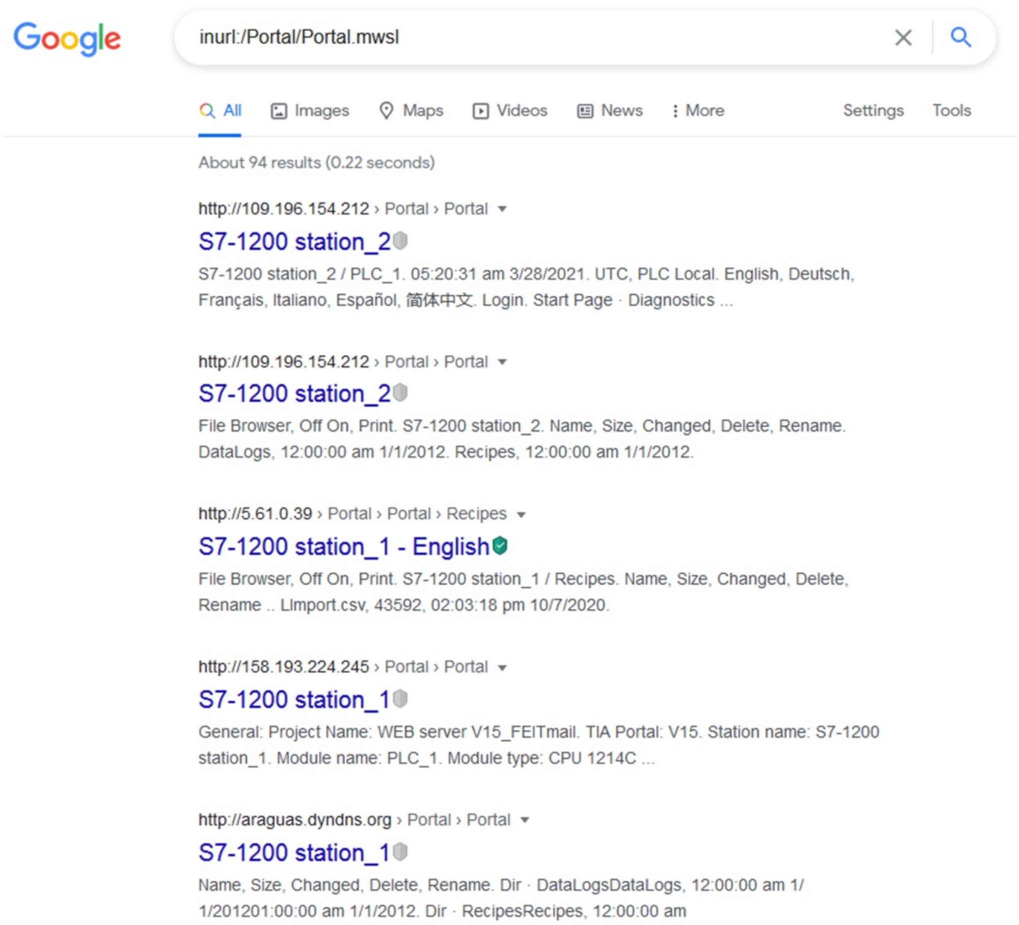

Figure 2: Google Dork work

There is no single Google Docs that would disclose every SCADA interface, instead, you need to learn about the manufacturer and used products. Each company creates its own embedded systems for automated process control systems. They use common protocols and procedures, but in general they are unique. In addition, each of these companies produces several products. To find these products used in APCS together with Google, we have developed separate Google Docs for each manufacturer and product. In Table 1, there is a short list according to manufacturers, products and developed Google Dorks.

Table 1
Short Google Dork table of companies and their products

Manufacturer	Product	Google Dork(inurl:)
Codesys	WebVisu	Webvisu
Schleifenbauer	Spbus gateway	Schleifenbauer Spbus gateway
Schneider Electric	Powerlogic EGX EGX100MG	HMI, XP277
Schneider Electric	Modicon M340	Modicon M340
Schneider Electric	PowerLogic PM800	PowerLogic PM800
Schneider Electric	PowerLogic PM820SD	S7-300
Schneider Electric	PowerLogic ECC21	Schneider Electric ECC21
Schneider Electric	PowerLogic PM870SD	Schneider Electric PM870SD
Siemens	Simatic S7	Portal0000.htm
Siemens	Simatic HMI Miniweb	Miniweb Start Page
Siemens	Scalance X	Scalance X
Trend	IQ3xcite	Server: iq3

4. Experiment and Discussion

We will conduct penetration testing for APCS and SCADA using Nmap. Nmap – is one of the main hacker tools, security researcher and penetration tester. Although Nmap has lots of features, including Nmap (NSE) scripts, it was started as a simple port scanner and remains the best port scanner ever. Nmap is a representative of the active method to obtain the information [22, 23, 24, 25].

As an aim, we chose shodan results by the search of "port:502 modbus", obtained earlier in Figure 1. Further, there is a fragment of the Nmap output in Figure 3.

```
Host is up (0.094s latency).
PORT    STATE SERVICE
502/tcp open  modbus
| modbus-discover:
|   sid 0x1:
|     error: ILLEGAL FUNCTION
|     Device identification: HMS Anybus-CC Modbus-TCP (2-Port) 1.04.01
|   sid 0x2:
|     error: ILLEGAL FUNCTION
|     Device identification: HMS Anybus-CC Modbus-TCP (2-Port) 1.04.01
...........................................
|   sid 0xf1:
|     error: ILLEGAL FUNCTION
|     Device identification: HMS Anybus-CC Modbus-TCP (2-Port) 1.04.01
|   sid 0xf2:
|_    error: ILLEGAL FUNCTION

Nmap done: 1 IP address (1 host up) scanned in 211.40 seconds
```

Figure 3: Fragment of the Nmap output

As we can see, Nmap can identify nodes as HMS Anybus-CC Modbus-TCP (2-Port) 1.04.01 and detected each of the nodes. It provides the intruder with valuable information, not only identifying the PLC-controller and version, but also the communication protocol and structure. Since attacks require deep knowledge of the automated control system technology, this information is sufficient to create an attack vector on the infrastructure.

5. Conclusion

There was formulated a new concept of the attack vector on the infrastructure (in particular, critical information infrastructure) on the basis of the information and energy approach and demonstrated its relevance in the field of information security of APCS and SCADA. It was proposed to deliberately limit the space of the attack vector on the infrastructure by the Descartes basis of information leaks and digital footprints. We developed separate Google Dorks for each manufacturer of embedded systems for APCS and SCADA. Penetration testing was performed as an example of APCS and SCADA on port 502 of the modbus protocol using Nmap. We obtained practical results that are valuable for any specialist in the information security field, as they allow to create an information security subsystem and its components for an intelligent integrated security management system, such as the fuel and energy complex.

6. References

[1] I. Kolosok, L. Gurina. Improvement of Cybersecurity of Smart Grid by State Estimation Methods. Voprosy kiberbezopasnosti [Cybersecurity issues], 2018, N 3(27). P. 63-69. DOI: 10.21681/2311-3456-2018-3-63-69. (In Russ.)

[2] S. Petrenko. Cyber resilient platform for internet of things (IIoT/IoT)ed systems: survey of architecture patterns. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2021. N 2 (42). P. 81-91. DOI: 10.21681/2311-3456-2021-2-81-91. (In Russ.)

[3] N. V. Korneev, Yu. S. Kustarev, Yu. Y. Morgovsky, Teoriya avtomaticheskogo upravleniya s praktikumom [Theory automatic control with workshop], Academia, Moscow, 2008. URL: https://www.academia-moscow.ru/ftp_share/_books/fragments/fragment_21122.pdf. (In Russ.).

[4] M. Shrestha, C. Johansen, J. Noll, D. Roverso, A methodology for security classification applied to smart grid infrastructures, International Journal of Critical Infrastructure Protection 28 (2020) 100342. doi:10.1016/j.ijcip.2020.100342.

[5] N. V. Korneev, Algorithmic both program methods and tools estimation of alternative projects of the guard data reduction system of firm on the basis of the multicriteria analysis, Sputnik+, Moscow, 2013. (In Russ.).

[6] A. Barabanov, A. Markov, V. Tsirlov. Procedure for Substantiated Development of Measures to Design Secure Software for Automated Process Control Systems. In Proceedings of the 12th International Siberian Conference on Control and Communications (Moscow, Russia, May 12-14, 2016). SIBCON 2016. IEEE, 7491660, 1-4. DOI: 10.1109/SIBCON.2016.7491660.

[7] A. S. Sani, D. Yuan, P. L. Yeoh, J. Qiu, W. Bao, B. Vucetic, Z. Y. Dong, CyRA: A real-time risk-based security assessment framework for cyber attacks prevention in industrial control systems, IEEE Power and Energy Society General Meeting 2019-August (2019) 8973948. doi:10.1109/PESGM40551.2019.8973948.

[8] G. Assenza, L. Faramondi, G. Oliva, R. Setola, Cyber threats for operational technologies, International Journal of System of Systems Engineering 10(2) (2020) 128–142. doi:10.1504/IJSSE.2020.109127.

[9] Z. Yichao, Z. Tianyang, G. Xiaoyue, W. Qingxian, An improved attack path discovery algorithm through compact graph planning, IEEE Access 7 (2019) 59346–59356. doi:10.1109/ACCESS.2019.2915091.

[10] N. V. Korneev, Intelligent complex security management system FEC for the industry 5.0, IOP Conference Series: Materials Science and Engineering 950(1) (2020) 012016. doi:10.1088/1757-899X/950/1/012016.

[11] N. Korneev, V. Merkulov. Intellectual analysis and basic modeling of complex threats. CEUR Workshop Proceedings. 2019. Vol-2603. P. 23–28. URL: http://ceur-ws.org/Vol-2603/paper6.pdf.
[12] N. V. Korneev, A Neurograph as a Model to Support Control over the Comprehensive Objects Safety for BIM Technologies, IOP Conference Series: Earth and Environmental Science 224 (2019) 012021. doi:10.1088/1755-1315/224/1/012021.
[13] A. H. Dakheel, A. H. Dakheel, H. H. Abbas, Intrusion detection system in gas-pipeline industry using machine learning, Periodicals of Engineering and Natural Sciences 7(3) (2019) 1030–1040. doi:10.21533/pen.v7i3.512.
[14] L. Wei, K. Chuipin, N. Qiang, J. Jingguo, Z. Xionghui, A method of NC machine tools intelligent monitoring system in smart factories, Robotics and Computer-Integrated Manufacturing 61 (2020) 101842. doi:10.1016/j.rcim.2019.101842.
[15] V. N. Nanisura Damanik, S. U. Sunaringtyas, Secure code recommendation based on code review result using owasp code review guide, International Workshop on Big Data and Information Security (IWBIS), Depok, Indonesia, IEEE, 2020, pp. 153–157. doi:10.1109/IWBIS50925.2020.9255559.
[16] K. Nagendran, A. Adithyan, R. Chethana, P. Camillus, K. B. Bala Sri Varshini, Web application penetration testing, International Journal of Innovative Technology and Exploring Engineering 8(10) (2019) 1029–1035. doi:10.35940/ijitee.J9173.0881019.
[17] N. D. Thai, N. H. Hieu, A framework for website security assessment, ACM International Conference Proceeding Series (ICCCM), Bangkok, ACM, New York, NY, 2019, pp. 153–157. doi:10.1145/3348445.3348456.
[18] A. V. Barabanov, A. S. Markov, V. L. Tsirlov. Information Security Controls Against Cross-Site Request Forgery Attacks On Software Application of Automated Systems. Journal of Physics: Conference Series. 2018. V. 1015. P. 042034. DOI :10.1088/1742-6596/1015/4/042034
[19] M. Bada, I. Pete, An exploration of the cybercrime ecosystem around Shodan, International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Paris, France, IEEE, 2020, 9340224. doi:10.1109/IOTSMS52051.2020.9340224.
[20] A. K. Phulre, M. Kamble, S. Phulre, Content management systems hacking probabilities for admin access with google dorking and database code injection for web content security, International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, IEEE, 2020, 9170655. doi:10.1109/IDEA49133.2020.9170655.
[21] L. Hartmann, S. Wendzel, Anomaly detection in ICS based on data-history analysis, ACM International Conference Proceeding Series (EICC), Rennes, ACM, New York, NY, 2020, pp. 1–2. doi:10.1145/3424954.3424963.
[22] P. Manzanares-Lopez, J. P. Muñoz-Gea, J. Malgosa-Sanahuja, A. Flores-de la Cruz, A virtualized infrastructure to offer network mapping functionality in SDN networks, International Journal of Communication Systems 32(10) (2019) e3961. doi:10.1002/dac.3961.
[23] S. Lau, J. Klick, S. Arndt, V. Roth, POSTER: Towards highly interactive honeypots for industrial control systems, ACM Conference on Computer and Communications Security (CCS'16), Vienna, ACM, New York, NY, 2016, pp. 1823–1825. doi:10.1145/2976749.2989063.
[24] Z. Ammar, A. AlSharif, Deployment of IoT-based honeynet model, ACM International Conference Proceeding Series (ICIT 2018: IoT and Smart City), Hong Kong, ACM, New York, NY, 2018, pp. 134-139. doi:10.1145/3301551.3301586.
[25] L. Rosa, M. Freitas, S. Mazo, E. Monteiro, T. Cruz, P. Simoes, A comprehensive security analysis of a SCADA protocol: From OSINT to mitigation, IEEE Access 7 (2019) 42156–42168. doi:10.1109/ACCESS.2019.2906926.