This is a pre-print version of the paper entitled "Risk Analysis of DNP3 Attacks. The published version is available in IEEE Xplore: https://ieeexplore.ieee.org/document/9850291" - V. Kelli, P. Radoglou-Grammatikis, T. Lagkas, E. K. Markakis and P. Sarigiannidis, "Risk Analysis of DNP3 Attacks," 2022 IEEE International Conference on Cyber Security and Resilience (CSR), 2022, pp. 351-356, doi: 10.1109/CSR54599.2022.9850291.

Risk Analysis of DNP3 Attacks

1st Vasiliki Kelli
Dpt. of Electrical & Computer Engineering
University of Western Macedonia
Kozani 50100, Greece
vkelli@uowm.gr

2nd Panagiotis Radoglou-Grammatikis
Dpt. of Electrical & Computer Engineering
University of Western Macedonia
Kozani 50100, Greece
pradoglou@uowm.gr

3rd Thomas Lagkas
Dpt. of Computer Science
International Hellenic University
Kavala Campus 65404, Greece
tlagkas@cs.ihu.gr

4th Evangelos K. Markakis
Dpt. of Electrical & Computer Engineering
Hellenic Mediterranean University
Heraklion 71004, Greece
emarkakis@hmu.gr

5th Panagiotis Sarigiannidis
Dpt. of Electrical & Computer Engineering
University of Western Macedonia
Kozani 50100, Greece
psarigiannidis@uowm.gr

***Abstract*—The integration of intelligent devices in the industry allows the automation and control of industrial processes, in an efficient and effective manner. Such systems have contributed to the rapid evolution of production infrastructures, increasing the reliability, reducing production costs, and automating the entire manufacturing operations. However, the utilization of intelligent devices has led to an increased attack surface in critical infrastructures, threatening to compromise regular operations. Attacks against such environments can have disastrous consequences in case their goal is achieved, due to the critical nature of such infrastructures. Thus, the timely identification of vulnerable spots through high-quality risk assessment, is considered highly important for avoiding or mitigating potential risks. In this paper, we focus on Distributed Network Protocol 3 (DNP3), a protocol with high utility in smart grids. Specifically, we investigate, identify and describe the vulnerabilities-by-design of DNP3 through 8 DNP3-centered cyberattacks. In addition, we present a novel method for conducting risk assessment, stemming from the combination of two techniques, namely, Attack Defence Trees (ADTs) and Common Vulnerability Scoring System v3.1 (CVSS). Through our proposed technique, the risk of a cyberattack occurring is calculated, thus contributing in securing the critical infrastructure.**

***Index Terms*—Cybersecurity, DNP3, ICS, Risk Analysis, SCADA**

I. Introduction

In recent years, the evolution of industrial development has been extremely noteworthy [1][2]. Demand and supply of industrial products and services have grown exponentially [3][4]. In order to address the high demand [5], new technologies have started being created in order to be integrated to facilitate the manufacturing processes [6][7]. Specifically, contemporary manufacturing infrastructures call for automation in industrial operations [8][9]. This has led to the utilization of Supervisory Control and Data Acquisition (SCADA) systems, as a means to automate the supervision, control, and data acquisition in industrial settings [10][11].

Such a technological evolution in the industrial domain has brought multiple advantages, such as the increase in efficiency and speed in manufacturing [12][13]. However, at the same time, the integration of Internet of Things (IoT) devices in such Critical Infrastructures (CIs) has led to an escalation of cyberattacks and incidents in recent years [14][15]. As intelligent devices and SCADA systems are used in highly critical domains such as power, water, and nuclear plants, malicious actions can have catastrophic consequences if they succeed [16][17]. The impact of cyberattacks can range from loss of revenue to power outages and possibly nuclear disasters, as the Ukrainian power plant incident [18][19] and STUXNET [20][21][22] have indicated in the past.

Considering the implications a cyberattack can have on CIs, the need to identify and describe potential attacks against the system and their impact in case they complete their objective has emerged [23]. The process of locating the cyberattacks the infrastructure is vulnerable against, and assessing the possibility of the described attack to occur, is called risk assessment [24]. Through the procedure of risk assessment, the identification of weak spots in the infrastructure can take place, thus, appropriate countermeasures can be found and adopted, in order to ensure regular industrial operations, and minimize the hazard of a cyber incident [25]. As described, the identification of possible malicious actions against the infrastructure, can act as a critical preventative measure against the identified vulnerabilities. In this paper, we describe and analyze the Distributed Network Protocol 3 (DNP3), a protocol highly utilized in the industrial domain and especially, in smart grids. In addition, we focus on the vulnerabilities-by-design of DNP3 and exploit the protocol's aforementioned weak spots in order to perform DNP3-centered cyberattacks. Finally, we model and analyze the risk of the attacks, through a novel method stemming from the pairing of the Attack Defence Trees (ADTs) and the Common Vulnerability Scoring System v3.1 (CVSS).

The paper is organized as follows. Section II presents previous work that has been done in the field. Next, Section III demonstrates DNP3, how it operates, and the layers it is composed of. Following, Section IV identifies and implements eight vulnerabilities-by-design, DNP3-centered cyberattacks. Next, Section V presents our method of combining ADTs and

CVSS to conduct a risk assessment process in DNP3-enabled infrastructures, with Section VI concluding our paper.

II. Related Work

SCADA systems are not novel as they have been utilized since 1950 for controlling industrial operations. Notably, exploitation gaps of such systems still exist, even in contemporary environments. To tackle such issues and mitigate the implications of potential cyberattacks, a lot of research has been conducted in the field, ranging from risk analysis and modeling, to deep learning-based Intrusion Detection Systems (IDS), able to rapidly detect any malicious attempt.

Radoglou-Grammatikis et.al. [26] address cybersecurity threats against Industrial Healthcare Systems through the combination of Software-Defined Networking and Reinforcement Learning. The authors focus on the IEC 60 870-5-104 industrial protocol, which is considered to be of high utility in healthcare systems. Specifically, the authors investigate and describe 14 IEC 60 870-5-104-centered cyberattacks; next, threat analysis is performed based on the aforementioned attacks, through the combination of ADTs and CVSS. Following, the authors implement an SDN and machine learning-based Intrusion Detection and Prevention System (IDPS), capable of performing cyberattack mitigation actions. The evaluation results of the proposed methodology show a high detection accuracy of IEC 60 870-5-104 cyberattacks.

Darwish et.al. [27] focus on addressing internal security threats associated with smart grids, by performing vulnerability analysis on DNP3 and penetration testing the protocol with Man-in-The-Middle (MiTM)-based attacks. Specifically, the authors present the identified security threats in DNP3 and describe the implementation of the attack scenarios. The aforementioned attacks were modeled using game theory analysis and were used to optimize their RTTD-based attack detection methods.

Li et.al. [28] focus on the vulnerability analysis of the DNP3 protocol and the utility of the open-source signature-based IDS "Snort" to categorize the abnormal behavior of DNP3 [29]. Specifically, they identify the security problems DNP3 is facing and categorize the abnormal behavior of DNP3 in five categories based on former DNP3 vulnerability analysis. To aid in the protection of DNP3-enabled ICS, they constructed a Snort-based rule template, based on the vulnerability analysis conducted.

Cherdantseva et.al. [30] provide an overview of risk assessment techniques for SCADA systems. Specifically, the authors identify and describe 24 methods utilized for SCADA environments. They provide a summary of the security challenges of such systems and proceed by describing the aim, application domains, stages and concepts of risk management addressed, impact measurements, data sources, evaluation methods, and tool support for each one of the techniques.

Kalogeraki et.al. [31] propose a novel risk assessment methodology for application in maritime logistics infrastructures and specifically, Maritime Logistics and Supply Chain (MLoSC) services, systems that are characterized by their highly complex nature. Their risk assessment approach namely MITIGATE involves the location of vulnerabilities in assets, and then the estimation of the risk in the entire supply chain. Their solution supports a total of 8 security assessment services, validated through real-world maritime scenarios.

Another work in information security of SCADA systems by H. Kholidy [32] addresses security concerns on Oil and Gas Transmission SCADA systems (OGTSS). The author suggests a novel risk assessment model based on Hierarchical Risk Correlation Trees (HRTC), which is able to assess quantitatively the risk in SCADA systems, while it is also capable of providing appropriate input parameters to response systems.

Justindhas et.al. [33] aim to tackle the disadvantages of contemporary attack detection techniques, by proposing a Normalized K-Means clustering hybridized with a Recurrent Neural Networks (NK-RNN) classifier to detect intrusions in SCADA systems. The multi-step method proposed, utilizes Elephant Herding Optimization (EHO) for performing feature selection and optimization processes in the datasets. Then, data is classified by the NK-RNN classifier and gets assessed. Finally, the authors propose a combination of two cryptographic approaches, namely, Caesar ciphering and elliptic curve cryptography, for security enhancement purposes.

Existing works have covered significant ground on risk analysis, threat modeling, and Intrusion Detection in SCADA and Industrial Control Systems (ICS). However, a gap in DNP3-central vulnerabilities has been identified, despite the protocol's high utility in the industry and especially, in the highly critical smart grids. In this work, we aim to present our threat analysis of DNP3, by combining two widely used techniques to perform the risk assessment process.

III. Overview of DNP3 Protocol

DNP3 is an application layer protocol, which is heavily utilized in the industrial domain and especially in the energy sector and smart grids [34]. DNP3 is mostly used to automate and control industrial processes, by utilizing a client-server model, according to which the master station handles the control and supervision of the various servers, or outstations according to DNP3 terminology. In detail, DNP3 is used to enable communications between devices able to perform control functions, and devices able to act or measure data, such as Intelligent Electronic Devices (IEDs), Remote Terminal Units (RTUs), etc. The master or controlling device can request data or actions to be performed by the outstations, and the outstations respond to the master station accordingly.

DNP3 messages can be transmitted over serial transportation media, although it is more common to use Transmission Control Protocol (TCP) for DNP3 packet transportation. DNP3 is comprised of three layers to perform the data acquisition and supervision functions, namely, the Data Link layer, the Transport layer, and the Application layer. In case the packet transmission occurs via TCP, the information from the three layers is wrapped in TCP, and Internet Protocol (IP), whereas in case of serial transportation, data from the three layers is placed directly on the media.

The Data Link layer functions similarly to Ethernet. Specifically, it transmits frames between the various DNP3 entities, including source and destination DNP3 addresses, while it also implements error calculation functions through Cyclic Redundancy Check (CRC). The Transport layer handles the fragmentation of large messages generated by the Application layer, while its header contains the required information to reassemble the fragments. The Application layer is responsible for handling the requests and responses for the DNP3 entities. Specifically, it describes the requests ordered by the masters, and the outstations' responses, through function codes, different for each entity. Figure 1 demonstrates the data flow for message creation, through the DNP3 architecture.

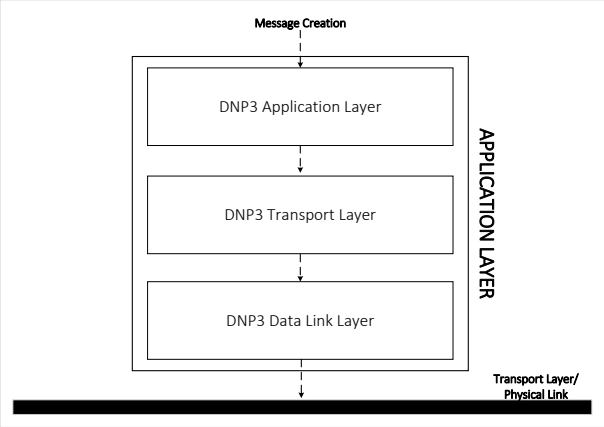

Fig. 1: Flow of data within DNP3

IV. DNP3 Attacks

DNP3 is a protocol heavily utilized in highly critical environments such as SCADA, for automating and controlling the industrial processes. The utilization of DNP3 is especially highlighted in power plants, as over 75% of North America's smart grids utilize this protocol for device communications [35]. As such, any cyberattack aiming to compromise DNP3 poses a threat to the entire critical infrastructure's regular operations. In this section, we describe the implementation of 8 DNP3-centered attack scenarios, and the impact the malicious attempts can have on the infrastructure.

A. Disable Unsolicited Messages

The first attack conducted had the aim of instructing the outstation to disable the functionality of sending unsolicited messages to the master. This functionality is used by the outstation to notify the master of detected abnormalities, without the need for a preceded master request. Ordering the outstation to disable unsolicited messages means that it is no longer able to notify the master of emergencies and thus, any incident may remain undetected. To implement this attack, we took advantage of the fact that the outstation responds to any master sending requests, and used a malicious master to send disable unsolicited requests to the victim outstations.

B. Cold Restart

The second attack executed had the objective of forcing the outstation to perform a full restart and go through the self-check processes, through a cold restart packet. This attack takes advantage of the DNP3 function able to instruct the outstation to remain offline for some time and cause a Denial of Service (DoS) as the outstation remains unresponsive to the masters' requests. The implementation of this attack follows the logic of the first attack, where a malicious master sends cold restart requests to the victim outstations.

C. Warm Restart

The third attack conducted had the aim of instructing the outstation to restart DNP3 applications only. As a result, the outstation is unable to respond to master requests for a while, until the application's restart process is completed. To implement this attack, we followed the same logic as the first and second cyberattacks, where a malicious master sends warm restart requests to the victim outstations.

D. Slave Discovery

Our fourth and fifth cyberattacks against DNP3 used two Nmap Scripting Engine (NSE) scripts against the outstations. The objective of the scripts was to recognize whether the given Internet Protocol (IP) address was used by a DNP3 outstation. The first script requests the status of the link, with data link layer function code 9, to the first 100 DNP3 data link addresses. The second script sends requests to the first 100 DNP3 data link addresses of the target IP address. In case the outstation produces a response, then the NSE succeeded in recognizing a DNP3 outstation.

E. Initialize Data

The sixth attack conducted against DNP3 had the objective of ordering the outstation to reset its data to default values. As a result, updates sent by the outstation will not reflect its actual status. This attack was implemented by intercepting a packet originating from the master via Man-In-The-Middle (MiTM), manipulating it via scapy [36], a packet manipulation tool, in order to set the function code of the application layer to 15, and then re-injecting it back into the traffic.

F. Stop Application

The seventh attack conducted had the aim of ordering the outstation to stop running the DNP3 application thus making the outstation unable to respond to DNP3 requests by the master. The implementation of this attack followed the same logic as the sixth attack, where a request packet was intercepted via MiTM, and then the application layer function code was set to 18 with scapy; following, the packet was injected back into the traffic.

G. Replay

Our eighth attack had the objective of delaying by a random time period the transmission of a request packet, thus obstructing regular DNP3 communications in the SCADA system. To implement this cyberattack, MiTM approaches were used in order to intercept, save and delay the transmission of packets originating from the master by a random time, in the [5, 10] second interval.

V. DNP3 Risk Assessment

The continuous increase in the utilization of intelligent devices in information-sensitive domains such as the industrial sector has led to an expanding attack surface, threatening to disrupt normal operations and possibly damage critical equipment. This has led to the need for identifying, mapping, and predicting the vulnerabilities of industrial assets and assessing the severity of possible attacks. In this section, we model attacks targeting DNP3 and calculate the risk of each attack, by pairing the two most widely utilized attack modeling schemes, namely CVSS and ADTs.

CVSS is an open framework for assessing vulnerabilities against software. It was developed by the National Infrastructure American Council, aiming at the development of a scoring system that helps security professionals assess the risk level of threats targeting their software. It consists of three metrics, namely Base, Temporal and Environmental, with the score ranging in the $[0, 10]$ interval. For the purpose of demonstrating the impact of the attacks presented in this paper, base metrics were implemented. Specifically, base metrics refer to the quantitative assessment of the exploitability and the impact of an attack against a system. Both the exploitability and the impact of an attack, are described and quantified by a set of parameters, in order to produce each attack's base score.

Exploitability refers to the requirements and exploitation easiness of a system. The parameters that evaluate the exploitability of a system include Attack Vector (AV), which refers to how far an attacker has to physically be in order to execute their attack, Attack Complexity (AC), which measures how complex an attack may be, referring to the conditions that have to be fulfilled outside of the attacker's control, in order for the attack to be successful, Privileges Required (PR), which describes the privileges an attacker must obtain before initiating the attack, User Interaction (UI), which refers to the number of people, excluding the attacker, that have to be involved for this attack to take place, and finally, Scope (S), which indicates whether a vulnerability in one system can impact other systems beyond the first system's privileges.

Impact parameters measure the consequence a vulnerability can have in terms of compromising the Confidentiality, Integrity, or Availability in a system. Specifically, attacks targeting the Confidentiality (C) of a system aim in obtaining information that otherwise should not have been disclosed to the attacker. Compromising the Integrity (I) of a system means that its data veracity is impacted as a direct result of the attack. Finally, attacks against Availability (A) aim in influencing the accessibility of the targeted system.

ADTs aim in visualizing in a tree format, the flow of actions an attacker has to follow in order to complete their objective, and the applicable countermeasures for each action. In detail, the nodes of an ADT may represent a malicious action, or a protection technique, utilized to mitigate the impact of the parent attack node. The objectives of parent nodes are achievable through the completion of at least one child node's objective, depending on the parent node's characterization. Specifically, the goal of a conjunctive (AND) node is considered as achieved, through the successful completion of all its children's aims. On the other hand, the objective of a disjunctive (OR) node is completed if at least one child has completed its aims. Through these rules, ADTs describe all actions necessary until the compromise of the system, from the bottom up.

Figure 2 depicts the ADT generated through our vulnerability analysis of the DNP3 protocol. Each node representing an attack or an action leading to one is additionally described by the CVSS score quantifying the severity of the respective attack. The propagation of the attack risk within the tree is performed based on whether the parent node is a product of conjunctive or disjunctive connections. Specifically, we calculate the CVSS scores for all the nodes and then calculate the risk based on the propagation Equations (1) and (2) for disjunctive and conjunctive nodes, respectively. The risk and CVSS scores for leaf nodes are considered equal, and the risk is propagated towards the root according to the aforementioned equations, where N denotes the total amount of children, n corresponds to one child node at a time, $Risk_n$ indicates the calculated risk of each child node, and $Risk_{ParentNode}$ corresponds to the calculated risk for the parent node.

$$Risk_{ParentNode} = \prod_{n=1}^{N} Risk_n \tag{1}$$

$$Risk_{ParentNode} = max(Risk_1, Risk_2 \ldots, Risk_N) \tag{2}$$

On the other hand, we consider defense measures to be specific and targeted to the root node, describing the ultimate goal of the malicious entity, to compromise the system. Similarly, Table I provides an overview of the actions leading to the attacks performed, with respect to CVSS and specifically, the resulting CVSS score and representation string.

VI. Conclusions

The utility of Industrial Control Systems is undeniable, as they offer efficient ways to enhance and manage the production operations. As highlighted in our work, the vulnerabilities of CIs call for rapid measures, as exploitable spots pose a threat to the harmonic functionality of the entire infrastructure. To tackle this issue, we identified the exploitable aspects of DNP3, by describing and implementing 8 DNP3-centered cyberattacks. The conducted cyberattacks had the ability to cause DoS, disrupt communications, and falsify outstation measurements, in order to interfere with industrial operations. Furthermore, we suggested a risk assessment process for

DNP3 Cyberattack	Description	CVSS Score	CVSS Representation
MiTM	The intentional placement of a malicious entity between two communicational endpoints with the aim of intercepting their network traffic	7.0	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L
Packet assembly	Generation of a packet with the desired attributes	5.6	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
Injection	Insertion of the crafted packet in the traffic stream	7.7	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L
Master impersonation	The operations and behavior of a legitimate master is immitated by a malicious entity	8.1	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Function code modification	The desired function code reaches the slave thus resulting in operations including the full or partial restart of the outstation, initializing data, ceasing operations, and disabling the ability to send unsolicited messages	9.0	AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
Nmap	Gathering intelligence regarding whether the targeted IP address belongs to a DNP3 outstation	5.3	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Replay scripting	Generation of a script to replay or delay packets	5.6	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
Traffic delay (Replay)	The traffic of the targeted endpoint is being maliciously delayed to obstruct regular communication	8.9	AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:L

TABLE I: DNP3 cyberattacks, their CVSS score and CVSS representation

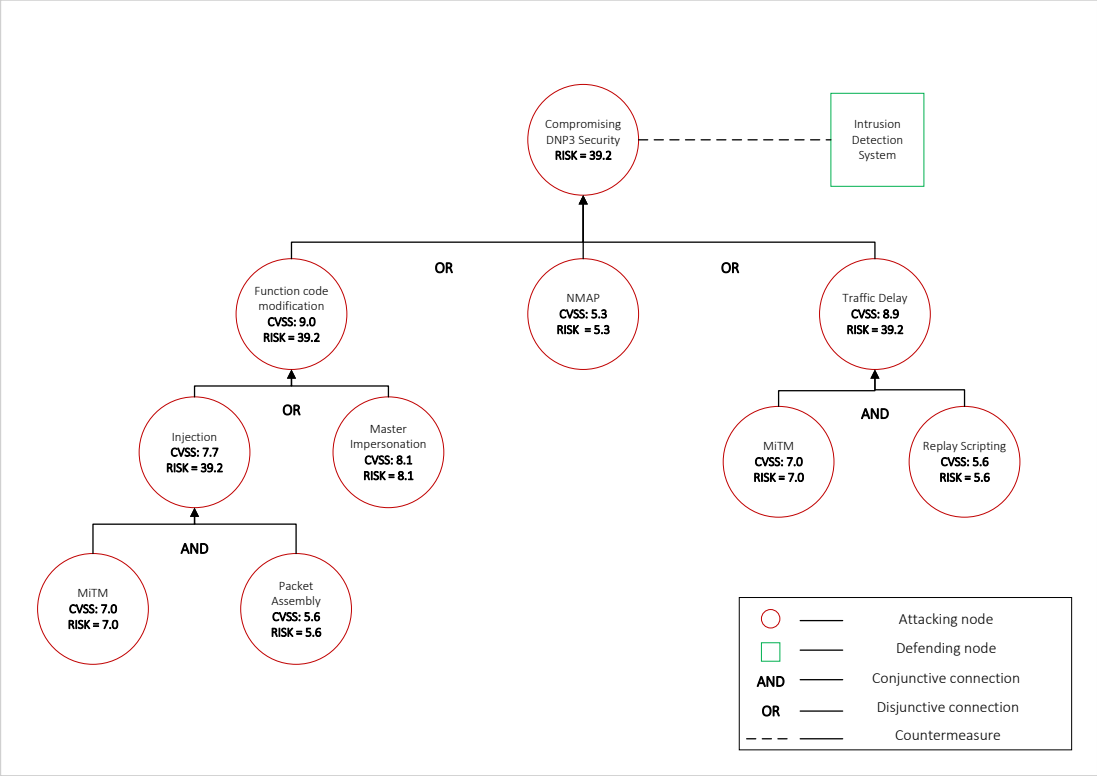

Fig. 2: Suggested DNP3 ADT

DNP3 cyberattacks, stemming from the combination of the two most commonly used attack modeling schemes, namely ADTs and CVSS. Specifically, in our approach, we break down each one of the described 8 DNP3 cyberattacks in multiple steps and merge the information in a common ADT. In parallel, we calculate the CVSS score for each malicious action and proceed with the calculation of the attack risk for each step. The risk score for each attack gets propagated in the ADT according to Equations 1 and 2, forming the final consolidated CVSS-based ADT.

VII. Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936 (ELECTRON).

References

[1] N. Hossain, M. A. Chowdhury, and M. Kchaou, "An overview of green corrosion inhibitors for sustainable and environment friendly industrial development," *Journal of Adhesion Science and Technology*, vol. 35, no. 7, pp. 673–690, 2021. [Online]. Available: https://doi.org/10.1080/01694243.2020.1816793

[2] R. Heffron, M.-F. Körner, J. Wagner, M. Weibelzahl, and G. Fridgen, "Industrial demand-side flexibility: A key element of a just energy transition and industrial development," *Applied Energy*, vol. 269, p. 115026, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261920305389

[3] A. Ahmad, S. Rozaimah, H. A. Hasan, A. R. Othman, and N. I. Ismail, "Aquaculture industry: Supply and demand, best practices, effluent and its current issues and treatment technology," *Journal of Environmental Management*, vol. 287, p. 112271, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0301479721003339

[4] A. Roozbeh Nia, A. Awasthi, and N. Bhuiyan, "Industry 4.0 and demand forecasting of the energy supply chain: A literature review," *Computers and Industrial Engineering*, vol. 154, p. 107128, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360835221000322

[5] A. Löschel and S. Managi, "Recent advances in energy demand analysis—insights for industry and households," *Resource and Energy Economics*, vol. 56, pp. 1–5, 2019, recent Advances in the Economic Analysis of Energy Demand - Insights for Industries and Households. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0928765519301356

[6] C. Bai, P. Dallasega, G. Orzes, and J. Sarkis, "Industry 4.0 technologies assessment: A sustainability perspective," *International Journal of Production Economics*, vol. 229, p. 107776, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925527320301559

[7] A. G. Frank, L. S. Dalenogare, and N. F. Ayala, "Industry 4.0 technologies: Implementation patterns in manufacturing companies," *International Journal of Production Economics*, vol. 210, pp. 15–26, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925527319300040

[8] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5g-enabled iot for industrial automation: A systematic review, solutions, and challenges," *Mechanical Systems and Signal Processing*, vol. 135, p. 106382, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S088832701930603X

[9] C. Gehrmann and M. Gunnarsson, "A digital twin based industrial automation and control system security architecture," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 669–680, 2020.

[10] A. Tidrea, A. Korodi, and I. Silea, "Cryptographic considerations for automation and scada systems using trusted platform modules," *Sensors*, vol. 19, no. 19, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/19/4191

[11] N. Nadgauda, S. A. Muthukumaraswamy, and S. U. Prabha, "Smart automated processes for bottle-filling industry using plc-scada system," in *Intelligent Manufacturing and Energy Sustainability*, A. Reddy, D. Marla, M. Simic, M. N. Favorskaya, and S. C. Satapathy, Eds. Singapore: Springer Singapore, 2020, pp. 693–702.

[12] A. El-Menshawy, Z. Gul, and I. El-Thalji, "Azure machine learning studio and SCADA data for failure detection and prediction purposes: A case of wind turbine generator," *IOP Conference Series: Materials Science and Engineering*, vol. 1201, no. 1, p. 012086, nov 2021. [Online]. Available: https://doi.org/10.1088/1757-899x/1201/1/012086

[13] a. uossef gomrokchi and A. Haghayeghi, "An overview of the capabilities of telemetry and scada systems in pressurized irrigation systems," *Irrigation and Drainage Structures Engineering Research*, vol. 21, no. 81, pp. 139–156, 2021. [Online]. Available: https://idser.areeo.ac.ir/article_123862.html

[14] J. Bhayo, R. Jafaq, A. Ahmed, S. Hameed, and S. A. Shah, "A time-efficient approach toward ddos attack detection in iot network using sdn," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3612–3630, 2022.

[15] A. D. Raju, I. Y. Abualhaol, R. S. Giagone, Y. Zhou, and S. Huang, "A survey on cross-architectural iot malware threat hunting," *IEEE Access*, vol. 9, pp. 91 686–91 709, 2021.

[16] P. Santhosh, A. K. S. Singh, M. Ajay, K. Gaayathry, H. S. Haran, and S. Gowtham, "Iot based monitoring and optimizing of energy utilization of domestic and industrial loads," in *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2021, pp. 393–397.

[17] G. Antzoulatos, C. Mourtzios, P. Stournara, I.-O. Kouloglou, N. Papadimitriou, D. Spyrou, A. Mentes, E. Nikolaidis, A. Karakostas, D. Kourtesis, S. Vrochidis, and I. Kompatsiaris, "Making urban water smart: the SMART-WATER solution," *Water Science and Technology*, vol. 82, no. 12, pp. 2691–2710, 08 2020. [Online]. Available: https://doi.org/10.2166/wst.2020.391

[18] D. Sebastian-Cardenas, S. Gourisetti, M. Mylrea, A. Moralez, G. Day, V. Tatireddy, C. Allwardt, R. Singh, R. Bishop, K. Kaur, J. Plummer, G. Raymond, B. Johnson, and A. Chawla, "Digital data provenance for the power grid based on a keyless infrastructure security solution," in *2021 Resilience Week (RWS)*, 2021, pp. 1–10.

[19] Y.-C. Chen, V. Mooney, and S. Grijalva, "Electricity grid cyber-physical security risk assessment using simulation of attack stages and physical impact," in *2020 IEEE Kansas Power and Energy Conference (KPEC)*, 2020, pp. 1–6.

[20] J. Kaniewski, H. Jahankhani, and S. Kendzierskyj, *Usability of the CBEST Framework for Protection of Supervisory Control and Acquisition Data Systems (SCADA) in the Energy Sector*. Cham: Springer International Publishing, 2021, pp. 1–20. [Online]. Available: https://doi.org/10.1007/978-3-030-72120-6_1

[21] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[22] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[23] K. Huang, C. Zhou, Y.-C. Tian, W. Tu, and Y. Peng, "Application of bayesian network to data-driven cyber-security risk assessment in scada networks," in *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, 2017, pp. 1–6.

[24] P. Ralston, J. Graham, and J. Hieb, "Cyber security risk assessment for scada and dcs networks," *ISA Transactions*, vol. 46, no. 4, pp. 583–594, 2007. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0019057807000754

[25] C. Sheng, Y. Yao, Q. Fu, and W. Yang, "A cyber-physical model for scada system and its intrusion detection," *Computer Networks*, vol. 185, p. 107677, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128620312883

[26] P. Radoglou-Grammatikis, K. Rompolos, P. Sarigiannidis, V. Argyriou, T. Lagkas, A. Sarigiannidis, S. Goudos, and S. Wan, "Modeling, detecting, and mitigating threats against industrial healthcare systems: A combined software defined networking and reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2041–2052, 2022.

[27] I. Darwish, O. Igbe, and T. Saadawi, "Experimental and theoretical modeling of dnp3 attacks in smart grids," 09 2015.

[28] H. Li, G. Liu, W. Jiang, and Y. Dai, "Designing snort rules to detect abnormal dnp3 network data," 10 2015, pp. 343–348.

[29] M. Roesch, "Snort - lightweight intrusion detection for networks," in *Proceedings of the 13th USENIX Conference on System Administration*, ser. LISA '99. USA: USENIX Association, 1999, p. 229–238.

[30] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *Computers and Security*, vol. 56, pp. 1–27, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404815001388

[31] E.-M. Kalogeraki, S. Papastergiou, H. Mouratidis, and N. Polemi, "A novel risk assessment methodology for scada maritime logistics environments," *Applied Sciences*, vol. 8, no. 9, 2018. [Online]. Available: https://www.mdpi.com/2076-3417/8/9/1477

[32] H. A. Kholidy, "State compression and quantitative assessment model for assessing security risks in the oil and gas transmission systems," 2021.

[33] Y. Justindhas and P. Jeyanthi, "Attack detection and prevention in iot-scada networks using nk-classifier," *Soft Comput*, vol. 26, pp. 1–13, 2022.

[34] H. Lin, A. Slagell, C. Di Martino, Z. Kalbarczyk, and R. K. Iyer, "Adapting bro into scada: Building a specification-based intrusion detection system for the dnp3 protocol," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, ser. CSIIRW '13. New York, NY, USA: Association for Computing Machinery, 2013. [Online]. Available: https://doi.org/10.1145/2459976.2459982

[35] S. East, J. Butts, M. Papa, and S. Shenoi, "A taxonomy of attacks on the dnp3 protocol," in *Critical Infrastructure Protection III*, C. Palmer and S. Shenoi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 67–81.

[36] P. Biondi, "Scapy," 2003. [Online]. Available: https://github.com/secdev/scapy/