International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 1, February 2021, pp. 611~619
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i1.pp611-619

Demilitarized network to secure the data stored in industrial networks

José R. Nuñez Alvarez[1], Yelena Pérez Zamora[2], Israel Benítez Pina[3], Eliana Noriega Angarita[4]
[1,4]Department of Energy, Universidad de la Costa, Colombia
[2,3]Department of Automatic, Universidad de Oriente, Cuba

Article Info

Article history:

Received Jan 29, 2020
Revised Jun 18, 2020
Accepted Jul 29, 2020

Keywords:

Control system
Demilitarized network
Electrical network
Firewalls
Industrial network

ABSTRACT

Currently, the data and variables of a control system are the most important elements to be safeguarded in an industrial network, so it is vitally important to ensure their safety. This paper presents the design and simulation of a demilitarized network (DMZ) using firewalls to control access to all the information that is stored in the servers of the industrial network of the Hermanos Díaz Refinery in Santiago de Cuba, Cuba. In addition, the characteristics, configurations, methods, and rules of DMZs and firewalls are shown, select the configuration with three multi-legged firewalls as the most appropriate for our application, since it allows efficient exchange of data guaranteeing security and avoiding the violation of the control system. Finally, the simulation of the proposed network is carried out.

Corresponding Author:

José Ricardo Nuñez Alvarez,
Department of Energy,
Universidad de la Costa,
Calle 58 No 55-66. Código Postal: 080002, Barranquilla, Atlántico, Barranquilla, Colombia.
Email: jnunez22@cuc.edu.co

1. INTRODUCTION

In the search for integration of computer and industrial communications, Industrial Communications Networks (RCI) [1-3] were developed based on FIELDBUS standards, which carry out the data acquisition process and then transmit them to manageable levels communicating to over the Ethernet network [4, 5]. With the development and wide use of these networks, it is necessary to create a security policy to prevent computer attacks due to vulnerabilities that can be generated in industrial processes, which constitute a threat to the production process [6-8].

In this way it is necessary to design and implement safety schemes to maintain production reliability and thus avoid economic losses. The change from the proprietary protocol to the open TCP/IP [4, 5], the evolution of convergent networks, human error and the failure to apply security regulations, are causes that can cause undue access to industrial networks directly or indirectly.

Given the importance of the data on the industrial processes stored in servers, it is necessary to have access to them in a secure way, so the objective of this work is the design and simulation of a demilitarized network (DMZ) using firewalls, which allows the exchange of data from an industrial network (internal network) to external networks (business or Internet) and vice versa, guaranteeing data security and thus avoiding the violation of the control system [9, 10].

At the Hermanos Díaz Oil Refinery in Santiago de Cuba, Cuba, there is an infrastructure implemented through an industrial and a business network, isolated from each other. The business network has Mail, Jabber, Internet, Domain, VoIP telephony, Intranet, WEB and FTP services. The industrial

network, since 2007, has a SIEMENS PCS7 distributed control system, based on the use of field buses, Profibus PA and Profibus DP communication networks, ET 200 communication cards, as well as a wide range of field equipment and instrumentation capable of providing process data. This network is supported on a bank of redundant servers in real-time [11].

Given the need to communicate the industrial network with the business network and the Internet, and their importance in making accurate and correct decisions, it is necessary to use security mechanisms between these networks. These mechanisms must guarantee that the information is supplied digitally in a secure manner to all customers who need to use the data, which would result in a faster process and a better analysis of the information. In this way, possible human error could be avoided when filling out the run sheet, as currently performed in the refinery, or used in automated decision-making of the intelligent integrated automation system that is intended to be implemented in the future.

In the theoretical framework section, the fundamental characteristics of industrial and demilitarized networks are explained, and the existing firewalls are analyzed with the aim of implementing a DMZ network that guarantees the security of data from an industrial network for use on the network business. In the Methodology section, we analyze how to adapt DMZ networks and the use of firewalls to the particularities of the refinery. In the Results and Discussion section, the design of the DMZ network is explained, the experimental tests carried out are analyzed and a general assessment of the results is provided.

2. THEORETICAL FRAMEWORK

An industrial control network presents attractive infrastructures to threatening subjects or hackers, whose purpose is to enter the system to collect various information, such as installation design, critical work thresholds, device settings, among others. These intrusion actions can cause, among other factors, the interruption of services, loss of data, breaches of security protocols, outcome of dangerous situations, among others.

In the industry, the general communications network is made up of the business network and the control network. The business network develops monitoring operations of the system and the users that access it; in addition, it requires rigorous authentication procedures to access database information, and thus know the alarms generated, conduct trend studies, variable behavior, among other advantages [12]. In the modern industrial complex processing of industrial process data is used to support intelligent integrated decision making [13] and to create the foundations of Industry 4.0 [14-16].

The control network develops activities of configuration, maintenance and operation of sensors and actuators, variable reading, process monitoring, and so on. Communication between the various devices that make up the network uses different protocols and sometimes support other technologies such as telephone lines, satellites, microwaves, fiber optics, among others [17-19]. The incorporation of commercial and computer equipment has introduced risks associated with the operation of industrial communication systems, for example,

- Many administrative or privileged accounts that allow access to the control system.
- Use of shared accounts that allow access to critical systems.
- Use of industrial applications with encrypted credentials.
- Use of workstations with all administrative rights.

Industrial automation protocols based on TCP/IP for remote control or based on the common industrial protocol (CIP) under the open deviceNet vendors association (ODVA) such as Ethernet/IP, DeviceNet, CompoNet, and ControlNet. However, most of these protocols present vulnerabilities in the protection and security of the data [20, 21]. Some of these vulnerabilities are,

- Identity theft or traffic capture.
- Passive network monitoring.
- Injection of malicious traffic.
- Manipulation of the transmission route.

Among the methods to avoid these vulnerabilities are DMZ networks. These are local networks, located between the internal and external networks of an organization that allows implementing security policies against computer attacks. Its main advantage is that the DMZ network, allows a direct connection from the internal and external network, while from the DMZ only communications to the external network are allowed, that is, that the local computers (hosts) in the DMZ cannot connect to the internal network, allowing the hosts in the DMZ to provide services to the external network, while protecting the internal network in case intruders compromise the security of the hosts in the DMZ zone [22]. The main features of a DMZ network are:

- Traffic from the external network to the DMZ is authorized.
- Traffic from the external network to the internal network is prohibited.

- Traffic from the internal network to the DMZ and to the external network is authorized.
- DMZ traffic to the internal network is prohibited.
- DMZ traffic to the external network is denied.

In this way, DMZ networks have an intermediate level of security, since they are not enough to store all the essential data of an industrial network. Therefore, a more secure design is proposed that consists of the integration of a DMZ network and the use of firewalls, helping to prevent access from external to internal networks, also called monitored subnet firewalls. A firewall is a filter that controls communications from one network to another, allowing or denying permissions according to the organization's policies. Two types of firewalls can be used to create the DMZ, the first, called the "front-end," allows traffic only from the network external to the DMZ, and the second called the "back-end," allows only traffic from the DMZ to the internal network [3].

There are several configurations to implement the DMZ using firewalls, it can be with 1 three-legged firewall, DMZ with 2 five-legged firewalls and DMZ with 3 multi-legged firewalls. The firewall is a filter that controls communications from one network to another, allowing or denying permissions according to the organization's policies. To admit or reject the communication, the firewall examines the type of service it corresponds to in order to decide whether the communication is incoming or outgoing and whether or not it should be allowed. Being located between the internal and external network protects the internal network from unauthorized access that can exploit its vulnerabilities [23].

There are three parameters to consider when configuring firewalls. The first and most important one considers the organization's security policy, the second analyzes the level of monitoring and the third one is based on the economic part. Once the configuration is decided, you must choose which physical elements to use. The elements for which protection mechanisms should be implemented are packet filtering, application proxy, and monitoring and detection of suspicious activity. Conceptually, there are two types of firewalls that provide greater robustness and security, the network level and the application level [24, 25]. The firewall topologies are:

- Dual-Homed Host: firewall that is installed on a host with two network cards and acts as a router between the two networks.
- Screened Host: firewall that is combined with a bastion host located in the external network and a bastion host located on the internal network.
- Screened Subnet (DMZ): firewall used in a Demilitarized network where two routers are used, one in the external network and the other on the internal network, and among them the bastion host is included.

Based on this theoretical framework, the application case of the Santiago de Cuba Refinery is studied to create a secure industrial communications system that guarantees the use of plant information in business management.

3. DESIGN METHODOLOGY OF A DMZ USING FIREWALLS

As mentioned in the introduction, the industrial network of the "Hermanos Díaz" Refinery was isolated from external networks, so that the servers located in the industrial network were not accessible from any client (PC) located in the refinery. This resulted in the fact that there was no access to the data involved in the process, which evidenced the need to integrate the industrial network with the business network and this in turn to the Internet. This integration generated vulnerabilities in terms of data security since a computer attack could be received at any time and from any client.

To achieve integration between these networks, investigations were carried out with the aim of achieving computer security mechanisms in the refinery, where various protection options applied in refineries worldwide were analyzed. Among these options, there are works where the use of DMZ networks is proposed and others where the use of firewalls is proposed [3, 7, 8, 11]. The need to subdivide the refinery networks into three networks was also taken into account: two external networks (Internet and business) and an internal network (industrial or control, with data and process variables). This helps increase computer protection when access comes from an external network.

The Hermanos Díaz Refinery is undergoing a process of updating its computer security systems to protect the control and supervision system. As each company must comply with various security policies to satisfy protection protocols and given that the processes carried out in a refinery are critical, an in-depth analysis was carried out where the proposal for the implementation of a network was reached. DMZ and its integration with 3 multi-legged firewalls. With the integration of protection mechanisms provided by DMZs and firewalls, greater security can be guaranteed against hostile conditions, making it almost impossible to circumvent security protocols.

3.1. Security design integrating DMZ and firewall

For the design of the DMZ network using firewalls that can provide security to the data and variables in an industrial network, security measures were adopted for greater defense against intruders. In addition, the DMZ network has technological equipment, such as programmable controllers and fiber optic routers, which guarantee communication with the servers. Three networks were also considered: two external networks (Internet and business) and an internal network (industry, with the data and process variables). The field buses and the distributed are Profibus PA and DP, connected to the servers that store the data. The connections between the devices on an industrial network are made redundantly, that is, if a fault occurs, the process continues to work, giving the operator the possibility of solving the fault [26, 27].

Analyzing that the servers that store data and industrial process variables can be accessed from any device connected to the network, an exhaustive study of the security policies that the industry must comply with to ensure the necessary protection protocols were performed; selecting the configuration of a DMZ with 3 multi-legged firewalls, because it is the most reliable and guarantees high security against undue access and computer attacks. Firewall topologies will be distributed between the *Screened Subnet* and the *Dual-Homed Host*. The firewalls were located between external and internal networks as follows:

- Between the external connection (can be the Internet or another company) and a business network within the industry.
- Between the business network within the industry and the DMZ.
- Between the DMZ and the industrial network.

Routers with intrinsic security were used as firewalls, since they have internal firewalls and packet filtering using the Linux *iptables*. They also have the NetFilter tool that allows the administrator to define rules applicable to IP packets that enter and/or leave a host. It should be noted that the more routers installed on the network, the more security will be provided, making it impossible to circumvent so many protocols. In the design proposal, servers were installed that prohibit the traffic of an external network to the industrial network and vice versa. If a client needs to see, for example, the combustion process of a boiler, he must access the corresponding server in the DMZ network and not the real server of the industrial network; guaranteeing that changes cannot be made in the real variables of the processes [28-31].

4. RESULTS AND ANALYSIS

Below are the details of the integrated network architecture, industrial-business-internet, and the implementation and validation tests carried out on computer security at the refinery.

4.1. Description of the design and configuration of the DMZ network proposed for the business and industrial network

Figure 1 shows the business network where computer security measures were adopted for the installation of the DMZ network. Between the business network and the external network (in the case of the Internet), a router configured by the administrator representing the application-type firewall developed in Linux called iptables, used for packet filtering, was installed. Between the business network and the DMZ, another router was located that represents another firewall also of the application type called iptables, also used for packet filtering. This firewall tool is considered one of the most effective and robust against intrude of an intruder. To achieve the required security in information traffic, the packet filtering rules set out above were defined, which approve or not the request to or from the DMZ network servers.

The proposed DMZ network is shown in Figure 2 and is located between the business network and the industrial network as an indirect path between them so that if a host of the business network wishes to access a process that occurs in the In real-time, you must access the corresponding server in the DMZ and not the one in the industrial network directly, thus demonstrating the importance of the DMZ network as a bastion host. In the DMZ network, servers such as FTP, WEB, WEB MONITOR, DATA MONITOR, and PROCESS HISTORY are established. It is important to note that to achieve the DMZ objective, traffic must be from external networks (Internet and/or business) and internal (industrial) to it, everything else will be prohibited. The DMZ is connected to the industrial network through a router and the firewall is configured under the security protocol established above, thus regulating data traffic.

In the Industrial network, see Figure 3, the ring of an Office network is located, at the entrance of it, there are two routers communicated with each other via serial via the WAN interfaces (Serial0) of each of them, which represent firewalls located between the DMZ network and the industrial network. For communication between the Office network and the industrial network, connections are established through four switches via their LAN interfaces (GigaEthernet). These switches, in turn, can be connected to client PCs or Servers that are connected to other client PCs and Servers within the plant network (industrial network).

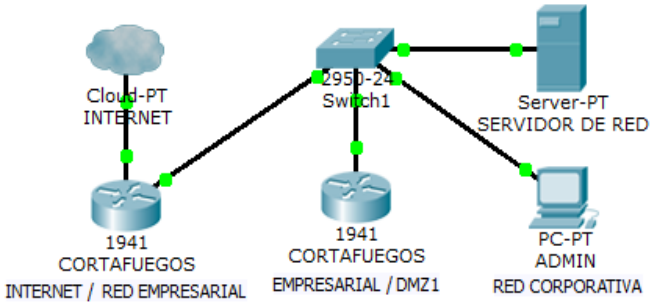

Figure 1. Communication between the business network and the internet

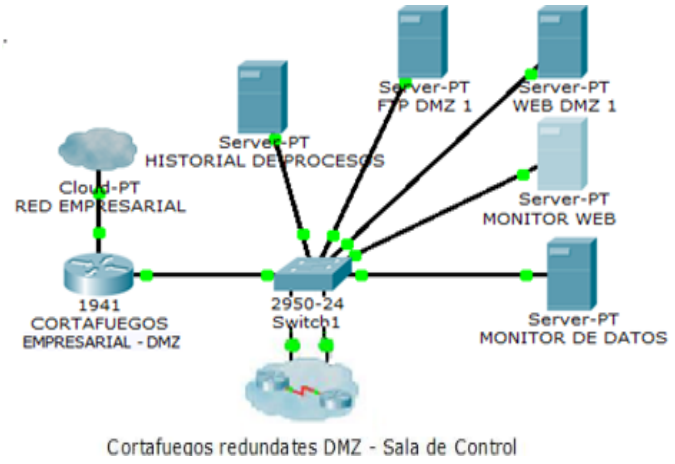

Figure 2. Proposed DMZ network

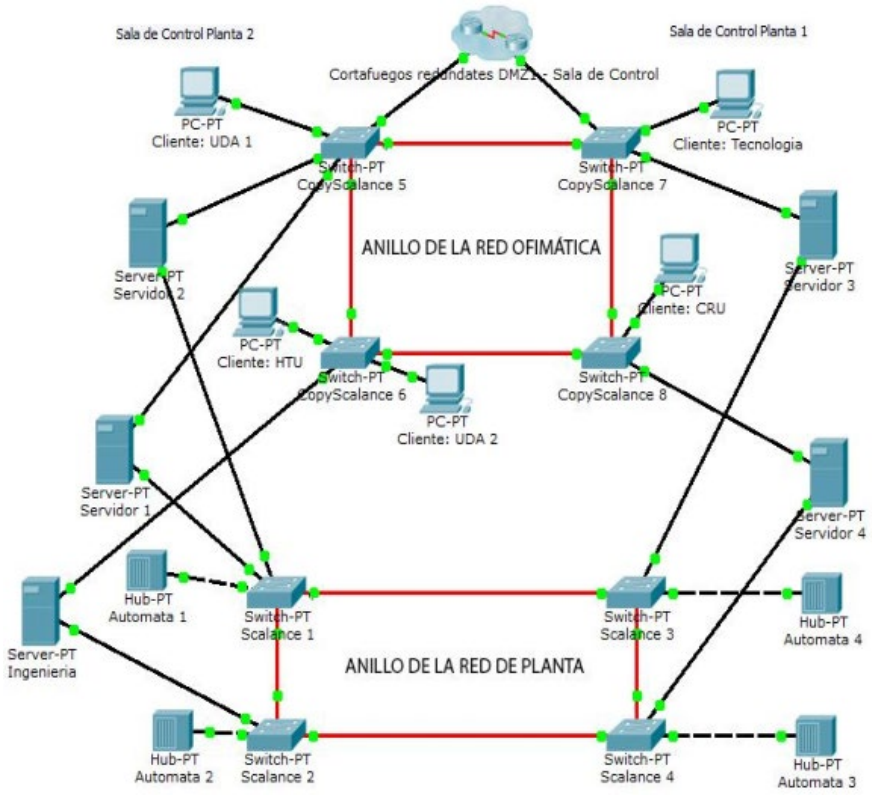

Figure 3. Proposed industrial network

4.2. Firewall configuration in iptables Linux

To define the application-type firewall rules, the *iptables* tool was used that defines the security policies for packet filtering and which takes into account 2 fundamental premises:

1. Allow all traffic and then ban it according to security needs.
2. Prohibit all traffic and then allow it according to security needs.

Defining default policies for any connection.

For the realization of this work, the second premise was used since it guarantees greater security.

iptables -P INPUT DROP # is initially discarded inbound packets.

iptables -P OUTPUT DROP # is initially discarded outbound packets.

iptables -P FORWARD DROP # are initially discarded forwarding packets.

Defining packet filtering rules.

iptables -t filter -A INPUT -p tcp --dport 3000 -j ACCEPT # the package entry to port 3000 is accepted, which is from a website in the DMZ.

iptables -t filter -A OUTPUT -p tcp --sport 3000 -j ACCEPT # packet output from port 3000 is accepted.

iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT # opens port 80 for a plant's web monitor.

Open ports 25 and 110 to provide mail services.

iptables -t filter -A INPUT -p tcp --dport 110 -j ACCEPT # opens port 110 to enable the mail protocol.

iptables -t filter -A INPUT -p tcp --dport 25 -j ACCEPT # opens port 25 to enable the email transfer protocol (SMTP).

iptables -t filter -A INPUT -s 192.168.0.0/24 -d 192.168.1.0/24 -j ACCEPT # allows the connection of the business network to the DMZ.

iptables -t filter -A INPUT -s 192.168.2.0/24 -d 192.168.1.0/24 -j ACCEPT # communication from the industrial network can send the process data to the DMZ.

Figure 4 shows the configuration where the connection from the business network to the DMZ and from the industrial network to the DMZ respectively is allowed. To verify that the result of the design proposal is correct, tests were performed using the previous configuration where packet shipments to the business network were executed from the DMZ, evidencing that the communication is successful, see Figure 5. To confirm that there is no direct traffic between the industrial and business network, packet shipments were made, as shown in Figure 6, between hosts of both networks, where it is evident that the sending is not made and that there is no response between them, demonstrating that the proposed design of the DMZ using firewalls is adequate.

In accordance with all of the above, it can be affirmed that the design and programming of the integrated DMZ network with multi-legged firewalls allowed to increase the security of the data of the industrial network. The proposal uses physical firewalls applying the configuration known as screened-subnet firewall, the first, called "front-end", creates a barrier between the corporate network and the DMZ, and the second, called "back- end ", and serves for protection between the DMZ and the industrial network. These firewalls were configured by defining policies for any type of connection in order to prohibit traffic directly to the industrial network, and then begin to allow it according to security needs through the definition of packet filtering rules. The design also took into account that the proposed firewalls must be from different manufacturers, in order to avoid that, even if one of them is violated, they can apply the same methodology to violate another, and thus also increase security. of the industrial network.

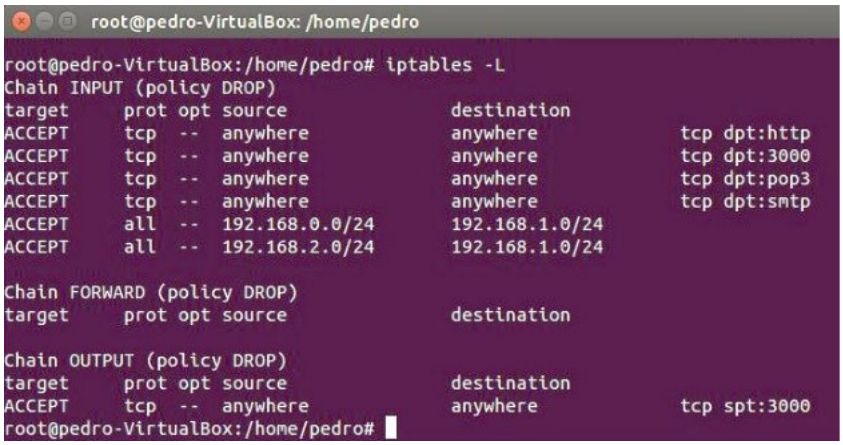

Figure 4. Firewall configuration using iptables

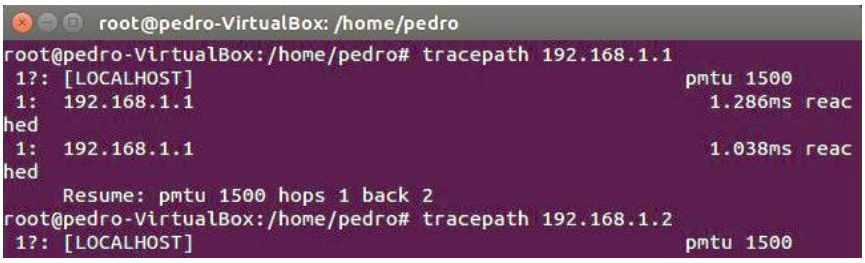

Figure 5. Packets sent to the business network from the DMZ network

Figure 6. Attempt to send packages from the industrial network to the business network

Finally, the design proposal allowed evaluating the level of security provided by the integration of DMZ networks with firewalls from different manufacturers, demonstrating its advantages in the face of intrusion attempts in the tests carried out. The result achieved allowed the interconnection of the business network with the industrial network of the refinery in a more secure way, achieving the transmission of the process data registered in the control system to the business network with the required security, thus avoiding violation of the control system.

Secure access of industrial network information from the enterprise network allows the creation of distributed intelligent systems that use the results of the automated processing of process variables, for intelligent business decision-making, with the objective of guaranteeing the efficiency of the integrated system in As for planning and production control, predictive maintenance, logistics, finance and business of the company. All this opens up the possibilities of safely applying the advantages of the Internet of Things (IoT) for industry (Industry 4.0) at the Santiago de Cuba Refinery.

5. CONCLUSION

The design of the proposed DMZ network is based on the configuration of a DMZ with 3 multi-legged firewalls that integrate with the firewalls located between the external and internal networks. The selected configuration proves to be a useful tool, since it starts from the premise of prohibiting all traffic and then allowing, it according to the data security needs of the processes of the industrial network in question, where filtering rules apply of packages only to the DMZ, which is responsible for creating a perimeter of defense between the networks to be interconnected. All the design and configuration of the proposal was put to the test in the "Hermanos Díaz" Refinery in Santiago de Cuba, through the project for the acquisition of a system that allows the union of the industrial network with its business network. Multiple attempts were made to violate the industrial network from the business and the Internet for a period of six months and each of them was controlled, which allows demonstrating the feasibility of the proposal and the high level of security it presents.

The proposed system and the results achieved in terms of data security serve as the basis for continuing with the modernization of automated systems and increasing the protection of plant control systems. In this way, the safe processing of variables, data and process information in real-time is possible, which would help in making accurate and accurate decisions using artificial intelligence and would create the conditions to implement the advantages of Industry 4.0 in the future.

REFERENCES

[1] A. Loulijat, et al., "DFIG use with combined strategy in case of failure of wind farm," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp. 2221-2234, 2019.

[2] S. Maity, et al., "Formal integrated network security analysis tool: Formal query-based network security configuration analysis," *IET Networks*, vol. 4, no. 2, pp. 137-147, 2015.

[3] K. Dadheech, et al., "De-Militarized Zone: A Next Level to Network Security," in *Proceedings of the International Conference on Inventive Communication and Computational Technologies (ICICCT 2018)*, pp. 595-600, 2018.

[4] M. G. I. Cedeño, et al., "Sizing of a networked self-consumption system at the Technical University of Manabí, Ecuador," in *CISCI 2019 Decima Octava Conferencia Iberoamericana en Sistemas, Cibernetica e Informatica, Decimo Sexto Simposium Iberoamericano en Edu., Cibernetica e Informatica-Memorias*, vol. 1, pp. 6-11, 2019.

[5] Y. Li, et al., "Complex networks in advanced manufacturing systems," *Journal of Manufacturing Systems*, vol. 43, no. 3, pp. 409-421, 2017.

[6] V. Varadharajan, et al., "A policy-based security architecture for software-defined networks," *IEEE Transaction on Information Forensics and Security*, vol. 14, no. 4, pp. 897-912, 2019.

[7] I. Ahmad, et al., "Security in Software Defined Networks: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2317-2346, 2015.

[8] Z. Chen, et al., "Collaborative network security in multi-tenant data center for cloud computing," *Tsinghua Science and Technology*, vol. 19, no. 1, pp. 82-94, 2014.

[9] J. García, et al., "Reconfigurable distributed network control system for industrial plant automation," *IEEE Transaction on Industrial Electronics*, vol. 51, no. 6, pp. 1168-1180, 2004.

[10] P. Tenti and T. Caldognetto, "Optimal control of Local Area Energy Networks (E-LAN)," *Sustainable Energy, Grids and Networks*, vol. 14, pp. 12-24, 2018.

[11] J. Neeli and N. K. Cauvery, "Trust-based secure routing against lethal behavior of nodes in wireless adhoc network," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 1592-1598, 2020.

[12] J. R. Núñez A., et al., "Metodología de diagnóstico de fallos para sistemas fotovoltaicos de conexión a red," *Revista Iberoamericana de Automática e Informática Industrial*, vol. 17, no. 1, p. 94, 2020.

[13] J. Aguilar, et al., "Sistemas MultiAgentes y sus Aplicaciones en Automatizací on Industrial," Universidad de Los Andes, Merida, Venezuela, 2013.

[14] H. Hosseinian, et al., "Blockchain outlook for deployment of IoT in distribution networks and smart homes," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp. 2787-2796, 2020.

[15] D. Vuksanović, et al., "Industry 4.0: the Future Concepts and New Visions of Factory of the Future Development," *International Scientific Conference on Ictand E-Business Related Research (SINTEZA 2016)*, pp. 293-298, 2016.

[16] C. G. Machado, et al., "Sustainable manufacturing in Industry 4.0: an emerging research agenda," *International Journal of Production Research*, vol. 58, no. 5, pp. 1462-1484, 2020.

[17] J. Zhang, et al., "Improved minimum entropy control for two-input and two-output networked control systems," in *2016 UKACC International Conference on Control, UKACC Control 2016*, 2016.

[18] M. E. M. B. Gaid, et al., "Optimal integrated control and scheduling of networked control systems with communication constraints: Application to a car suspension system," *IEEE Transactions on Control Systems Technology*, vol. 14, no. 4, pp. 776-787, 2006.

[19] B. Rahmani and A. H. D. Markazi, "Variable selective control method for networked control systems," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 3, pp. 975-982, 2013.

[20] J. Nuñez, et al., "Tools for the Implementation of a SCADA System in a Desalination Process," *IEEE Latin America Transactions*, vol. 17, no. 11, pp. 1858-1864, 2019.

[21] S. McLaughlin, et al., "The Cybersecurity Landscape in Industrial Control Systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1039-1057, 2016.

[22] P. T. Tin, et al., "Hybrid protocol for wireless EH network over weibull fading channel: Performance analysis," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 1085-1091, 2020.

[23] K. Liu, et al., "Survey on time-delay approach to networked control," *Annual Reviews in Control*, vol. 48, pp. 57-79, 2019.

[24] S. Amin, et al., "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, no. 1, pp. 186-192, 2013.

[25] E. Henriksson, et al., "Multiple-Loop Self-Triggered Model Predictive Control for Network Scheduling and Control," *IEEE Transactions on Control Systems Technology*, vol. 23, no. 6, pp. 2167-2181, 2015.

[26] J. Ponniah, et al., "A clean slate approach to secure wireless networking," *Foundations and Trends in Networking*, vol. 9, no. 1, pp. 1-105, 2015.

[27] J. Zhu, et al., "Review and big data perspectives on robust data mining approaches for industrial process modeling with outliers and missing data," *Annual Reviews in Control*, vol. 46, pp. 107-133, 2018.

[28] A. Mungekar, et al., "Augmentation of a SCADA based firewall against foreign hacking devices," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 1359-1366, 2020.

[29] C. Shen, et al., "Hybrid-Augmented Device Fingerprinting for Intrusion Detection in Industrial Control System Networks," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 26-31, 2018.

[30] Y. S. Jeong and J. H. Park, "Artificial intelligence for the fourth industrial revolution," *Journal of Information Processing Systems*, vol. 14, no. 6, pp. 1301-1306, 2018.

[31] F. A. Budes, et al., "Energy, economic, and environmental evaluation of a proposed solar-wind power on-grid system using HOMER Pro®: A case study in Colombia," *Energies*, vol. 13, no. 7, p. 1662, 2020.

BIOGRAPHIES OF AUTHORS

José Ricardo Nuñez Alvarez, Ingeniero Electricista y Máster en Automatización Industrial de la Universidad de la Costa, Barranquilla, Colombia. Sus áreas de interés son: Sistemas de Automatización Industrial, Generación, Transmisión y Distribución de Energía Eléctrica, Sistemas Domóticos e Inmóticos.

Yelena Pérez Zamora, Ingeniera Informática y estudiante de la Maestría en Ingeniería Automática en la Universidad de Oriente (UO), Cuba. Desde 2013 es docente del Departamento de Ingeniería en Automática perteneciente a la Facultad de Ingeniería Eléctrica la Universidad de Oriente. Sus intereses de investigación incluyen: Sistemas de Control y Adquisición de Datos, seguridad en los Sistemas de Control Industrial. Desde 2018 participa en el proyecto de investigación nacional en Automatización Industrial, en el tema de Seguridad Industrial.

Israel F. Benítez Pina received his BsC. Eng. in Automatic Control in 1984, and the PhD degree in Automatic and Informatics Systems in 1999, both from the Universidad de Oriente (UO), Santiago de Cuba. His research interests include, intelligent automation, fault tolerant supervisory, discrete systems and Petri Nets.

Eliana María Noriega Angarita, Ingeniera Electricista y Magister en Ingeniería, énfasis Industrial de la Universidad de la Costa, Barranquilla, Colombia. Sus áreas de interés son: Eficiencia Energética, Normatividad Eléctrica, Energías Renovables y Generación, Transmisión y Distribución de Energía Eléctrica.