Journal of Theoretical and Applied Information Technology
31st October 2022. Vol.100. No 20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A REVIEW OF COMMUNICATION PROTOCOLS IN POWER SYSTEMS

[1]ANDRÉS FELIPE RODRÍGUEZ AYALA, [2]DANIELA JOHANNA ROJAS MARTÍNEZ, [3]DIEGO ARMANDO GIRAL-RAMÍREZ

[1,2,3] Facultad Tecnológica, Universidad Distrital Francisco José de Caldas, Bogotá D.C 111931, Colombia
E-mail: [1]andfrodrigueza@correo.udistrital.edu.co, [2]djrojasm@correo.udistrital.edu.co, [3]dagiralr@udistrital.edu.co

ABSTRACT

The objective of this article is to present a review of the communication protocols implemented for the power system. Communication protocols arise with the need to be able to perform immediate communication between one or several sectors of the system, in order to minimize possible failures that may occur along this, in addition to sending orders and signals that decrease manual operability, giving way to automatic control that aims to manipulate the largest amount of information remotely. The protocols shown here are intended to make known how new technologies have come to stay, but these will take time to implement, this is mainly due to the poor infrastructure conditions of the power system. Finally, it delves into new communication protocols opening up new and future ways of controlling the electrical power system

Keywords: *Automatic Control, Communication Protocols, Power System, Internet of Things*

1. INTRODUCTION

The electrical system has open communication protocols such as Modbus, DNP 3.0, IEC60870, PC/ICP, TCP/IP, in addition to IEC 61850 [1]. To carry out each of the communication protocols, the Open Systems Interconnection (OSI) model is presented, the main objective is to have a structural guideline to exchange information between computer systems, networks and terminals [2]. Divided into 7 layers, the OSI system facilitates the forms of communication, separating the responsibilities in each of the layer's, thus processing data is easier [3].

For the future, the term Internet of Things, its acronym in English (IOT), allows an interconnection between both physical and virtual parts, adapting to existing interoperable communication and information technologies, trying to give a global infrastructure which is the basis for smart networks, its main action is to allow intercommunication in an intelligent, reliable and secure way [4]. Regarding the previous review works, in the communications area there are several works that have been developed, however, these publications are oriented to describe specific methodologies. Unlike other publications, this article presents a more general vision, leaning from the OSI model to IEC 61850. Additionally, it is important to highlight that aspects based on IoT and artificial intelligence were addressed, elements not available in the current literature.

1.1. Definition

A protocol is an indication, procedure or norm that allows to guide an action or that establishes certain bases for the development of a process. Communication is an element with multiple uses that is generally used to name the transmission and reception of messages. Therefore, communication protocols are a set of guidelines that make it easier for different elements to form part of a system and establish communications with each other, exchanging information [5].

2. OSI MODEL

The open system interconnection model, its acronym in English (OSI), is a system created by ISO and CCITT in order to simplify communication on the network, thus dividing communication responsibilities into seven layers (Table 1) [3]. The main objective of the model is to have a clear structure for the exchange of information between the different actors [6]. The layers described above can be grouped into two groups, the lower level composed of the first three layers (physical, link and network), and the upper level composed of the last three layers (session, presentation and application), while the middle layer (transport layer), can be part of the lower layer or the upper layer, as required by the system [7].

Table 1: Layer of the OSI model

Layer	Definition	Examples
Physical	Specifies electrical, physical and procedural standards to access the data communication network, this layer quantifies the values required for the proper functioning of the machines.	V.35, RJ45, RS-232
Data binding	It is responsible for the primary and secondary nodes to communicate with each other, giving way to the data that is responsible for activating, maintaining and deactivating the link between data.	FFDI, IEEE 802.3, ETHERNET, PPP, ATM
Net	Determines which type of network configuration is best suited depending on what is required by the network.	IP, IPX, X.25, ICMP
Transport	Protects the integrity of the message, from departure to arrival, through the time of the message, the layer allows you to recover an error for the message, also includes its route and segmentation.	It is the highest layer as far as communications is concerned, since the layers above the transport layer do not intervene in the technological aspects of the network.
Session	It allows to have network availability for the different media, this means that it takes care of the storage capacity and its processor.	TCP, UDP
Presentation	This is what translates the code and character set and determines the message display mechanism.	SQL, NFS, NetBIOS
Application	This is the direct communication with the application used by the user.	HTTP, FTP, SMT

3. TCP/IP PROTOCOL

Created in the United States in order to design a new architecture that allows connecting multiple networks to each other. Like the ISO protocol, the TCP/IP protocol is divided into several layers (Table 2) [2], to facilitate its understanding, in addition to and equal to the OSI protocol, it divides its functions in each layer facilitating the transmission of the message [8]. In Table 3 the comparison of the layers between the OSI model and the TCP/IP model is appreciated.

Table 2: Layers of the TDP/IP model

Layer	Definition	Example
Physical Network	Specifies the characteristics of the hardware to be used for the network.	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI.
Data link	Identifies the type of network protocol of the packet.	PPP, IEEE 802.2.
Internet	Accepts and transfers packets to the network.	IPv4, IPv6, ARP, ICMP.
Transport	In this layer is the end-to-end protocol which is reliable oriented to your connection.	TCP, UDP, SCTP.
Application	Here we find the highest-level protocols, including mail.	NFS, NIS, DNS, LDAP, TELNET, FTP, RLOGIN, RSH, RCP, RIP, RDISC, SNMP.

Table 3: OSI System Vs TCP/IP System

Layer	OSI model	TCP/IP model
1	Physical	Network host
2	Data link	
3	Net	Interred
4	Transport	Transport
5	Session	Application
6	Presentation	
7	Application	

4. COMMUNICATION STANDARDS

4.1. Modbus

Created in 1979 implemented for unbalanced transmission using the RS232 communication standard, and later for balanced transmission with the RS485 standard, it is reliable, functional, adaptable and current, it has been on the market for more than 40 years, Modbus was born for the first PLCs, more precisely giving way to the programmed logic that by then only wired logic was contemplated, this was based on electromagnetic relays power contactors, timed relays, etc., since all this wired logic was too complex the programmed logic is created, starting the first PLC, (MODICON)

Journal of Theoretical and Applied Information Technology
31st October 2022. Vol.100. No 20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

084 of Modular Digital Controller, directed by Dick Morley [9].

In the world of protocols there are two types of protocols, open protocols and proprietary protocols, Modbus today is an open protocol, this is because Schneider Electric in 2004 headquarters the rights of the protocol to the Modbus organization so that this in turn is responsible for driving the adoption of the Modbus communication set and evolve addressing new architectures for distributed automation systems [10]. This model is a response request protocol that is located in layers 1, 2 and 7 of the OSI model, based on a master slave or client server relationship, which has become a standard protocol in the industry, thanks to its wide spectrum of functionalities and its great adaptability. The structure of the protocol revolves around the messages of the physical equipment, and not the physical equipment itself, or the means of communication, in this way regardless of the means of transmission the Modbus protocol lasts since its creation [11]. In Figure 1 the architecture of the Modbus protocol is observed.

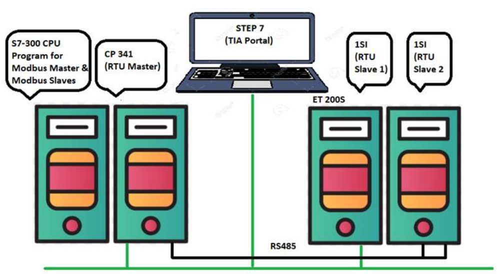

Figure 1: Modbus architecture

4.2. Profibus

The development of PROFIBUS began in 1987 in Germany, when 21 companies came together to create a standard for automated machines and other device interfaces. Profibus FMS was first created and followed by PROFIBUS DP in 1993. Currently, PROFIBUS is standardized by IEC 61158 and IEC 61784. The media-guided access protocol used in the Profibus network uses the second layer of the OSI model. This communication bus is designed for a wide variety of automation tasks [12].

PROFIBUS (Process Field Bus) is a Fieldbus standard that requires the German national standard DIN 19245 and the European standard EN50170. It is a Fieldbus technology for workshop-level monitoring of factory automation and data communications and control of field devices. PROFIBUS is composed of three compatible parts, PROFIBUS-DP, PROFIBUS-PA and PROFIBUS-FMS (Table 4). Fieldbus is widely used in the field of automation and industrial control with its openness and adaptability. A real-time communication solution based on PROFIBUS (RTCS_PROFIBUS), which is oriented to the field of automation and industrial control. In RTCS_PROFIBUS, users can monitor real-time data running on the xPC Target real-time operating system and PROFIBUS devices through the LabVIEW user control program on the Host PC. Communication between the host PC and the target PC is based on the TCPI/IP protocol over twisted pair. Real-time data between xPC Target and controlled devices is transmitted by PROFIBUS via the high-speed DPRAM interface.

Table 4: Components of the Profibus protocol.

PROFIBUS-DP	PROFIBUS-PA	PROFIBUS-FMS
Designed specifically for field-level distributed nodes.	It is commonly used in process automation.	It is a real-time multi-master network token structure for workshop monitoring.

In Table 5 the four types of interfaces are presented at the PROFIBUS physical level. In Figure 2 the architecture of Profibus is shown.

Table 5: Types of Profibus physical interface.

RS485	RS 485-IS	MBP	Fiber optics
For tasks where high transfer rates are essential. The highest possible transfer rate is 12 Mbit/s. The devices are interconnected through the bus topology, using the class A cable (shielded twisted pair). A maximum of 32 devices can be connected to a bus segment, the maximum number can be increased to 126 when using the repeaters.	It is a spark-proof version of the RS485 interface. The maximum transfer rate is 1.5 Mbit/s. At most, 32 devices can be connected to a bus segment.	(Manchester encoding and bus powered): a download-proof interface, the transfer rate of 31.25 kbit/s and the power supply of the device via the bus conductor. The network topology can be bus or star type. At most, 32 devices can be connected to a bus segment in a normal environment or 10 devices in an explosive environment. The data is encoded by the Manchester code.	It allows very high transfer rates of 12 Mbit/s for very long distances (kilometers). The line, star, or circle topology is supported. At most, 126 devices can be connected on the network.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

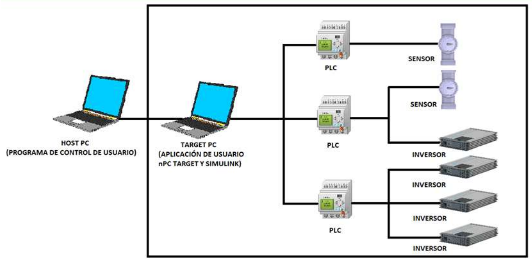

Figure 2: The user architecture RTCS_Profibus

4.3. IEC 60870-5

The IEC 60870-5 standard defines the communication protocol for remote control systems and for the monitoring and control of geographically large processes. It refers to a collection of standards that provides a detailed functional description for remote control equipment and systems for controlling geographically extended processes (SCADA systems). It is intended, but not limited to, applications in the electrical industry, and has data objects that are specifically intended for such applications; however, it is not limited to them. It consists of five basic standards and four complementary standards as shown in Table 6. The family of standards defines the frame format transmission services at the link level, the general data structure at the application level, and the basic functions for information [13].

Table 6: IEC 60870-5 protocol standards.

Basic standards		Common Standards	
IEC 60870-5-1	Transmission frame formats.	IEC 60870-5-101	Transmission protocols, common standards especially for basic remote-control tasks.
IEC 60870-5-2	Data link transmission services.	IEC 60870-5-102	Common standard for the transmission of totals integrated into electric power systems.
IEC 60870-5-3	General structure of application data.	IEC 60870-5-103	Transmission protocols, common standard for the informative interface of protective equipment.
IEC 60870-5-4	Definition and coding of information elements.	IEC 60870-5-104	Network access transmission protocols for IEC 60870-5-101 using standard transport profiles.
IEC 60870-5-5	Basic application functions.		

The most commonly used standards of the IEC 60870 protocol are the IEC 60870-5-101 standard and the IEC 60870-5-104 standard, which will be described in Table 7.

Table 7: Description of IEC 60870-5-101 and IEC 60870-5-104 standards

IEC 60870-5-101 standard	IEC 60870-5-104 standard
Defines a functional profile to the IEC 60870-5 definitions for interoperability between compatible remote-control devices. In telecommunications, a functional profile specifies how options and ambiguities in standards should be interpreted or implemented to provide a particular information technology function. It aims to recommend how existing standards, in this case the core 60870-5 standards, should be used without modifying them. The application environment is in the communication between remote control systems (SCADA), UTR devices and programmable controllers [13].	It is an international standard launched by the IEC in 2000. This is based on the IEC 60870-5-101 standard, with which it shares the same structure at the application layer. This protocol is responsible for establishing TCP/IP appointment communication, to ensure secure data transmission, between the control center of the SCADA system and the different controllers, it also establishes that the general port of use for TCP transmissions is 2404. This port corresponds to those packages considered as slaves. These slaves can only send answers or information to the question of a master, who will be in charge of giving orders or collecting the information provided by the slaves [14].

4.4. IEC 61850

The IEC 61850 standard defines the communication and services between different devices within an electrical substation. It is the result of the joint work of many global organizations in the field of electrical standardization. The standard uses the concept of virtualization, which offers insight into the operational aspects of a real device that are important for sharing with other devices. The standard only defines the details necessary for the interoperability of devices. It is based on the object-oriented model. The functionality that real devices have is divided into small entities, which are used for the exchange of information between different devices. These entities, or LN (Logical Nodes), represent virtually the real functions [13].

The change of the industry forces the creation of a protocol which unifies the IEC 60870-5 protocol, Modbus, DNP and others, capable of adapting to current needs, for this the IEC 61850 protocol is created which is not only a protocol, but an international standard for communication

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

between equipment, control and communication of a substation, which is part of the power system, also allowing maneuvers that could not be implemented before or with enough costs [15].

In Table 8 the protocols that make up the IEC 61850 standard are shown.

Table 8: Protocols that make up IEC 61850

Protocol	Definition
(SMV) SAMPLED MEASURED VALUES. (Sampled measured values).	It provides fast communication to measurement, control and protection values, manages an issuer-subscriber structure, where the sender sends the data to all the equipment on the network and each equipment subscribes to the data to access and the same.
(SNTP) SIMPLE NETWORK TIME PROTOCOL. (Simple network time protocol).	It is used for the synchronization of time of the devices, it is located in the transport layer of the OSI model.
(MMS) MANUFACTURING MESSAGE SPECIFICATION. (Manufacturing Message Specification)	The protocol is mainly used in industrial applications, according to ISO 9506, it is located in the transport layer of the OSI system, its physical transmission medium is SR 232c. It is also the base standard for transmission protocols.
(GSE) GENERIC SUBSTATION EVENTS. (Generic substation events). (GOOSE) GENERIC OBJECT-ORIENTED SUBSTATION EVENT. (Generic object-oriented substation event).)	It is a publisher-subscriber type communication, this protocol is used for the exchange of information between IED (Intelligent Electronic Device) in a substation over Ethernet.

The GOOSE protocol is the most used in the automation of substations, it is an event-based protocol, the concept of GOOSE communication is that the editor sends messages periodically and when an event occurs (Trigger, Closed Contactor, etc.), it sends a large number of messages with new data. Because the protocol is based on the publisher-subscriber, there is no confirmation that the subscriber correctly receives the message sent, so the large number of messages minimizes the possibility of message loss, all messages are advertised under the same theme. The subscriber receives all messages from the system, but filters and analyzes only messages sent within the registered topic. The inclusion of the LAN network in the substations benefits them from the costs and spaces, since a large amount of information that uses many cables is much more viable through a LAN network, with this it is possible to have a large amount of information without the need to expand infrastructure [16].

5. REDUNDANCY PROTOCOLS

5.1. PRP (Parallel Redundancy Protocol)

Its recovery time is 0 MS, its topology is independent, it is sent from a source node to a destination node, in two frames in this way if one fails the other responds, with different Lan's. It is a reliable and deterministic protocol that ensures successful communication in the SAS (substation automation system) [17].

5.2. HSR (High Availability Transparent Redundancy Protocol)

Based on ring topology, with full duplex nodes operating with two parallel ports such as PRP, two frames are sent from the source node, they are redundant, and each node forwards these two frames from one port to another [18].

6. APPLICATIONS

6.1. Artificial intelligence

With the development of the electricity grid, indices of its operation requirements have been proposed, such as safety, economy and convenience, among others. The traditional power grid faced serious challenges; it is difficult for the traditional power grid to meet the new requirements. To solve the problem of the requirement, such as security and high efficiency, as well as the observable and controllable state of the operation of the power grid in the context of the intelligence industry, the opinion is presented that 5G and artificial intelligence (Figure 3) [19] with multi-sensor data fusion technology are compatible in future smart energy operation. 5G technology is first presented as the basis of the communication technology of the electricity grid. Then artificial intelligence is the main method of monitoring the operation of the power grid in the future. It has the way in which it uses advanced big data technology and multi-sensor data fusion to complete the base data collection of the intelligent monitoring process and is smart to complete the process of monitoring the operation of the power grid with artificial intelligence and machine learning [20].

5G technology is the basis of electricity grid communication. The depth of the 5G application decides the scale and scope of the information interaction of the future power grid. The quality of the 5G application determines the effect of the future application of the electricity grid information. Artificial intelligence is the method of generating intelligent monitoring in the operation of the electricity grid in the future [21].

As long as 5G is satisfied with the real practice work and combined with artificial intelligence, it can meet the future demand for intelligent monitoring in the operation of the power grid. A case of 5G and artificial intelligence with multisensory data fusion technology is proposed that is applied in the field of substation operation and maintenance and provides the conceptual support for the construction of intelligent training, smart manufacturing, as well as smart China [19].

Figure 3: The system module

Artificial intelligence is currently an application in electrical engineering, it uses several intelligent algorithmic agents that can improve the rate of performance of a digital power grid system. Developing state-of-the-art technology in electrical grid control systems using multi-agent systems, this system is implemented using various microcontrollers and the IEC 61580 communication protocol for communication in automated electrical systems. The network and communication system in the cloud technology of wireless communication applies in efficient data communication for multi-agent systems. [22].

6.1.1. Internet of energy

It is a cyber-physical system (CPS) to directly and indirectly connect information, communication, control and protection devices to effectively generate, transmit, use and store various energies by merging new technologies such as artificial intelligence (AI), cloud computing and blockchain, etc. Recently, AI technology has become increasingly popular in many industrial and research fields because it can perform tasks well. However, applying artificial intelligence technologies to internet power is relatively minor [23].

6.2. Internet of things

The Internet of Things (IoT) is the connection of the physical world to the Internet (Figure 4) [24]. It is rapidly emerging as the sustainable solution to providing access to clean and affordable energy around the world. IoT-enabled utilities can have real-time feedback capabilities to better understand customer needs and thus make smart decisions to improve their service experience [25].

With IoT, electric power grids will become more secure, reliable, resilient and sustainable. IoT certainly opens the door to many opportunities, but it also has some challenges associated with it. Some of these challenges include sensing, power management, cybersecurity, system complexity, and wireless and cloud connectivity. To grow and develop IoT, it becomes essential to have innovative sensing technology, a wide variety of wired and wireless standards, the lowest power consumption solutions for any application, built-in hardware security technology, IoT solutions for everyone and not just experts, and an ecosystem of cloud partners to enable seamless integration [24].

Figure 4: Internet of things (IoT)

6.2.1. IoT in substations

To solve the problems in the current substation monitoring system, using Internet of Things technology, modern communication technology, information processing and technology, we have a substation detection monitoring system based on the Internet of Things (Figure 5) [26], the system performs real-time monitoring of substation equipment and operating environment, data intelligence analysis, alarm linking and visual visualization, provides assistance support for substation operation and maintenance,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

improved the management level of smart substation [26].

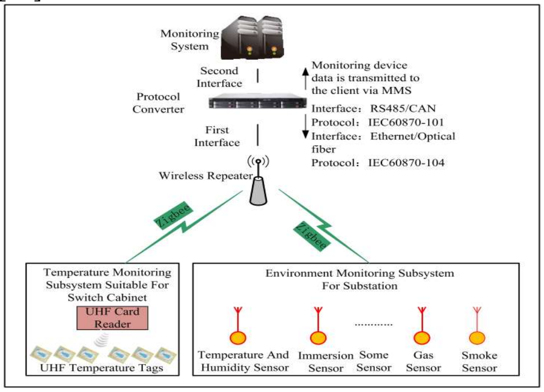

Figure 5: Diagram of IoT architecture in substations

IoT has been regarded as the third revolution in digital technology after the computer and the Internet. Currently, the power grid is transforming into a smart grid on the planet, automation and intellectualization requirements would lead to deep IoT integrations with the smart grid. The smart grid would generate a market of up to a trillion RMB, posing major challenges to make IoT technology more practical for industrial applications in smart grids. Mature wireless communication theory and network optimization theory have paved the way for the theoretical basis of IoT [27].

6.3. Transmission line monitoring system

The use of Internet of Things (IoT) technology in the smart grid is an important approach to speed up the computerization of the power grid system and is an improvement for the effective management of the power grid infrastructure (Figure 6). Disaster prevention and reduction of power transmission line is one of the most important application fields of IoT. Advanced IoT sensing and communication technologies can effectively avoid or reduce the damage of natural disasters on transmission lines, improve the reliability of power transmission, and reduce economic losses.

There are parts for the transmission line monitoring system, one part is installed together with the power transmission lines to monitor the condition of the conductors; the other part is installed on the transmission towers to monitor the environment and the status of the towers. Communication between IoT devices on power transmission lines and transmission towers is generally based on short-range wireless communication technology. The IoT-based online monitoring system of power transmission lines can transmit the information further through the multi-hop relay communication network, which can ensure effective information transmission for power transmission facilities. powerful and long distance. According to the different application scenes of the power transmission line, the network topology of the system can be cluster chain type [27].

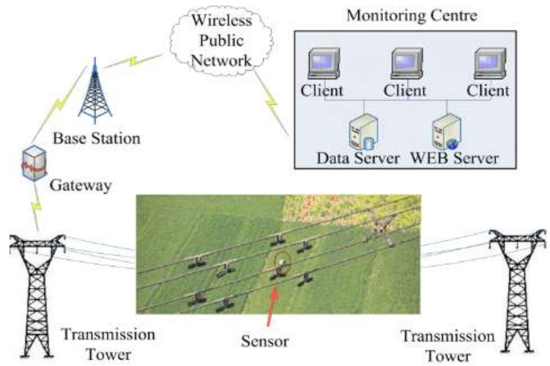

Figure 6: Data transmission network

Each sensor can communicate directly with the nearby main node, and the communication links between the sensors and the trunk nodes are usually one-way links; each node in the backbone can communicate with up to 256 sensors. The distance between the nodes of the backbone is several hundred meters and the communication link between the nodes of the backbone is a bidirectional link. Parts of the backbone nodes can access the public network via 3G, TD-LTE or power optical network. As shown in Figure 5 [27].

6.4. Information problems on the web

For the problems of network information and security in the power system, there is a self-defense solution for the ai-based energy information network. At the same time, there are new active defense technologies such as vulnerability scanning, baseline scanning, network security attack, and defense drills in the security of the energy information network, with the aim of improving the level of information security and ensuring the network security of the power system [22].

There is an information security prevention and control system based on artificial intelligence, and on this basis, a standard of evaluation of information security status indicators is developed, which provides the conditions to pre-discover the hidden dangers of information and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

improve information security prevention and control capabilities. At the same time, through the collection of information security status and hierarchical visualization of information security risks, the information security early warning artificial intelligence identification platform is built. Through the coordinated linking of the provincial, municipal and national levels, the management of information security can be carried out from wide to fine, from the punctual and frontal management to the management of the stereo of the system. In short, the construction and implementation of the information security prevention and control system based on artificial intelligence not only reinforces the control and standardization of the information and communications security of provincial, municipal and national energy supply companies, but also improves the management efficiency of the company. and the management of the electricity grid. And future development is of great importance [28].

Internet of Things (IoT) devices that have limited power and processing capabilities are susceptible to physical layer spoofing (PHY) (signal exploitation) attacks due to their inability to implement a full protocol stack for security. The overwhelming adoption of multi-carrier techniques such as orthogonal frequency division multiplexing (OFDM) for the PHY layer makes IoT devices more vulnerable to PHY phishing attacks [29].

These attacks that aim to inject false or spurious data into the receiver involve inferring transmission parameters and finding PHY characteristics of the transmitted signals to falsify the received signal. It has been argued that noncontiguous OFDM (NC) systems have low probability of exploitation (LPE) characteristics compared to classical attacks based on stationary cycle analysis, and the corresponding PHY has been considered safe. However, with the advent of machine learning (ML) algorithms, adversaries can design data-driven attacks to compromise such systems [27].

The PHY phishing performance of adversaries equipped with supervised and unsupervised ML tools is investigated. The supervised ML approach is based on estimation or classification using deep neural networks (DNNs), while the unsupervised one employs variational automatic encoders (VAEs). In particular, vaEs are shown to be able to learn representations of NC-OFDM signals related to their PHY characteristics, such as frequency pattern and modulation scheme, which are useful for PHY impersonation (Figure 7) [30]. In addition, there is a new metric based on the principle of untangling to measure the quality of such learned representations.

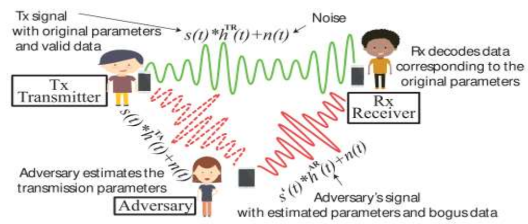

Figure 7: Spoofing PHY by an adversary listening to TX-XR streams

6.5. Wireless networks

Recently wireless sensor and actuator networks (WSANNs) have become a major innovation in the modern world [31]. This technology consists of two main parts, a group of sensors and actuators. Sensors act as an information-gathering tool that collects data about the physical world such as heat and humidity and then communicates this data with other nodes in the network. Upon receiving the collected data, the actuators can perform actions that interact with the physical world according to the collected data. This kind of interaction between devices and the physical world generated new horizons in IoT and other smart devices. Therefore, some WSAN-based applications can automate specific tasks such as controlling room temperature in a smart home [32]. But as technology advances, WSAN-based applications are deployed in mission-critical systems where Quality of Service (QoS) is very crucial and cannot tolerate packet loss or delays. Therefore, QoS has become an important factor when talking about mission-critical WSAN, as such systems can be life-threatening in many cases. Therefore, we have a comprehensive overview of the cutting-edge approaches, protocols, and applications that contributed to improving QoS in WSAN[33].

A solution for a routing protocol that uses deep learning techniques to recognize patterns in the path through which network traffic passes and assist in the decision-making process of the next best alternative route. The approach also tracks the alternate routes that packets take in case a node goes offline in the normal routing path. Therefore, it provides reliability and efficiency as it helps reduce route discovery and reduces power consumption on nodes. Finally, some interests in the field of WSN and its future. Current existing WSNs can be greatly improved and it is worth noting the great research opportunities in this field [31].

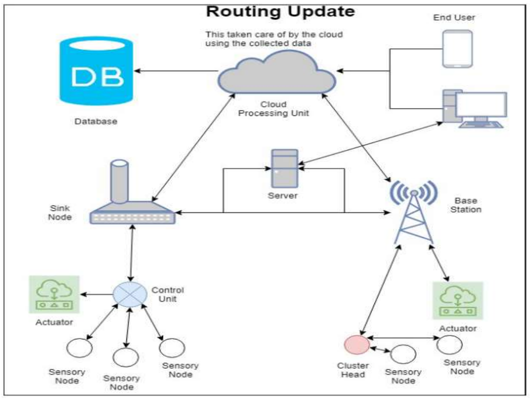

Figure 8: System architecture

6.6. Spider web topology

It is an improved protocol based on IEC 62439. (IEC 62439-3:2016 is applicable to high-availability automation networks based on Ethernet technology.) It guarantees great reliability, this protocol is exposed through a topology based on a double IED attachment (intelligent electronic device). The protocol evaluates the recovery time and latency of the network, these identify the important factors of the protocol's performance [34].

The evaluation of the performance of the improved proposal, the PRP based on the single web topology architecture, with double IED attached implies that it is a deterministic and reliable protocol that ensures successful communication in the SAS network. Dual-connection IEDs have been modeled according to IEC 62439 to analyze the network latency throughput of the proposed protocol. The simulations, which proceeded to evaluate the performance of the network latency for the time-critical GOOSE message, have indicated that the latency of the network is within the maximum of 3 MS standardized by IEC 61850. Therefore, the improved PRP based on a single web topology is safe to be applied in protection and control operation in intelligent substation either in normal situation or failure in the SAS communication network[16].

6.7. System configurators

According to IEC 61850, the description of single-line diagram substation, the assignment of protection functions to protected elements and the assignment of protection functions in protection IEDs is done using SCL language. However, the functions of relay protection devices are described according to the IEC 61850 information model containing logical nodes, logical and physical devices [35]. Currently, there is a sufficiently large number of special software tools for the development of relay protection configuration description files, which are known as system configurators. The application of system configurators is aimed at highly qualified specialists who, based on their experience and knowledge of regulatory and technical documents, develop the configuration of the functions of relay protection and automation devices. Developing the configuration of the substation relay protection is quite a difficult and laborious task, along with the solution of a number of creative tasks. In this case, the probability of errors associated with the human factor is quite high. The form of technological infusion of knowledge bases illustrates the possibility of significant simplification, acceleration and improvement of the quality of the design phase of digital substations in the format of IEC 61850 [36].

As well as offering one of the possible directions for the development of digital substations. The successful implementation of the described mission, the creation of PAC's educable global knowledge base would increase the level of automation and intellectualization of PAC, emergency automation, APCS, automated information and measurement system of commercial energy measurement complexes, which will significantly accelerate, reduce the cost and improve the quality of technological processes in the electric power industry [37].

7. CLEAN ENERGY

A transformation is underway in electric power and power systems (EPES) to provide distributed clean energy for sustainable global economic growth. The Internet of Things (IoT) is at the forefront of this transformation by imparting capabilities, such as real-time monitoring, situational awareness and intelligence, control and cyber security to transform existing EPES into cyber-enabled intelligent EPES, which is more efficient, secure, reliable, resilient and sustainable [38] . In addition, the digitalization of the electric power ecosystem through IoT improves asset visibility, optimal management of distributed generation, eliminates energy waste and generates savings. IoT has a significant impact on EPES and offers several opportunities for growth and development. There are several challenges with implementing IoT for EPES. It is necessary to develop viable solutions to overcome these challenges and ensure the continued growth of IoT for EPES. Aside from the numerous advantages of IoT for EPES, it also has some associated challenges, namely sensing, connectivity, power management, big data, computing, complexity, and security. To ensure the continued growth of IoT for EPES, it is essential to develop viable solutions to handle its increasing complexity. One possible direction for handling the complexity of the future IoT may be inspired by brain computing (with 100 billion neurons in a human brain, where each neuron is connected to another 10,000 neurons). Computational intelligence is the future of complexity management in artificial systems. EPES are composed of generation, transmission and distribution (T&D) networks and their customers (residential, commercial and industrial) [39]. EPES currently faces numerous constraints, including balancing the fuel mix, reliability of power delivery and quality, asset level visibility, identifying new revenue streams, capturing knowledge and an aging workforce, and integrating technology. The fuel mix for power generation is becoming more diverse and flexible and comprises centralized generation (fossil fuels and nuclear), distributed generation (renewables) and energy storage. Balancing this fuel mix is critical to maximizing the profitability and energy production of THE EPES. Digital innovations (collaboration, communication and digital memory creation) are necessary to capture the knowledge and experience of senior workers, incorporate it into the institutional memory of companies and make it accessible to the new workforce. With the advent of IoT, intelligent machines, and big data, traditionally separate information technology (IT) and operations technology (OT) must now be integrated to develop a new information-driven infrastructure to improve productivity using [40].

8. ANALYSIS OF THE INFORMATION

Table 9 refers to advantages and disadvantages that are evidenced in the different communication protocols, standards and emerging technologies; In addition, it is shown that from the differences previously described there are protocols adaptable to specific needs taking into account the different network topologies that can be found in a power system, on the other hand, the socio-economic conditions in which this system will be implemented are recognized in order not to require considerable change in economic terms for its operation. The new technologies are developed to fully meet the recent and growing demands of the power system today. However, no new infrastructure and telecommunications policies have been implemented in countries that are in the process of development, therefore, these territories do not have the technological advances that have been developed and implemented in developed countries to improve efficiency, reliability. , and safety throughout the power system, However, the technologies currently available to developing countries have managed to meet their needs in terms of energy efficiency. The protocols that have been on the market for 3 to 4 decades will still be available for several more decades, although there are several challenges to make the transition to the new communication protocols, already implemented in territories where technology is at its highest peak. One of the biggest challenges for developing countries are the fact of continuing to use protocols that have been on the market for several years mainly because of their low cost in terms of maintenance and implementation, considering making a transition or upgrade in technological scenarios is unthinkable for now, because of the high cost involved in a change of that magnitude, which at some point will be required. There is no doubt given that it is imperative to understand that technology is constantly developing and each territory must adapt to current policies and that arise in terms of energy efficiency.

9. PROBLEMS AND OPEN RESEARCH

Communications systems revolutionized the operation of power systems, it is an increasingly important factor. The challenges that must be assumed are diverse, the research work is permanent, its applications range from low-scale control and operation schemes, to stability controls, protection systems, protection coordination, among others. Additionally, it is essential to include the academic sector.

This work presented a description of the evolution of communication protocols in power systems, however, the topics analyzed were taken in a general way. As future work, it is required to carry out a detailed analysis according to the current regulations of each of the protocols, their operating methodology and their characteristics

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 9: Advantages And Disadvantages Of Communication Protocols In The Power System

Protocols/ Standards/ New technologies.	Advantages	Disadvantages
Modbus.	Simple, reliable and functional standard. Ideal for small and medium data connection.	High costs for its configuration. A complex connection in different modicon systems.
Profibus.	Large applications of automation and industrial control.	Only transfers little data, less than or equal to 244 Bytes High count in its programming
IEC 60870-5	Communicating over a standard network allows the transmission and reception of data on different services or devices. Designed for large remote control and monitoring systems.	The limitation of the types of information and parameters defined in IEC 60870-5-101, does not allow all functions to be supported by IEC 60870-5-104. In some cases, the outputs are strictly in RS-232 or RS-485, converters are needed for current protocols.
IEC 61850	Improved operational aspects for the exchange of information between one device and another. Compatible with artificial intelligence.	Its application focuses on electrical substations. It is highly dependent on the communication between intelligent electronic devices (DEI's).
PRP and HSR.	Speed for the response of possible failures, integral and deterministic.	Low reliability, the non-increase in security, forces the protocols that are above, at the application layer, to provide the level of security.
Artificial intelligence.	Self-defense solution for the energy information network based on artificial intelligence.	High costs in the infrastructure for its implementation.
Internet of Things.	IoT utilities can have real-time feedback capabilities to better understand customer needs. With IoT, electric power grids will become more secure, reliable, resilient and sustainable.	Challenges include: energy detection and management, cybersecurity, system complexity, and wireless and cloud connectivity.
5G networks.	High speeds in the transmission and reception of data in very small times.	High demand for infrastructure (Antennas) due to the use of high frequencies, there is a lower coverage. Users must purchase new devices to be compatible with the 5G network.

10. CONCLUSIONS

There are communication protocols used in the power system, some with more than 4 decades in the market, which still have great adaptation in underdeveloped countries, these due to great challenges that are still presented by different factors such as: infrastructure, economy, social impact among others, these protocols have a place even today due to their simple use, however the world is constantly changing, for this new protocols have been created to meet the new needs of the environment, these protocols combine the old protocols, allowing greater ease for the adaptation of new technologies, these can improve and facilitate the interaction of the human being with the equipment of the system, which through applications that day by day respond to different scenarios, they manage to give ease to problems, failures, interruptions of the energy service, among others.

Giving way to the new technologies that are already currently found in developed countries, such as China, Japan, Russia, the United States and part of Europe, they present protocols with a very high speed of response to each problem that arises throughout the power system, technologies such as the Internet of Things (IoT), Machine learning, artificial intelligence, 5G network and wireless networks, give greater reliability, less response times and better human-machine interaction, from generation through the transmission, distribution and commercialization of energy. Finally, there is a visualization of clean energies for which the communication protocols of new technologies are fundamental in their development.

REFERENCES

[1] No Title vol. 66, pp. 37–39, 2012.
[2] B. S. Rawal and A. Pipeline, "Multilayer Split-protocol," pp. 476–479.
[3] J. L. Cedillo Méndez, F. Salas Ramírez, and L. O. Linares, "Capítulo 3. Communication Protocols," *Thesis Bachelor' Degree. .Eng.*

*Mec. Electric. – Electric. and Electron. – Mód. Com,*pp. 55–70, 2012.
[4] W.M. Giral Ramírez, H. J. Celedón Flórez, E. Galvis Restrepo, and A. T. Zona Ortiz, "Redes inteligentes en el sistema eléctrico colombiano: Revisión de tema," *Tecnura,*vol. 21, no. 53, pp. 119–137, 2017, doi: 10.14483/22487638.12396.
[5] P. Line and C. Committee, *IEEE Standard for Smart Energy Profile Application Protocol,*vol. 2018. 2018.
[6] B. Zhang, "Fig.1. Transmission signal with Hart Protocol," *Hujiijiiii,*pp. 0–2.
[7] C. A. Zamai, D. Bavoso, A. A. Rodrigues, and J. A. S. Barbosa, Title," Resma*,*vol. 3, no. 2, pp. 13–22, 2016.
[8] P. Liu, Y. Lu, L. Chen, X. Kang, G. Lyu, and J. Du, "A data exchange protocol of physical gap device for power system," *ACM Int. Conf. Proceeding Ser.*, pp. 87–91, 2019, doi: 10.1145/3333581.3333601.
[9] S. Industry and O. Support, "Master-Slave Communication with Modbus RTU Protocol for S7-300 and ET 200S Systems," pp. 1–42.
[10] V. G. Găitan and I. Zagan, "Experimental implementation and performance evaluation of an IoT access gateway for the modbus extension," *Sensors (Switzerland),*vol. 21, no. 1, pp. 1–24, 2021, doi: 10.3390/s21010246.
[11] "Universidad Autónoma de Madrid," 2020.
[12] G. Gabor, C. Pintilie, C. Dumitrescu, N. Costica, and A. T. Plesca, "Application of Industrial PROFIBUS-DP Protocol," *EPE 2018 - Proc. 2018 10th Int. Conf. Expo. Electronic. Power Eng.*, pp. 614–617, 2018, doi: 10.1109/ICEPE.2018.8559857.
[13] J. Lobo, M. Cuenca, D. Gregor, M. Arzamendia, R. Gregor, and S. Toledo, "Design and implementation of a gateway between IEC 61850 and IEC 60870-5-101 standards for power electrical systems," *CHILECON 2015 - 2015 IEEE Chil. Conf. Electronic. Electron. Eng. Inf. Commun. Technol. Proc. IEEE Chilecon 2015,*pp. 535–541, 2016, doi: 10.1109/Chilecon.2015.7400429.
[14] D. Sanchez Gomes, "Universidad Autónoma de Madrid Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación Proyecto Fin de Grado," pp. 1–36, 2019.
[15] A. Networks, "FOR POWER SYSTEMS – A STEP TOWARDS SMART Engineering Networks," vol. 3, no. 2, p. 15, 2012.
[16] I. Del, P. Iec, E. N. La, A. Y. Protección, and D. E. S. D. E. Potencia, "Redes de Ingeniería DESIGNING AND IMPLEMENTING THE IEC 61850," 2012.
[17] M. G. Rubinstein and T.M. da Vinha, "Availability analysis of power substation automation architectures with PRP and HSR protocols," *IET Gener. Transm. Distrib.*, vol. 12, no. 22, pp. 6000–6003, 2018, doi: 10.1049/iet-gtd.2018.6364.
[18] J. Seppala, H. Koivisto, P. Jafary, and S. Repo, "Security and reliability analysis of a use case in smart grid substation automation systems," *Proc. IEEE Int. Conf. Ind. Technol.*, pp. 615–620, 2017, doi: 10.1109/ICIT.2017.7915429.
[19] M. Li and J. Wang, "5G and Artificial Intelligence with Multi-Sensor Data Fusion Technology Support Intelligent Operation Monitoring of Power Grid in the Future," *Proc. - 2020 Chinese Autom. Congr. CAC 2020,*pp. 177–180, 2020, doi: 10.1109/CAC51589.2020.9327727.
[20] E. Carrazana, "Universidad de la Habana Facultad de comunicación Master's Degree in Library and Information Sciences Final work of Information and Communications Technologies Title: Artificial intelligence and its impact on the search process and," no. March, 2015.
[21] I. Jara and J.M. Ochoa, "Uses and effects of Artificial Intelligence in Education," *Banco Interam. I develop. (IDB Group)*, pp. 3–27, 2020, [Online]. Available: https://siip.produccion.gob.bo/noticias/files/BI_19062020cb063_4artifBID.pdf.
[22] A. K. Sahoo, S. Rudra, and A. S. Mohanty, "Artificial intelligence based electric grid operation enabled with data encryption," *Int. Conf. Electronic. Electron. Optim. Tech. ICEEOT 2016,*pp. 275–280, 2016, doi: 10.1109/ICEEOT.2016.7755171.
[23] Z. Huang, T. Gao, X. Gong, Q. Li, and W. Gao, "The application of artificial intelligence in energy internet," *Proc. - 2020 35th Youth Acad. Annu. Conf. Chinese Assoc. Autom. YAC 2020,*pp. 878–882, 2020, doi: 10.1109/YAC51587.2020.9337503.
[24] G. Bedi, G. K. Venayagamoorthy, and R. Singh, "Navigating the challenges of Internet of Things (IoT) for power and energy systems," *Clemson Univ. Power Syst. Conf. PSC 2016,*pp. 16–20, 2016, doi: 10.1109/PSC.2016.7462853.
[25] L. Fedele, "From Basic Maintenance to Advanced Maintenance," *Methodol. Tech. Adv. Maint.*, pp. 63–112, 2011, doi: 10.1007/978-0-85729-103-5_5.

[26] Y. Tian, Z. Pang, W. Wang, L. Liu, and D. Wang, "Substation sensing monitoring system based on power Internet of Things," *Proc. 2017 IEEE 2nd Inf. Technol. Networking, Electron. Autom. Control Conf. ITNEC 2017,* vol. 2018-Janua, no. 5, pp. 1613–1617, 2018, doi: 10.1109/ITNEC.2017.8285066.

[27] Q. Ou, Y. Zhen, X. Li, Y. Zhang, and L. Zeng, "Application of internet of things in smart grid power transmission," *Proc. - 2012 3rd FTRA Int. Conf. Mobile, Ubiquitous, Intell. Comput. Music 2012,* pp. 96–100, 2012, doi: 10.1109/MUSIC.2012.24.

[28] H. Yang, Y. Bai, Z. Zou, Y. Shi, S. Chen, and C. Ni, "Research on Security Self-defense of Power Information Network Based on Artificial Intelligence," *Proc. 2019 IEEE 4th Adv. Inf. Technol. Electron. Autom. Control Conf. IAEAC 2019,* no. Iaeac, pp. 1248–1251, 2019, doi: 10.1109/IAEAC47372.2019.8997705.

[29] M. R. Pérez, "REGION."

[30] A. Nooraiepour, W. U. Bajwa, and N.B. Mandayam, "Learning-Aided Physical Layer Attacks Against Multicarrier Communications in IoT," *IEEE Trans. Cogn. Commun. Netw.*, vol. 7731, no.c, pp. 1–1, 2020, doi: 10.1109/tccn.2020.2990657.

[31] A. Zaza, S. Al-Emadi, and S. Kharroub, "Modern QoS Solutions in WSAN: An Overview of Energy Aware Routing Protocols and Applications," *2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020,* pp. 581–589, 2020, doi: 10.1109/ICIoT48696.2020.9089618.

[32] C. Darab, R. Tarnovan, A. Turcu, and C. Martineac, "Artificial Intelligence Techniques for Fault Location and Detection in Distributed Generation Power Systems," *Proc. 2019 8th Int. Conf. Mod. Power Syst. MPS 2019,* pp. 0–3, 2019, doi: 10.1109/MPS.2019.8759662.

[33] T. César, "Evaluation of Wireless Technologies in Home Area Networks to Obtain the Characteristic Load Curve in Smart Buildings.," pp. 1–47, 2019, [Online]. Available: https://dspace.ups.edu.ec/bitstream/123456789/17531/1/UPS - ST004133.pdf.

[34] B. Liu, L. Chen, and Y. Chen, "Network Topology," *SpringerReference,* 2011, doi: 10.1007/springerreference_19685.

[35] S. Mnukwa and A. K. Saha, "SCADA and substation automation systems for the port of durban power supply upgrade," *2020 Int. SAUPEC/RobMech/PRASA Conf. SAUPEC/RobMech/PRASA 2020*, p. 9041078, 2020, doi: 10.1109/SAUPEC/RobMech/PRASA48453.2020.9041078.

[36] F. A. Acevedo-cardozo, L.C. Calderón-soto, and J.C. G.C, "Communication of electrical systems based on IEC 61850 : Case development using sampled values in Client-Server services Communication of electrical systems in the IEC 61850 Standard : Development of cases using sampled values in Client-," vol. 18, no. 2, pp. 221–236, 2019.

[37] A. A. Voloshin, E. A. Voloshin, and T. G. Busygin, "The Application of Artificial Intelligence Techniques for Automatic Synthesis Substation Configuration Files in Accordance with IEC 61850," *2018 Int. Youth Sci. Tech. Conf. Relay Prot. Autom. RPA 2018*, 2018, doi: 10.1109/RPA.2018.8537211.

[38] F. Sasián, R. Theron, and D. Gachet, "Protocol for wireless communication in renewable energy installations," *RIAI - Rev. Iberoam. Autom. and Inform. Ind.*, vol. 13, no. 3, pp. 310–321, 2016, doi: 10.1016/j.riai.2016.05.003.

[39] C. A. Estrada Gasca, "Transition energetica, energıas renovables y energıa solar de potencia," *Rev. Mex. Physics,* vol. 59, no. 2, pp. 75–84, 2013, [Online]. Available: http://www.redalyc.org/articulo.oa?id=57030971010.

[40] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.C. Wang, "Review of the Internet of Things (IoT) in Electric Power and Energy Systems," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 847–870, 2018, doi: 10.1109/JIOT.2018.2802704.