A Review on Protection Systems in Smart Grids: Automation and Control Applications

SK. Shahnaaz Begum
Department of Electrical Engineering
JNTU Hyderabad, India
shaikshahnaazbegum786@gmail.com

G. Akanksha
Department of Electrical Engineering
JNTU Hyderabad, India
gurramakanksha143@gmail.com

L. Sindhu Rani
Department of Electrical Engineering
JNTU Hyderabad, India
Sindhu.sindhurani345@gmail.com

***Abstract*— This paper provides a synopsis of smart grid automation, control, and protection systems. The objective is to take a look at where things stand right now and see what kinds of challenges and barriers modern smart power systems provide to protection systems. In order to create a smart grid, there needs to be faster communication, more control to make sure the grid works smoothly all the time, and more coordination across the different network resources than in traditional power systems. This is where the control, automation, and protection system really shines. In addition to protecting against the unexpected, these systems must be able to operate normally. This paper provides a solution to the protection problem by covering numerous tactics that can be used on the Smart Grid. At last, the ENEA Smart Grid and Energy lab showcases a cutting-edge Protection, Automation, and Control system.**

Index Terms: IEC, PAC, Smart Grid, and protection systems

I. INTRODUCTION

In recent years, the power system's structure has experienced a profound metamorphosis, evolving from a conventional, static, unidirectional grid to a network that facilitates bidirectional energy and information transfer [1,2]. We refer to these news energy networks as Smart Grids (SGs).

In their efforts to control and coordinate the flow of energy and data, the SGs encounter several challenges. They must not only solve energy-related challenges, but also control and communication issues. 3, 4. In order to keep the grid running smoothly and reduce the likelihood of failures, there has to be close cooperation between end users and a wide range of DERs, including both conventional and renewable sources.

Within this framework, protection systems play a significant role. Apart from the primary functions of safeguarding people, property, and equipment; preventing power outages and voltage fluctuations; enhancing power quality and frequency; and reducing the frequency of power outages, protection systems at the SG level must guarantee quality ofservice (QoS) in the massive presence of DER.

In fact, a number of problems (such as protection blindness, recloser and fuse malfunctions, and fuse coordination errors) might arise when operating in the grid-connected mode. based on the DER's location, size, and kind. Lastly, the protection systems include measures to boost dependability, defend against cyberattacks, maintain privacy and security, and make sure that electricity is supplied to places unaffected byfaults [5].

It is suggested that more devices with protection and monitoring capabilities be placed along the power distribution network in order to achieve the aforementioned aims, and that these devices be used to develop self-healing and protective mechanisms.

In order to ensure the SG is protected to the best of our abilities, we must overcome several obstacles. Issues with the connection mode (island or grid connected), changes brought about by new devices like generators, storage, or loads, the intermittent and unpredictable nature of energy production from RES, the constant presence of rotating machinery that could increase fault currents beyond the nominal values allowed, and lastly, a major problem with intervention timing.

This study delves deeply into the role, characteristics, functions, and application field of Protection Automation and Control Systems (PACs), acknowledging the significance of the open research subject about the use of protection systems. Specifically, Section II gives a general review of PACs and their uses in SGs at both the AC and DC levels. The specifics of the protection schemes—both for the grid-connected and SG island modes—will be covered in Section III. The upcoming trends, obstacles, and challenges are discussed in Section IV, and the advanced PAC that is being developed at the ENEA Smart Grid and Energy Network Laboratory (SGRE) is provided in Section V. The conclusions are finally presented in Section VI.

II. OVERVIEW OF PAC SYSTEM

The SGs paradigm, which calls for Intelligent Electronic Devices (IEDs) to replace conventional system devices, has contributed to the rise in interest in PACs during the past few years.

The term "PACs" refers to a unified collection of power system functions that cover the field, process, and

operational zones and enable the protection, automation, and control of the electrical grid [6]. The IEC 61850 introduces architectures and communications standards, whose application is necessary for the PAC systems' operation and maintenance phases.

The following three subsystems make up PACs.
1. Protection state, which is equivalent to redundancy in electromechanical hardware.
2. An activation condition that enables the release of the contactor.

3. Control state, which is the central component of the entire system, including the device under consideration's command logic.

In Fig. 1, a PAC structure is displayed.

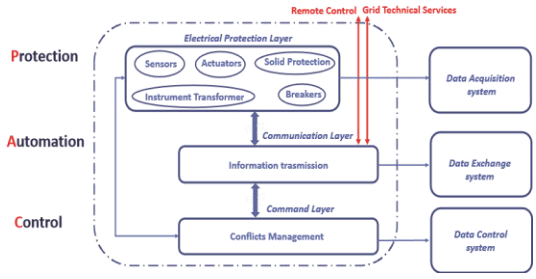

Fig.1. PAC structure and functions.

The first layer of hardware equipment includes smart actuators, solid-state and electromechanical relays, local area sensors, microprocessor-based devices, and other tools for controlling the SG's electrical needs. Among this layer's many functions is the regulation of the grid's frequency, voltage, current, selective fault detection and clearing, and rapid problem diagnostics. The structures being monitored are as near to the places of protective functions, like as lines or transformers, as is practically possible. Both individual components and the entire system are safeguarded by these two types of protection. First, there's the gear that controls network parameters in real time; second, the SG uses this gear—which includes differential, directional, overcurrent, and inverse time relays—to respond to any power system abnormality [7].

In order to derive control actions with a better understanding of the circumstances, the second layer of the PAC system, the communication layer, aims to boost information sharing among multiple devices. This layer is comprised of an appropriate bidirectional information and communication technology (ICT). Specifically, it starts by collecting data from the protection layer and sending it to the control layer together with all the measurements, values, and information. After that, it waits for the control layer to provide feedback before compiling directives to be transmitted to the security systems.

To put it more clearly, the controller sends an alarm signal to all upstream devices that are part of the protection layer as well as the communication layer in the The power system functionalities of PACs have evolved and been incorporated into sophisticated devices known as IEDs (Intelligent Electronic Devices), which are distinguished by a hardware/software coupling design. In particular, these devices perform the safety and dependability required for power systems to operate properly, as well as the adaptive logic functions common to the Information Technology (IT) field [12,13, 14].

event that a failure in the power line is discovered. Subsequently, all protection features—aside from those that are active on the device nearest the fault—are promptly disabled. The latter fixes the issue and permits all upstream portions to be powered on after a predetermined interval. It is essential that communication at this stage be quick and easily identifiable. The IEC 61580 standard imposes a number of requirements on communication, including user authentication and authorization, redundancy, robustness, and reliability to maintain a high level of service quality, as well as the protection of measurement data from potential tampering or eavesdropping (cyber security) [8,9,10].
It complies with a number of requirements regarding safeguarding the measured data and the information shared from access by unauthorized operators; specifically, it protects the measurement data from potential manipulation or alteration and guarantees that the measured data will be available when needed. At this point, requests from users or the external grid are sent via local remote control and grid technical support. In specifics, the grid technical service can function to demand service to the SG, while the users can switch, reconfigure, and restore the SG with the help of the local remote control.

When we talk about control functions, we're talking about the administration of coordinated actions by local automation/control software (as in DER plants or electrical substations). The Control layer bears the responsibility of handling potential conflicts inside the system.

The Control layer, once the communication layer has collected and verified data and information, sends control commands to the lower-level devices at a set rate. In the event of an information conflict, the layer will employ SGRE-developed machine learning and AI algorithms to handle the situation. Fault time grading and longer fault clearing times are two decision-making criteria upon which they are based. the eleventh.

The network operator's control center's automation features, which entail a thorough system view. The PAC's system communication is divided into two levels by the automation functions: local and central. These two tiers oversee multiple data and synchronize activities to provide real-time information sharing from various electrical grid components, guaranteeing the power system's dependability and efficiency.

The graph in Figure 2 linked the advancements in technology and research in the development of PACs from the turn of the 20th century to the present. Because of the advancements in edge computing technologies, the next generation of PAC will see the evolution of virtualized, distributed, and wide area PAC.

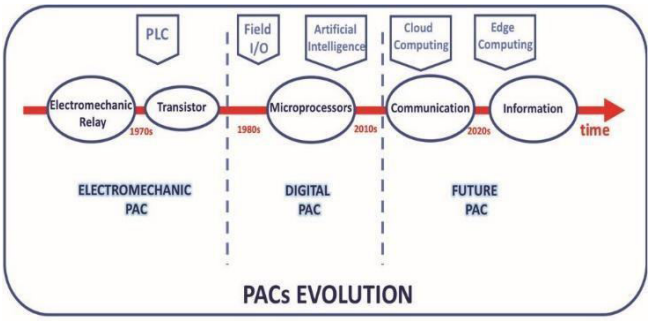

Fig.2. PACs evolution.

According to the international standard IEC 61850-5ED 2.0, autonomous electronic devices (IEDs) are "a device incorporating one or more processors with the capability to execute application functions, store data locally in a memory, and exchange data with other IEDs over a digital link" [15]. Various innovative devices have emerged as a result of developments in communication and power handling technology. These devices range from classic electro-mechanical to more current microprocessor-based devices.

The IEDs must meet the following criteria in order for the PAC functions to perform as best they can:

x dependability: in accordance with the anticipated specifications, is required to provide an adequate level of dependability, such as the success of the communication between the systems involved.

x Security: During all stages of system control and monitoring, the transmission of information and data must guarantee the confidentiality of the same. Data and information encryption will be necessary to avert cyber attacks that might jeopardize the proper delivery of the protection service.

x Appropriate Latency: Each application has to have a latency that is determined and guaranteed to meet its unique requirements. In order to prevent system damage and the loss of important data, the latter will need to take the "criticality" of the data into account before delivering it. For physical devices, for instance, implementation data must be sent at latency levels expected of "real time" applications.

x Redundancy: Redundancy of hardware or virtual services must be guaranteed in order to provide service continuity in the case of component failure or to restore service swiftly and automatically. x Interoperability: In order to support multi-vendor implementations and ensure communication between various system devices based on proprietary vendor hardware or software, communication technologies and heterogeneous protocols must cooperate. x Selectivity: Because automatic protection devices are selective, a hypothetical fault can be eliminated by installing a protection device right upstream of the fault. All other protection devices do not intervene because they are not "involved" in the fault, and as a result, a minimum number of customers are disconnected.

x Cost: In order to consistently ensure the same level of protection system reliability, low maintenance costs and an initial investment are required.

III. PAC SCHEMES: THE SOLUTION FOR THE PROTECTION ISSUES

Therefore, the switch from a traditional to a smarter power system necessitates the pertinent updating of current protection schemes and techniques in order to prevent them from becoming outdated in the future. It also calls for the development of new power protection techniques that can quickly respond to coordination needs that are typical of the Singapore Grid.

The automatic reconfiguration of the power network following disturbances is the goal of PAC techniques. The main advantages of a protection system in supergroups (SGs) can be summed up as follows: maximizing the use of the energy network, minimizing overall energy consumption, minimizing operation costs, improving service quality, and maximizing power supply reliability. Bidirectional energy flows also contribute to the improvement of interconnection system degrees. The AC SG makes advantage of both the suggested and existing protection plans. It requires extra thought to propose a protection strategy for DC systems because the traditional protection technique cannot be employed directly in DC SGs due to the absence of zero crossing and bidirectional power flow.

Protection plans are more important as preventative steps to ensure the power system operates well. In recent years, the systems have been constructed on common protection devices rather than custom goods in order to deliver PACs at the commercialization level. The standardization of software and hardware systems is responsible for this [16]. Figure 3 illustrates several SG protection plans.

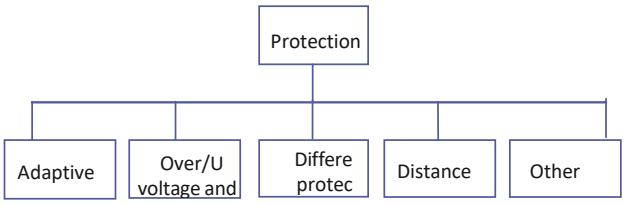

Fig.3 Main protection schemes.

Adaptive protection techniques: Mostly rely on the use of adaptive relays, which may also involve adjusting their settings and logic operations. The main concerns are the necessity of being aware of all potential SG configurations beforehand, the increased demand for

communication infrastructure, and the need to upgrade various pieces of protection equipment (fuses, etc.) in the current power system.

Differential protection techniques: These are built upon a differential strategy. This method is not widely used because of a number of problems, including those related to the communication infrastructure's dependability, load imbalances in systems, and excessive expenses.

Distance protection techniques:Impedance or admittance measurements are used by distance protection approaches to locate the problem and trigger the appropriate trip. The two main problems are the longer duration of tripping resulting from the downstream source infeed and the inaccuracy in the measured admittance caused by the fault resistance.

Overcurrent protection components: Techniques based on overcurrent protection components aim to enhance the functionality of traditional overcurrent safeguards. The main problem is to the requirement for a sophisticated and wide-ranging communication system, which if not operated properly might pose a threat to the entire overcurrent prevention system.

Voltage-Measurement-Based Protection Techniques: In DC SGs, Voltage-Measurement-Based Protection Techniques are commonly employed. Methods for providing the SGs with an adequate protective system are based on voltage monitoring. The main problems are with the variances in voltage drop that cause failures because the voltage gradient decreases, with the intricate computation, and with the challenging practical application when a lot of DGs are present in SGs.

Other Unique Methods and Strategies: Although not widely employed, wavelet transformation (WT), artificial intelligence (AI) techniques like particle swarm optimization (PSO), artificial neural networks (ANNs), data mining, etc., constitute the foundation of novel control schemes. In order to regulate the power input into the network and prevent overcurrent relay miscoordination via grid failures, ANNs are utilized to propose proportional integral (PI) control schemes [17].
In the SG context, multi-agent systems are especially adaptable because of their unique ability to adjust more quickly to changing system conditions. However, because DG units put a significant load on the system, the existence of DER reduces system dependability.

Therefore, a variety of approaches based on the Multi-Agent System (MAS) have been put forth in the literature to address the identify problem. A multistage strategy is demonstrated, for instance, in [18], where the first level establishes an efficient communication infrastructure in order to ensure that the relays are properly coordinated. The DGs are overseen by a single agent in each scattered region, with the second level managing the DGs. In [19], MAS is demonstrated as a helpful method that forms the foundation of a novel defect diagnostic method. In [20], a hybridization strategy based on MAS and artificial intelligence is given. Furthermore, the Intelligent Multi-Agent System (IMAS) is a novel method for pinpointing and isolating the SG issue.

IV. OPEN QUESTIONS, BARRIERS, AND DIFFICULTIES

The protection mechanisms in place in SG are designed to identify the single area of the grid that is impacted by faults and isolate it as quickly as possible. This prevents service outages, which might have a major negative influence on productivity and services. The development of SG PACs is hindered primarily by technological obstacles related to interoperability, scalability, coordination of protective devices, time synchronization, dependability, and security.

To provide proper connection between various SG and PAC system devices as well as external networks, communication technologies and heterogeneous protocols must function together. In addition to the connection between SG equipment and IEDs from various models or suppliers, it is necessary to guarantee the efficient and cost-effective delivery of electricity to the numerous SG clients. These devices, which are often very well-established commercially in the reference product market, have proprietary languages and protocols that need costly protocol converters and experimental advancements in order to be integrated with other SG devices.

A system is said to be scalable if it can accommodate an increase in workload, the inclusion of cutting-edge features, or the installation of new network access points in a flexible and dynamic manner. It should be mentioned that applying system scalability can result in both economic and technical communication consequences, such as network congestion and increased expansion costs due to the addition of hardware resources. Furthermore, managing and maintaining more resources is a function of having more units in the system. Therefore, it is obvious that device makers' participation in PACs trials would be crucial to overcoming the interoperability and scalability obstacles.

Another issue is the new distributed power system's complexity in comparison to the conventional electrical system, which makes it difficult to coordinate the PACs [2]. Since distributed energy generating systems (RES) cannot be programmed, any excess energy must be managed locally in order to minimize or eliminate possible faults and redistribute it to nearby locations. These procedures have a significant impact on any system's dependability and security. Therefore, it is essential to create well-coordinated strategies for each PAC in the SG in this creative energy setting. The quality of power supply may be improved by quickly resolving faults through the application of strategies that consider the selectivity, sensitivity, and proper protective function of the PACs. In fact, adaptive protection scheme-based solutions have recently been proposed to address the issue of PAC coordination. These solutions involve the use of switches and disconnectors that have the

ability to automatically reconfigure the network in the event of a failure, minimizing the amount of isolated sections, through remote communication and synchronization functions.

Since the configuration of the power system might change quickly, energy dispatching and protection coordination concerns should generally be controlled dynamically. Real-time monitoring data and information collection is essential for observing and managing SG activities. Indeed, in recent years, a large number of synchro phasors have been manufactured in an effort to increase the power grid's observability. The high-precision time synchronization makes it possible to compare measured data from several SG-affiliated systems.

This situation also has serious issues with reliability. Every possible grid failure scenario must be discovered by the PACs as soon as possible because the reliability of the SG is what ultimately decides the continuation of the power supply. With the help of well-designed controls, these devices should be able to automatically detect, measure, and change protection settings in response to different types of blackouts, as well as share this information with each other and the grid's breakers. Traditional protection devices keep their settings constant when a failure happens during real-time operation. The IEC61850 smart sensor improves the SG's dependability by decreasing the activation time of the grid breakers compared to the previous generation of protection devices [14].

A. Description of ENEA Laboratory Facilities

In the context of project 2.1 "Energy Systems' cybersecurity" (Piano Triennale Della Ricerca di Sistema 2022-2024), an advanced PAC is detailed in this section. It is being developed at the ENEA SGRE laboratory. The SGRE experimental nano grid incorporates the SGRE PAC system, which is composed of three levels: physical, communication, and logical. This infrastructure is a versatile testing ground for smart macro-, micro-, and nano-grids and associated technologies, situated at the C.R. Portici of ENEA. In order to meet the demands of future energy scenarios, it is possible to experimentally mimic models and methodologies for management and protection, as well as advanced devices and grid topological solutions.

Lay down the foundation for the grid. By integrating the nano grid's integrated electronic devices (IEDs) and meters with the HIL-simulated grids, it is possible to conduct real-time simulations using a software controller and HIL to study the conditions of the extended power system. These controllers include AI-based modules that can be used to conduct experimental research on state-of-the-art energy systems and enabling technologies. The logical architecture of the nano grid is shown in Figure 4.

However, management problems may arise and contradicting instructions may be sent to the nano grid's physical components (for example, a storage system may get instructions to "charge" from the HIL controller and "discharge" from the "nano grid control system"). Without a sophisticated protective mechanism, the component—like the load in the preceding example—may sustain significant harm.

Based on these tenets, the power lab control and management system is made to safeguard network components from both electrical problems (such overvoltage) and "management" errors. In further detail, high performance switching technologies enable Solid-State electronic protection, which makes up the physical layer. The communication layer links each protection device to the logical layer.

With its manager and coordinator functions, the latter layer makes up the PAC core. Its response is especially essential when there are conflicting commands transferred to a particular component. Under these circumstances, the protective layer sends an error signal to the "nano grid control system" and stops the operation (for example, by halting both storage charging and discharging processes). Subsequently, the priority controller of the nano grid control system initiates a "emergency procedure" with the aim of promptly restoring the functioning.

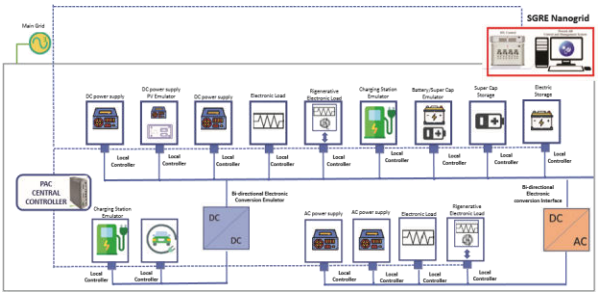

Fig.4 ENEA PAC Nano grid

VI. CONCLUSION

The SG gains several benefits from the automation, protection, and management of the feeders, distribution networks, and substations. Specific advantages include lower power costs, more beneficial network implementation, longer component lifespans, energy savings, and even the ability to postpone network upgrades. In terms of safety, peak loads may be managed to prevent significant grid damage because to SG control and automation. Utilities are able to lower maintenance costs by managing and controlling power plants from remote locations, particularly in the case of unexpected breakdowns.

Other functionalities in modular logic, like significant function re-allocation flexibility, significant cost-efficiency redundancy, new levels of scalability, and virtualization of the infrastructure with the goal of decoupling PACs software from their dedicated hardware solution, will be implemented soon in order to further boost the commercialization of the PACs.

ACKNOWLEDGMENT

Under the terms of the "Accordo di Programma 2022-2024 between ENEA and Ministry of the Environment and Energetic Safety - Project 2.1," this study was supported by the Research Fund for the Italian Electrical System.

REFERENCES

[1] O. Majeed Butt, M. Zulqarnain, T. Majeed Butt, "Recent advancement in smart grid technology: Future prospects in the electrical power network," Ain Shams Engineering Journal vol. 12, Issue 1, 2021, pp. 687-695,ISSN20904479, https://doi.org/10.1016/j.asej.2020.05.004.

[2] S. Ali, "Smart Grids: Opportunities, Developments, and Trends" Springer, New York, US, 2013.

[3] B. G. Costa, J. S. Damiani, G. Marchesan, A. P. Morais, A. S. Bretas, G. Cardoso Jr., "A multi-agent approach to distribution system fault section estimation in smart grid environment," Electric Power Systems Research, vol. 204, 2022, 107658, ISSN 0378-7796, https://doi.org/10.1016/j.epsr.2021.107658.

[4] M. Escobar, J.J. M. Matamoros, O.; T. Padilla, R.; L.Reyes, I.; Quintana Espinosa, H. A "Comprehensive Review on Smart Grids: Challenges and Opportunities". Sensors vol. 21, no. 21: 6978, 2021. https:// doi.org/10.3390/s21216978.

[5] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, N. Ghadimi, "A comprehensive review of cyberattacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future", in Electric Power Systems Research, vol. 215,PartA,2023, https://doi.org/10.1016/j.epsr.2022.108975..

[6] N. Kabbara, M.O.N. Belaid, M. Gibescu, L. R. Camargo, J. Cantenot, T. Coste, V. Audebert, H. Morais, "Software Defined Protection, Automation, and Control in Power Systems" Encyclopedia. Available online:https://encyclopedia.pub/entry/39036 (accessed on 14 April 2023).

[7] A. Wadood, S. G. Farkoush, T. Khurshaid, C. H. Kim, J. Yu, Z.W. Geem, S.-B. Rhee, "An Optimized Protection Coordination Scheme for the Optimal Coordination of Overcurrent Relays Using a Nature-Inspired Root Tree Algorithm" *Open Access Applied Science.*,vol.*8*,no.9:1664,2018. https://doi.org/10.3390/app8091664.

[8] S. Ahmed, T. M. Gondal, M. Adil, S. A. Malik, R. Qureshi, "A Survey on Communication Technologies in Smart Grid" IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia), Bangkok,Thailand,pp.7-12,2019,doi: 10.1109/GTDAsia.2019.8715993.

[9] L. Wang, Y. Qin, Z. Tang, P. Zhang "Software-Defined Microgrid Control: The Genesis of Decoupled CyberPhysical Microgrids" IEEE Open Access J. Power Energy vol. 7, pp. 173–182, 2020 10.1109/OAJPE.2020.2997665.

[10] Abrahamsen, F. Ege, Y. Ai, M. Cheffena, "Communication Technologies for Smart Grid: A Comprehensive Survey" Sensors vol. 21, no. 23:8087. 2021. https://doi.org/10.3390/s21238087.

[11] A. C. Aleixo, J. Cabac¸a, P. Neves, R. D. Jorge, R. D. Paulo, and A. Rodrigues, "Smart grid protection and automation enabled by IEC 61850 communications over 5g networks," 2019.

[12] N. Kabbara, M.O. Nait Belaid, M. Gibescu, L.R. Camargo, J. Cantenot, T. Coste, V. Audebert, H. Morais, "Towards Software-Defined Protection, Automation and Control in Power Systems: Concepts, State of the Art, and Future Challenges", Energies, vol. 15, 9362, 2022.

[13] P. Khajuria, D. Samara-Rubio, "Power of Infrastructure Modernization"; Intel Corporation 2021.

[14] Z.Q. Bo, X.N. Lin, Q.P. Wang, Y.H. Yi, F.Q. Zhou, "Developments of power system protection and control" Springer Open Access Protection Control of Modern Power Systems", vol.1, no. 7, 2016..https://doi.org/10.1186/s41601-016-0012-2.

[15] IEC 61850-5; "Communication Networks and Systems for Power Utility Automation—Part 5: Communication Requirements for Functions and Device Models" International Electrotechnical Commission, Geneva, Switzerland, 2013.

[16] A. Kole "A review on advanced protection, automation, control functions and future control for thermal power plant", International Journal of Automation and Control vol.8, no.3, pp. 211-241, 2014. 10.1504/IJAAC.2014.064161

[17] M. I. Mosaad, F. Salem, "LFC based adaptive PID controller using ANN and ANFIS techniques" Journal of Electrical Systems and Information Technology, vol. 1, pp. 212-222, 2014 https://doi.org/10.1016/j.jesit.2014.12.004

[18] B. Fani, E. Abbaspour, A. Karami-Horestani, "A faultclearing algorithm supporting the MAS-based protection schemes", International Journal of Electrical Power & Energy Systems, vol. 103, pp. 257-266,2018ISSN01420615, https://doi.org/10.1016/j.ijepes.2018.06.001..

[19] E. Abbaspour, F. Bahador, E. Heydarian-Forushani, "A bilevel multi agent-based protection scheme for distribution networks with distributed generation" International Journal of Electrical Power & Energy SystemsVol.112,pp.209220,2019. 10.1016/j.ijepes.2019.05.001.

[20] L. Lin, C. Jiantian, L. Guan, Z. Dong, H. Chen, M. Xiao, "Fault Location and Isolation for Distribution Network with DGs Based on Intelligent Multi-Agent System", Energy Procedia, vol. 145, pp. 234-239, 2018 https://doi.org/10.1016/j.egypro.2018.04.041.

[21] R. Dashti, M. Daisy, H. Mirshekali, H. R. Shaker, M. H. Aliabadi, "A survey of fault prediction and location methods in electrical energy distribution networks, Measurement", vol. 184, 109947, ISSN 0263-2241,2021 https://doi.org/10.1016/j.measurement.2021.109947.