IJEMME

INTERNATIONAL JOURNAL of ELECTRONICS, MECHANICAL and MECHATRONICS ENGINEERING

Year: **2019** Volume **9** Number **2**

VISUAL DESIGN & ACADEMIC STUDIES COORDINATION OFFICE

Nabi SARIBAŞ - Gamze AYDIN - Elif HAMAMCI - Seçil DURNA

PRINTED BY

Renk Matbaası Basım ve Ambalaj San. Tic. A.Ş.
Ziya Gökalp Mah. Süleyman Demirel Bulvarı İş Modern D Blok No:27D D:D8 34104 Başakşehir / İstanbul

ISSN: 2146-0604

International Journal of Electronics, Mechanical and Mechatronics Engineering (IJEMME) is peer-reviewed journal which provides a platform for publication of original scientific research and applied practice studies. Positioned as a vehicle for academics and practitioners to share field research, the journal aims to appeal to both researchers and academicians.

Internationally indexed by EBSCO and DOAJ

CONTENTS

From the Editor

International Journal of Electronics, Mechanical and Mechatronics Engineering (IJEMME), is an international multi-disciplinary journal dedicated to disseminate original, high-quality analytical and experimental research articles on Robotics, Mechanics, Electronics, Telecommunications, Control Systems, System Engineering, Biomedical and Renewable Energy Technologies. Contributions are expected to have relevance to an industry, an industrial process, or a device. Subject areas could be as narrow as a specific phenomenon or a device or as broad as a system.

The manuscripts to be published are selected after a peer review process carried out by our board of experts and scientists. Our aim is to establish a publication which will be abstracted and indexed in the Engineering Index (EI) and Science Citation Index (SCI) in the near future. The journal has a short processing period to encourage young scientists.

Prof. Dr. Hasan HEPERKAN
Editor

INTERNATIONAL JOURNAL OF ELECTRONICS, MECHANICAL AND MECHATRONICS ENGINEERING
Vol.9 Num.2 - 2019 (1657-1667)

Cyber Security Algorithm Development For Microgrid And Smart Grid Systems

Ahmet DURMUŞ [1] , Mehmet Emin TACER [2]

Abstract: Smart grids are advanced grids that use intelligent ways to distribute power and manage it with high level of technical and physical safety in its different components. In these types of grids, the power station and the consumer are both considered as effective power supplier. They can generate, buy, and sell power as of kWh to the other. Thus, financial channels are concerned, so that the safety and privacy for each of them are important. This paper will be concerned on developing a cybersecurity algorithm used to apply a flexible way for determining to either isolate the network, reauthorize access, or successfully accept the access for financial transactions made by normal users.

Keywords: *Renewable Energy, Smart Grids, Cyber Security.*

Introduction

Smart grid is a type of grid that applies improvement of normal grids in a way of combination between computer-based systems of information technologies and traditional electrical grid. This type of grids uses two-way communication to enhance the network behavior in generation, consumption, reliability, stability and cost effect between the generation station and the consumer demand with momently updated information. Generally smart grid is contained of other small smart partitions - called microgrids - each of them should be in connection with the other simultaneously. Smart grid has some advantages in energy savings through consumption reduction, fraud detection and technical losses, reduced balancing cost, peak reduction, and reduction of carbon emissions (Hamilton & Miller , 2010). Although it consists of some Intelligent Appliances, Smart Power Meters and AMI's, Smart Substations, Super Conducting Cables, Integrated communications, and Phasor Measurement Units (PMU) [2] [3] [4].

Despite of the advantages that smart grids have, and the role of user control which appear between of smart components, a technical awareness and countermeasures should be taken to satisfy the stable control of the network. In other words; the user role is made over smart appliances turning them ON or OFF, or by

[1] *Dept. of Electrical and Electronics Engineering, Istanbul Aydin University, Istanbul, Turkey, ah.durmus.93@gmail.com*
[2] *Dept. of Electrical and Electronics Engineering, Istanbul Aydin University, Istanbul, Turkey, emintacer@aydin.edu.tr*

generating power, so an import and export processes of KWh's are made in a channel between user and the grid. This means financial transactions are made. So that, to protect the stability of processes in the grid, and by knowing that the normal user also could be an attacker at the same time, cyber security issues are shown up for concern. In this paper, an algorithm [which is a procedure that could be used for data processing, automated reasoning and calculations; using step by step process] is developed for cybersecurity protection in smart grid systems. It is going to be discussed after taking a review of cyber security in normal grids and other works related with.

Cyber Protection of Normal Power Grid

Cyber protection requires a widely used component protection which is the SCADA systems. This because main central network keeps collecting data from other widely distributed substations using controlled systems. Thus, SCADA systems are considered as the nerve of that operation. The collected data are used by the energy management system EMS in normal grids, and this usage could be considered as a weak point when a communication down fault or delay occurs, due to the trim in control process which means a possible power outage. (Ten, Manimaran, & Liu, JULY 2010)

A SCADA Security Protection Framework called RAIM Framework introduced and it is contained from 4 steps mainly: real time monitoring, anomaly detection, impact analysis, and mitigation strategy. A simplified methodology for impact analysis of a computer network systems, called Attack Tree Modeling used for identifying the adversary objectives. It is a graph that shows the connection of more than one attack of each node in the system as shown in figure 1.

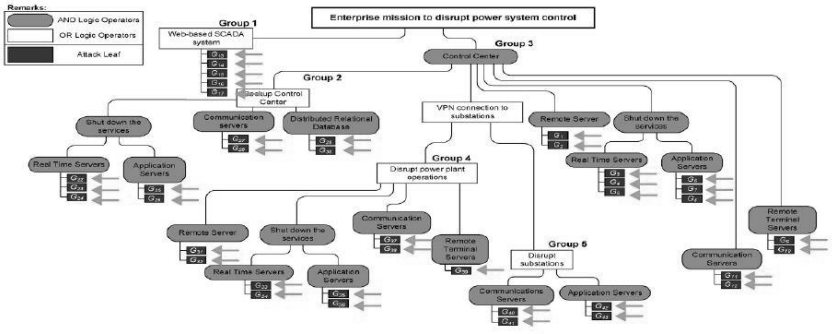


Figure 1: Normal network connection

A likelihood measure is presented to show the vulnerability level starting from 0 to 1, which means an index of vulnerability between most invulnerable to the most vulnerable one and called Vulnerability index which is determined based on evidence of intrusion attempts, existing counter measurement, and password policy enforcement. Hypothesis in this modeling presents:

- Condition 1: The system is clean and free of any intrusion attempt that is concluded from the electronic evidence in the system.
- Condition 2: 1 or more of countermeasures are implemented to protect against attack leaf.
- Condition 3: 1 or more password policies are enforced corresponding to each attack leaf.

Condition 1 is met when there is no evidence of system intrusion suggestion. Condition 2 is met such as a web server is installed which contains a firewall to prevent attacks. Condition 3 once password is implemented; taking in consideration that poor passwords result unauthorized access. (Ten, Manimaran, & Liu, JULY 2010)

After the cyber security principles in normal power grid introduced, and because of all advantages that smart grid has over the normal one (Hamilton & Miller , 2010) ; a need for examining the cyber security in smart grid systems appears. Especially that the coming future will depend over smart grid systems completely, after transferring to it from the normal grid being completed.

Cyber Protection of Smart Grid Systems

Some papers that describe the cyber protection of smart grid systems like Stefanov et al [6]; explaining that the cyber-attack could be discovered by tracking either voltage leakage or step change in frequency and another one like Diovu et al [7] which is developing a firewall scheme against DDoS attacks which mainly affect the AMI, in addition to Liu et al [8] which introduce a scheme for intrusion detection mechanism against false data injection attack over AMI; especially by exploiting the CPN [Colored Petri Nets which is a graphical oriented language for design, specification, simulation and verification of systems] of smart meters. Each of them has its own way for decrement the effect of cyber-attack over AMI units, but the common point between them is that assuming the attacker may not be one of the normal users. This point is the main difference between previous works and what is described in this paper here. This paper is proposing that control should be applied as nearest as possible to the user himself. So that more accurate security could be implemented for all other users of the smart network.

Types of cyber-attacks which could be done over the system could be divided for 3 groups, the first one concerned in DDoS attacks, second one “Man in the middle” technique, the final one is metering data falsification. DDoS attack depends on flowing and pumping extremely high traffic to the server which contains sensitive data in order to take the control over the server under cover of this traffic. The second one (man in the middle) is a technique used to track sent and received data; it may not affect them but can easily have a copy of them and edit these data such as measurements of consumed and generated power which are sent between the smart meter and the AMI unit. This type can change those values or even change transactions done in between. Finally, for metering data falsification which may be considered as cyber and physical attack at same time; for physical one it is simply changing the reading and writing values over meters. For cyber one it appears as changing in recorded values when being transmitted (such as man in the middle technique described previously). This could easily be detected and fixed by re-read of original data sent from other small fixed sensors which are spread over all parts of smart grid network and appliances. [7]

Proposed Smart Grid Cybersecurity

Proposed algorithm is highly flexible, and code could easily be injected into the framework of the microgrid systems with zero cost and can detect the vulnerability degree over the system; then to either isolate, reauthorize or to successfully access for the system as will be shown later here. Now, for proposed hypothesis in AMI modeling contains five conditions which could be presented as :

Table 1: Proposed hypothesis in AMI modeling

Proposed conditions	Occurs when
Condition 1	The system is clean and free of any intrusion attempt that is concluded from the electronic evidence in the system.
Condition 2	1 or more of countermeasures are implemented to protect against attack leaf in any of **one-way of communication way**.
Condition 3	1 or more of countermeasures are implemented to protect against attack leaf in **two way of communication at the same time**.
Condition 4	1 or more password policies are enforced corresponding to each attack leaf in any of **one-way of communication way**.
Condition 5	1 or more password policies are enforced corresponding to each attack leaf in **two way of communication at the same time.**

While the power is converted between HP to LP in order to accomplish the loads needs, small power stations are needed for feeding process [2]. In same principle the need for smaller partitions in smart grid systems appear, and those are called microgrids. These microgrids normally designed to derive the required power to loads. So that; it has a limit of power transmitted and received. While designing is processed for these microgrids; steady state conditions are also considered, and it differs according to load types. These steady state conditions considered as the norm one of the system, which represent the clear condition of the system; which is also named as condition 1 as shown in Table 1.

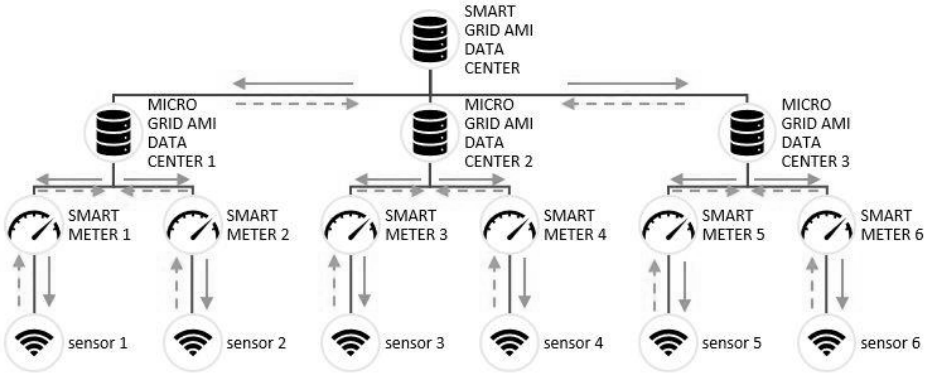


Figure 2: Proposed connection between AMI unites and Smart meters

Figure 2 shows concerned parts in this study of smart grid systems. Each part uses normally two way of communication with other components. Sensors are fastened over appliance itself and gives information

about its consumed or generated power to the smart meter as analog signals which convert it in its turn to digital one and send it to the AMI data center to store it in the memory. As known for digital systems, there is a firewall for each of them in which it can protect its digital data. As example in smart homes, digital devices are connected to sensors of microwave or freezer or oven, …. etc; those digital devices are used to monitor the system status and are maybe normally working with android system; which is also has its own firewall for protecting the digital data. Also; for AMI data centers, it consists of servers to store the data, so that firewall is also exists.

Now, while considering the firewall of the system, between data center and appliance; if data are sent from server to the consumer side; data is transmitted from server (which may has a firewall) to the appliance (which may also has a firewall); this represent a one way communication with one countermeasure applied as a firewall; then it gives us condition 2. If data are transmitted from server to the consumer side, and another data are also delivered to server from the consumer side at the same time; this give us 2 way communication at the same time; thus condition 3 is satisfied.

In same procedure and principle if password policy is applied for one way communication between server and consumer side then condition 4 is satisfied. If it is applied on both way of communication, then condition 5 is also satisfied. Knowing that instead of password policies, human related prints could be used to access the system instead of passwords, such as fingerprints, or eye scan or both of them at the same time.

The system could be attacked once it is prepared for work but not yet connected to any loads, in other words; it is in the stage of testing it before being completely connected to work in full load to the system; in this stage bugs could be inserted from a hacker in the server to steal consumer billing information or changing the read data in future. In this case condition 1 is satisfied only, because there is no countermeasure or passwords are applied to the system yet; due to it is in the stage before full connection to the load. After that if it is connected, another conditions of 2,3,4, and 5 could be considered; because the system is fully connected now, so that different conditions could be counted in after.

χ will indicate the vulnerability level over all the system or in other word the system condition whether it is vulnerable or not. It will be considered for the smallest leaf in the system between sensor and smart meter, or smart meter and microgrid data center, or microgrid data center and smart grid data center, etc… After that to calculate the system vulnerability completely; all of these χ's will be multiplied together as it will be shown later.

- If [condition 1 ∩ condition 2 ∩ condition 3 ∩ condition 4 ∩ condition 5] are satisfied will give us $\chi = 0.2$
  Here all conditions are satisfied, therefore there is no evidence that the system is subject to malicious attempts. i.e: password and countermeasures are implemented for one way and two way of communications and the system is clean from any previous intrusions.

- If any 2 of 5 conditions are satisfied, then $\chi = 2*1/5 = 0.4$

1: for condition 1, 2: for condition 2, 3: for condition 3, 4: for condition 4, 5: for condition 5. And by eliminating repeated conditions:

~~1,1~~	1,2	1,3	1,4	1,5
~~2,1~~	~~2,2~~	2,3	2,4	2,5
~~3,1~~	~~3,2~~	~~3,3~~	3,4	3,5
~~4,1~~	~~4,2~~	~~4,3~~	~~4,4~~	4,5
~~5,1~~	~~5,2~~	~~5,3~~	~~5,4~~	~~5,5~~

Thus □= 10 / 25 = 0.4
This gives indicate that the system is vulnerable by 40%.

In same principle:

- If any 3 of 5 conditions are satisfied, then: □= 0.6
- If any 4 of 5 conditions are satisfied, then □= 0.8.
- If condition 1 or condition 2 or condition 3 or condition 4 or condition 5 or none of them is met, then □ = 1. This indicates that the system is highly vulnerable.

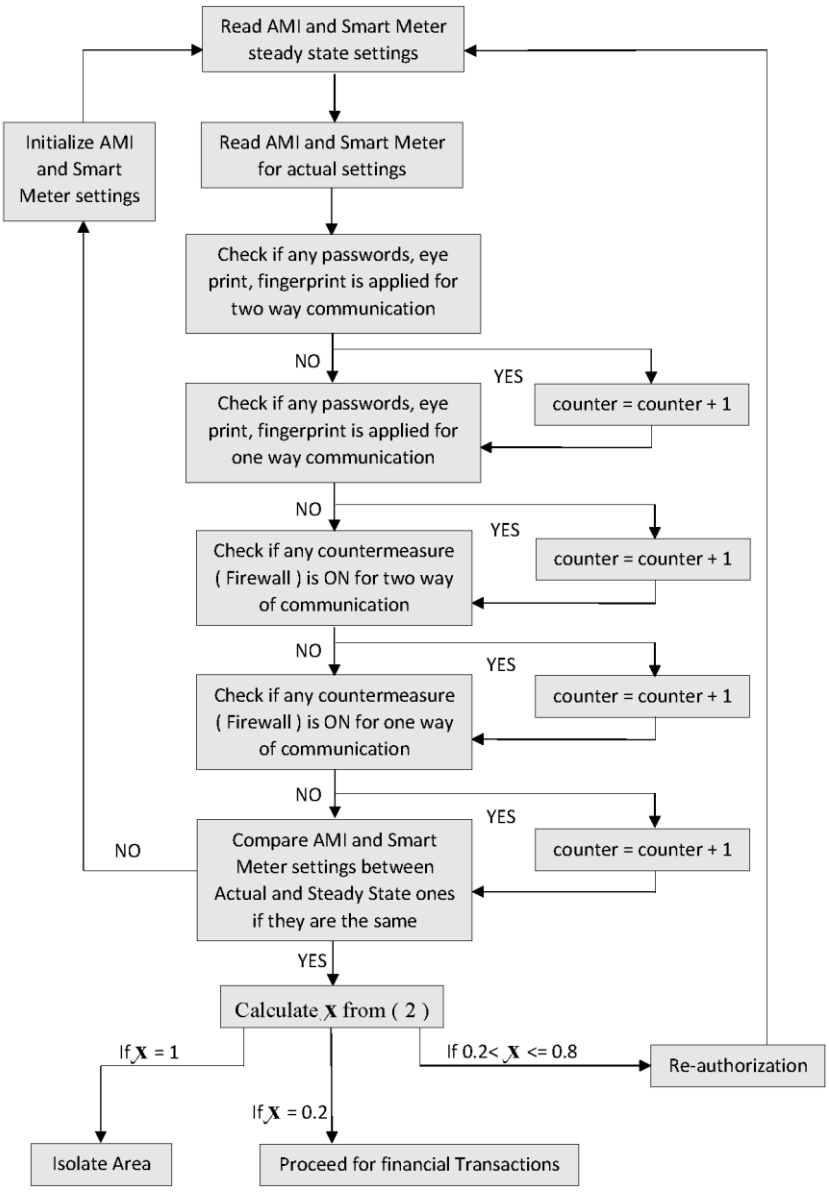
To know the overall system attack indices, and after calculating □ for every leaf (□$_i$), the overall will be:

$$\text{counter} = \text{counter} + 1 \text{ , counter: \# of countermeasures or password applied} \quad (1)$$

$$\chi_i = \begin{cases} \text{counter} * 0.2 \text{ , } 2 <= \text{counter} <= 4 \\ 1 \text{ , counter} <= 1 \\ 0.2 \text{ , counter} = 5 \end{cases} \quad (2)$$

$$\chi_{system} = \prod \chi_i \text{ , } i = 1,2,3,4, \ldots. \quad (3)$$

Proposed Smart Grid Cybersecurity Algorithm



Simulation of Proposed Smart Grid Cybersecurity Consumer Algorithm

The simulation process is tested for small leaves or microgrids only. So that; equation (1) and (2) are basically considered. Equation (3) could be easily inserted later to calculate the overall system vulnerability indices.

To prove that proposed algorithm here can be applied in programmable way, which should be implemented in AMI unites programming, 3 stage codes had been simulated. Knowing that the program is basically used

to know the internal process inside AMI unites and smart meters for how it could be applied and to display this in easier way; a display function had been used to show the internal status of code running.

First of all, the code started by clearing any previous value and initialize the simulation program for starting. After that, AMI control unites are directed to read the steady state conditions of its internal settings from internal physical memory and also for smart meters. Then actual readings of those settings are also gathered in order to compare the match between steady state and real readings.

Then the program will send a signal code to the framework of server or system to test if any countermeasure or password policy is applied weather for 1 or 2 way of communication. If any of them is detected, a counter will start increasing; which aims to give us the total number of satisfied conditions in our microgrid system. Then depending on this value, the vulnerability indices is calculated in order to either isolate the system, require a reauthentication again, or to successfully access the financial data.

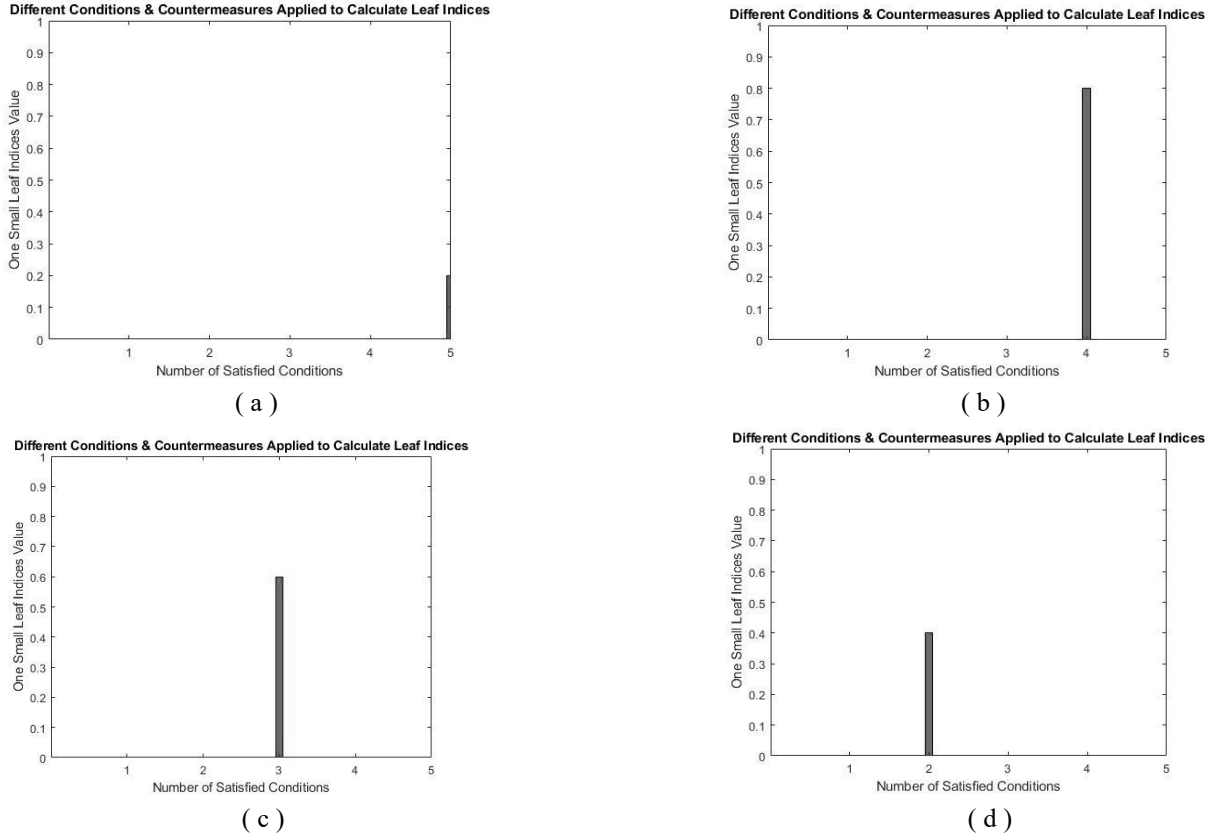


Figure 3: (a), (b), (c), (d) results for 5,4,3,2 conditions satisfied respectively

If number of conditions satisfied are either 2, 3, or 4; then a reauthorization for accessing the system will be required as shown below. This message could be transferred to the consumer screen to make attention and control over process.

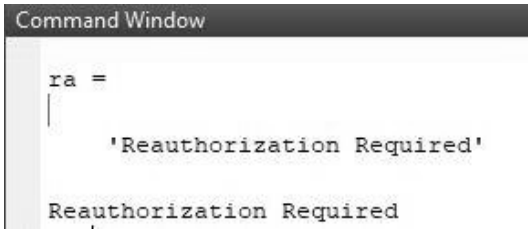


Figure 4: Appearing Message if 2,3 or 4 Conditions Satisfied

For 1 condition satisfied and detected by the program the result will be as in figure 5.

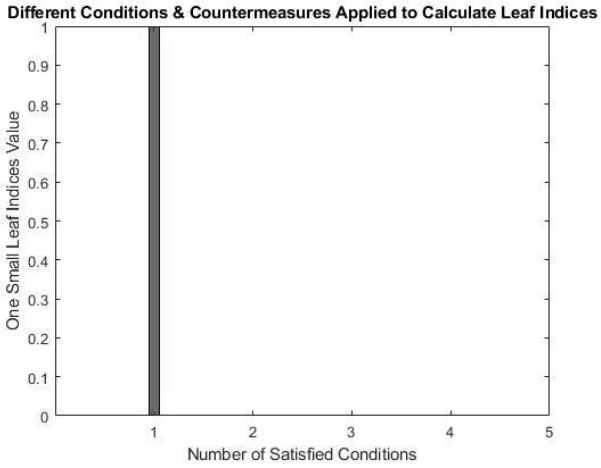


Figure 5: 1 Condition Satisfied

If number of conditions satisfied is 1; then an isolation of the area is required because the system is highly vulnerable and figure 6 shows the related message.

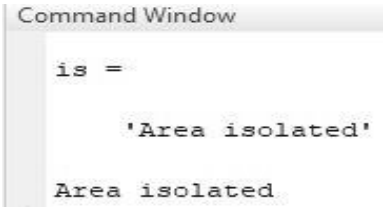


Figure 6: Appearing Message if 1 Condition Satisfied

Another code is applied for testing the microgrid if smart meter and AMI settings are changed or not. If not, the code will work correctly, if yes a message will appear in order to reload the steady state conditions for both and it is automatically loaded internally as shown in figure 7.

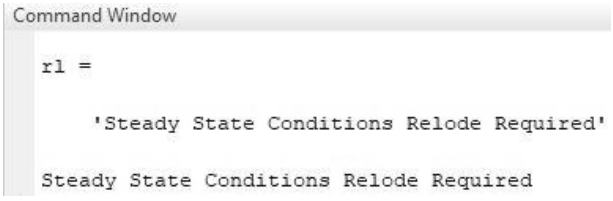


Figure 7: Appearing Message if bugs are inserted or settings between SS and actual readings are not in match

Results show that proposed algorithm and code are highly flexible and could easily be injected into the framework of the micro systems with zero cost and can detect the vulnerability degree over the system; then to either isolate, reauthorize or to successfully access for the system.

Conclusion

As the results show that, implementing defenses methods starting from the consumer side will ensure a higher level of security. On the other hand, two way of communication in smart meters provide the advantage of high response to isolate the risky area, if there is no chance to maintain it remotely. This isolation could be continued until maintenance team arrive to the concerned area. Then they can start by initializing setting of hardware such as AMI unites and smart meters and then load the latest safe information into it. That information is backed up instantly and could be separated than specific attack starting time.

Table 2: Comparison between previous work [7] and proposed algorithm.

Comparison Topic	Previous work	Proposed Work
Type of Grid	Smart Grid	Smart Grid
Assumed level of attacker to access information	Skilled attacker	Innocent attacker, or skilled one
Concerned attack types	DDoS	Not specific for only one, it is general
Cost effect	May need upgrading server in which data are stored. (for framework upgrade)	No need for any changes, only inserting the algorithm or the code in a programmable way for any framework generation will take direct effect.

Future Work

This paper could be used in developing other security ways, such as the use of firewalls, control the access for the network, and limitation of accessible data, to prevent cyber-attack over smart grid systems. Also it could be used to develop the proposed algorithm in paper here in order to enhance the security of the smart systems or to propose another algorithm which could be used on the both sides of communication channel between AMI's unites or between several microgrid data centers.

References

[1] B. A. Hamilton And J. Miller , "Smart Grid Implementation Strategy," In Understanding The Benefits Of The Smart Grid , National Energy Technology Laboratory, 2010, Pp. 1-33.

[2] P. C. Jain, "Trends In Smart Power Grid Communication And Networking," In International Conference On Signal Processing And Communication (ICSC), Noida, India, 2015, Pp 374-379.

[3] P. Umang And M. Mitul, "A Review On Smart Meter System," International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering, Vol. 3, No. 12, Pp. 70-73, December 2015.

[4] Q. Sun, H. Li, Z. Ma, C. Wang, J. Campillo, Q. Zhang, F. Wallin And J. Guo, "A Comprehensive Review Of Smart Energy Meters In Intelligent Energy Networks," IEEE Internet Of Things Journal, Vol. 3, No. 4, Pp. 464-479, August 2016.

[5] C. W. Ten, G. Manimaran And C. C. Liu, "Cybersecurity For Critical Infrastructures: Attack And Defense Modeling," IEEE Transactions On Systems, Man, And Cybernetics—Part A: Systems And Humans, Vol. 40, No. No. 4, Pp. 853-865, July 2010.

[6] A. Stefanov And C. C. Liu, "Cyber-Power System Security In Smart Grid Environment," Science Foundation Ireland (SFI), Dublin, 2011.

[7] R. Diovu And J. Agee, "A Cloud-Based Openflow Firewall For Mitigation Against Ddos Attacks In Smart Gridami Networks.," In 2017 IEEE Pes Powerafrica, Accra, Ghana, 27-30 June 2017.

[8] X. Liu, P. Zhu, Y. Zhang And K. Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack In Advanced Metering Infrastructure," IEEE Transactions On Smart Grid, Vol. 6, No. 5, Pp. 2435-2443, September 2015.

INTERNATIONAL JOURNAL OF ELECTRONICS, MECHANICAL AND MECHATRONICS ENGINEERING
Vol.9 Num.2 - 2019 (1669-1676)

Autonomous Photovoltaic Solar Cell Using Tracking System Design and Implementation

Metin BİLGİN*[1], Kübra ÇELEBİ[2]

Abstract: Nowadays with the rapidly evolving technology, the need for sustainable and clean energy has become evident due to the inadequacy of existing resources or the damage caused by these resources. It is aimed by all countries that the minimum effect of these resources on the environment and maximum efficiency. This situation makes renewable energy sources valuable and this study, a solar tracking system was designed and prototyped in servo motor control with the help of photoresistors which will serve as a sensor to increase the energy capacities produced by solar panels.

Keywords: *Photoresistor, Solar Energy, Renewable resources, Photovoltaic*

1. Introduction

These days and in the past, this process has resulted in global warming, climate changes and acid rain with decreasing resources and harmful effects of fossil fuels such as petroleum, coal and natural gas. Renewable energy resources' importance is not ignored anymore. On the other hand, the energy requirement in the World could be maximum because of the increasing population and technology. The countries have started to choose reusable energy resources and their aim is increasing their efficiency.

The largest source for heating the houses and obtaining electricity, the product of thermal power plants, is coal. When latent fossil fuels are burned, harmful gases such as carbon dioxide and carbon monoxide are released into the atmosphere. After years, societies cause respiratory diseases and global warming in the World.

Solar energy is one of the energy production options without any adverse effects and can be renewed at the same time. Photovoltaic batteries are semiconducting materials used to convert solar radiation directly onto the surface of the earth. They are a kind of battery that stores solar energy.

1Bursa Uludağ University-Computer Engineering, metinbilgin@uludag.edu.tr
2Bursa Technic University-Mechatronic Engineering, kbrcelebi@gmail.com

The average output of a standard photovoltaic battery is the amount of energy consumed by devices that will consume less power. Solar panels are required in large dimensions, which combine photovoltaic batteries for devices that will draw much more power. Increasing the size has always caused problems in practice. Rather than increasing the size of the panel, it is reasonable to maximize the efficiency of each photovoltaic cell.

The efficiency of solar cells depends on two main factors;

1) The intensity of radiation on the cell from the source
2) The cell efficiency

One of the most important factors limiting efficiency is the materials from which photovoltaic batteries are produced. These materials limit the performance of the photovoltaic cell. However, changing the ratio of the amount of light falling on the photovoltaic cell from the source is more convenient and cheaper. The first thing to do to increase the light intensity is to always keep the panel surface clean and controlled. If the panel is always clean, the energy obtained is maximum. It is aimed to provide an approach that requires little maintenance and very little money to clean the solar panel systems that do not require commercial maintenance using minimum water and power.

The movement of the sun changes depending on the season and day length. Depending on these two parameters, the maximum number of photons falling on the solar panel surface during the day cannot be expected, and therefore algorithms have been developed by these parameters.

Kelly and Gibson's work has increased the efficiency of the solar panel in cloudy weather as a result of the solar tracking system. By improving this work after their first work, Kelly and Gibson provided adaptation of the system to various environmental conditions and seasons. In other words, after the feasibility of the work done, productivity increased [1].

In those same years, Chong and Wong tried to increase sensitivity to follow the collector, which acts as a sensor to track the sun [2].

Subsequently, Abdallah and Badran studied the efficiency of the solar tracking system concerning the use of stationary systems in their study [3].

With Abdallah and Nijmeh PLC control, they designed a solar tracking system that can move two axes. For control purposes, they measured the position of the sun four times during the day and estimated the speed of the sun as the result of the measurement. My site is rotated at the estimated speed. The energy obtained from the moving system was compared with the energy generated from the fixed solar panel located at an inclination angle of 32 ° in the south direction. As a result, it was observed that the moving solar panel produced about 41% more energy than the fixed solar panel. However, it has been understood that the energy they spend to pursue has passed 3% of the energy they produce [4].

Huang and Sun have increased the solar panel output power by about 23% with the reflector with low condensation rate, which they place in the uniaxial three positions (morning, noon, afternoon) solar tracking system [5].

With PLC control Abu-Khader worked on a solar tracking system that can move two axes. During the day the sun has rotated four times according to its position. The yield according to the fixed system ranges from 30 to 45%. The energy expenditure for the follow-up system is less than 3% of the total generated energy [6].

2. Photovoltaic Battery

Solar batteries are semiconductor materials that convert the sunlight that falls on their surfaces into electrical energy. The surfaces of the solar cells, whose surfaces are found in various geometric shapes, are about 100 cm2 in area, with thicknesses of 0.2-0.4 mm [7]. The solar cell is shown in Figure 1.

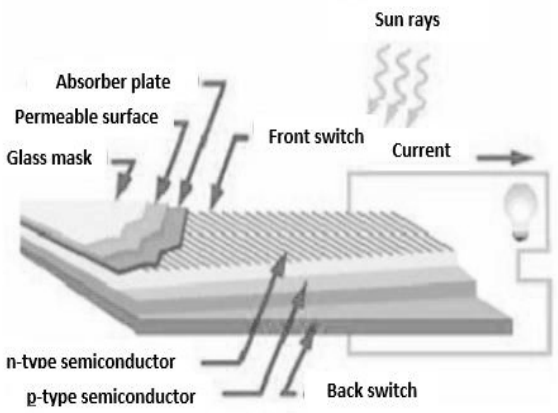


Figure 1: Structure of photovoltaic battery

The copper that is material is generally preferred. The coating layer is under the switches and it isn't reflector. Reflecting radiation that falling on the battery surface prevent to produce energy. That is, the covering layer prevents reflection from the battery surface. The front faces of the battery are shaped like pyramids and cones to better capture the reflected rays [8].

Under the non-reflecting layer, a portion where the electric current of the battery occurs. It creates two different layers. The N-layer is the negative part of the battery and consists of silicon and phosphor. The P-layer is the positive part of the pili, as well as the silicon and the bend. Between the P-layer and the N-layer, there is a region where the charges compare. The rear surface of the battery serves as a rear contact and is a positive contact [8].

A silicon solar battery produces about 0.5 V of electricity. The voltage batteries to be obtained are connected in series. Generally, when 30-40 solar cells are connected in series, they can output 15-18 V [7].

This voltage is enough to charge 12 volts of the current [8]. A photovoltaic cell with a diameter of 1 dm in sunny weather produces approximately 1 Watt.

2.1. The Effects and Factors of Solar Light

The Sun is approximately 58000 K temperature, it spreads a high amount of energy. There are two components of sunlight. These are direct radiation and stray radiation. Direct radiation (also called beam radiation) the sun is the undisturbed sun rays (causing the shadow). Direct radiation overflows about 90% of solar energy, and the rest floats "stray sunlight". Stray radiation is spread with solar radiation (full radiation on cloudy days). The reflected glow is reflected from the earth. The sum of the rays, scattered and reflected radiation is considered as global radiation on a surface. When much of the energy is in direct sunlight, raising the accumulation to the highest level requires the sun to reach the panels for as long as possible. It depends on the deflection angle, hour angle, sun height, sun angle.

3. System Design

In terms of the overall operation, the application of solar tracking system with servo motor control with LDR followed by an algorithm of sun position during the day was carried out to take the energy generated by the solar panel to the maximum level during the day and keep it at that level.

Two servo motors are used for the dynamic movement of the solar tracking system. The amount of light intensity from the source varies with the value of the resistance generated in the photocell, and this analogue information is transferred to the microprocessor. In this system, the sensor serves as a circuit element. The analog information obtained from the sensors is converted into digital information to be compared within the microprocessor. The software in the microprocessor is positioned concerning the light source, the sun, with the help of panel servo motors. As a result, placed in the middle of the edges of the solar panel and the intensity of the falling light were calculated.

According to the difference, the direction of rotation of the motor is decided. The flow diagram of the system is shown in Figure 2.

Figure 3 shows the detailed circuit diagram. RA0, RA1, RA2 the input is four LDR sensors that are indirectly connected to the RA3, which can read the analog signal and convert it to a digital signal (pulse).

For example, if the East LDR sensor reads more light intensity than the western density, the engine rotates east until it is equal to the two readings from the sensor.

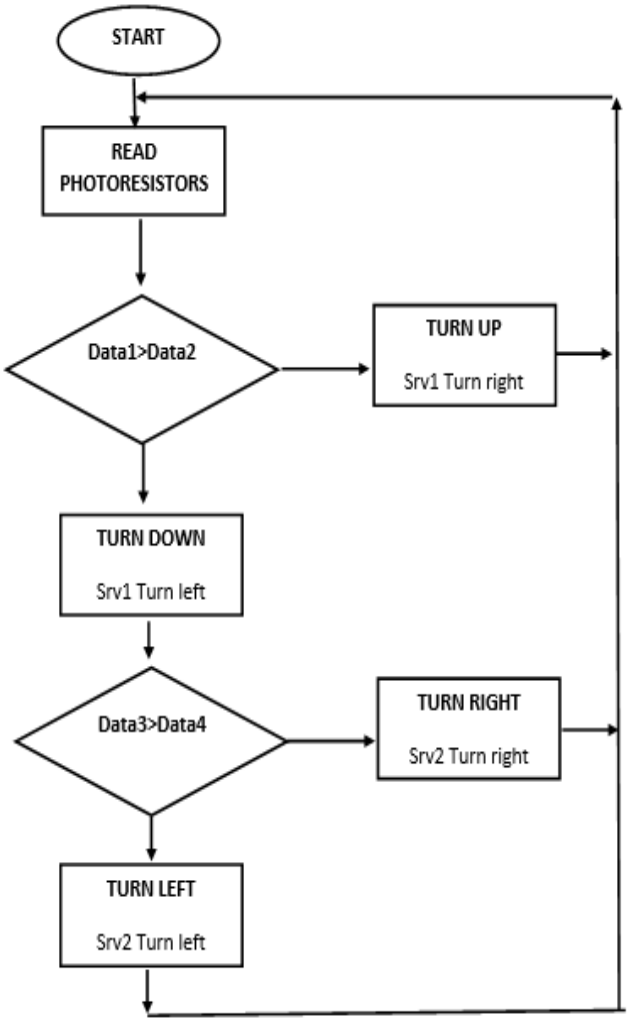


Figure 2: Flow diagram of the system

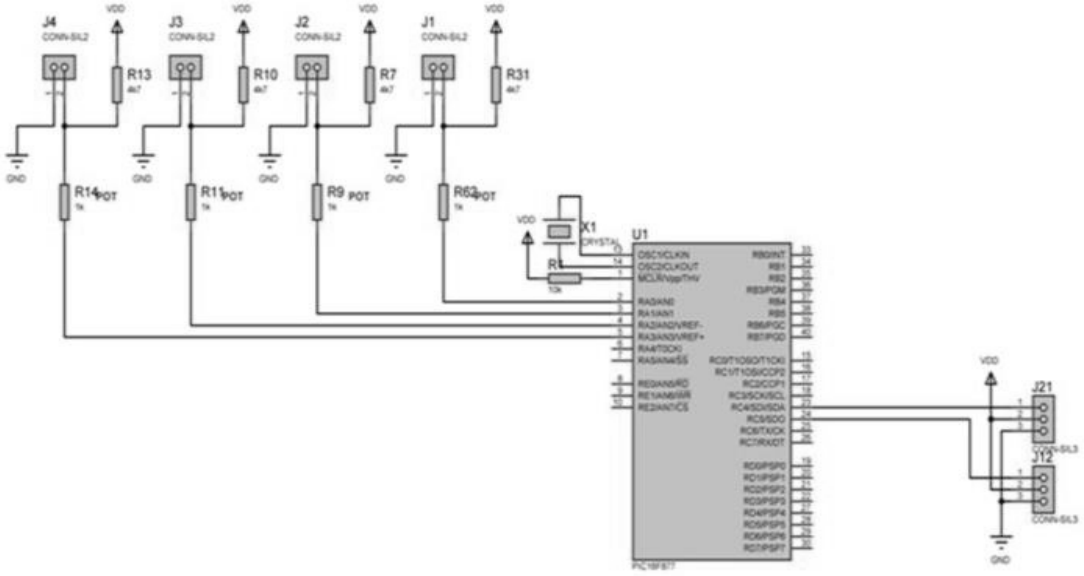


Figure 3: Circuit diagram

The reason for choosing PIC16F877 among the PIC types in the designed system is; reliability, speed, and flash. If you have Flash ROM, it shows that the installed program can be deleted, and another program can be installed. It is a microcontroller unit with input-output ports that will work with minimum hardware for every area used. It has a working speed of 20 Mhz, three timers and a 10-bit A / D converter [9].

Jal is a high-level programming language manufactured by Microchip to be compatible with PIC microcontrollers. There is no need for extra descriptions thanks to the libraries available inside. This will help speed up and improve the project.

There are various "USB pic programmers" available for loading microprocessor with "Hex" extension. MicroPro is preferred among these programmers.

With the help of "Microbrn", USB / serial port is created between microprocessor. By selecting the microprocessor series that we want to load, it is written into the file with "hex" extension.

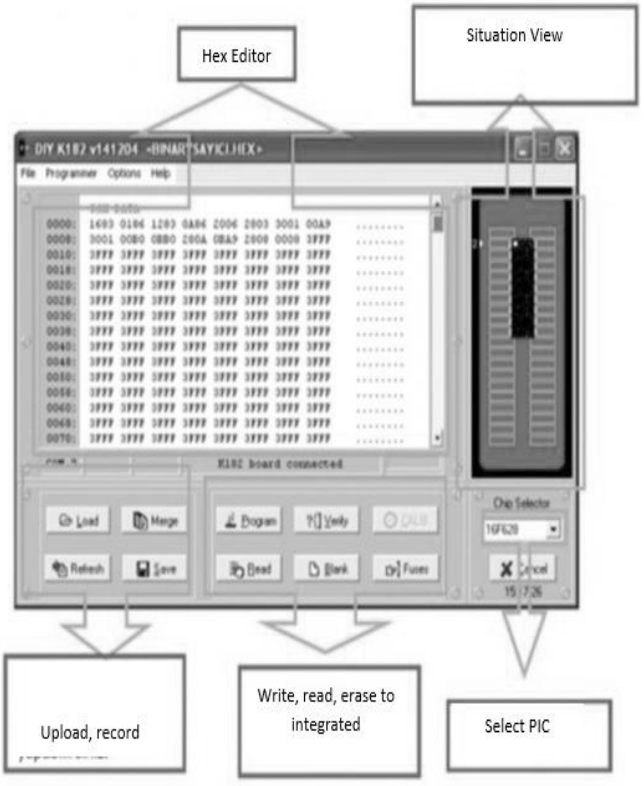


Figure 4: Microbrn interface

Figure 5: Designing system

4. Conclusion

An autonomous solar tracking system based on photovoltaic batteries has been designed and implemented. At the same time, the system's tolerance values should be paid attention. Continuous active motion of the system can cause too much energy to be expected. Selection motors are important with system design.

At the next stage of the system, a kind of cleaning system will be designed with a sun tracking system. The photoresistor which is a sensor works again like a sensor. When it could be dirty, it could not pass the light and the cleaning system will be active. Designing wipers start to work for cleaning.

5. References

[1] Kelly, Nelson A., and Thomas L. Gibson. "Improved photovoltaic energy output for cloudy conditions with a solar tracking system." Solar Energy 83.11 (2009): 2092-2102.
[2] Chong, K. K., and C. W. Wong. "General formula for on-axis sun-tracking system and its application in improving tracking accuracy of solar collector." Solar Energy 83.3 (2009): 298-305.
[3] Abdallah, S., and O. O. Badran. "Sun tracking system for productivity enhancement of solar still." Desalination 220.1-3 (2008): 669-676.
[4] Abdallah, Salah, and Salem Nijmeh. "Two axes sun tracking system with PLC control." Energy conversion and management45.11-12 (2004): 1931-1939.
[5] Huang, B. J., and F. S. Sun. "Feasibility study of one axis three positions tracking solar PV with low concentration ratio reflector." Energy conversion and management 48.4 (2007): 1273-1280.
[6] Abu-Khader, Mazen M., Omar O. Badran, and Salah Abdallah. "Evaluating multi-axes sun-tracking system at different modes of operation in Jordan." Renewable and sustainable energy reviews12.3 (2008): 864-873.
[7] Diken, Ö. "Fotovoltaik ünite tasarımı, elektrik enerjisi üretimi ve maliyet analizi." YTÜ Fen (2000).
[8] Altın, V. "Güneş Pillerinin Yapısı ve Çalışması." Bilim ve Teknik Dergisi 464 (2006): 41.
[9] Microchip Inc., "PIC16F87X Datasheet," www.microchip.com, (Erişim zamanı; Şubat, 8, 2018).

INTERNATIONAL JOURNAL OF ELECTRONICS, MECHANICAL AND MECHATRONICS ENGINEERING
Vol.9 Num.2 - 2019 (1677-1685)

New Control Method For Dual Voltage Rectifier

Rai Muhammad OMAR[1], Murtaza FARSADI[2]

Abstract: In this paper, a novel AC-DC converter having dual stage voltage rectifiers and voltage summation architecture is designed. Voltages of the two DC-buses are added together at the output port via down-stream DC-DC transformers (DCXs). The DC output voltage is controlled by regulating the voltage of the adjustable DC-busses of the DV-rectifiers. Therefore, voltage regulation is not required for the DCXs, which can always operate at their highest operation point to guarantee maximum efficiency. As the voltage of the adjustable DC-buses are changeable, multilevel voltages can be obtained with the DV-rectifier, which is benefit for reduction of switching losses and improvement of conversion efficiency. To achieve current regulation of AC input port and voltage regulation of the two DC-buses simultaneously, multi-mode operation and smooth mode transition strategies are proposed for the DV-rectifier. Operation principles, control strategies and characteristics of the DV-rectifier and DCX-based AC-DC converter are analyzed in detail. Feasibility and effectiveness of the proposed solutions are verified with experimental results.

Keywords: *AC-DC converter, dual-voltage-rectifier, dual-dc-bus, sigma structure, multiport converter*

1. Introduction

In today's modern life converters play a pivotal role. Every electronic device uses DC input for working. Digital devices require constant voltages, thus to get those constant voltage levels (DC levels) we need to convert AC into DC using rectifiers. Moreover, AC signals cannot be stored, and DC power or signals can be stored. Thus, to store the electrical energy we need to convert it into DC.

They have been widely used in electric vehicle charger, energy storage, smart-grid and power supplies for datacenter and telecommunications, etc. With the rapid development of electrical vehicles and battery storages, AC-DC converters with wide DC output voltage ranges are necessary to meet the requirements of batteries and dc loads. How to achieve high efficiency and flexible voltage control on both AC input side and DC output side has been an emergent research topic in various AC-DC power systems [2]-[4]. As a result, new topological and control variations and innovations have been continuously emerging.

[1] *Electrical Electronics Engineering, Engineering Faculty, Istanbul Aydin University, Istanbul, Turkey, raiomar@stu.aydin.edu.tr*
[2] *Application and Research Centre for Advanced Studies, Istanbul Aydin University, Istanbul, Turkey, murtazafarsadi@aydin.edu.tr*

This paper is organized as follows:

First it will discuss about our main circuit its configuration and working. Second portion will discuss about control scheme and how it will control our output voltage. In the third portion we shall discuss graphs at different loads and frequencies. And at the end conclusion and future work.

2. Main Circuit:

Basic dual-stage AC-DC converter is shown in fig. 1. In which buck type or boost type or may be both converters are used according to desired requirement. Second stage consist of filter which is used to remove harmonics and fluctuations.

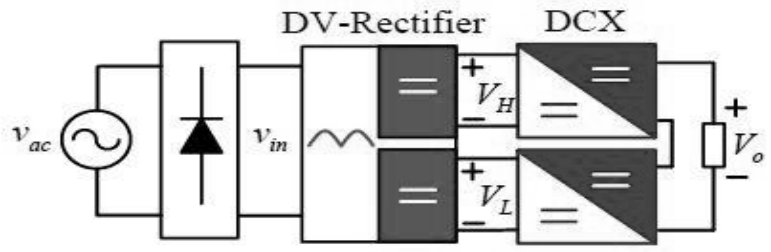


Figure 1: Dual Stage AC-DC Converter

The block diagram of proposed DV-rectifier-based AC-DC converter is shown in Fig. 2. To avoid efficiency reduction of the DC-DC stage due to wide voltage regulation range, the basic idea of the proposed AC-DC converter is based on dual-DC-bus method. Two DC-buses, i.e. a constant voltage DC-bus V_H and an adjustable DC-bus V_L, have been established by the DV-rectifier.

Different types of DV-rectifiers topologies can be made, and their control topology will be changed according to their working. DV-rectifier which we are considering, its working techniques are clearly discussed in [1]. That is not included in our scope. Our control scheme will be only main concern.

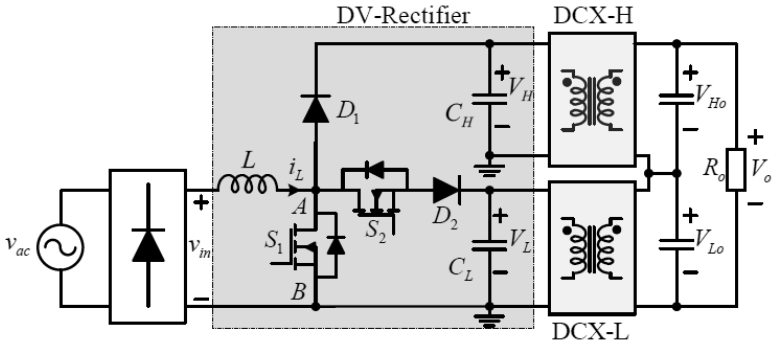


Figure 2: Proposed Dual Voltage Rectifier

3. Control Scheme:

Scope is to compare Pulse Width Modulation (PWM) efficiency with Fuzzy Logic Control scheme. We will see the voltages, power and current graphs of both control schemes and then conclude which one is best and beneficent for us. First, we shall consider PWM control scheme.

3.1 PWM Control Circuit:

Fig. 3 shows the control block diagram of the proposed AC-DC converter. The front-end DV-rectifier is responsible for input current regulation and the two DC-link bus voltage control, while the down-stream DCX is used to regulate the load voltage, current or power control. As shown in Fig. 3, a voltage control loop and a current control loop are employed for the DCX, so that constant voltage and constant current output can be achieved.

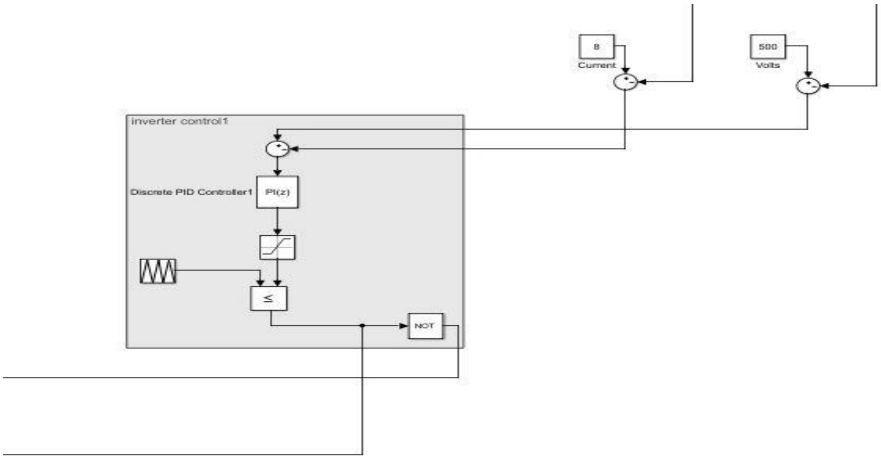


Figure 3: Voltage & Current Loop for the DCXs

The operation frequency of the two DCXs, i.e. f_{DCX}, is always the same. Therefore, only one controller and one pulse frequency modulator (PFM) are needed for the two DCXs, which can simplify the implementation of control. It should be noted that, when the switching frequency of the two DCXs is the same, the low frequency ripples on V_H and V_L will affect the output voltage ripple of each DCX, but the total output voltage *Vo* can still be regulated to suppress the low frequency voltage ripple by slightly changing the gain *GDCX* of the two DCXs simultaneously.

The relationship between the control signal V_{ctrl} and the average value of v_{AB} is as follows:

$$\bar{v}_{AB} = V_{Hi}\left(1 - d_{1_{VHi-SM}}\right) = V_{Hi}(2 - v_{ctrl})$$

When the rectifier operates in the *VL*-SOM, the terminal-3 of the SPTT is disabled and the switch pole is connected to terminal-1 and terminal-2 alternatively. In this case, the relationship between the control signal $V_{c1}$and the average value of v_{AB} is as follows:

$$\bar{v}_{AB} = V_{Low}\left(1 - d_{1_{VLow-SM}}\right) = V_{Low}(2 - v_{C1})$$

When the rectifier operates in the DOM, the terminal-1 of the SPTT is disabled and the switch pole is connected to terminal-2 and terminal-3 alternatively. In this case, the relationship between the control signal V_{c2} and the average value of v_{AB} is as follows:

$$\bar{v}_{AB} = V_{Low} d_{2\_DM} + V_{Hi}\left(1 - d_{2_{DM}}\right) = V_{Low} v_{c2} + V_{Hi}(1 - v_{C1})$$

where d_2_DOM is the duty cycle of S_2 in the DOM.
PWM control strategy and graphs of output voltage, output power and total harmonic distortions are shown in fig. 4, 5, 6 and 7 respectively.

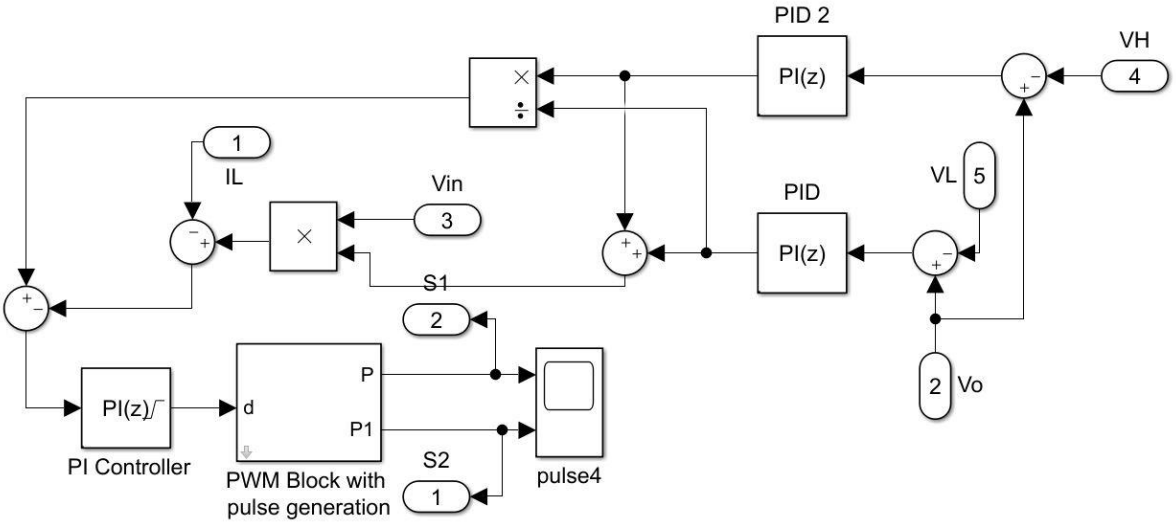


Figure 4: PWM Control Circuit for DV-Rectifier

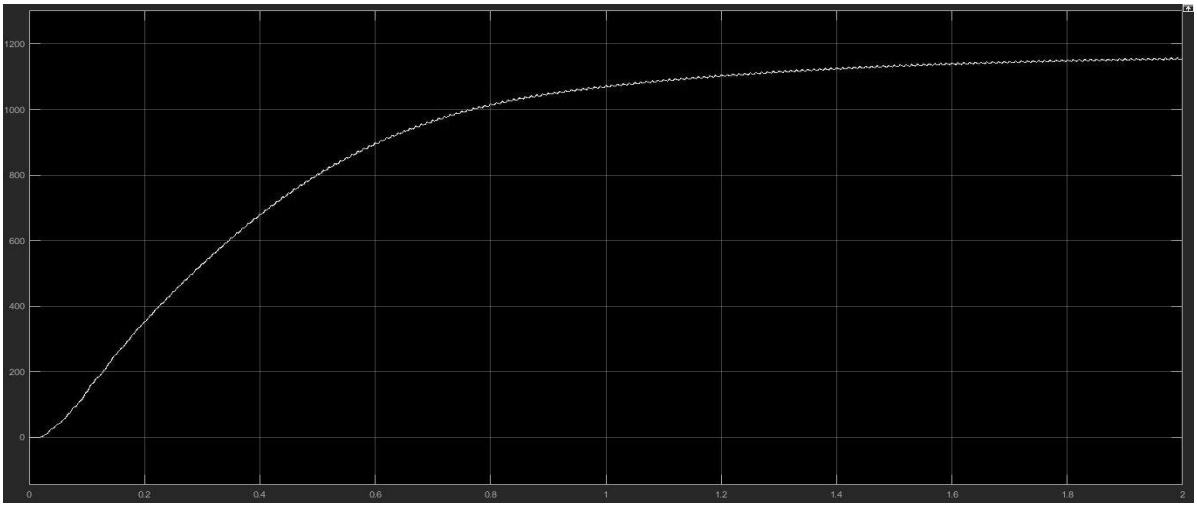


Figure 5: Output Power Graph of DV-Rectifier Using PWM

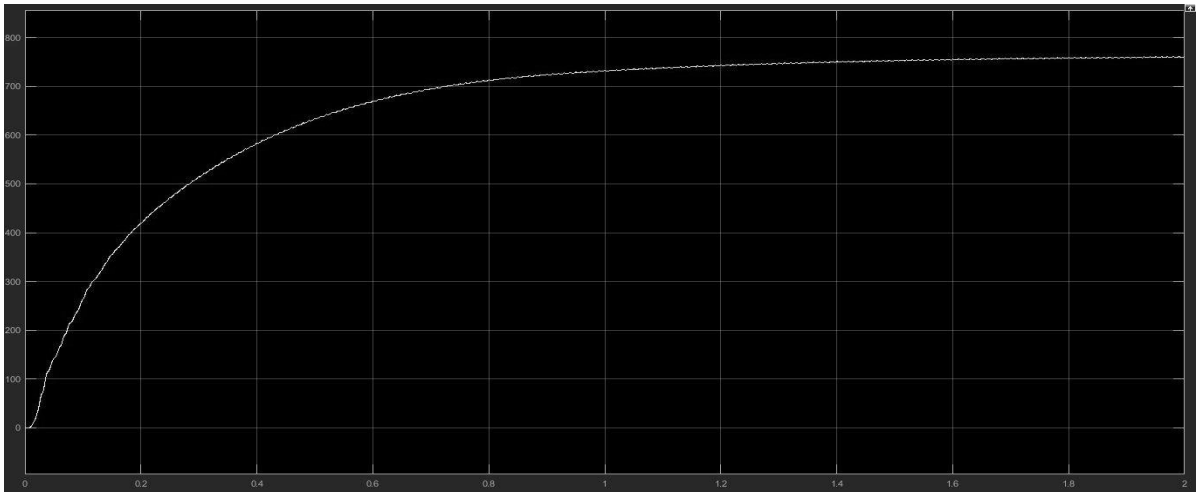


Figure 6: Output Voltage Graph of DV-Rectifier Using PWM

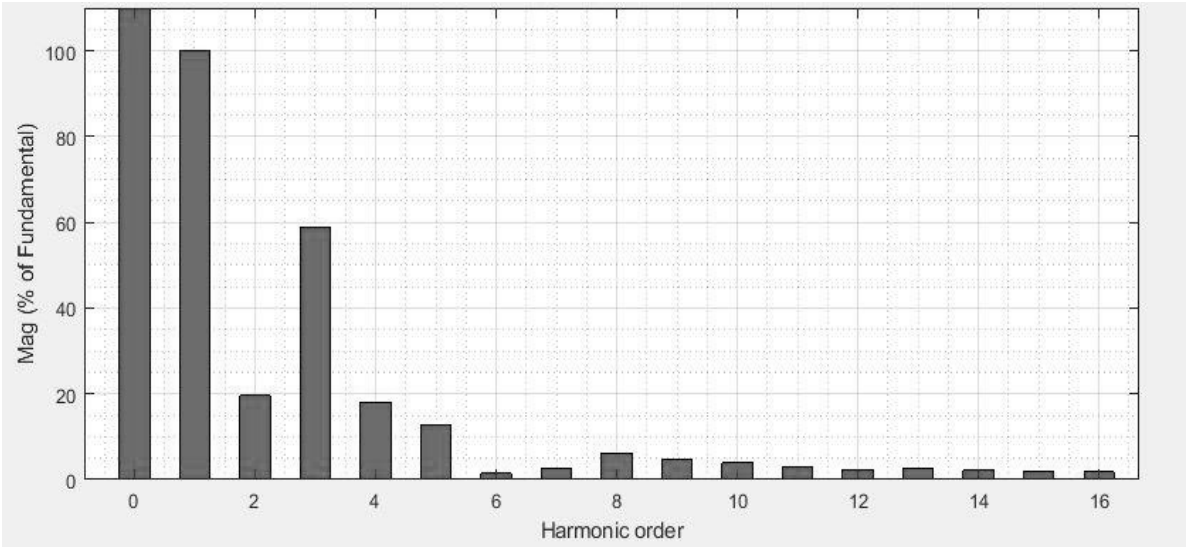


Figure 7: Total Harmonic Distortion (THD)

3.2 Fuzzy Logic Controller:

Why are we relying on Fuzzy Logic controller?

Fuzzy logic controllers (FLC's) have the following advantages over the conventional controllers: they are cheaper to develop, they cover a wider range of operating conditions, and they are more readily customizable in natural language terms. A self-organizing fuzzy controller can automatically refine a starting approximate set of fuzzy rules. PI-type fuzzy controller applications can increase the quality factor.

3.3 Mamdani Fuzzy Logic Controller:

Mamdani fuzzy inference system was applied as a decision-making model to classify aqua sites based on water, soil, support, infrastructure, input, and risk factor related information. Mamdani fuzzy inference system was used to develop the fuzzy rule-based model. It consists of five operating mechanisms named as fuzzification, calculation of weight factor, implication, aggregation and defuzzification.

Design of fuzzy controllers is based on expert knowledge of the system to be controlled instead of accurate mathematical model. There are two inputs in the fuzzy controller. The first is the error e(k) between the output voltage V[k] and the reference value Vref and the second is the difference between successive errors i.e. change of error ce(k) and are given by [6]

$e(k) = Vref - V(k)$
$ce(k) = e(k) - e(k-1)$

FLC control strategy and graphs of output voltage, output power and total harmonic distortions are shown in fig. 8, 11, 12 and 13 respectively.

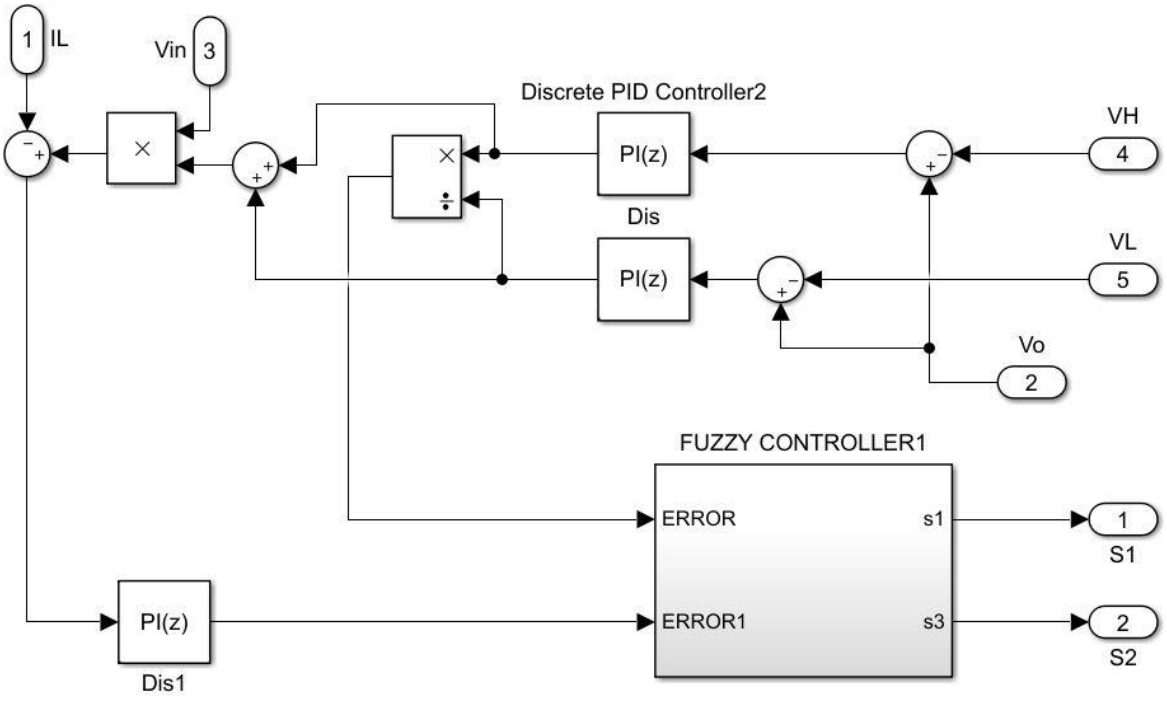


Figure 8: Fuzzy Logic Controller for DV-Rectifier

Fuzzification is the process of converting input data into suitable linguistic values. The first step in the design of a fuzzy logic controller is to define membership functions for the inputs. Five fuzzy levels are chosen and defined by the following fuzzy-set values for the error e and change in error ce:
NB negative big; NS negative small; ZE zero; PS positive small; PB positive big.

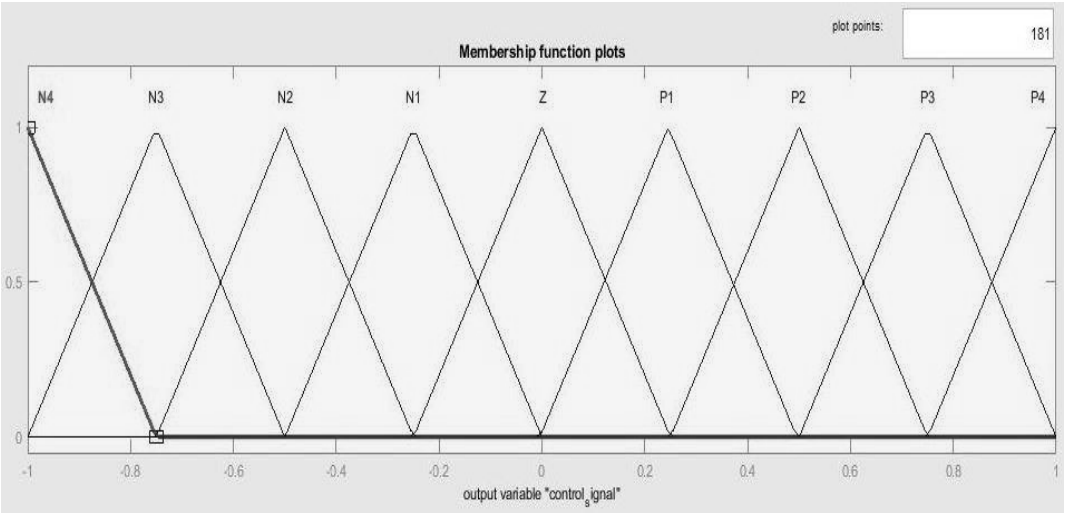


Figure 9: Control Signal Membership Function Plot

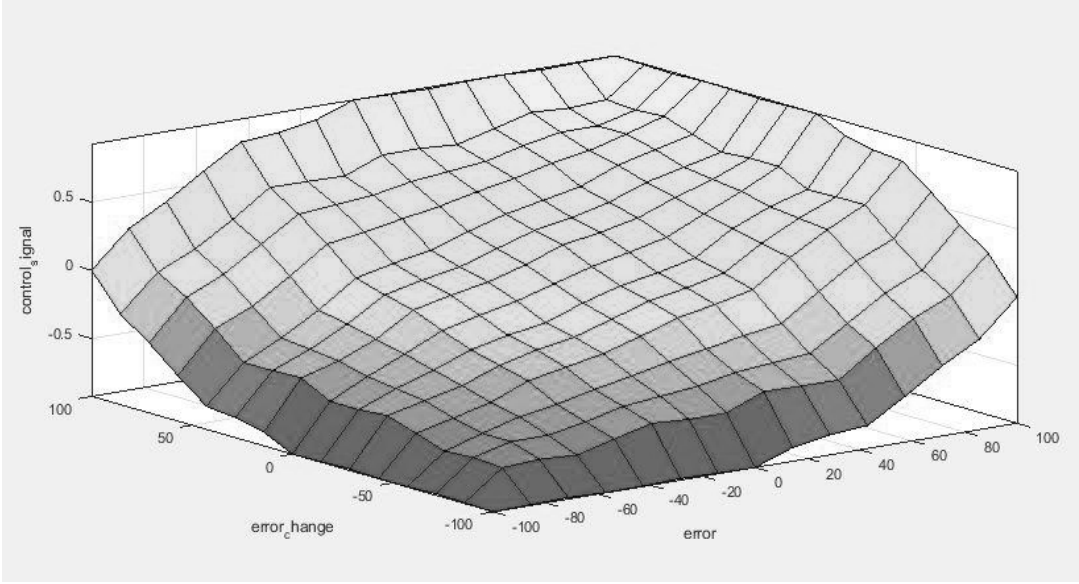


Figure 10: Control Surface Plot for Fuzzy Logic Controller

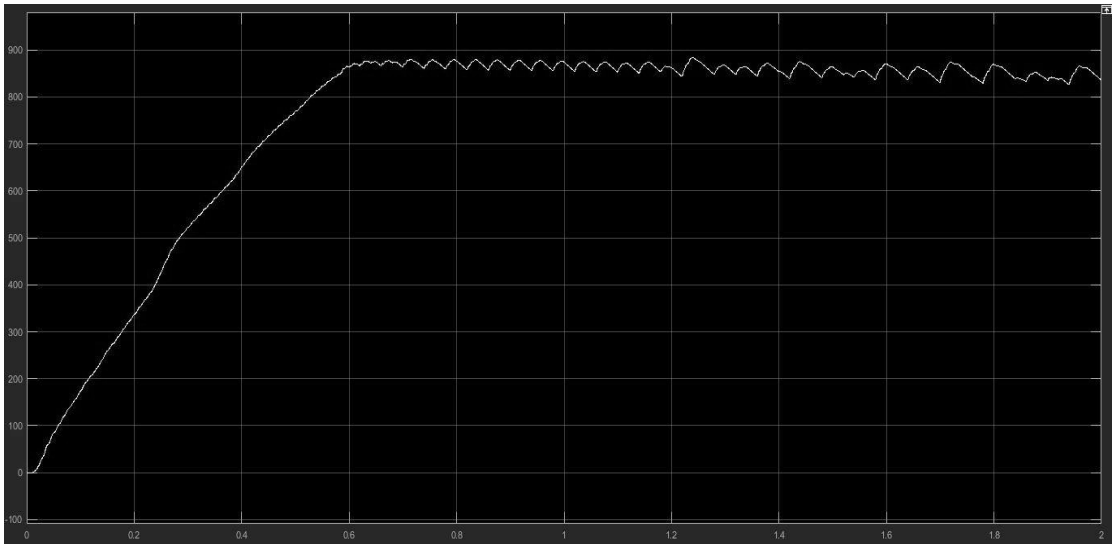


Figure 11: Output Voltage Graph of DV-Rectifier Using FLC

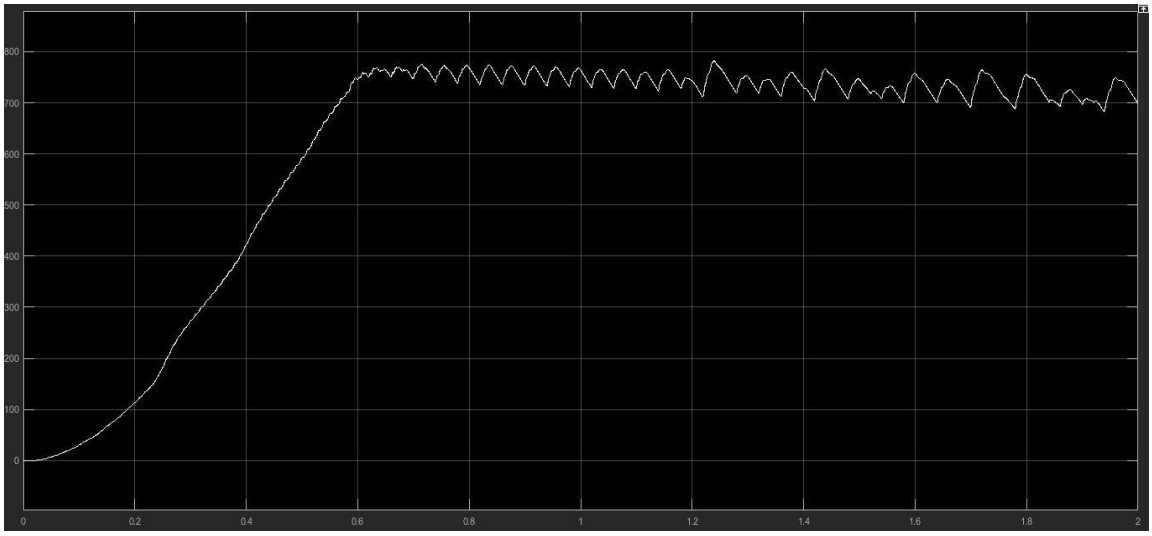


Figure 12: Output Power Graph of DV-Rectifier Using Fuzzy Logic Controller

4. Conclusion:

We have seen in our upper given graphs related to power and output voltages at same conditions of input voltages and frequencies, we have concluded that fuzzy logic controller is better than the PWM logic controller as the output of FLC circuit reaches its desired output faster than the other one. Although FLC is faster than PWM controller we have noticed that we got more harmonics in circuit controlled by FLC instead of PWM controlled circuit.

5. References

[1] H. Wu, M. Han and K. Sun, "Dual-Voltage-Rectifier-Based Single-Phase AC–DC Converters with Dual DC Bus and Voltage-Sigma Architecture for Variable DC Output Applications," in *IEEE Transactions on Power Electronics*, vol. 34, no. 5, pp. 4208-4222, May 2019.

[2] C. Saber, D. Labrousse, B. Revol and A. Gascher, "Challenges Facing PFC of a Single-Phase On-Board Charger for Electric Vehicles Based on a Current Source Active Rectifier Input Stage," in *IEEE Transactions on Power Electronics*, vol. 31, no. 9, pp. 6192-6202, Sept. 2016.

[3] H. Wu, S. Wong, C. K. Tse and Q. Chen, "Control and Modulation of Bidirectional Single-Phase AC–DC Three-Phase-Leg SPWM Converters With Active Power Decoupling and Minimal Storage Capacitance," in *IEEE Transactions on Power Electronics*, vol. 31, no. 6, pp. 4226-4240, June 2016.

[4] J. M. Guerrero, M. Chandorkar, T. Lee and P. C. Loh, "Advanced Control Architectures for Intelligent Microgrids—Part I: Decentralized and Hierarchical Control," in *IEEE Transactions on Industrial Electronics*, vol. 60, no. 4, pp. 1254-1262, April 2013.

[5] N. F. N. Ismail, I. Musirin, R. Baharom and D. Johari, "Fuzzy logic controller on DC/DC boost converter," *2010 IEEE International Conference on Power and Energy*, Kuala Lumpur, 2010, pp. 661-666. doi: 10.1109/PECON.2010.5697663

[6] https://dergipark.org.tr/download/article-file/344935

[7] L. Huber, Y. Jang and M. M. Jovanovic, "Performance Evaluation of Bridgeless PFC Boost Rectifiers," in *IEEE Transactions on Power Electronics*, vol. 23, no. 3, pp. 1381-1390, May 2008.

[8] J. Baek, J. Kim, J. Lee, H. Youn and G. Moon, "A Boost PFC Stage Utilized as Half-Bridge Converter for High-Efficiency DC–DC Stage in Power Supply Unit," in *IEEE Transactions on Power Electronics*, vol. 32, no. 10, pp. 7449-7457, Oct. 2017

[9] Wu, Hongfei & Han, Meng & Zhang, Yanfeng. (2017). Three-Port Rectifier-Based AC–DC Power Converters With Sigma Architecture and Reduced Conversion Stages. IEEE Journal of Emerging and Selected Topics in Power Electronics. PP. 1-1. 10.1109/JESTPE.2017.2648859.

[10] L. Huber, J. Yungtaek, and M. M. Jovanovic, “Performance evaluation of bridgeless PFC boost rectifiers,” *IEEE Trans. Power Electron.*, vol. 23,no. 3, pp. 1381–1390, May 2008.

[11] C. Fei, F. C. Lee, Q. Li, "High-efficiency high-power-density LLC converter with an integrated planar matrix transformer for high-output current applications," IEEE Trans. Ind. Electron., vol. 64, no. 11, pp. 9072-9082, Nov. 2017.

INTERNATIONAL JOURNAL OF ELECTRONICS, MECHANICAL AND MECHATRONICS ENGINEERING

Submission Instructions

The scope of International Journal of Electronics, Mechanical and Mechatronics Engineering (IJEMME) covers the novel scientific papers about Electronics, Image Processing, Information Theory, Electrical Systems, Power Electronics, Control Theory, Embedded Systems, Robotics, Motion Control, Stochastic Modeling, System Design, Multidisciplinary Engineering, Computer Engineering, Optical Engineering, Design Optimization, Material Science, Metamaterials, Heat and Mass Transfer, Kinematics, Dynamics, Thermo-Dynamics, Energy and Applications, Renewable Energy, Environmental Impacts, Structural Analysis, Fluid Dynamics and related topics of the above subjects.

IJEMME is an international journal published four times a year (January, April, July and October). Manuscripts reporting on original theoretical and/or experimental work and tutorial expositions of permanent reference value are welcome. IJEMME Editorial Board is authorized to accept/reject the manuscripts based on the evaluation of international experts. The papers should be written in English.

The manuscript should be sent in electronic submission via IJEMME paper submission system of web address (www.aydin.edu.tr/ijemme)

Submission instructions of manuscripts.

Page Design: Text body area is (195mm x 275mm). 30 mm margin from top, 20 mm from down and 25 mm margin should be left on right/left sides.

Title should be in 16 pt. bold, capital letters with Times New Roman font in Microsoft Word format. Authors' names, affiliations, e-mail addresses should follow the title after double line spacing with authors' names and surnames in lower case except first letters in 14 pt, the rest is 10 pt. italic.

Abstract should not exceed 200 words with the word "Abstract" in 10 pt. italic, bold, abstract text in 9 pt. italic, all in Times New Roman font in Microsoft Word format.

Key Words not exceeding 5 should be in bold.

Document Character: Subtitles should be in 10 pt. bold, capital letters and text body 10 pt. both with Times New Roman font in Microsoft Word format. The manuscripts should be written on a single column, be double spaced with single line spacing between paragraphs. The subtitle of the first section should start after a single space following the keywords, the other subtitles also with a single line space following the text, there should also be single line spacing between the previous text and the subtitle.

Conclusion: section should have a title written in 1o pt. bold, capital letters and the text in 10 pt. all in Times New Roman font in Microsoft Word format.

Reference numbers should be given in brackets as illustrated below:

Referencing books:
[1] Özsu M., T, Valduriez, P., *Principles of Distributed Database Systems*, Prentice Hall, New Jersey, 128-136,1991.

Referencing papers:
[2] G. Altay, O. N., Ucan, "Heuristic Construction of High-Rate Linear Block Codes," *International Journal of Electronics and Communications (AEU),* vol. 60, pp.663-666, 2006.

Page number is to be placed at the top left corner of each page with pencil.
Length of the Manuscript should not exceed 20 pages excluding Figures and Tables.

INSTRUCTIONS ABOUT THE ACCEPTED MANUSCRIPTS:

Page Design: Text body area is (195mm x 275mm). 30 mm margin from top, 20 mm from down and 25 mm margins should be left on right/left sides.

Title should be in 16 pt. bold, capital letters with Times New Roman font in Microsoft Word format. Authors' names, affiliations, e-mail addresses should follow the title after double line spacing with authors' names in lower case and surnames in capital letter in 14 pt. the rest in 10 pt. in the same format.

Abstract should not exceed 200 words with the word "Abstract" in 12 pt. italic, bold, abstract text in 9 pt. italic, all in Times New Roman font in Microsoft Word format.

Key Words not exceeding 5 should be in 9 pt. bold.

Document Character: Subtitles should be in 10 pt. bold, capital letters and text body 10 pt. both with Times New Roman font in Microsoft Word format. The manuscripts should be written on two columns, be single spaced with single line spacing between paragraphs. The subtitle of the first section should start after a single space following the keywords, the other subtitles also with a single line space following the text, there should also be single line spacing between the previous text and the subtitle.

Sections: Formulas should be numbered sequentially. Referring to formulas should be as Eqn (.). Figures and Tables should be placed into the text body and captions for both should be 10 pt. Table numbers and captions should be placed before the Table. If necessary, both columns may be used for large Figures and Tables.

Conclusion section should have a title written in 12 pt. bold, capital letters and the text in 10 pt. all in Times New Roman font in Microsoft Word format. Conclusion should not be a version of the Abstract.

Reference numbers should be given in brackets as illustrated below:

Referencing books:
[1] Özsu M., T, Valduriez, P., *Principles of Distributed Database Systems*, Prentice Hall, New Jersey, 128-136,1991.

Referencing papers:

[2] G. Altay, O. N., Ucan, "Heuristic Construction of High-Rate Linear Block Codes*," International Journal of Electronics and Communications (AEU),* vol. 60, pp.663-666, 2006.

Short Biography of the authors should follow references after a single line space, names in 9 pt. surnames in 9 pt. and the text in 9 pt. The text should not exceed 100 words.

CORRESPONDENCE ADDRESS:

Editor in Chief
Prof. Dr. Hasan Alpay HEPERKAN
Istanbul Aydın University, Faculty of Engineering
Mechanical Engineering Department
Florya Yerleskesi, Inonu Caddesi, No.38, Kucukcekmece, Istanbul, Turkey
Fax: +90 212 425 57 59 - Tel: +90 212 425 61 51 / 22001
E-mail: hasanheperkan@aydin.edu.tr

Prepared by
Instructer:Saeid KARAMZADEH
Engineering Faculty
Electrical and Electronics Eng. Dept.
Inonu Caddesi, No.38, Florya, Istanbul, TURKEY
E-mail: saeidkaramzadeh@aydin.edu.tr

Published by
Istanbul Aydın University
Graphic Design Department

İSTANBUL AYDIN ÜNİVERSİTESİ

KÜTÜPHANE VE BİLGİ MERKEZİMİZ
7/24 HİZMET VERİYOR

56.000
Basılı Kaynak

1.000.000
E-Kaynak

Engelsiz
Kütüphane

Mobil
Uygulamalar

24/7

- Kütüphane 7/24/365 gün hep açık
- 75.000 aylık kullanıcı
- Mimarlık ve Mühendislik Fakültesi için çizim salonları
- **Galeri Aydın**
- **Kafeterya**

instagram: kutuphaneiau twitter.com/iaukutuphane facebook.com/iaukutuphane