Mu'tah University

JJE
Jordan Journal of Energy

Mutah University

ISSN (Online) 2790-7678
ISSN (Print) 2790-766X

Jordan Journal of ENERGY

(JJE)

An International Peer-Reviewed Research Journal

JORDAN JOURNAL OF ENERGY (JJE)

Jordan Journal of Energy (JJE) is an international, multi-disciplinary journal in energy. It is peer-reviewed journal with ISSN (print): 2790-766X and ISSN (online): 2790-7678.

JJE publishes free of charge high quality, original research articles in various fields of energy. The Journal publishes original articles that contribute to promoting knowledge in all disciplines of all energy-related research. The journal covers research on energy analysis, energy modelling and prediction, integrated energy systems, energy planning and energy management. The journal also welcomes papers on related topics such as electrical and mechanical energy, energy conservation, energy efficiency, biomass and bioenergy, renewable energy, electricity supply and demand, energy storage, energy in buildings, and on energy related economic and policy issues. Articles published in JJE provide rigorous and innovative analyses of interest to academics and energy industry professionals. JJE also publishes review articles, short communication as well as technical notes.

JJE's editorial and international advisory boards are very committed to making JJE a leading platform and an authoritative source of information for analyses, reviews and evaluations related to energy.

JJE is published quarterly by the Deanship of Scientific Research at Mutah University. It applies the highest practices and professional standards of publication ethics.

SUBMISSION ADDRESS

https://dsr.mutah.edu.jo/index.php/jje/submissions

JORDAN JOURNAL OF ENERGY (JJE)

Aims and Scope

JJE aims to providing a highly readable and a valuable addition to the literature in the field of energy to reflect the evolving needs of energy sector. All energy-related research is in scope, including interdisciplinary and multidisciplinary studies. The journal will serve as an indispensable reference tool for years to come. The journal's scope includes all new theoretical and experimental findings that cover a wide range of topics in energy. JJE aims to strengthen relations between the energy sector, research laboratories, and universities. All the manuscripts must be prepared in English and are subject to a rigorous and fair peer-review process.

Specific Topics

The Journal might cover the energy & environmental issues; energy analysis; optimization; modelling and prediction; petroleum (upstream & downstream); natural gas; oil shale research; electricity markets; renewable energies (e.g., geothermal, solar, wind, hydro, tidal, wave, biomass); energy policy issues; energy market and power issues; econometric modeling; alternative transportation fuels; energy efficiency; regulatory economics; nuclear power issues; carbon emissions reduction; carbon capturing and storage technologies; energy efficiency; clean coal technologies; energy conversion; energy conservation; CO_2 sequestration and storage; energy management; energy systems; batteries; supercapacitors; hybrid/combined/integrated energy systems for multi-generation; hydrogen energy and fuel cells; hydrogen production technologies; micro- and nano-energy systems and technologies; smart energy system; electrical power systems; smart electric grids; physics of energy; artificial intelligence in complex power and energy systems; organic and inorganic photovoltaics; energy and power forecasting; waste energy management; reliability evaluation and risk analysis of energy systems; energy and environmental data acquisition and remote sensing.

Publishing Rules

In line with the strategic plan of the University of Mutah and its vision to achieve the standards of international classifications of universities, and based on the strategic plan and the vision of the Deanship of Scientific Research, which states:

"Towards a Deanship that hosts distinguished scientific research that elevates the University's classification locally, regionally and globally."

and, Its Mission that includes:

"Providing an environment capable of producing scientific research that contributes to enhancing the role of the University in research and innovation locally, regionally and globally."

The Deanship of Scientific Research has decided to develop **Jordan journal of Energy (JJE)**

When submitting your research for publication in the Journal, the followings shall be considered:

- Adopting the Modern Language Association (MLA) system, for more information: visit https://www.mla.org
- The research and all the required files should be electronically uploaded online at https://ejournal.mutah.edu.jo.
- The technical specification for printing of the research appeared at the website of the Journal should be strictly followed, keeping in mind that the research is subordinated to precise technical auditing when received, in case these specification is violated, the research will be returned.
- Failure to comply with any of the foregoing points exempts the Journal from proceeding with the arbitration proceedings.

Publication Procedures (Steps)

The Jordan Journal of Energy (JJE) follows the highest standards of publication ethics, and it takes all measures necessary to prevent publication misconduct.

Our editorial board does not accept any type of plagiarism. This means that works replicating another author's work without acknowledging him/her shall be automatically disqualified. All authors submitting their papers to JJE affirm that their papers are their own creations and have not been copied in whole or in part from other works.

1. The author(s) submit the research manuscript to the Deanship of Scientific Research at Mutah University at the Journal's Website http://dsr.mutah.edu.jo/
2. The author(s) signs a publication pledge in an official form available at the Journal's website.
3. The manuscript is registered in the Journal special records.
4. The submitted manuscript is technically checked and initially reviewed by the Editorial Board to determine its eligibility for peer review. The board is entitled to assign peer reviewers or to reject the manuscript without giving reasons.

5. If initially accepted by the Editorial Board, the manuscript will be sent to two reviewers, who should reply within a maximum period of one month. In case of failure to reply within the specified time, the manuscript shall be sent to another reviewer. Once receiving the reports of the reviewers, the Editorial Board decide the following:
6. The manuscript will be accepted for publication if receiving positive reports from the two reviewers, and after the author(s) make(s) the required corrections, if any.
7. If negative reports are received from both reviewers, the manuscript is rejected.
8. If a negative report is received from one reviewer, and a positive one from the other, the manuscript will be sent to a third reviewer to decide its validity for publication.
9. The author must make the suggested corrections of the reviewers within a maximum period of two weeks. Failing to meet this requirement will stop the procedure of publishing the manuscript.
10. If the reviewer rejects the required corrections, the author will be given a period of two weeks to make the necessary corrections, otherwise, the paper will be rejected.
11. Even if the reviewers approve the required corrections, the author(s) must abide by completing the essential technical specifications to be eligible to obtain the letter of acceptance.
12. The accepted manuscripts in the Journal are arranged for publication in accordance with the policy of the Journal.
13. What is published in the journal reflects the point of view of the author(s) and does not necessarily represent the views of Mutah University or the Editorial Board.

Publication Ethics

First: Duties of Editorial Board

- Justice and independence: Editors evaluate the manuscripts submitted for publication on the basis of importance, originality, validity, clarity and relevance of the journal, regardless of the gender of the authors, their nationality or religious belief, so that the editor has full authority over the entire editorial content and timing of publication.
- Confidentiality: Editors and editorial staff are responsible for the confidentiality of any information about the submitted manuscripts and not to disclose this information to anyone other than the author, reviewers, and publishers, as appropriate.
- Disclosure and Conflicts of Interest Editors and editorial members are responsible for the non-use of unpublished information contained in the research submitted for publication without the written consent of the authors. The editors themselves will consider manuscripts for which they have conflicts of interest such as competitive, collaborative, or other relationships with any of the authors; instead they will ask another member of the editorial board to deal with the manuscript.
- Publishing Decisions: Editors shall ensure that all manuscripts submitted for publication are subjected for reviewing by at least two reviewers who are experts in the field of manuscript. The editor-in-chief is responsible for determining which of the research papers will be published, after verifying their relevance to researchers and readers, and the comments of the reviewers.

Second: Duties of the reviewers

- Contributing to the decisions of the editorial board.
- Speed and accuracy in time: Any reviewer who is unable to review the submitted manuscripts for any reason should immediately notify the editors and reject the invitation for reviewing so that other reviewers can be contacted.
- Confidentiality: Any manuscript received by the Journal for reviewing and publishing is confidential; it should not appear or discussed with others unless authorized by the Editor. This also applies to the invited reviewers who have rejected the invitation for reviewing.
- Objectivity criteria: The reviewing process of the submitted manuscript should be objective and the reviewer comments should be clearly formulated with the supporting arguments so that the authors can use them to improve the quality of their manuscript away from the personal criticism of the authors.
- Disclosure and Conflict of Interests: Any invited reviewer must immediately notify the editors that he/she has a conflict of interest resulting from competitive, cooperative or other relations with any of the authors so that other reviewers may be contacted.
- The confidentiality of information or ideas that are not published and have been disclosed in the manuscript submitted for reviewing and not use without the express written consent of the authors. This applies also to the invited reviewers who refused the reviewing invitation.

Third: Duties of the Authors

- Criteria for the preparation of the manuscript: Authors must provide an accurate description of the presented work and the achieved results, including a subjective discussion of the importance of work.
- Originality and plagiarism: Authors must ensure that their work are original and that the works of other authors in the same field must be consulted and referenced in their manuscript. In all of its forms, plagiarism behavior is an immoral behavior and takes many forms, such as the adoption of the research of other author, copying or rephrasing large parts of other researches (without referencing) ... etc.
- The authors should not send or publish the manuscript to different journals simultaneously. Also, authors should not submit a manuscript that has already been published in another journal, because submitting the manuscript simultaneously to more than one journal is unethical and unacceptable.
- Authorship of the manuscript: Only persons who meet the following authorship criteria should be listed as one of the authors of a manuscript as they should be responsible for the manuscript content: 1) present significant contributions to the design, implementation, data acquisition, analysis or interpretation of the study; 2) critically contribute to the manuscript writing and revision or 3) have seen and approved the final version of the manuscript and agreed to submit it for publication.
- Disclosure and conflicts of interest: Authors must report any conflict of interest that can have an impact on the manuscript and its reviewing process. Examples of potential conflicts of interest to be disclosed such as personal or professional relationships, affiliations, and knowledge of the subject or material discussed in the manuscript.
- Risks and Human or Animal subjects: If the research involves the use of chemicals, procedures or equipment that may have any unusual risks, the authors must clearly identify them in their work. In addition, if it involves the use or experimentation of humans or animals, the authors must ensure that all actions have been carried out in accordance with the relevant laws and regulations and that the authors have obtained prior approval of these contributions. Moreover, the privacy rights of human must also be considered.
- Authors must fully cooperate and respond promptly to editors' requests for clarifications, proof of ethical approvals, patient approvals, and copyright permissions.
- In the case of making an initial decision on the submitted manuscript of some the necessary amendments and corrections, the authors must respond promptly to the comments of the reviewers and carry out the required corrections and re-submit it to the journal by the deadline.
- When authors find significant errors or inaccuracies in their submitted manuscripts, they must immediately notify editors or publishers of the journal and collaborate with them to either correct or withdraw their work.

Contents

Jordan Journal of Energy
Volume 1, Number 2, 2023

ISSN (Online): 2790-7678
ISSN (Print): 2790-766X

Jordan Journal of Energy (JJE)
Journal Homepage: http://dsr.mutah.edu.jo/index.php/jje
JEE an official peer review journal of Mutah University,

Damping Undammed Low Frequency Oscillations in Power Systems: An ANN-Based Approach Using Pre-Disturbance Data

Mohammad M. Al-Momani[1]*, Amneh Al-Mbaideen[2], Seba F. Al-Gharaibeh[2],

*[1]Electrical Engineering department, Iowa State University, Ames, USA

mmomani@iastate.edu

[2]Mutah University, Electrical Engineering Department, Jordan

a.mbaideen@mutah.edu.jo

Received 14th June 2023; Accepted 12th August 2023

*Corresponding Author Email: mmomani@iastate.edu, monqedmohammad@gmail.com

ABSTRACT. *The paper examines undammed low frequency oscillations (LFOs) that can lead to system collapse, citing the Jordan power network incident on May 21, 2021. Traditional model-based methods for studying LFOs' small-signal stability have limitations. To address this, an online damping controller based on an artificial neural network (ANN) is proposed. Unlike existing ANN-based methods relying on offline controllers, this novel approach utilizes pre-disturbance data from phasor measurement units (PMUs) to dampen oscillations effectively. The paper addresses challenges of partially observable systems in online eigenvalue prediction using ANN. MATLAB is used to implement a feedforward ANN system trained on PMU data. The study involves a three-area test system with various operational scenarios, training the ANN across 406 scenarios to predict eigenvalues and damp LFOs.*

Keywords: Undammed low frequency oscillations (LFOs), System collapse, Small-signal stability, Model-based methods, Measurement-based identification, Phasor measurement units (PMUs), Wide area damping controller, artificial neural network (ANN), Post-disturbance data, Ring-down method.

1. Introduction. The paper presented herein delves into the critical analysis of undammed low frequency oscillations (LFOs) and their potential repercussions, notably demonstrated by the incident in the Jordan power network on May 21, 2021. These oscillations, with the capacity to induce system collapse, are intricately linked to small-signal stability in power networks. Traditional approaches for understanding LFOs, primarily reliant on model-based techniques, have shown limitations as expounded in prior research. In response, this paper introduces an innovative solution in the form of an online wide area damping controller. This controller is grounded in artificial neural network (ANN) technology and is adept at identifying LFOs through real-time data acquired from phasor measurement units (PMUs). Unlike prevailing

methods, which necessitate offline controllers, the proposed approach leverages pre-disturbance data, eliminating the need for such controllers. The paper also addresses the challenges posed by partial observability in predicting system behavior using ANN. The study emulates real-world scenarios, particularly focusing on the Jordanian power system, while incorporating fully observable systems as a representation of the future landscape. Employing a feedforward ANN system with a backpropagation training algorithm implemented in MATLAB, the research utilizes comprehensive PMU measurements encompassing generator angles, reactive powers, and bus angles. Through an extensive array of operational scenarios, the paper trains the ANN to predict eigenvalues, providing a robust framework for effectively managing and mitigating the impact of LFOs in power networks.

The utilization of advanced wide-area monitoring through the incorporation of phasor measurement units (PMUs) facilitates a continuous evaluation of the operational health of power grid systems. Over the past two decades, the practice of dynamically monitoring power systems for real-time operation and control has become increasingly prominent within the field. A spectrum of both linear and nonlinear methodologies have been proposed by scholars to effectively gauge the dynamic responses and proficiently estimate the key parameters associated with prevailing low-frequency oscillatory modes. The assessment of power system modes is conventionally carried out through two distinct avenues: the modal-based approach, characterized by its propensity to linearize governing equations surrounding operational points [1], and the measurement-based approach, which inherently engages in data-driven analyses of system measurement data [2]. The IEEE task force focused on the identification of electromechanical oscillatory modes substantiates a comprehensive compendium of techniques deployed across modal and data-driven paradigms [3]. Although the efficacy of model-based techniques in accommodating the intricacies of large-scale power systems is restricted due to computational exigencies, concurrently, measurement-based methods, particularly those harnessing synchrophasor technology, are widely adopted to discern and delineate low-frequency modes [4]. This category of measurement-based techniques, encompassing methodologies such as Prony analysis [5], matrix pencil method (MPM) [6], signal parameter estimation via rotational invariant techniques (ESPRIT) [7], auto-regressive moving average (ARMA) technique [8], and eigenvalue realization algorithm (ERA) [9], is ubiquitously present within a myriad of scholarly works. These techniques feature prominently in investigations pertaining to ring-down oscillation studies. Similarly, concerning ambient oscillation studies, techniques encompass transfer function methods [10] alongside subspace methods [11], [12]. Notably, the subspace approach garners enhanced precision, thereby rendering superior results in terms of accuracy; nevertheless, transfer function methods persist as the favored recourse in consideration of computational efficiency [13].

This paper initiates by performing online mode identification through an Artificial Neural Network (ANN). Subsequently, the influence of partial observability on predicting online eigenvalues is addressed. The research employs a feedforward ANN system along with a

backpropagation training algorithm, executed using MATLAB 2020b. Each training dataset is partitioned into 80% for training, 10% for validation, and 10% for testing purposes. To validate the model, diverse scenarios are generated for each system after undergoing training within the MATLAB toolbox.

2. ANN-Based Electromechanical Modes Identification. Within this section, the estimation of electromechanical modes in the three-area test system with string configuration [14] is undertaken employing three distinct inputs: generators' angles, generators' reactive powers, and bus angles. These data sets can be effectively acquired using PMUs during the pre-fault duration.

The three-area test system [14] encompasses five PV synchronous generators and a slack generator. The angles of these generators are contingent upon the operational state and system topologies. Herein, an Artificial Neural Network (ANN) structure is trained utilizing generator angles across various scenarios. The ANN system is trained using a comprehensive set of 406 scenarios, comprising:

- Load 9 ranging from 1300 MW to 1900 MW, incremented by 100 MW, for operation point A.
- Load 12 ranging from 900 MW to 1500 MW, incremented by 100 MW, for operation point A.
- Load 16 ranging from 800 MW to 1500 MW, incremented by 100 MW, for operation point A.
- Load 12 ranging from 1300 MW to 1900 MW, incremented by 100 MW, for operation point B.
- Load 16 ranging from 900 MW to 1500 MW, incremented by 100 MW, for operation point B.
- Load 9 ranging from 800 MW to 1500 MW, incremented by 100 MW, for operation point B.
- Load 16 ranging from 1300 MW to 1900 MW, incremented by 100 MW, for operation point C.
- Load 9 ranging from 900 MW to 1500 MW, incremented by 100 MW, for operation point C.
- Load 12 ranging from 800 MW to 1500 MW, incremented by 100 MW, for operation point C.

All the aforementioned 63 scenarios are systematically replicated for various system topologies.

TABLE 1. Number of cases collected at different topologies.

Topology	Numbers of cases
Normal	63
TL9-16 tripped	63
TL12-16 tripped	63
TL15-16 tripped	63
TL9-16 and TL 15-16 are tripped	63
TL12-16 and TL 15-16 are tripped	63
TL9-16 and TL 12-16 are tripped	63
TL9-16, TL 12-16, and TL15-16 are tripped	63
Unsuccess Load flow	98
Total	406

An additional set of 160 validation cases has been meticulously selected to thoroughly scrutinize the proposed framework. These validation instances encompass a diverse range of load and capacitor values, introducing a comprehensive spectrum of scenarios.

Within each scenario, employing small-signal analysis (as elaborated [14]), the real and imaginary components of the eigenvalues (both local and interarea) are meticulously computed. The prediction of these five eigenvalues (comprising three local and two interarea modes) is executed through the utilization of four distinctive parameters:

- Generators' angles.
- Generators' reactive power.
- Generators and load voltage angles.
- Buses' voltage angles.

The configuration of each system engenders ten outputs, split into the real components (five outputs) and imaginary components (five outputs) of the eigenvalues. Every system undergoes five rounds of training, encompassing an exhaustive array of 100,000 diverse architectures, each characterized by varying numbers of layers and neurons. This encompasses all possible permutations of 1-5 layers housing 4-13 neurons per layer for each respective system. The outcome of this extensive experimentation is the identification of optimal structures that yield minimal mean square error for each system, as meticulously tabulated in Table 2.

TABLE 2. Optimal structures of the proposed ANN.

System input	No. Layer	No. Neurons per Layer
Generator buses' angles	4	[10 6 7 10]
Generators' reactive power	4	[10 10 11 11]
Buses' voltage angels	4	[7 11 9 11]
Generators and load buses' angles	4	[11 8 10 11]

The optimal structure for each system is trained 500 times. The optimal design is selected based on the mean square error of all 406 samples. The best mean square error of the training, validation, and testing stages are shown in Figures 1 to 4 for each system.

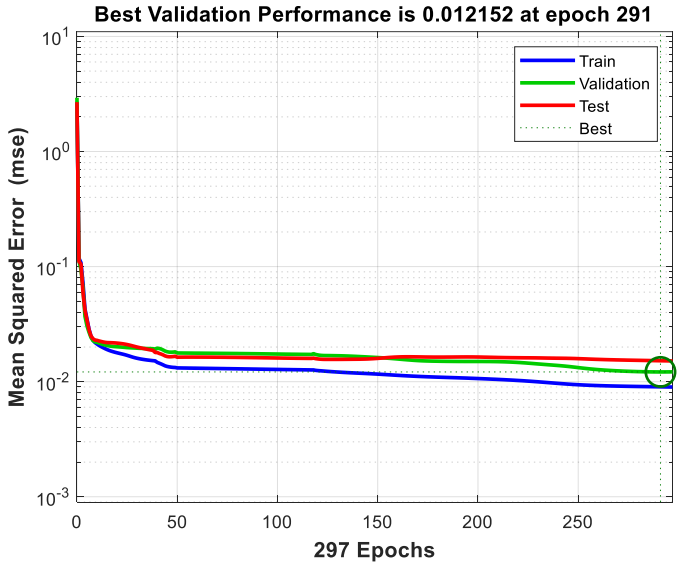


FIGURE 1. Performance criterion for the generator bus angle-based system.

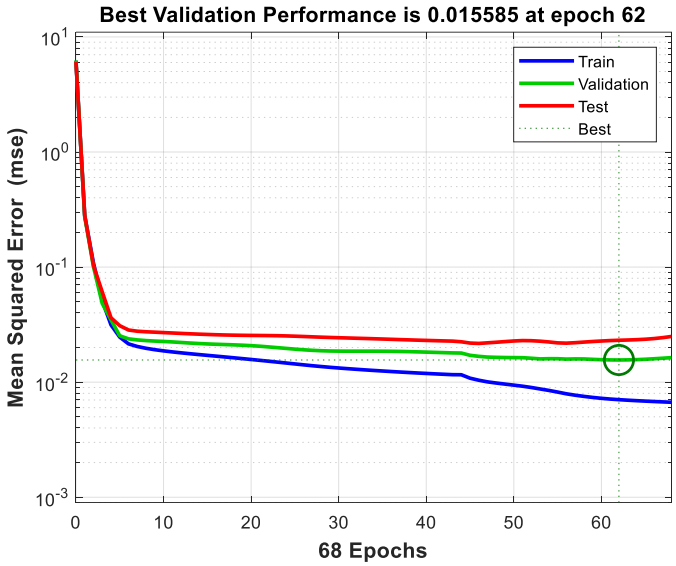


FIGURE 2. Performance criterion for the generator reactive power-based system.

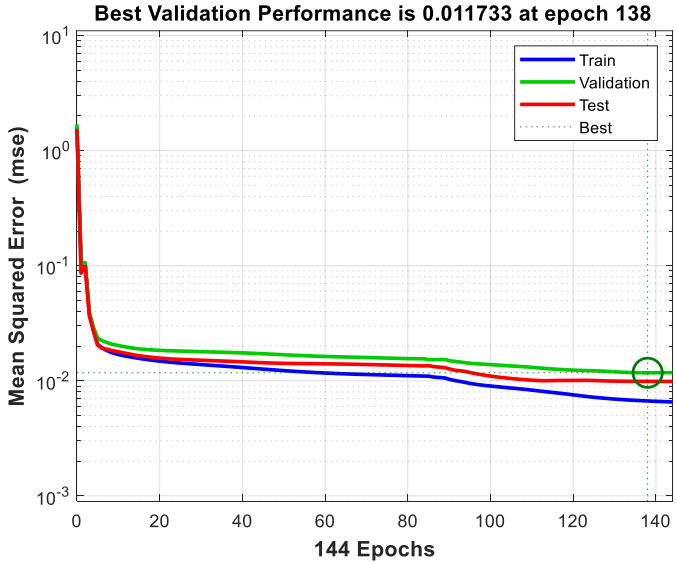


FIGURE 3. Performance criterion for the buses' angles-based system.

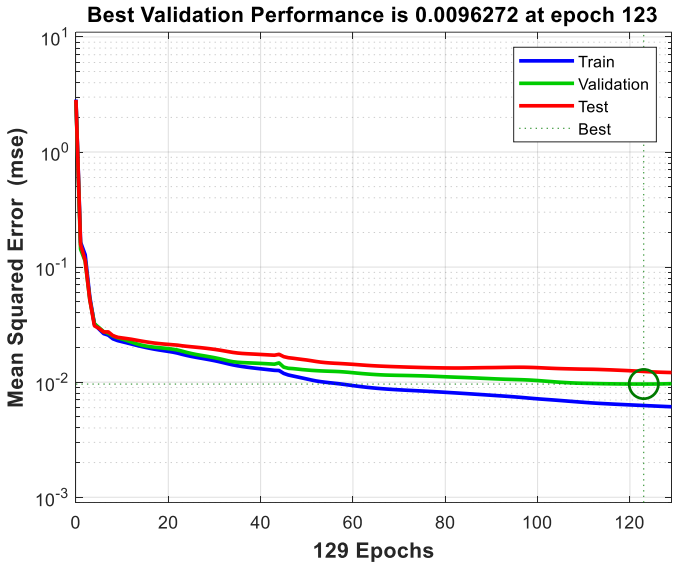


FIGURE 4. Performance criterion for generator and load bus angle-based system.

Figures 1 to 4 provide a comprehensive insight into the optimization process for each system's optimal structure, which was subjected to 500 training iterations. The selection of the most effective design was based on the mean square error calculated across all 406 samples. These figures elucidate the best mean square errors achieved throughout the training, validation, and testing stages for each individual system.

- Figure 1 illustrates the performance criterion for the system centered on generator bus angles. Notably, the graph showcases the evolution of validation performance, with the most noteworthy achievement being a validation performance of 0.012152, attained at epoch 291.
- Figure 2 outlines the performance criterion associated with the generator reactive power-based system. The graph captures the trajectory of validation performance over iterations, with the optimal validation performance of 0.015585 materializing at epoch 62.
- Figure 3 expounds upon the performance criterion for the bus angle-based system. The graph elegantly captures the fluctuations in validation performance, with a strikingly favourable validation performance of 0.011733 recorded at epoch 138.
- Figure 4 delineates the performance criterion for the system predicated on both generator and load bus angles. The graph showcases the dynamics of validation performance, culminating in a remarkable validation performance of 0.0096272, observed at epoch 123.

In essence, these figures meticulously portray the dynamic nature of the optimization process for each system's optimal structure, spotlighting the epochs at which the most favorable validation performances were achieved across the training iterations.

Based on the performance criterion depicted in Figure 4, the most optimal system is determined to be founded on generator and load bus angles. This particular system was refined over 123 iterations through the utilization of the backpropagation technique for training the ANN structure. The ensuing model is explored in the subsequent analysis.

The interconnections between layers, as showcased in Figure 5, contribute to elucidating the system's architecture. Within these figures, the larger squares represent relatively substantial values, while the smaller squares denote diminutive values. Moreover, the coloring of these

squares is indicative of the value's sign (negative: red (dark), positive: green (light)). These figures collectively grant insights into the relative magnitudes of the weights employed within the system.

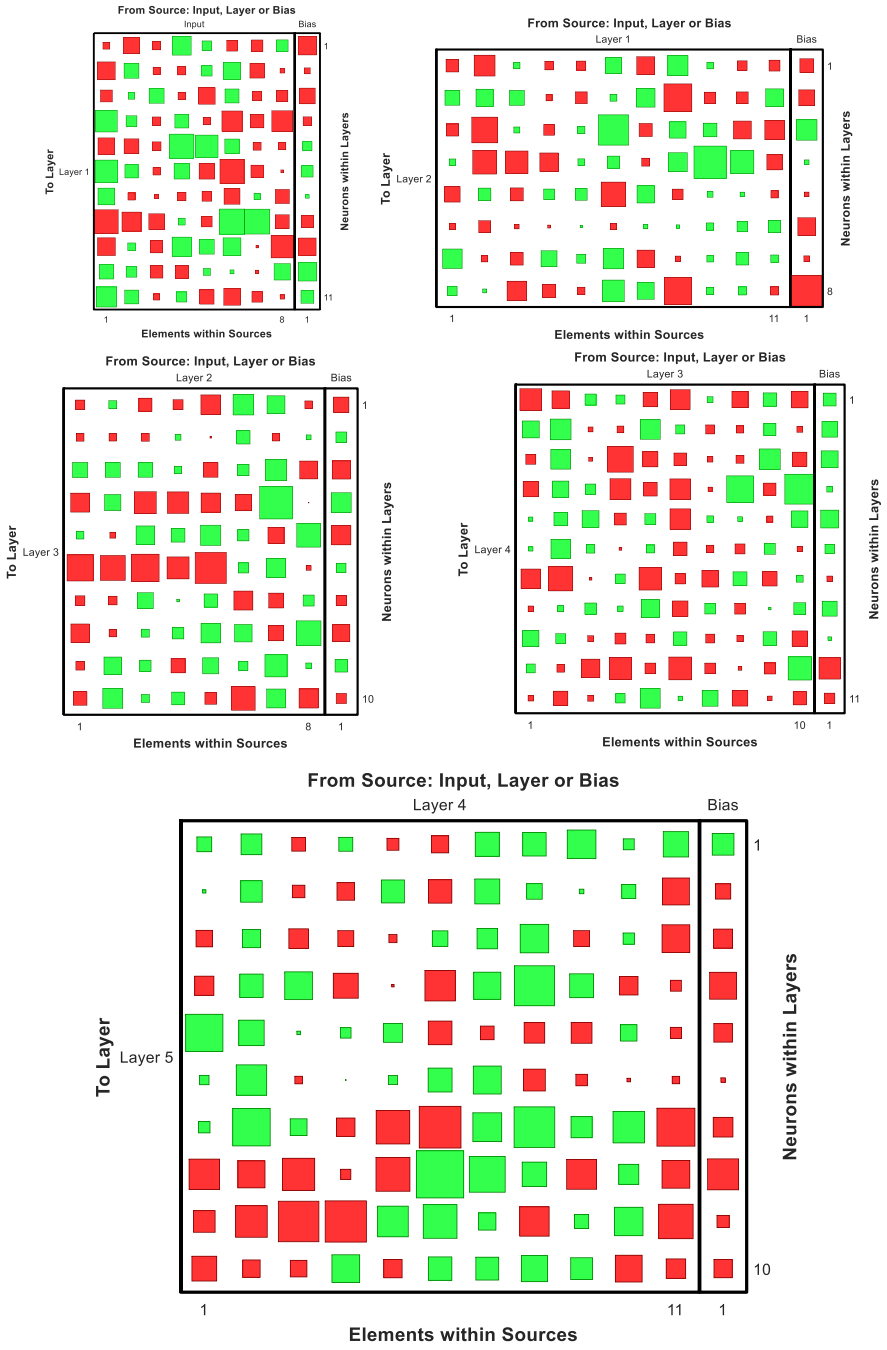
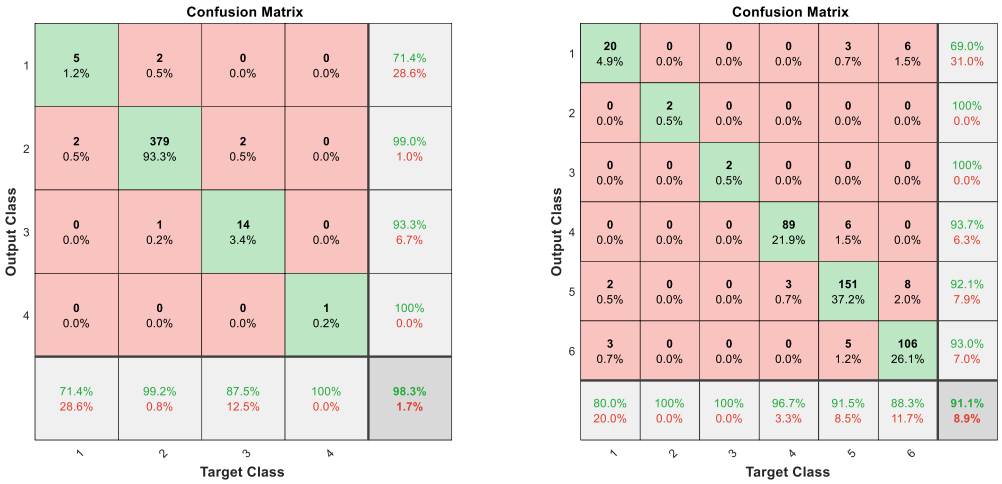


FIGURE 5. system Wights.

Figure 6 showcases the confusion matrix encompassing both interarea and local-area modes. This matrix serves to validate the efficacy of eigenvalue classification. As evident from Figure 6 (a), the accuracy of correct predictions stands at 98.3%, with a mere 1.7% attributed to incorrect predictions. The most pronounced confusion within outputs materializes between the initial two outputs, corresponding to the real parts of interarea eigenvalues. This occurrence is

deemed acceptable, given the proximity of real parts for both interarea modes. The concept underpinning the confusion matrix relies on a strict equality criterion with minimal tolerance. The robustness of the model is substantiated by the higher occurrence of correct predictions compared to incorrect ones. Consequentially, in light of these confusion matrix findings, the utilization of the mode index [15] is deemed unnecessary for oscillation mode categorization within this model.



(a) (b)

FIGURE 6. Confusion matrix for (a) interarea modes (real 1, real 2, imaginary 1, imaginary 2) (b) local modes (real 1, real 2, real 3, imaginary 1, imaginary 2, imaginary 3)

The histogram error is presented in Figure 7. From Figure 7, the maximum error is within 0.002952. The online wide-area controller sensitivity should cover this error in both real and imaginary parts of the eigenvalues.

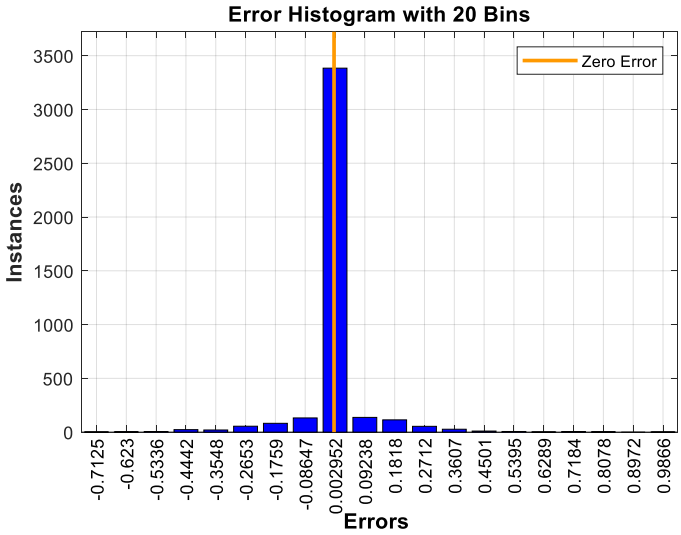


FIGURE 7. Histogram error for all samples (training samples)

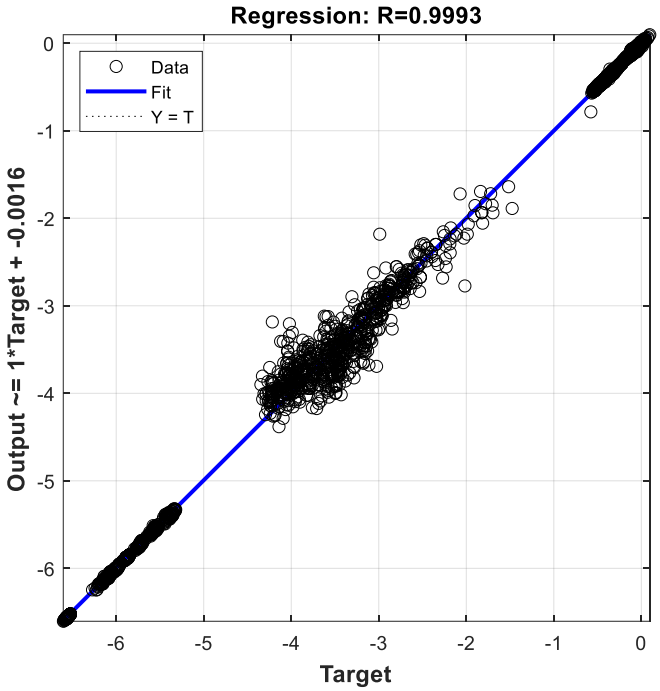


FIGURE 8. Output/target regression

Output and target regression for the trained data is presented in Figure 8. From the Figure, the behavior of the system is very good. The validation data (160 samples) is applied to the model, and the prediction eigenvalues and the true eigenvalues are plotted at the same graphs in Figures 9 for the local modes and Figure 10 for the interarea modes.

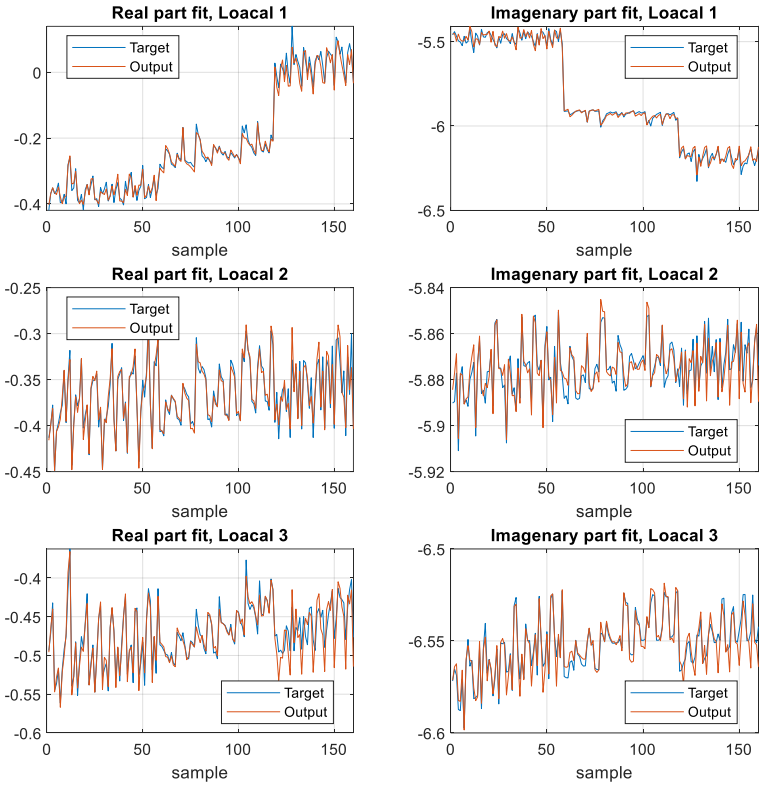


FIGURE **9.** Local modes prediction for the validation data (160 samples)

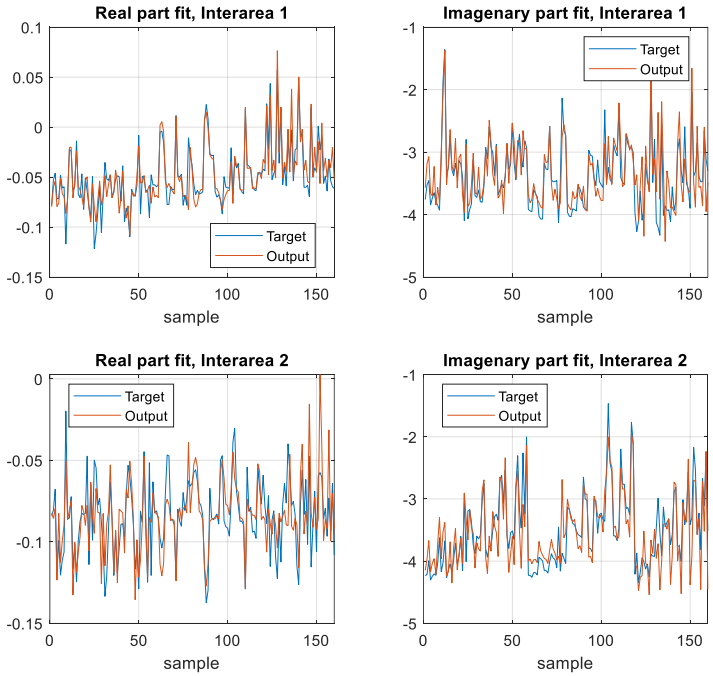


FIGURE **10**. Interarea modes prediction for the validation data (160 samples)

Figures 9 and 10 prove the effectiveness of the application of the ANN in eigenvalues' prediction using loads and generators angles. The fitting in the local-area modes is more accurate than that in the interarea modes.

3. Oscillation mode identification for partially observable system. In this section, the assumption that the first area's PMUs has a variance of (10^{-12}), the second area's PMUs has a variance of (10^{-11}) and the variance of the third area's PMUs is (10^{-10}). It supposed that the data of the SCADA system has a variance of (10^{-6}). Based on these assumptions, the measured data of each PMUs and the SCADA system are generated for all training (406 samples) and validation data (160 samples) in the previous section.

Based on [16], the optimal PMU placement for the partially observable system by PMUs is obtained (bus 4 then 11 then 14). The three scenarios are considered here to obtain the eigenvalues from the measured data. The trained generator and load angle model in the previous section is selected here

3.1. Partial Observable System by 1 PMU. In the three-area test system, three PMUs are needed to make the system fully observable. If the system is observable by the SCADA only, the white standard error with variance 10^{-6} are added to the actual data.

For the first PMU location (bus 4 or 11 or 14), the error from PMUs is added to the measured data. the eigenvalues (real and imaginary parts) of the five modes are estimated using the trained model in the previous section. The error between the actual outputs (real and imaginary part of the eigenvalues) and the estimated are:

Table 3. One PMU in the three-area test system.

Error	True data	SCADA data	One PMU at Bus 4	One PMU at Bus 11	One PMU at Bus 14
Average absolute	0.066398	0.068022	0.066511	0.067927	0.067981
Mean square	0.009904	0.010329	0.009943	0.010299	0.010321

From the table, the optimal location of the first PMU is bus 4. The average absolute error is decreased from 0.068022 to 0.066511 by the first PMU. For all locations (Bus 4, bus 11, or bus 14), the PMU enhances the prediction of the Eigenvalues. On the other hand, the high sampling rate of the PMUs makes the prediction is effective for the transient scenarios. The mean square error is also decreased for any location, but the optimal location (minimum error) is bus 4. The results validate the OPP for partial observability-based on the participation factor of the gain matrix.

Figure 11 shows the average absolute error of the 556 samples for different PMU location. From the figure, the real part of the first local mode (output 1) and the real part of the interarea modes (outputs 4 and 5) prediction are enhanced when a PMU is installed at bus 4. The imaginary part of the interarea mode 1 prediction is also enhanced (output 9). The absolute error in output 7 (imaginary part of the third local mode) is decreased in the case of the PMU installed at bus 4, but this output is not affected if the PMU is installed at other locations.

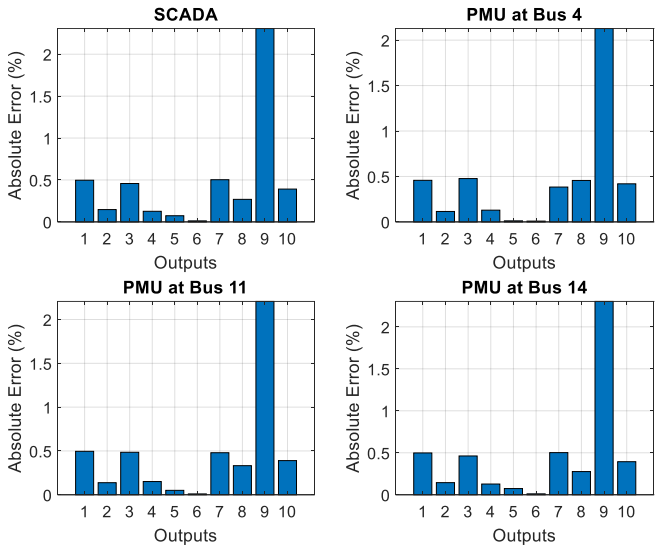


FIGURE **11**. Prediction eigenvalues error for the first PMU location

3.2. **Partial Observability System by 2 PMUs.** The first PMU is installed at bus 4. Two choices for the second PMU are available (buses 11 and 14). The average absolute error of each output prediction in these two choices is shown in figure 12. The average absolute error, and the mean square error of these locations are:

Table 4. Two PMUs in the three-area test system

Error	True data	SCADA data	PMUs at Bus 4 and 11	PMUs at Bus 4 and 14
Average absolute	0.066398	0.068022	0.066414	0.066486
Mean square	0.009904	0.010329	0.009911	0.009935

From the table, the optimal location of the second PMU is Bus 11. Once the third PMU is installed at bus 14, the average and mean square errors decrease to 0.066398, and 0.0009904, respectively. The results of the full system observability by PMUs are very close to the prediction using the true data. Figure 13 shows the average absolute error in case of the three PMUs are installed in the system (Full observable system).

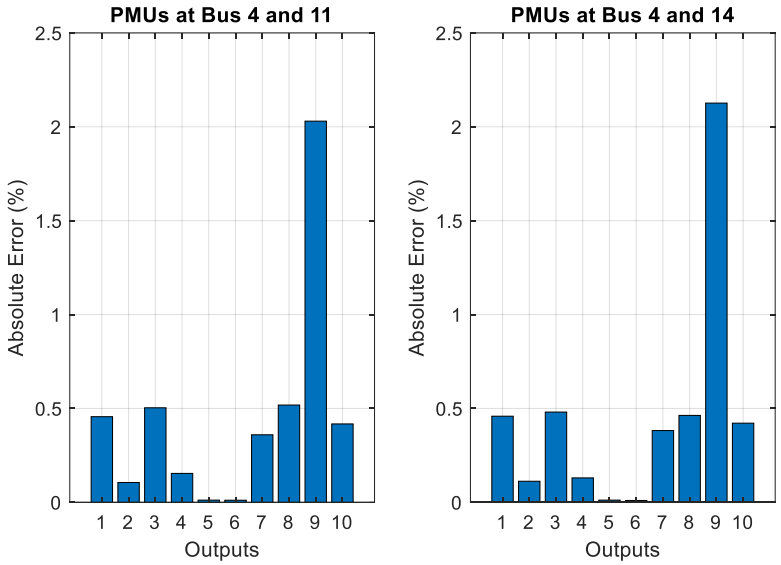


Figure 12. Prediction eigenvalues error for the second PMU location

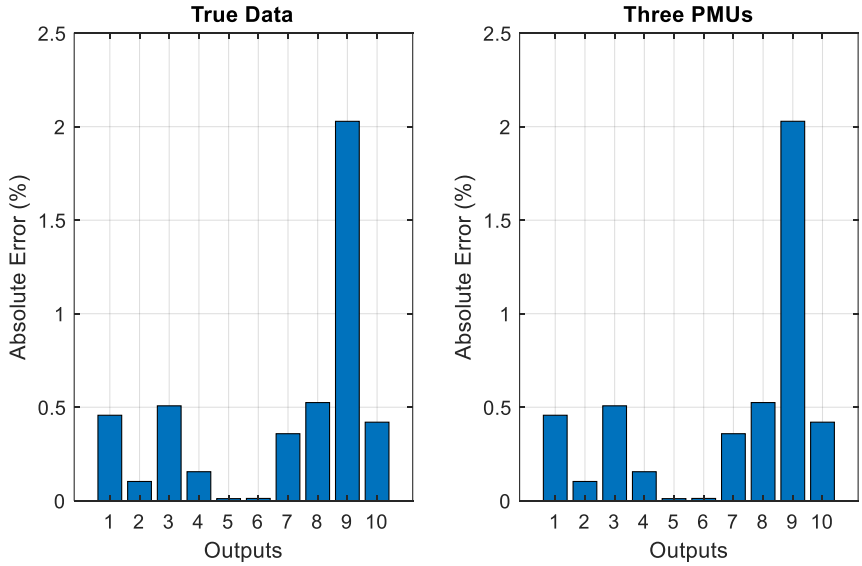


Figure 13. Prediction eigenvalues error for the third PMU location

4. CONCLUSION. In conclusion, the findings presented in this study underscore the significant potential of Artificial Neural Networks (ANN) in accurately predicting oscillation modes based on bus angle measurements obtained through Phasor Measurement Units (PMUs). The success of this prediction process is grounded in the utilization of ambient measurements, showcasing the applicability and effectiveness of data-driven methodologies in power grid stability assessment.

The results vividly demonstrate that the ANN model achieves commendable accuracy in forecasting oscillation modes, a critical facet of ensuring power system stability and resilience. This achievement is a testament to the intricate capabilities of the ANN model to harness the inherent patterns within the measured angles of buses, thereby providing a valuable tool for real-time decision-making and control in power systems.

Furthermore, this study introduces a novel approach to optimizing the sequence of PMU installations, leveraging the predictive power of the ANN-based oscillation mode prediction. By strategically placing PMUs based on the anticipated oscillation modes, system operators can enhance situational awareness and expedite response times, bolstering the overall stability and operational efficiency of the power grid.

As the energy landscape continues to evolve, the integration of advanced data-driven techniques like ANN promises to be instrumental in fortifying power system resilience and adaptability. This research contributes not only to the understanding of oscillation mode prediction but also offers practical insights into enhancing the deployment strategy of PMUs, thus heralding a new era of intelligent and predictive power grid management.

Acknowledgment. This work was supported by The Scientific Research and Innovation Support Fund (SRISF) / Jordan under project number (ENE/1/3/2020).

REFERENCES

[1] S. Okubo, H. Suzuki, and K. Uemura, ‘‘Modal analysis for power system dynamic stability,’’ IEEE Trans. Power App. Syst.*(through 1985), vol. PAS-97, no. 4, pp. 1313–1318, Jul. 1978.

[2] P. Ray, ‘‘Power system low frequency oscillation mode estimation using wide area measurement systems,’’ Eng. Sci. Technol., Int. J., vol. 20, no. 2, pp. 598–615, Apr. 2017.

[3] J. Sanchez-Gasca et al., ‘‘Identification of electromechanical modes in power system,’’ IEEE Task Force Rep., IEEE PES, Piscataway, NJ, USA, Tech. Rep. TP462, 2012. [Online]. Available: https://resourcecenter.ieeepes.org/publications/technical-reports/PESTR15.html

[4] K. S. Shim, H. K. Nam, and Y. C. Lim, ‘‘Use of Prony analysis to extract sync information of low frequency oscillation from measured data,’’ Eur. Trans. Electr. Power, vol. 21, no. 5, pp. 1746–1762, Jul. 2011.

[5] T. Sarkar and O. Pereira, ‘‘Using the matrix pencil method to estimate the parameters of a sum of complex exponentials,’’ IEEE Antennas Propag. Mag., vol. 37, no. 1, pp. 48–55, Feb. 1995.

[6] J. G. Philip and T. Jain, ‘‘Analysis of low frequency oscillations in power system using EMO ESPRIT,’’ Int. J. Electr. Power Energy Syst., vol. 95, pp. 499–506, Feb. 2018.

[7] C. Jakpattanajit, N. Hoonchareon, and A. Yokoyama, ‘‘On-line estimation of power system low frequency oscillatory modes in large power systems,’’ J. Int. Council Electr. Eng., vol. 1, no. 3, pp. 352–358, Jul. 2011.

[8] A. Almunif, L. Fan, and Z. Miao, ‘‘A tutorial on data-driven eigenvalue identification: Prony analysis, matrix pencil, and eigensystem realization algorithm,’’ Int. Trans. Electr. Energy Syst., vol. 30, no. 4, Apr. 2020, Art. no. e12283.

[9] J. R. Smith, F. Fatehi, C. S. Woods, J. F. Hauer, and D. J. Trudnowski, ‘‘Transfer function identification in power system applications,’’ IEEE Trans. Power Syst., vol.

8, no. 3, pp. 1282–1290, Aug. 1993.

[10] H. Khalilinia, L. Zhang, and V. Venkatasubramanian, ‘‘Fast frequencydomain decomposition for ambient oscillation monitoring,’’ IEEE Trans. Power Del., vol. 30, no. 3, pp. 1631–1633, Jun. 2015.

[11] T. Jiang, H. Yuan, H. Jia, N. Zhou, and F. Li, ‘‘Stochastic subspace identification-based approach for tracking inter-area oscillatory modes in bulk power system utilising synchrophasor measurements,’’ IET Gener., Transmiss. Distrib., vol. 9, no. 15, pp. 2409–2418, Nov. 2015.

[12] S. A. N. Sarmadi and V. Venkatasubramanian, ‘‘Electromechanical mode estimation using recursive adaptive stochastic subspace identification,’’ IEEE Trans. Power Syst., vol. 29, no. 1, pp. 349–358, Jan. 2014.

[13] L. Dosiek, N. Zhou, J. W. Pierre, Z. Huang, and D. J. Trudnowski, ‘‘Mode shape estimation algorithms under ambient conditions: A comparative review,’’ IEEE Trans. Power Syst., vol. 28, no. 2, pp. 779–787, May 2013.

[14] Al-Odienat, Abdullah, et al. "Low frequency oscillation analysis for dynamic performance of power systems." 2021 12th International Renewable Engineering Conference (IREC). IEEE, 2021.

[15] Gupta, Abhilash Kumar, Kusum Verma, and K. R. Niazi. "Wide-area PMU-ANN based monitoring of low frequency oscillations in a wind integrated power system." 2018 8th IEEE India International Conference on Power Electronics (IICPE). IEEE, 2018.

[16] Al-Odienat, A. I., et al. "Connectivity Matrix Algorithm: A New Optimal Phasor Measurement Unit Placement Algorithm." IOP Conference Series: Earth and Environmental Science. Vol. 551. No. 1. IOP Publishing, 2020

Jordan Journal of Energy
Volume 1, Number 2, 2023

ISSN (Online): 2790-7678
ISSN (Print): 2790-766X

Jordan Journal of Energy (JJE)
Journal Homepage: http://dsr.mutah.edu.jo/index.php/jje
JEE an official peer review journal of Mutah University,

Developing a Cybersecurity Risk Management Framework for Non-Technical Losses in National Power Distribution Companies

Abdel Rahman Alzoubaidi[1]*, Asma Najdawi[2], Mutasem Alzoubaidi[3]

*[1]Electrical Engineering department, Al Balqa Applied University, Amman, Jordan

[1]alzoubaidi@bau.edu.jo

[2] Greater Amman Municipality, Amman , Jordan

[2]najdawiasma@gmail.com

[3] HNTB corporation, Kansa City, Missori, United States

[3]malzoubaidi@hntb.com

Received 2nd July 2023; Accepted 16th August 2023

*Corresponding Author Email: alzoubaidi@bau.edu.jo

ABSTRACT. *Traditionally, power companies are the driving force behind a country's economy and disturbances in its services have severe effects. Advanced metering infrastructure (AMI) grids are vulnerable to network & web security attacks. The objective of this study is to pinpoint the risk mitigation measures that should be integrated into the electric power advanced metering grids of Jordan. The study investigates and proposes a Risk Management Framework (RMF) to minimize the risks of power fraudulent activity. AMI is vulnerable to electricity losses and hence the need to develop a system that would help mitigate this risk. To develop the RMF, we integrate security and privacy into the management activities, to assist in the organizational preparation of the processes and technologies needed for the ongoing energy system IT and OT convergence and digital transformation poses more cybersecurity concerns and essential requirements. We used the Quantitative Risk Management process utilizing the NIST RMF standards for financial risk impacts mitigation of energy losses in the AMI grid. The dependencies and influences between the dimensions considered are investigated, information gathering, and the collection of work data were carried out and used for quantitative analysis. This paper presents a pilot project study in collaboration with EDCO the developed and proposed RMF requirements, risk assessment and, finally recommends the implementation of the selected security controls for the AMI profile protection to mitigate the identified cyber risk.*

Keywords: Smart grid, AMI, Organizational Risk Management Framework (RMF), EDCO, security controls, SCADA security.

1. Introduction. In recent years, the great development in renewable energy resources and increasing of electric power demand poses new challenges on the distribution networks [1]. The present passive distribution networks (PDN) are of dual structure as they consist of substations and loads [2]. Nowadays, there is a need to convert the current PDN into an Active Distribution Network (ADN) of a ternary structure; distributed generations (DGs), substations and loads [3].

In recent years, the great development in renewable energy resources and increasing of electric power demand poses new challenges on the distribution networks [1]. The present passive distribution networks (PDN) are of dual structure as they consist of substations and loads [2]. Nowadays, there is a need to convert the current PDN into an Active Distribution Network (ADN) of a ternary structure; distributed generations (DGs), substations and loads [3]].

The future of electricity is on the Internet of Things (IoT) and recently the Internet of Everything (IoE). Traditional power grids are getting abandoned for smart and more efficient power grids [1]. According to the U.S. Department of Energy, energy reliability is one of the primary reasons behind the move toward smart grids. However, smart grids come with their challenges, such as the need to ensure cybersecurity [2]. As such, cyber security experts need to be involved in the development, and maintenance. Also, monitoring smart grids ensure maximum customer satisfaction and ensure that one of the primary sources of any country's security is maintained [3]. Energy is an essential resource for any country that wishes to ensure maximum security for its citizens, especially from external attacks [4,5,6,7].

The need to ensure cybersecurity in these smart grids is not a matter of convenience or mere speculation, given the recent attacks on various power grids by hackers. On December 23rd, 2015, in Ukraine, for example, the information systems of the three major energy distribution companies got hacked [8]]. Hackers allegedly sponsored by forces and states against the government in Ukraine successfully hacked the power grid and gained control. In the days after this, the country had no electricity, and cybersecurity professionals were the ones who helped to bring the electricity back online. The hack on Ukraine's power grid marked the first-ever successful hack on a power grid, and it marked the turning point in how countries viewed the need to have secure power grids [9,10]. The latter becomes more important with the move to use smart grids in most countries.

The example above about a hack in Ukraine's power grid for political reasons is an extreme one to show why cybersecurity is essential for any power grid. However, there are other lesser reasons why it is vital to protect power grids from intrusion. One such reason is to ensure that energy there is no theft. Smart grids work using advanced metering where the consumers are charged depending on their usage, and the electricity cuts itself off if the subscription of the consumer is depleted. However, malicious consumers and intruders might override such instructions and steal energy from the grid. In addition to this, using a smart grid requires that

consumers share their personal information, and this information might get stolen [7] which poses a risk.

Jordan has appreciated the need to use smart grids in its energy distribution. To this end, the Jordan Electrical Power Company is responsible for distributing about 66% of the country's energy consumers, and it intends to use advanced metering systems. Given that energy theft is one of the significant cybersecurity issues that would face such a smart grid, it is crucial to assess the possible vulnerabilities and possible solutions to mitigate this risk [11,12,13,14].

In summary, the critical issue in this study is to investigate the advanced metering infrastructure from an energy theft perspective. Energy theft is one of the most important reasons to implement risk cybersecurity management for energy power distribution in Jordan. The study will also explore the control measures that power companies can take to manage cyber risk to reduce theft energy risk. It will also assess the physical and digital attack surface and vulnerabilities associated with each AMI then make recommendations for appropriate security requirements.

The organization of the rest of this paper are as a follow, in section 2 background, related work in section 3, RMF AMI pilot project in section 4, Finally, the results and conclusion are presented in section 5.

2. Background

2.1 Motivation

The Energy and Minerals Regulatory Commission (EMRC) is responsible for regulating and monitoring the energy sector, generation, transmission, distribution, and electricity supply. EMRC recorded 19,962 cases of electricity theft in 2018. Also, Law enforcement personnel at the EMRC recorded 10,443 cases of theft, while employees at the three electricity distribution companies discovered 6,768 cases [12,13,15]. This month's report on the largest electricity and water theft in the Kingdom, which will now get submitted to the Judicial Authority, stipulated that the thief must get fined 2.7 million JOD. Finally, last month, a joint force of the Public Service Directorate and Gendarmerie seized equipment worth 300 thousand JOD used to embezzle electrical power. The above formal reported issues constitute the driver motivations for conducting this empirical research. Conducting this empirical research will help provide a solution to mitigate the energy theft problem in the Kingdom of Jordan [12,13,15].

2.2 Project Description

The project objective is to conduct pilot project research to investigate electricity losses being the leading concern for power distribution companies for decades. Power distribution companies throughout the world are trying various new methods for detecting electricity non-technical loss. In combination with the innovation in information and communication, technologies Cyber Security threats, more unique and effective non-technical losses detection methods recommended by NIST aiming to implement RMF in the Jordanian power distribution companies to mitigate the risks affecting the smart grid infrastructure. The proposed development and implementation process of risk analysis solution allows for the practical consideration of

potential risk determinations. For this pilot project, the Quantitative Risk Management process methodology is employed utilizing the NIST RMF risk mitigation of energy loss in AMI.

3. Related work

Previously various studies have been conducted on smart electricity grid protection against theft and other malicious activities associated with cybersecurity. These projects and studies have identified various vulnerabilities in smart grids and solutions to these vulnerabilities. Langer, Skopik, Smith, and Kammer stetter assessed cybersecurity issues that face smart grids as they evolve from the traditional forms of electricity grids to the new types of smart grids [3]. The researchers understood that smart grids are made of various ICT components that are all vulnerable to theft and other malicious activities. In their article, the researchers sought to provide a solution to assess any possible cybersecurity issues with these smart grids. The researchers recommended a two-stream risk assessment method to determine the various risks in a given smart grid. The research suggested covered both the existing components and the near future developments of any current system. Fig.1 represents the model that the researchers recommended.

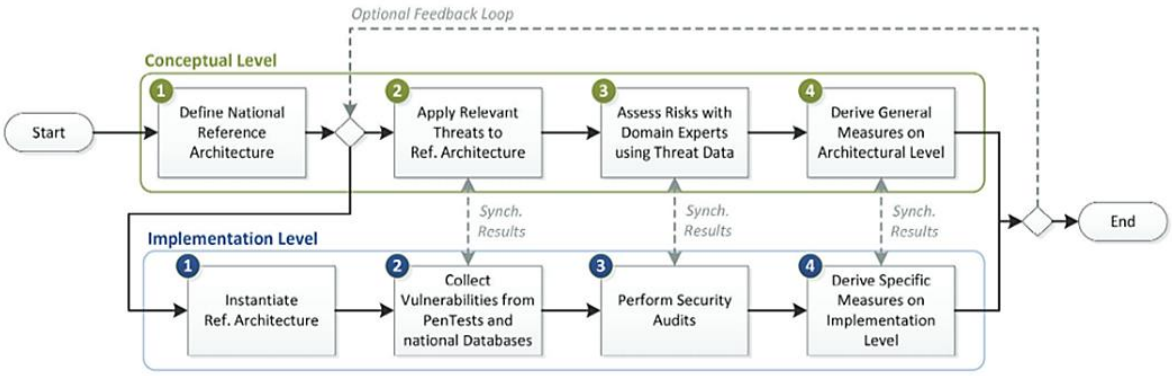


FIGURE. 1. Conceptual and implementation-based risk assessment in several interrelated steps [3].

The above method got implemented in Australia, and it was also evaluated in the course of the Austrian Research Project. The level of threats in smart buildings, e-mobility, customer premises, low-abvolt generation, medium-abvolt generation, grid test points, primary substation, secondary substation, grid service, and metering were all identified using this assessment process. Authentication, authorization, security mechanisms, integrity, availability, internal and external interfaces, confidentiality, data protection, system maintenance, and system monitoring were among the risks found. This method can be a great place to start while assessing the Jordan electricity grid risks.

In their research, Mathas et al. explored the problems of Advanced Metering Infrastructures (AMI) [5]. The scientific and industrial progression through installing smart meters has

increased the demand side of technical and security risk management. Smart meters are an essential element of the AMI, where they enable two-way data communication between service users and utilities provider. The smart meter's real-time measurements generate a large volume of data that can be quickly transmitted to customers. Consumers may benefit from the smart meter's soundless functionality, but security issues and threats are significant problems and risks that should be tackled. Consumers will be unable to use the excellent features provided by smart meters if they are not properly prepared and risk-managed. The feasibility, investment, and need to preserve an acceptable degree of privacy through cybersecurity risk management must all be considered during implementation.

Khattak, Khanji, and Khan also understood the possibility of vulnerabilities in smart meters, given that the Internet of Electricity was getting appreciated by energy companies and governments [2]. Given the advanced metering infrastructure implementations, the researchers decided to investigate the cybersecurity concerns in the increasingly complex smart energy grids. The researchers identified the AMI security issues as smart meter security, data collector security, communication, and network security. The paper suggested the following security control and countermeasure. a) Having the smart meters encrypted that protecting the communication between devices and networks. It would also help to reduce the chances of data and information security getting compromised. b) Authentication mechanism serves the same purpose as smart grid encryptions and ensures that only authorized people have access to critical controls and information in the energy networks, c). The availability mechanism ensures that the availability of the AMI infrastructure does not get compromised through vulnerabilities such as network jamming and packet flooding, and d). Jamming prevention mechanism to help with preventing the jamming vulnerability technique that malicious people might use on the AMI devices and networks. This study is essential for this research since it gives direction on some of the vulnerabilities to look for when assessing the Jordan electric grid and possible solutions for these cybersecurity issues.

Yadav, Kumar, Sharma, and Singh conducted a study to determine the possible cybersecurity issues in smart grids and the possible solutions to these problems [11]. The researchers understood that given that smart grids rely on IoT, various cybersecurity issues must get addressed. The researchers identified the protection of consumer information, system availability, integrity and reliability, and confidentiality as some of the key cybersecurity issues that face the Smart grids. The researchers identified that the key goals of any smart grid cybersecurity are the availability of service, the confidentiality of data, and the integrity of the information shared. The researchers determined that the security of the smart grids would get compromised through 5 main methods, the use of malware, unauthorized access by internal users, the use of replay or repeat false messages, traffic analysis, and DoS attacks. The researchers suggested that the other cybersecurity measures for protecting networks ensure that the above methods do not work on a given smart grid. However, the researchers identified that this is only related to providing the users with efficient electricity availability, protecting their data, and focusing less on other security concerns.

Nonetheless, this is not the first study to identify energy theft as a possible issue in ensuring the cybersecurity of smart grids. Lopez, Sargolzaei, Santana, and Huerta also conducted a study to determine the threats and countermeasures present in smart grids when it comes to cybersecurity and identified energy theft as a possible threat facing smart grids [4]. According to researchers, the intention to steal energy from the grid will interrupt measurements before taking place, tampering with the stored data before, when, or after the measurements have been taken and stored in the meter. Also, one might modify the networks before or during the data logging by the meter. It is thus imperative to ensure that smart grids get protected against energy thefts. The use of theft detectors was the researchers' approach to the issue of energy theft. Theft detectors work by determining the average use of electricity per day against a certain predetermined threshold to assess whether electricity is stolen. If the average use is less than the minimum threshold per day, the assumption is that the energy is stolen.

McLaughlin, Pdkuiko, and McDaniel [6], and [1] went further than Lopez, Sargolzaei, Santana, and Huerta to demonstrate where energy theft might take place in a given smart grid [4]. McLaughlin, Pdkuiko, and McDaniel studied the phenomenon of energy theft in advanced metering structures and found vulnerabilities that help malicious people steal energy [6]. Byres, Franz, and Miller, on the other hand, investigated the phenomenon of vulnerabilities in the SCADA systems using attack trees [1]. When the two are combined, it becomes easy to see the various stages in which malicious persons might steal energy from the systems. Using the concepts developed by [6] and [1] to investigate energy theft would be helpful for this research since it creates a benchmark and a body of knowledge in which the research can progress. The studies by [6] and [1] were limited in that they did not focus on the specific circumstances surrounding Jordan's energy networks and the possible solutions for these energy theft vulnerabilities.

Perhaps, one of the best solutions offered to counter energy theft in smart power grids is provided by Sun, Hahn, and Liu [9]. According to Sun, Hahn, and Liu, various cyberattacks have happened that focused on AMI, including energy theft. The researchers concentrated on energy theft caused by network intruders from external interfaces including smart meters and information hackers. To address the issue of cyber-attacks, the researchers recommended using Anomaly and Intrusion detection systems (ADSs) [9]. These ADSs detect any type of anomaly or possible intrusions in the system and communicate them, alerting those people tasked with ensuring the security of the smart grid system. [1] presented a technique, This report, which focuses on the known sources of AMI threats, offers a holistic view as to how various security issues contribute to electricity theft being addressed. Future research should look at each of the known sources of threats in greater detail, and then apply suitable intelligent algorithms to evaluate data to create a model for timely decision support. [22]..

Summary

The above studies describe the research conducted in line with ensuring the cybersecurity of smart grids. The studies show the different methods and techniques used to detect security threats or possible intrusions and the solutions for ensuring that these security threats and

possible intrusions repetition. Given that this study seeks to focus on Jordan, these papers will form a basis for the following research areas, including offering solutions to the vulnerabilities identified in Jordan AMI that may enable intruders to steal energy.

4. RMF AMI pilot project

This pilot project is ongoing research on the Jordanian Power Distribution Companies (PDC) to investigate electrical losses risk mitigation. due to cyber-attacks for the evolving national Smart Grid components implementation and grid digitalization. As a follow-up to our research field of interest, we are harnessing our studies to solve national problems in the field of cybersecurity for energy distribution in Jordan. This pilot research will propose and implement RMF for selected security controls to mitigate risks at the AMI. The RMF developed a risk-based approach process study that incorporates cybersecurity and privacy into the company management activities to aid in the organizational preparation of the processes and technology required to meet the energy system digitalization transformation requirements. The goal is to install smart grid AMI grid security controls on the electric grid for securing a designated region.

4.1 The Study Preparation

This research is carried out along with the agreement and authorization of the Electricity Distribution Company (EDCO) to provide the data and unclassified information and resources for a limited pilot project aimed at RMF implementation. The preliminary kick-off meeting is headed by the company's former General Director and attended by the director-general deputies for administrative, technical, and planning affairs and the concerned CEOs.

National PDCs, EDCO alike various worldwide, is facing electricity theft and bribery in electricity usage as the two most serious issues facing PDCs. The broadness, security, and privacy of these issues limited the scope of the study to a partial RMF controls selection and implementation; other issues and controls are considered for any future collaborative work.

Accordingly, data & information collection was achieved via several meetings with CEOs, department teams, staff, and published reports by national energy stakeholders to lay the floor to collect the data for the scope of this pilot project, making use of the company IT unclassified resources. EDCO has a mandate for distributing electrical energy purchased from the National Electric Power Company (NEPCO) to the southern part of Jordan, the Jordan valley, and many rural areas in the country, operating different transmission and distribution electricity voltages to end-user facilities. This pilot project's scope is restricted to investigating energy losses caused by SMI devices network equipment for a selected area in the company service coverage areas as a model to develop and recommend the RMF to be approved and implemented in phases to mitigate loss risk.

Typically, energy distribution companies, and EDCOs alike, have massive data gathered in their electricity distribution network databases to monitor, control, and manipulate, among other issues, it's Smart Grid electrical loss.

An electrical loss gets caused by resistance in the flow of electric current in electrical networks and transformers. The loss is influenced by the square of the value of the electrical load flowing through medium and low-voltage networks. The voltage at which the networks get operated also affects it. If the current and voltage increase, so the electrical loss increase. Table 1 represents the real electricity loss rates on medium and low voltage networks in EDCO electricity distribution company (2018-2020) [12,13,15].

Table 1 and Fig. 2. shows the company's electric loss rate for 2018 and 2019 was (11.88%), which was higher than the (11.32 %) allowed by the Electricity Sector Regulatory Authority for the tariff period (2018-2019) without penalties. It also shows; that in 2020 the electricity loss increased to (12.88%), consequently exceeding the allowed limits and resulting in financial losses. The loss rate on low voltage increased from (8.2%) in 2018 to (8.6 %) in 2019, while the percentage of loss on MV networks increased from (4.0 %) to (4.5 %) compared the year 2018, 2020 the MV increased to (5.58%). The increased MV and LV are the impact of COVID-19.

Table 1. Electricity loss rates on medium and low voltage networks

Total losses	MV	LV	Year
11.88%	**4.0%**	**8.2%**	**2018**
11.88%	**4.5%**	**8.6%**	**2019**
12.88%	**5.58%**	**5.55%**	**2020**

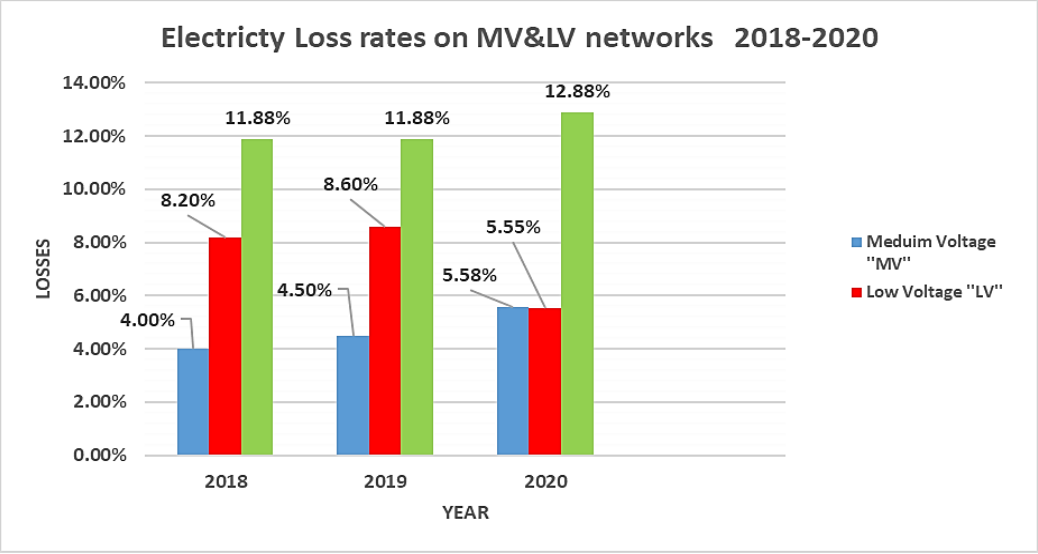


FIGURE. 2. Electricity loss rates on medium and low voltage networks

The company reported a loss rate of (12.88 %) in 2020, an increase from the previous year's loss rate of 11.88 %, and the reasons for this increase are due to the circumstances of the COVID-19, full and partial closures in the Kingdom of Jordan, which have directly affected the increase in electrical loss rates. That reduced the implementation plans to reduce non-technical losses, which led to an increase in the loss by (0.5%) and the most important of these procedures. Increased network tampering and attacks in 2019 were 569 cases, while in 2020, it increased to 710 cases. The latter was a result of customers' behavior and difficult financial circumstances. Also, it was caused by a lack of monitoring, decreased inspection, and detection due to closures and injuries to company staff. Particularly during the first phase of the pandemic, as this resulted in a decrease in the number of meters identified. It also caused an increase in cases of tampering, particularly given the company's inability to take any action, particularly at the stage of complete closure.

During the year 2019, the company worked to make all possible efforts to reduce electrical losses in all its forms through the following:

- Identifying the electrical feeders and areas in which the electrical loss exceeded the performance indicators and determining the necessary measures to reduce the losses on these feeders and regions. The company has implemented several major projects to improve the performance of electrical networks and contribute to reducing electrical loss in the company according to the loss reduction plan.
- To prevent tampering and misuse, the company conducted procedures for the detection and inspection of subscriptions, as well as prosecutions of cases of tampering, in cooperation with the Commission's judicial police and security authority (Public Security and the Gendarmerie), and filed an invitation with the courts. In 2019, there were 892 cases, and in 2020, there were 882 cases.

4.2 Security Control

The presented recommendations are a cornerstone step to studying losses by specifying criteria for cyber-physical and knowledge networks in smart grids. Cybersecurity controls for protections, safeguards, or defensive measures (processes, protocols, applications, procedures, or even other intentions) intended to protect a system or its resources from cyberattacks[17,18,24].

Also, to investigate and characterize principles that define selected cybersecurity controls applied to AMI to protect the smart grid, essential for the RMF development and implementation in the allocated region.

Security controls can be classified as management, technical and operational controls. Management controls apply to problems that management must deal with, and focuses on security policy, preparation, guidelines, and requirements that influence the set of organizational and technological controls to reduce risk and protect the purpose of the company. The proper use of device hardware and software protection capabilities are examples of technical controls, steps that perform in parallel to protect critical and sensitive data, information, and I.T. system functions [16]. Establish automated protection against unauthorized access or misuse, aid in identifying security breaches, and support application and data security standards. Operational controls are mainly concerned with implemented and executed processes by those responsible for the system's use. Operating controls aim to enhance

the security of a specific technique or group of systems and are often based on management and technical controls [25].

The smart grid is a complicated system of systems, and to secure its mission of efficient power delivery, it needs more than one layer of security controls. Physical fences and surveillance cameras are only a few of the security controls available, as are encryption algorithms and digital certificates. Applying these security controls on the smart grid prevents the unauthorized disclosure of information, ensures that the information was not modified by an unauthorized source, and ensures that the services and information are available when a user or system requires them. Confidentiality, Integrity, and Availability (CIA) are the priorities of every physical or information security program.

The fact that the smart grid would include both legacy and advanced technologies is an added challenge, making defining the specifically required security controls, and where to put those security controls a difficult decision. The evolving nature of information flow in a smart grid network, as well as new applications for that information, further complicates the security landscape [26].

4.3 Security Controls for AMI

Smart Electricity Meters (SEMs) installation at both client's end and substations is part of Smart Grids' modern digitalization of energy usage and costing scheme, which is controlled by the AMI. The latter supports the bidirectional data connectivity between SEMs and utilities, allowing for the development of a smart grid for the PDCs. The AMI is controlled and managed via instructions in real-time transmission the consumption data, and pricing information to both the utility company and the consumer. The SEM, customer gateway, verbal communication network, and headend are all components of AMI networks. Energy-related data is recorded and communicated by SEMs. Typically, they get arranged to record and supply customers' power usage and billing data at regular intervals, typically every minute.

The client gateway connects the AMI network to customer systems and appliances. This network acts as a connection between the SEM and the AMI headend, permitting transmitted data to flow in both directions. Normally such connections are implemented utilizing Virtual Private Networks (VPN), Fiber, or wireless connections communication technologies owned, controlled, and managed by a third party. AMI security standards, threat sources, and SEM attacks all aim to manipulate data and are major cyber security concerns, although it jeopardizes revenue and customer privacy. Moreover, it is also capable of harming the overall operations of the power grid. Fortunately, the presence of these assaults and other criminal actions such as unauthorized procurement processes, sale, and manipulated equipment by company employees, involvement with consumers, typically via third parties, to commit energy thefts, and the illegitimate purchasing and selling of reserved vouchers. The existence of compromised data in the AMI indicates this. AMI Communications Network serves as a link between the SEM and the AMI headend, allowing data to flow back and forth.

As a result, the protection methods to cope with AMI data, similar to those used to secure data in general, are justified based on access control, analysis and feedback, authentication, authorization, availability, confidentiality, integrity, non-repudiation, privacy, and accountability.

Confidentiality, integrity, availability, and non-repudiation are the four basic AMI specifications (CIAN). However, the continued operation of CIAN is jeopardized due to cyber-attacks, which usually seek to disrupt the AMI for energy theft. Risks to AMI's CIAN mitigation

occur in two ways: Viz ensuring the AMI's security requirements are maintained. Furthermore, automatically restored after any security breach or through diligent identification of threat sources [18]. Finally, the eventual following is that relevant models and algorithms are used to manage the parameters of the required systems. It is worth noting that an indication of a violation or threat indicates you have failed to meet all the CIAN's requirements; additionally, analyzing the threats and attackers offers more useful information for proper device management and surveillance [24].

Control is defined as an operation, process, method, or another measure that eliminates damage by avoiding or stopping a security breach, mitigating the risk it can inflict, or finding and revealing it such that corrective action is taken.

When analyzing the smart grid and security to identify Smart Grid Security Controls, it is crucial to determine what needs to be protected and why protection is so critical. The global power grid comprises various technologies and components, and electric utilities have evolved several business practices to ensure the reliable delivery of electricity [19].

AMI Security Profile provides a collection of baseline controls for safeguarding the AMI components. The controls are the outcome of a four-phase procedure that entails the following: 1) smart grid use cases assessment 2) risk assessment, 3) domain analysis, and 4) analyzing and adapting national authority-specified controls. The collection of security measures is comprehensive. Aside from its definition, each step includes an explanation for adoption and, where applicable, future improvements or supplementary guidelines [24].

4.4 Risk Management Framework Methodology

Research methodologies used for cyber security risk are the study of the documents of the act’s norms, international standards, procedures, international legislation, content analysis, comparative methods, and statistical and graphical presentation methods. Information gathering and the collection of work data were carried out by using the statistics of operational plans, risk analyses, and operational procedures. This contribution is the result of the above method in the form of a pilot project research methodology. This interactive research methodology has two parts: investigation and achievement, to establish the practice's progress based on the learning of individuals and workgroups. This pilot study provides the research team and others with a better insight into the problem and potential solutions. The NIST Special Publications 800-53 Rev.4 & Rev.5 to control the security and privacy of information systems, organizations' standard and compliance framework are continuously updated that attempts to flexibly define standards, controls, and assessments based on risk, capabilities, and cost-efficiency, [31]. The NIST SP 800-53 rev4, NIST SP 800-82, and AMI security profile structures, as well as the associated practice standard and controls for risk reduction, provided the theoretical basis for this proposed risk management approach. The selected used rules to perform a quantitative risk analysis, plan risk responses; and apply controls to mitigate risks for this pilot case project are presented in Table 2.

This section includes the pilot project chosen security controls guidelines from the Industrial management and Automation Systems Security measures (IACS) and NIST. IACS is an important part of the smart grid because it tracks and controls industrial processes in the entire power supply chain, from generation to disruption. As shown in Table 2, their safety is critical to the proper functioning of the power grid. Although this pilot project does not include all the smart grid's command and control areas, the security principle remains the same. When

implementing a control command, the control system must know that the command is transmitted from an authorized and authenticated source [24].

TABLE 2. Cybersecurity NIST controls specified in power systems' standards.

NIST SP 800-53 Rev.4	NIST SP 800-82	Security Profile for AMI
Access control	Access control	Access control
Audit and accountability	Audit and accountability	Audit and accountability
Awareness and training	Awareness and training	System and communication protection
Identification and authentication	Identification and authentication	System and information integrity
System and communications protection	System and communications protection	System development and maintenance
System and information integrity	System and information integrity	Information and document management

Security measures and practices specific to IACS

Table 3 shows general implementation standards for security controls and procedures, IACS adoption, smart grid adoption, and AMI adoption.

TABLE 3; general application standards within an AMI smart grid security control

NIST SP 800-53
NIST SP 800-82
Security Profile for AMI

4.5 NIST SP 800-53 rev4

Security and Privacy controls for AMI data systems and organizations lay out a foundation of controls for securing information systems in government, based on a variety of statutory and regulatory documents, guidelines, and business criteria. Policy formulation and management, awareness and training, contingency planning, incident response, staff protection, systems procurement, and other security aspects are addressed by the controls, which are organized into 18 families that represent unique security topics. Furthermore, it devotes a substantial portion of its material to illustrating the control selection process, which can be used as part of a risk management strategy.

4.6 NIST SP 800-82

Limiting physical access to IACS networks and reducing access to IACS networks (e.g., through network isolation, DMZ, multilayer, access control), protecting against vulnerabilities, detecting security incidents, maintaining a multidisciplinary security unit, successful networking and information sharing, fault tolerance, graceful decay, device restoration, and defense-in-depth are some of the Key protection priorities identified in NIST SP 800-82. As an outcome, an IACS defense strategy can include IACS-centric policies and procedures, knowledge and training, security across the life cycle of IACS components (from design to disposal), a multi-layered

network with critical operations performed in the most protected subnetwork, and other elements derived directly from security objectives. The paper goes through each of these points in detail.

4.7 Electricity Regulatory Framework in Jordan

Jordan has laws and regulations governing the responsible use of nuclear energy and general electricity. The safe use of nuclear energy issues in April, has provisions for authorization, disposal of radioactive material, emergency preparation requirements, administrative sanctions, inspection, safeguards, safety responsibilities, liabilities and punishment, enforcement, and physical protection. It is important to follow the stipulated regulations when dealing with nuclear energy sources, given their toxicity and lethality in case they are not handled well. These are enforced with the help of the Jordan Nuclear Regulatory Commission, which was established in 2007. The rules used to regulate the nuclear energy climate in the country follow the IAEA safety standards, and EU, USDOE, CNSC, IRSN, and KINS commissions to ensure the responsible use of nuclear energy[14].

The general Electricity Law concerns the illegal use of the electrical system, unlawfully connecting, stealing electrical power, or even assisting a person in such activities will result in imprisonment from 6 months to two years. Other Punishments that one might also face include fines of less than two thousand dinars but not more than 10,000 dinars or both imprisonment and a fine. Sabotage will result in imprisonment for a period of one month to one year or a fine of fewer than 500 dinars (not more than 2,000 dinars) or both imprisonment and fine. Negligence results in one week's imprisonment to three months or a fine of not more than 500 dinars or both imprisonment & fine.

These general electric laws are regulated with the help of the EMRC. Electricity tariffs, payment fees, service fees, disbursements, royalties, and link charges to the transmission and distribution system are all determined by the Electricity Regulatory Commission, which was instituted in 2001.

5. Results and conclusion

Figure the RMF framework proposed in this pilot project results from an actual initiation process in which the company team and the researcher (research team) worked together consciously. Losses for real-time data processing over three years. The RMF, as well as the assessment processes for cybersecurity-related threats and mitigation management methodologies, as well as active project team participation, aids the study in becoming more successful in risk management methodology adjustments.

Because of the pilot project's limitations, development and implementation are limited to; General application requirements measures and procedures that specify cybersecurity areas and controls, with the adoption of a smart grid and Security Profile for AMI profile summarized in appendix A [29].

Adapted from NIST 800-53 shows a set of guidelines for conducting security and privacy control assessments for information systems. We recommend systematic assessments, performed in phases for the system implementation. The access control family catalog procedure to assess the security controls and control enhancements in NIST Special Publication 800-53, Rev. 4 & Rev. 5 protection and privacy controls.

The implemented procedures are adaptable and customizable, allowing the company to conduct security and privacy control assessments that aid internal risk management processes and are

coherent with the company's acceptable risk tolerance, aiming to develop effective protection and privacy evaluation plans with this information.

5.1 Future Work

The recent annual 2021 report of The National Electric Power Company (NEPCO) stated that the Company's accumulated losses amounted to JD 5,135,023,755 as of 31 December 2021, which exceeds 75% of the paid-in capital. This report is another strong motivation fueling the researcher to undergo this vital research challenge that needs continuous risk assessment, identification & mitigation. Also, Jordan's PDC undergoing digital transformation activities ought to improve its cybersecurity strategies. A Risk Management Plan is needed to guide the project team and managers during the implementation and development of the RMF cyclical process to incorporate principles of security and risk management into the organization's system policies and procedures. A defined document for the RMF Plan that collects all necessary and valuable information for the researcher to manage the appropriate risks, including the RMF objectives and tolerances, the identified methods, strategies, and procedures to detect, assess, plan responses, monitor and control risks, utilizing the defined models to use.

To expand the RMF development and implementation with continuous improvements, extra information from the company team may be required to identify the security requirements and utilize a systematic asset assessment required for RMF practices by acquiring knowledge and encouraging them to engage in the risk management process' phases and feel their contribution in the improvements through effective engagement.

A risk Monitoring and Control process for implementing risk mitigation plans, controlling identified risks, monitoring risks, identifying potential risks, and evaluating the efficacy of risk management systems that have been put in place.

A further direction is to study SCADA security risks associated with data communication networks utilizing Virtual Private Network (VPN) connectivity to connect the AMI and SEMs grids. VPN data communication security on the public network is based on the CIA triad concept in network security. To investigate when VPN may be used, and when to recommend the use of VPN to have protected communication based on anonymity communication. Also SCADA, OT (Operational Technology), and IT (Information Technology) systems have become increasingly interconnected, creating new cybersecurity threats and vulnerabilities.

5.2 Research limitations

As predicted, some challenges arose during the pilot project's implementation and creation of the RMF methodology due to the adoption of a new practice. These challenges were due to the following factors: novelty, the timing of the research study during COVID-19 together with staff working remotely from home; restricted time available; and public awareness of the importance of cybersecurity and risk management. As an innovative approach, the suggested technique, method, and procedures were placed on the project team.

Acknowledgment. This work has been carried out during a sabbatical leave granted to the author Abdel Rahman Alzoubaidi from Al-Balqa' Applied University (BAU) during the academic year 2021-2022. I would like to thank the EDCO power distribution company general

manager, deputies, and engineers for their support and assistance in providing the data & information to complete this project.

REFERENCES

[1] B. S. Munir, A. Trisetyarso, M. Reza and B. S. Abbas, Application of Artificial Neural Networks for Power System Oscillation Prediction, *ICIC Express Letters*, vol. 13, no. 9, pp. 815-822, 2019.

[2] L. M. W. G. Fan Zhang, An Integrated Wide Area Protection Scheme for Active Distribution Network Based On Fault Component Principle, *IEEE Transaction on Smart Grid*, vol. 10, no. 1, pp. 392-402, 2019.

[3] V. F. Martins and C. L. T. Borges, Active distribution network integrated planning incorporating distributed generation and load response uncertainties, *IEEE Transactions on Power Systems*, vol. 26, no. 4, pp. 2164-2172, 2011.

[4] X. Chen, Y. Li, M. Zhao, A. Wen and N. Liu, A coordinated strategy of protection and control based

[5] C. Chandraratne, W. L. Woo, T. Logenthiran and R. T. Naayagi, Adaptive Overcurrent Protection for Power Systems with Distributed Generators, *2018 8th International Conference on Power and Energy Systems* (ICPES), 2018.

[6] J. Ma, X. Xiang, R. Zhang, J. L. a. P. Li and J. S. Thorp, Regional protection scheme for distribution network based on logical information, *IET Generation, Transmission & Distribution*, vol. 11, no. 17, pp. 4314-4323, 2017.

[7] J. Bertsch, C. Carnal, D. Karlson, J. McDaniel and K. Vu, Wide-Area Protection and Power System Utilization, *Proceedings of the IEEE*, vol. 93, no. 5, pp. 997-1003, 2005.

[8] M. N. Alam, S. Chakrabarti, A. Sharma and S. C. Srivastava, An Adaptive Protection Scheme for AC Microgrids Using μPMU Based Topology Processor, *2019 IEEE International Conference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe* (EEEIC / I&CPS Europe), 2019.

[9] Shalini, S. R. Samantaray and A. Sharma, Enhancing Performance of Wide-Area Back-Up Protection Scheme Using PMU Assisted Dynamic State Estimator, *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5066-5074, 2019.

[10] E. J. Holmes, *Protection of Electricity Distribution Networks*, 3rd Edition, 2011.

[11] E. J., Byres, M., Franz, & D. Miller. (2004, December). The use of attack trees in assessing vulnerabilities in SCADA systems. In Proceedings of the international infrastructure survivability workshop (pp. 3-10). Citeseer.

[12] A. M., Khattak, S. I., Khanji, & W. A. Khan, (2019, January). Smart meter security: Vulnerabilities, threat impacts, and countermeasures. In International Conference on Ubiquitous Information Management and Communication (pp. 554-562). Springer, Cham.

[13] L., Langer, F., Skopik, P., Smith, & M. Kammerstetter, (2016). From old to new: Assessing cybersecurity risks for an evolving smart grid. computers & security, 62, 165-176.

[14] C., Lopez, A., Sargolzaei, H., Santana, & C. Huerta (2015). Smart Grid cybersecurity: An overview of threats and countermeasures. Journal of Energy and Power Engineering, 9(7), 632-647.

[15] C. M., Mathas, K. P., Grammatikakis, C., Vassilakis, N., Kolokotronis, V. G., Bilali, & D. Kavallieros, (2020, August). The threat landscape for smart grid systems. In Proceedings of the 15th

International Conference on Availability, Reliability, and Security (pp. 1-7).

[16] S., McLaughlin, D., Podkuiko, & P. McDaniel, (2009, September). Energy theft in the advanced metering infrastructure. In International Workshop on Critical Information Infrastructures Security (pp. 176-187). Springer, Berlin, Heidelberg.

[17] M., Nabil, M., Ismail, M., Mahmoud, M., Shahin, K., Qaraqe, & E. Serpedin, (2019). Deep learning-based detection of electricity theft cyber-attacks in smart grid AMI networks. In Deep Learning Applications for Cyber Security (pp. 73-102). Springer, Cham.

[18] S., Saini, R. K., Beniwal, R., Kumar, R., Paul, & S. Saini, (2018). Modeling for improved cybersecurity in Smart distribution system. International Journal on Future Revolution in Computer Science & Communication Engineering, 4(2), 56-59.

[19] C. C., Sun, A., Hahn, & C. C., Liu, (2018). Cybersecurity of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems, 99, 45-56.

[20] L., Streltsov, (2017). The system of cybersecurity in Ukraine: principles, actors, challenges, accomplishments. European Journal for Security Research, 2(2), 147-184.

[21] S. A., Yadav, S. R., Kumar, S., Sharma, & A. Singh, (2016, February). A review of possibilities and solutions of cyber-attacks in smart grids. In 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH) (pp. 60-63). IEEE.

[22] Ro'ya daily newspaper, https://en.royanews.tv/news/14184/The-shocking-consequences-of-electricity-theft-in-Jordan, retrieved 8/3/2021 Published: 2018-05-06 10:31

[23] Alghad daily newspaper, https://alghad.com/jordans-biggest-power-theft/, retrieved 8/3/2021

[24] Jordan Regulation Commission. 2020. https://web.archive.org/web/20120617064232/http://www.jnrc.gov.jo/About.html

[25] Jordan time's daily newspaper,https://www.jordantimes.com/news/local/15511-power-theft-cases-reported-first-10-months-year-%E2%80%94-emrc retrieved 8/3/2021

[26] Gueltoum Bendiab, Konstantinos-Panagiotis Grammatikakis, Ioannis Koufos, Nicholas Kolokotronis, Stavros Shiaeles: Advanced Metering Infrastructures: Security Risks and Mitigation, https://doi.org/10.1145/3407023.3409229, The 15th International Conference on Availability, Reliability, and Security (ARES 2020), Dublin – Ireland

[27] A. k., Masood "Smart Meter Security: Vulnerabilities, Threat Impacts, and Countermeasures," May 2019, https://www.researchgate.net/publication/333305127_Smart_Meter_Security_Vulnerabilities_Threat_Impacts_and_Countermeasures

[28] I., Mkpong-Ruffin, D., Umphress, J., Hamilton, & J. Gilbert (2007, October). Quantitative software security risk assessment model. In Proceedings of the 2007 ACM workshop on Quality of protection (pp. 31-33).. DOI: 10.1145/1314257.1314267.

[29] J., Yao, P., Venkitasubramaniam, S., Kishore, L. V., Snyder, & R. S., Blum, (2017, March). Network topology risk assessment of stealthy cyber attacks on advanced metering infrastructure networks. In 2017 51st Annual Conference on Information Sciences and Systems (CISS) (pp. 1-6). IEEE.

[30] R. W., Habash, V., Groza, & K., Burr, (2013). Risk management framework for the power grid cyber-physical security. Current Journal of Applied Science and Technology, 1070-1085.

[31] Y., Guo, C. W., Ten, S., Hu, & W. W., Weaver, (2015, February). Modeling distributed denial of service attack in advanced metering infrastructure. In 2015 IEEE power & energy society innovative smart grid technologies conference (ISGT) (pp. 1-5). IEEE. DOI: 10.1109/ISGT.2015.7131828

[32] M. A., Faisal, Z., Aung, J. R., Williams, & A., Sanchez, (2012, May). Securing advanced metering infrastructure using intrusion detection system with data stream mining. In Pacific-Asia Workshop on Intelligence and Security Informatics (pp. 96-111). Springer, Berlin, Heidelberg.

[33] A. O., Otuoze, M. W., Mustafa, O. O., Mohammed, M. S., Saeed, N. T., Surajudeen-Bakinde, & S., Salisu. (2019). Electricity theft detection by sources of threats for smart city planning. IET Smart Cities, 1(2), 52-60.

[34] R., Leszczyna. (2019). Standards with cybersecurity controls for smart grid A systematic analysis. International Journal of Communication Systems, 32(6), e3910.DOI:10.1002/dac.3910. https://onlinelibrary.wiley.com/doi/10.1049/iet-smc.2019.0045

[35] DHS Sensitive Systems Policy Directive 4300A Version 13.1 July 27th, 2017. https://www.dhs.gov/

[36] P., McDaniel, & S., McLaughlin, (2009). Security and privacy challenges in the smart grid. IEEE Security & Privacy, 7(3), 75-77.

[37] e., Fernandes, J., Jung, and A. Prakash. 2016. Security Analysis of Emerging Smart Home Applications. In 2016 IEEE Symposium on Security and Privacy (S.P.). IEEE, 636–654.

[38] A., Hansen, J., Staggs, and S., Shenoi. 2017. Security analysis of an advanced metering infrastructure. International Journal of Critical Infrastructure Protection, 18, pp.3-19. https://doi.org/10.1016/j.ijcip.2017.03.004

[39] NIST Special Publication 800-53A Assessing Security and Privacy Controls in Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations http://dx.doi.org/10.6028/NIST.SP.800-53Ar4.

[40] The National Electric Power Company (NEPCO) annual 2021 report, https://www.nepco.com.jo/store/docs/web/2021_en.pdf , accessed 25nov2022.

[41] NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, retrieved, Nov. 22 from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

APENDIX A

A catalog of procedures to assess the security controls and control enhancements in Special Publication 800-53.

FAMILY: ACCESS CONTROL

AC-1	**ACCESS CONTROL FOR EMPLOYEES**
	Assessment Objective: Determine if the organization
AC-1(a)(1)	
AC-1(a)(1)[1]	develops and documents an access control policy that addresses:
AC-1(a)(1)[1][a]	purpose;
AC-1(a)(1)[1][b]	scope;
AC-1(a)(1)[1][c]	roles;
AC-1(a)(1)[1][d]	responsibilities;
AC-1(a)(1)[1][e]	management commitment;
AC-1(a)(1)[1][f]	coordination among organizational entities;
AC-1(a)(1)[1][g]	compliance;
AC-1(a)(1)[2]	defines personnel or roles to whom the access control policy are to be disseminated;
AC-1(a)(1)[3]	disseminates the access control policy to organization-defined personnel or roles;
AC-1(a)(2)	
AC-1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the access control policy and associated access control controls;
AC-1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated;
AC-1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;
AC-1(b)(1)	
AC-1(b)(1)[1]	defines the frequency to review and update the current access control policy;
AC-1(b)(2)[2]	reviews and updates the current access control policy with the organization-defined frequency;
AC-1(b)(2)	
AC-1(b)(2)[1]	defines the frequency to review and update the current access control procedures; and
AC-1(b)(2)[2]	Reviews and updates the current access control procedures with the organization-defined frequency.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine** [SELECT FROM Access control policy and procedures; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with access control responsibilities; organizational personnel with information security responsibilities]	

AC-2(12)	**ACCOUNT MONITORING / ATYPICAL USAGE**
	Assessment Objective: Determine if the organization
AC-2(12)(a)	
AC-2(12)(a)[1]	defines atypical usage to be monitored for information system accounts;
AC-2(12)(a)[2]	monitors information system accounts for organization defined atypical
AC-2(12)(b)	
AC-2(12)(b)[1]	defines personnel or roles to whom atypical usage of information system accounts are to be reported; and
AC-2(12)(b)[2]	Reports atypical usage of information system accounts to organization-defined personnel or roles.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [SELECT FROM: Access control policy; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system monitoring records; information system audit records; audit tracking and monitoring reports; other relevant documents or records]. **Interview:** [SELECT FROM organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities]. **Test:** [SELECT FROM: Automated mechanisms implementing account management functions]	

AC-3(7)	ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL
	Assessment Objective: Determine if the organization
AC-3(7)[1]	the organization defines roles to control information system access;
AC-3(7)[2]	the organization defines users authorized to assume the organization-defined roles;
AC-3(7)[3]	the information system controls access based on organization-defined roles and users authorized to assume such roles
AC-3(7)[4]	the information system enforces a role-based access control policy over defined:
AC-3(7)[4][a]	subjects, and
AC-3(7)[4][b]	Objects.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [SELECT FROM: Access control policy; role-based access control policies; procedures addressing access enforcement; security plan, information system design documentation; information system configuration settings and associated documentation; list of roles, users, and associated privileges required to control information system access; information system audit records; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers]. **Test**: [SELECT FROM: Automated mechanisms implementing role-based access control policy].	

AC-7	UNSUCCESSFUL LOGIN ATTEMPTS
	Assessment Objective: Determine if the organization
AC-7(a)	
AC-7(a)[1]	the organization defines the number of consecutive invalid logon attempts allowed to the information system by a user during an organization-defined time period;
AC-7(a)[2]	the organization defines the time period allowed by a user of the information system for an organization-defined number of consecutive invalid logon attempts;
AC-7(a)[3]	the information system enforces a limit of organization-defined number of consecutive invalid logon attempts by a user during an organization-defined time period;
AC-7(b)	
AC-7(b)[1]	the organization defines account/node lockout time period or logon delay algorithm to be automatically enforced by the information system when the maximum number of unsuccessful logon attempts is exceeded;
AC-7(b)[2]	the information system when the maximum number of unsuccessful logon attempts is exceeded, automatically:
AC-7(b)[2][a]	locks the account/node for the organization-defined time period;
AC-7(b)[2][b]	locks the account/node until released by an administrator; or
AC-7(b)[2][c]	Delays next logon prompt according to the organization-defined delay algorithm.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Access control policy; procedures addressing unsuccessful logon attempts; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with information security responsibilities; system developers; system/network administrators]. **Test:** [SELECT FROM: Automated mechanisms implementing access control policy for unsuccessful logon attempts].	

AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
	Assessment Objective: Determine if the organization
AC-14(a)	
AC-14(a)[1]	defines user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions;
AC-14(a)[2]	identifies organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
AC-14(b)	documents and provides supporting rationale in the security plan for the Information system, user actions not requiring identification or authentication.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Access control policy; procedures addressing permitted actions without identification or authentication; information system configuration settings and associated documentation; security plan; list of user actions that can be performed without identification or authentication; information system audit records; other relevant documents or records]. **Interview:** [SELECT FROM: System/network administrators; organizational personnel with information security responsibilities]	

AC-18(5)	WIRELESS ACCESS | ANTENNAS/TRANSMISSION POWER LEVELS
	Assessment Objective: Determine if the organization
AC-18(5)[1]	selects radio antennas to reduce the probability that usable signals can be received outside of organization-controlled boundaries; and
AC-18(5)[2]	Calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [SELECT FROM: Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview:** [SELECT FROM: System/network administrators; organizational personnel with information security responsibilities]. **Test:** [SELECT FROM: Wireless access capability protecting usable signals from unauthorized access outside organization-controlled boundaries].	

FAMILY: AWARENESS AND TRAINING

AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
	Assessment Objective: Determine if the organization
AT-1(a)(1)	
AT-1(a)(1)[1]	develops and documents an security awareness and training policy that addresses:
AT-1(a)(1)[1][a]	purpose;
AT-1(a)(1)[1][b]	scope;
AT-1(a)(1)[1][c]	roles
AT-1(a)(1)[1][d]	responsibilities;
AT-1(a)(1)[1][e]	management commitment;
AT-1(a)(1)[1][f]	coordination among organizational entities;
AT-1(a)(1)[1][g]	compliance;
AT-1(a)(1)[2]	defines personnel or roles to whom the security awareness and training policy are to be disseminated;
AT-1(a)(1)[3]	disseminates the security awareness and training policy to organization-defined personnel or roles;
AT-1(a)(2)	
AT-1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;
AT-1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated;
AT-1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;

AT-1(a)(2)	
AT-1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;
AT-1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated
AT-1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;
AT-1(b)(1)	
AT-1(b)(1)[1]	defines the frequency to review and update the current security awareness and training policy;
AT-1(b)(1)[2]	reviews and updates the current security awareness and training policy with the organization-defined frequency;
AT-1(b)(2)	
AT-1(b)(2)[1]	defines the frequency to review and update the current security awareness and training procedures; and
AT-1(b)(2)[2]	Reviews and updates the current security awareness and training procedures with the organization-defined frequency.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Security awareness and training policy and procedures; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with security awareness and training responsibilities; organizational personnel with information security responsibilities].	

AT-2	**SECURITY AWARENESS TRAINING**
	Assessment Objective: Determine if the organization
AT-2(a)	provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users;
AT-2(b)	provides basic security awareness training to information system users (including managers, senior executives, and contractors) when required by information system changes; and
AT-2(c)	
AT-2(c)[1]	defines the frequency to provide refresher security awareness training thereafter to information system users (including managers, senior executives, and contractors); and
AT-2(c)[2]	provides refresher security awareness training to information users (including managers, senior executives, and contractors) with the organization-defined frequency
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records]. **Interview: [**SELECT FROM: Organizational personnel with responsibilities for security awareness training; organizational personnel with information security responsibilities; organizational personnel comprising the general information system user community]. **Test:** [SELECT FROM: Automated mechanisms managing security awareness training]

AT-2(2)	**SECURITY AWARENESS TRAINING| INSIDER THREAT**
	Assessment Objective: Determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: Examine: [SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; security plan; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel that participate in security awareness training; organizational personnel with responsibilities for basic security awareness training; organizational personnel with information security responsibilities].

AT-3(1)	**ROLE-BASED SECURITY TRAINING | ENVIRONMENTAL CONTROLS**
	Assessment Objective: Determine if the organization

AT-3(1)[1]	defines personnel or roles to be provided with initial and refresher training in the employment and operation of environmental controls;
AT-3(1)[2]	provides organization-defined personnel or roles with initial and refresher training in the employment and operation of environmental controls
AT-3(1)[3]	defines the frequency to provide refresher training in the employment and operation of environmental controls; and
AT-3(1)[4]	provides refresher training in the employment and operation of environmental Controls with the organization-defined frequency.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Security awareness and training policy; procedures addressing security training implementation; security training curriculum; security training materials; security plan; training records; other relevant documents or records]. **Interview**: [SELECT FROM: Organizational personnel with responsibilities for role-based security training; organizational personnel with responsibilities for employing and operating environmental controls]	

AT-2(2)	**SECURITY AWARENESS TRAINING| INSIDER THREAT**
	Assessment Objective: Determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; security plan; other relevant documents or records]. **Interview**: [SELECT FROM organizational personnel that participate in security awareness training; organizational personnel with responsibilities for basic security awareness training; organizational personnel with information security responsibilities].

FAMILY: AUDIT AND ACCOUNTABILITY

AU-6	**AUDIT REVIEW, ANALYSIS, AND REPORTING**
	Assessment Objective: Determine if the organization
AU-6(a)	
AU-6(a)[1]	defines the types of inappropriate or unusual activity to look for when information system audit records are reviewed and analyzed;
AU-6(a)[2]	defines the frequency to review and analyze information system audit records for indications of organization-defined inappropriate or unusual activity;
AU-6(a)[3]	reviews and analyzes information system audit records for indications of organization-defined inappropriate or unusual activity with the organization-defined frequency;
AU-6(b)	
AU-6(b)[1]	. defines personnel or roles to whom findings resulting from reviews and analysis of information system audit records are to be reported; and
AU-6(b)[2]	Reports findings to organization-defined personnel or roles.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security responsibilities].	

FAMILY: IDENTIFICATION AND AUTHENTICATION

IA-2	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**
	Assessment Objective: Determine if the organization: Determine if the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated	

documentation; information system audit records; list of information system accounts; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with information system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with account management responsibilities; system developers]. **Test**: [SELECT FROM: Organizational processes for uniquely identifying and authenticating users; automated mechanisms supporting and/or implementing identification and authentication capability]

IA-3	**DEVICE IDENTIFICATION AND AUTHENTICATION**
	Assessment Objective: Determine if
IA-3[1]	the organization defines specific and/or types of devices that the information system uniquely identifies and authenticates before establishing one or more of the following:
IA-3[1][a]	a local connection;
IA-3[1][b]	a remote connection; and/or
IA-3[1][c]	a network connection; and
IA-3[2]	
IA-3[2][a]	a local connection
IA-3[2][b]	a remote connection; and/or
IA-3[2][c]	a network connection
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; list of devices requiring unique identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators; system developers]. **Test**: [SELECT FROM: Automated mechanisms supporting and/or implementing device identification and authentication capability].]	

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

SC—1	**SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**
	Assessment Objective: Determine if the organization
SC-1(a)(1)	
SC-1(a)(1)[1]	develops and documents a security awareness and training policy that addresses:
SC-1(a)(1)[1][a]	purpose;
SC -1(a)(1)[1][b]	scope;
SC-1(a)(1)[1][c]	roles
SC -1(a)(1)[1][d]	responsibilities;
SC -1(a)(1)[1][e]	management commitment;
SC -1(a)(1)[1][f]	coordination among organizational entities;
SC -1(a)(1)[1][g]	compliance;
SC-1(a)(2)	
SC-1(a)(1)[2]	defines personnel or roles to whom the security awareness and training policy are to be disseminated;
SC-1(a)(1)[3]	disseminates the security awareness and training policy to organization-defined personnel or roles;
SC-1(a)(2)	
SC-1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;
SC-1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated;
SC -1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;
SC -1(a)(2)	
SC -1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;
SC -1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated

SC -1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;
SC -1(b)(1)	
SC -1(b)(1)[1]	defines the frequency to review and update the current security awareness and training policy;
SC -1(b)(1)[2]	reviews and updates the current security awareness and training policy with the organization-defined frequency;
SC -1(b)(2)	
SC -1(b)(2)[1]	defines the frequency to review and update the current security awareness and training procedures; and
SC -1(b)(2)[2]	Reviews and updates the current security awareness and training procedures with the organization-defined frequency.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Security awareness and training policy and procedures; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with security awareness and training responsibilities; organizational personnel with information security responsibilities].	

FAMILY: SYSTEM AND INFORMATION INTEGRITY

SI—1	**SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES**
	Assessment Objective: Determine if the organization
SI-1(a)(1)	
SI -1(a)(1)[1]	develops and documents a security awareness and training policy that addresses:
SI -1(a)(1)[1][a]	purpose;
SI -1(a)(1)[1][b]	scope;
SI-1(a)(1)[1][c]	roles
SI -1(a)(1)[1][d]	responsibilities;
SI -1(a)(1)[1][e]	management commitment;
SI -1(a)(1)[1][f]	coordination among organizational entities;
SI -1(a)(1)[1][g]	compliance;
SI-1(a)(2)	
SI -1(a)(1)[2]	defines personnel or roles to whom the security awareness and training policy are to be disseminated;
SI -1(a)(1)[3]	disseminates the security awareness and training policy to organization-defined personnel or roles;
SI -1(a)(2)	
SI-1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;
SI-1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated;
SI -1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;
SI -1(a)(2)	
SI -1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;
SI -1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated
SI -1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;
SI -1(b)(1)	
SI -1(b)(1)[1]	defines the frequency to review and update the current security awareness and training policy;
SI -1(b)(1)[2]	reviews and updates the current security awareness and training policy with the organization-defined frequency;
SI -1(b)(2)	
SI -1(b)(2)[1]	defines the frequency to review and update the current security awareness and training procedures; and
SI -1(b)(2)[2]	Reviews and updates the current security awareness and training procedures with the organization-defined frequency.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Security awareness and training policy and procedures; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with security awareness and training responsibilities; organizational personnel with information security responsibilities].	

FAMILY: Maintenance

MA-6	**TIMELY MAINTENANCE**
	ASSESSMENT OBJECTIVE: **Determine if the organization:**
MA-6[1]	defines information system components for which maintenance support and/or spare parts are to be obtained;
MA-6[2]	defines the time period within which maintenance support and/or spare parts are to be obtained after a failure;
MA-6[3]	
MA-6[3][a]	obtains maintenance support for organization-defined information system components within the organization-defined time period of failure; and/or
MA-6[3][b]	obtains spare parts for organization-defined information system components within the organization-defined time period of failure
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Information system maintenance policy; procedures addressing information system maintenance; service provider contracts; service-level agreements; inventory and Availability of spare parts; security plan; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with information system maintenance responsibilities; organizational personnel with acquisition responsibilities; organizational Personnel with information security responsibilities; system/network administrators]. **Test:** [SELECT FROM: Organizational processes for ensuring timely maintenance].	

MA-6(2)	**TIMELY MAINTENANCE/PREDICTIVE MAINTENANCE**
	ASSESSMENT OBJECTIVE: **Determine if the organization:**
MA-6(2)[1]	defines information system components on which predictive maintenance is to be performed;
MA-6(2)[2]	defines time intervals within which predictive maintenance is to be performed on organization-defined information system components; and
MA-6(2)[3]	performs predictive maintenance on organization-defined information system Components at organization-defined time intervals.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine: [SELECT FROM: Information system maintenance policy; procedures addressing information system maintenance; service provider contracts; service-level agreements; security plan; maintenance records; list of system components requiring predictive maintenance; other Relevant documents or records].** **Interview: [SELECT FROM: Organizational personnel with information system maintenance responsibilities; organizational personnel with information security responsibilities. System/network administrators].** **Test: [SELECT FROM: Organizational processes for predictive maintenance; automated mechanisms Supporting and/or implementing predictive maintenance].**	

Jordan Journal of Energy
Volume 1, Number 2, 2023

ISSN (Online): 2790-7678
ISSN (Print): 2790-766X

Jordan Journal of Energy (JJE)
Journal Homepage: http://dsr.mutah.edu.jo/index.php/jje
JEE an official peer review journal of Mutah University,

The Impact of Adding Solar Panels on The Wind Turbine Performance During Transient Disturbances

Basel Taha Alkhamis
IDECO, JORDAN
alkhamisbasel@gmail.com

Received 19th May 2023 ; Accepted 1st August 2023

ABSTRACT. *Recently electrical engineers look forward to replace the conventional power grid with a smart grid. This replacement requires massive changes, one of them is the integration of distributed generations and renewable energy sources in the distribution networks of the grid. These changes may affect the transient stability of the grid. In this paper, IEEE 9-bus system is used to perform transient stability analysis for a three-phase fault contingency. A 20 MW wind turbine was installed to study its performance and impact on the transient stability of the system. Then, a 3.6 MW PV station was added to study its impact on the wind turbine performance during the contingency. ETAP® 2016 software is used for simulation. The results show that the critical clearing time (CCT) of the system increases when the wind turbine is added and decreases when the PV station is installed. The impact of PV station on the wind turbine performance is not significant and it mainly affects the reactive power of the wind turbine generator after the fault is cleared.*

Keywords: Critical clearing time, IEEE 9-bus system, Photovoltaic panels, Rotor angle, Solar system, Transient stability, Wind turbine.

1. Introduction. Any power system is prone to disturbances during its operation such as; faults, large generation loss, load variations, and loss of critical branches [1]. These disturbances may lead to system instability under some circumstances [2]. Therefore, it is important to analyze the stability of the system during planning stage in order to prevent; huge economical losses, and service disconnection.

One of the important types of power system stability is the transient stability. Transient stability means the ability of the power system to regain its steady-state operation after being subjected to a large disturbance such as faults [2]. In order to analyze the transient stability of any power system, two terms are needed to be studied and they are; the rotor angle (or load angle), and the critical clearing time. The rotor angle (delta) means the P-V generator rotor angle with respect to the swing generator angle. The critical clearing time (CCT) means the maximum allowable time for the fault to be stayed before the system becomes unstable.

However, by moving towards a smarter grid, the distributed energy resources (DERs) become the point of interest. The DERs are small generators that are installed in the distribution networks in order to support the main conventional generating units economically and operationally. One of the important types of the DERs are the renewable energy sources (RES) such as; wind turbines and solar panels.

In this study, the performance and impact of a 20 MW wind turbine on the transient stability will be studied.

The impact of a 3.6 MW PV station on the wind turbine performance during a transient contingency will be studied. The impact of wind turbine and PV panels on the critical clearing time will be analysed.

Eftekharnejad, S., et al. have studied the effect of large-scale penetration of PV panels on both the transient stability and the steady-state operation of the system [3]. Simulations were done and their results show that by increasing the penetration of the PV panels in the system, the voltage dips that follows the disturbance will be larger [3].

On the other hand, Munkhchuluun, E., and L., Meegahapola have studied the impact of PV panels on the voltage stability [4]. Simulations were done and their results show that the integration of PV panels in the system enhanced the voltage stability especially when the grid is stressed [4].

Moreover, Tamimi, B., et al. have studied the impact of PV panels on the power system stability [5]. Simulations were done and their results show that there will be no changes on the transient stability of the system when the PV panels have reactive power control [5].

Furthermore, Achilles, S., et al. study the impact of large penetration of PV panels on a power system under real circumstances [6]. Simulations were done and their results show that by increasing the penetration of PV panels, the risk of transient instability will become greater [6].

Acharya, S., and M., Ramezani have done a study on the performance of a 100 MW wind turbine during a transient contingency [7]. The simulations were done using ETAP® software and their results show that the wind turbine support the system by injecting reactive power at the point of connection during the occurrence of the fault [7].

Nunes, M., et al. have studied the impact of doubly-fed induction generators (DFIG) wind turbines on the transient stability margins [8]. Simulations were done and their results show that the DFIG wind turbines positively affect the transient stability of the system compared to the fixed-speed wind turbines [8].

Meegahapola, L., et al. have studied the impact of high penetration of wind turbines on the transient stability of the system [9]. Simulations were done on the IEEE-14 bus system and their results show that by increasing the penetration of wind turbines to 50%, the system stability will be decreased due to the high reactive power absorbed by the wind turbines from the system [9].

Gautam, D., et al. have studied the impact of high penetration of DFIG wind turbines on the transient stability of the system [10]. Simulations were done and their results show that the high

penetration of wind turbines will negatively affect the system stability due to the lack of inertia problem [10].

2. Methodology:

2.1. The swing equation and the equal area criteria

In order to analyze the system dynamic behavior during a transient disturbance, a very important term must be taken into account and it is called the synchronous machine dynamics [1].

The synchronous machine normally consists of a rotational masses which give us the very important mechanical feature that is called the moment of inertia. Usually, we need the inertia in the system in order to mitigate the damage that caused by the disturbance in the system. Hence, the inertia helps in increasing the boundaries of the stability in the system [11-13].

In order to represent the electrical and mechanical features of the synchronous generator mathematically, then, we need the swing equation:

$$\frac{2H}{\omega_{synch}}\omega_{pu}(t) * \frac{d^2\delta(t)}{dt^2} = P_{mp.u.}(t) - P_{ep.u.}(t) - \frac{D}{\omega_{synch}\frac{d\delta(t)}{dt}} = P_{ap.u.(t)} \quad (1)$$

Where,

H : The inertia constant in (pu.s).

ω_{synch} : The synchronous angular velocity of the rotor in (rad/sec).

ω_{pu} : Rotor angular velocity in (pu).

δ : Rotor angle in (deg.)

As shown in equation (1), the swing equation mainly consists of two parts; electrical, and mechanical. The left-side of the equation shows the acceleration of the rotor multiplied by the inertia constant. The right-side of the equation shows the acceleration power which is the result from subtracting the damping part and electrical power from the mechanical power of the turbine.

There is an analytical method for studying the transient stability especially in the single machine – infinite bus (SMIB) system. This method is called the equal – area criteria. In this method, the swing equation is used in order to determine; the stability state, and the critical clearing time of the system. Figure (1) shows the equal area criteria.

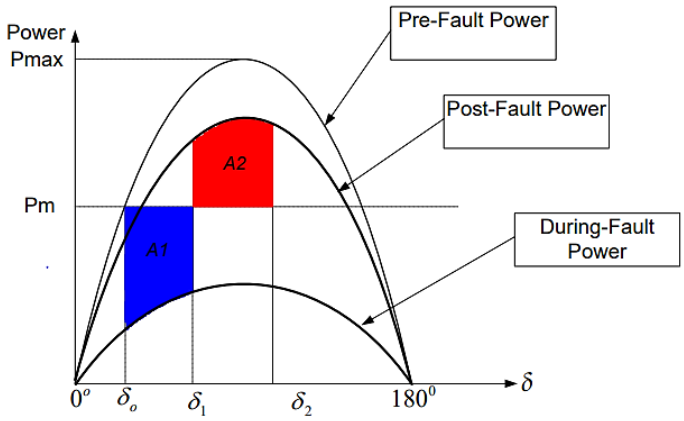


FIGURE.1. The equal area criteria

The two areas A1 and A2 in figure (1) represent the accelerating and decelerating areas for the synchronous machine respectively. in order to have a stable system, the accelerating area of the machine must be equal to the decelerating area, this is achieved by making the swing equation equals to zero. The following equation explain this criteria:

$$\int_{\delta_0}^{\delta_1}(P_{mp.u.} - P_{ep.u.})\,d\delta = \int_{\delta_1}^{\delta_2}(P_{mp.u.} - P_{ep.u.})\,d\delta \qquad (2)$$

As shown in equation (2), the left – side represents area 1 (accelerating area), and the right – side represents area 2 (decelerating area). By looking at figure (1), if A1 is greater than A2, then the system is unstable, if A1 equals or less than A2 then the system is stable.

From the equal area criteria, the critical clearing time (CCT) of the system can be found. When a large fault occurs within the system, the electrical power goes to zero, and by implying this case to the swing equation, the CCT can be calculated by the following equation:

$$CCT = \sqrt{\frac{4H}{\omega_{synch}P_{mp.u.}}}(\delta_{cr}(t) - \delta_0) \qquad (3)$$

Where,

δ_{cr} : Critical clearing angle in (dig.).
δ : Initial rotor angle in (dig.).

All of the above calculation can be solved without using any software, but, in the case of multi-machine system, the mathematical solution becomes more complex and requires specialized software to judge system stability and find the CCT.

2.2. Building the system

The IEEE 9-bus system was built using ETAP® 2016 software. The system was tested using power flow analysis. After that, a contingency case of a three-phase fault on bus 5 was added to the system in order to study the transient stability of the system and find the critical clearing time. A 20 MW wind turbine was added to the system through bus 4 to study its performance during the same contingency that was applied in the previous section.

A 3.6 MW solar station was added to the system through bus 4 to study its effect on the performance of the wind turbine during the same contingency that was applied before.

3. Results and Discussion:

3.1. The normal system without adding PV or wind

The power flow analysis of the built IEEE 9-bus system is shown in figure (2). Bus 1, bus 2, and bus 3 are working on 100% of their voltage. From bus 3 to bus 9 the percentage of the operating voltages ranges between 99% and 96%. The power flow from the generating units to the loads is seem to be very good. Hence, it is verified that the system is working correctly without any problem.

A case study of a three-phase fault was added to the system. The fault was applied on bus 5 at 1 second firstly without clearing the fault. The transient stability of the system were analyzed and the results of buses voltages, buses frequencies, and generators data are shown in figures (3) and (4).

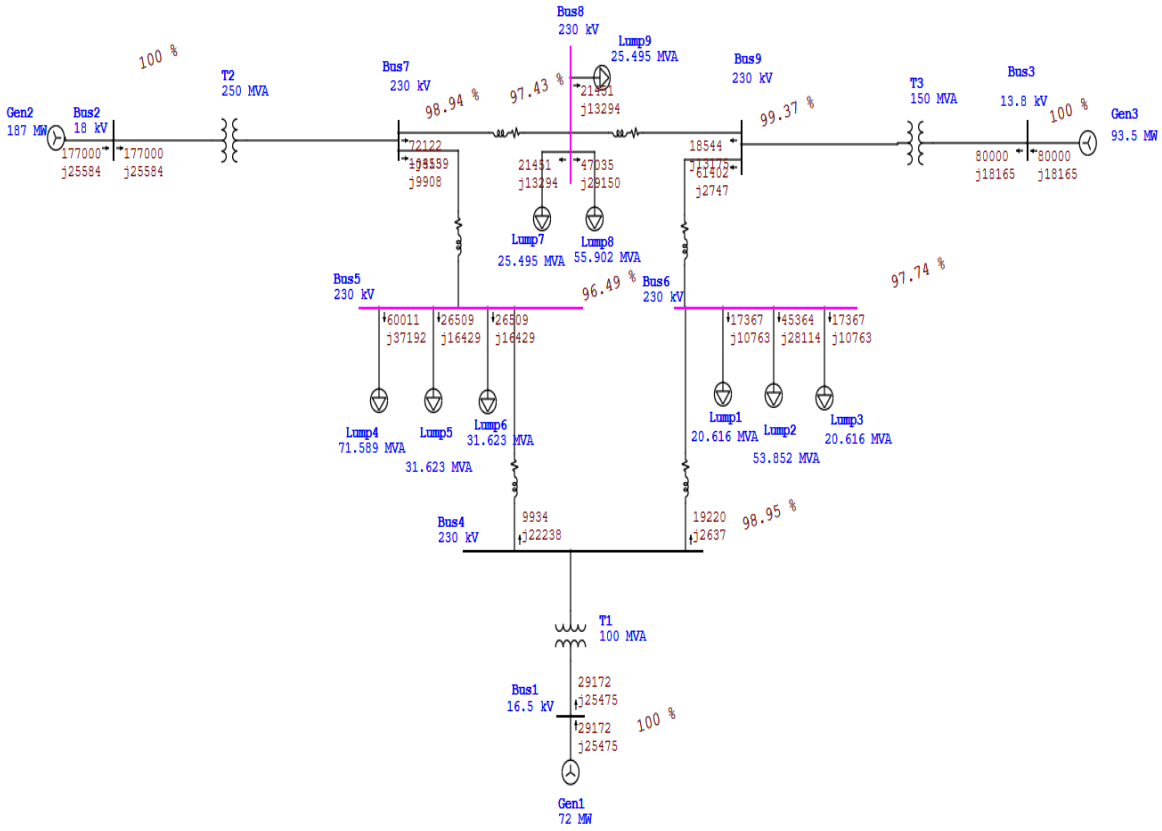
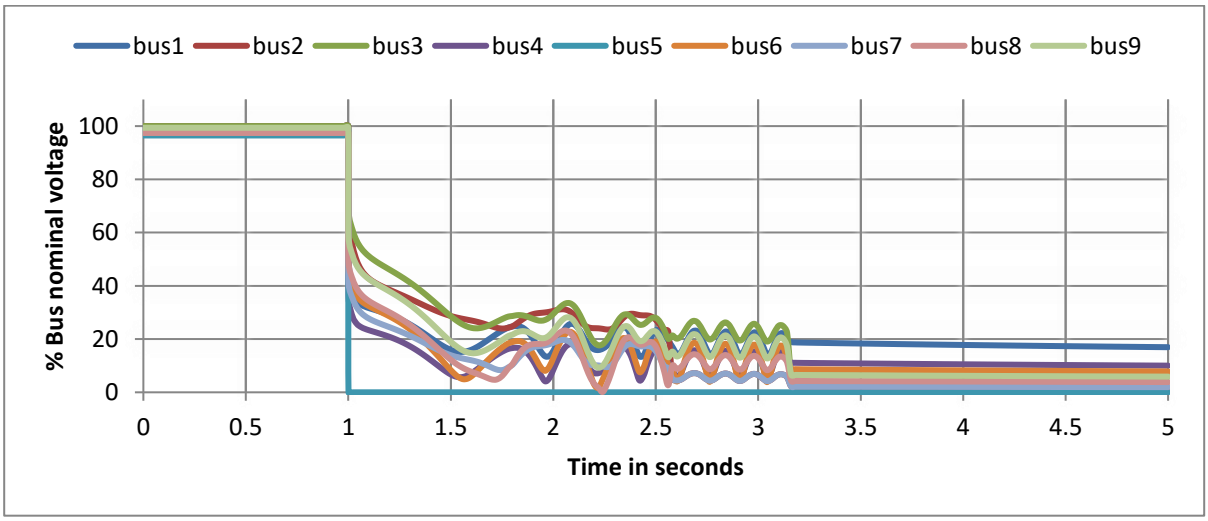
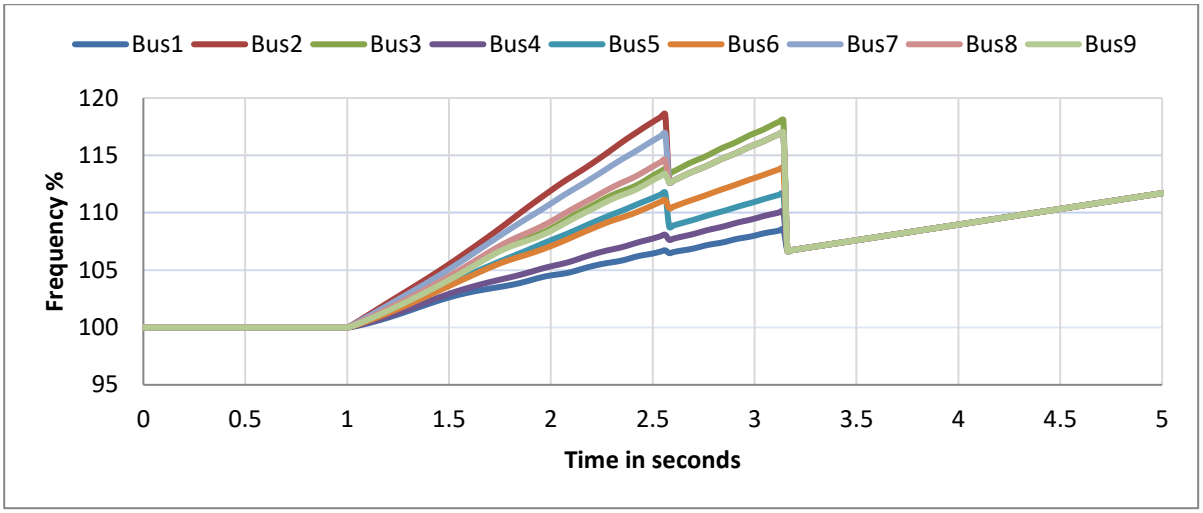


FIGURE.2. Power flow analysis for the normal system



(a)

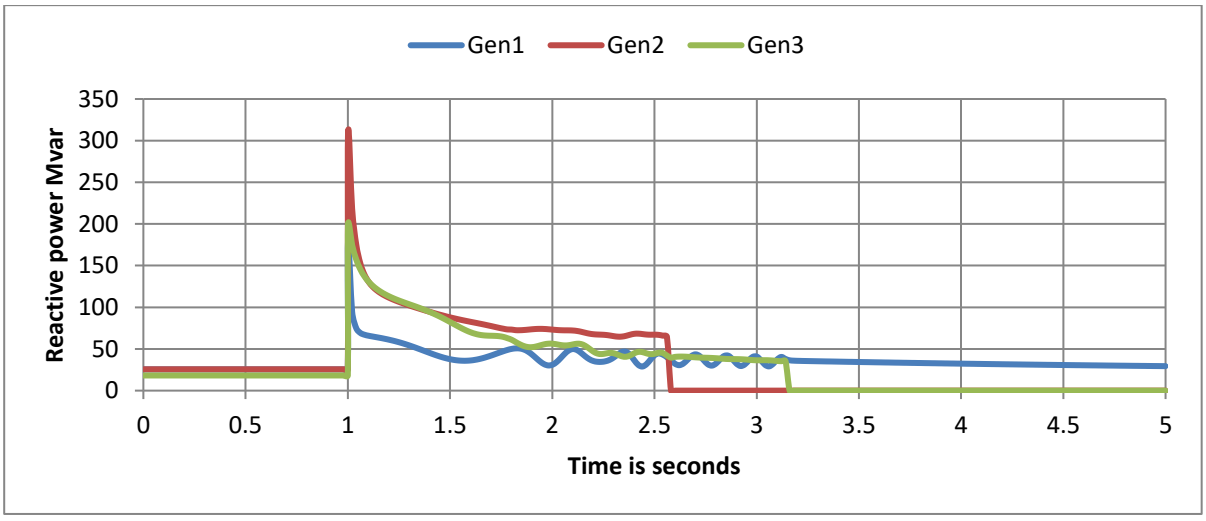


(b)

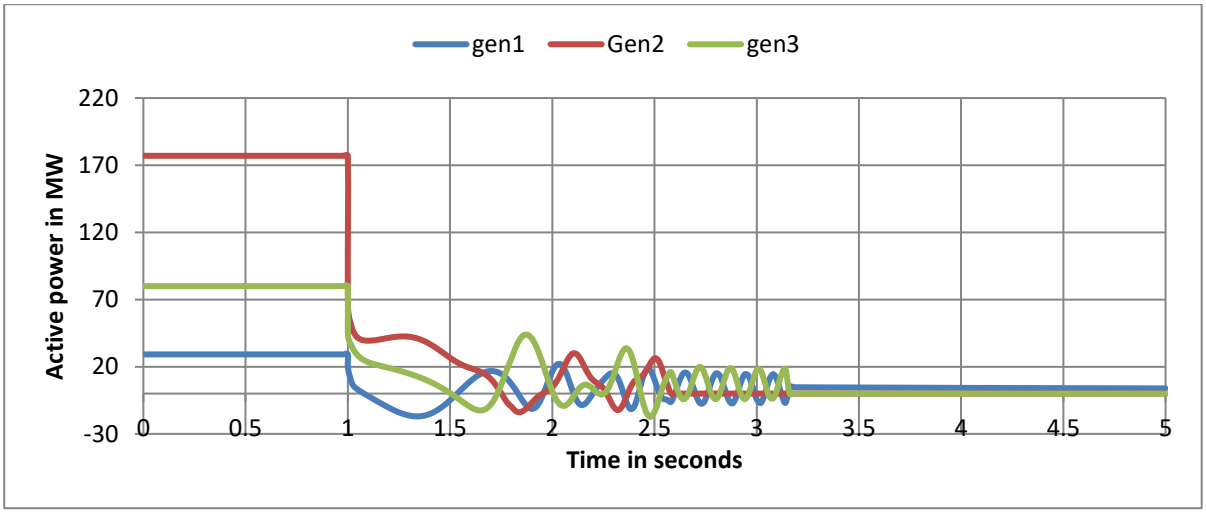
FIGURE.3. All buses voltages, (a) percentage of buses nominal voltages, (b) buses frequencies.

As shown in figure (3-a), before second one, all of the voltages were in steady-state. After second one, the voltage of bus 5 became zero and all of the voltages became unstable and decrease to a very low values.

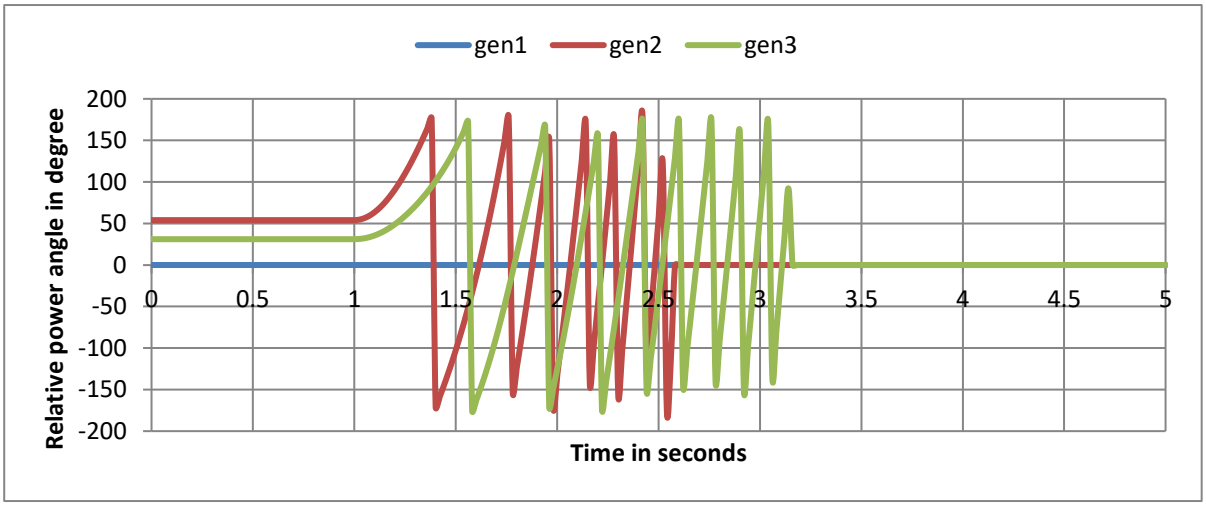
From figure (3-b), before second one, the frequencies of all buses were the same (60Hz). After second one, the frequencies of all buses lost synchronism, and around second three, the system became unstable.



(a)



(b)



(c)

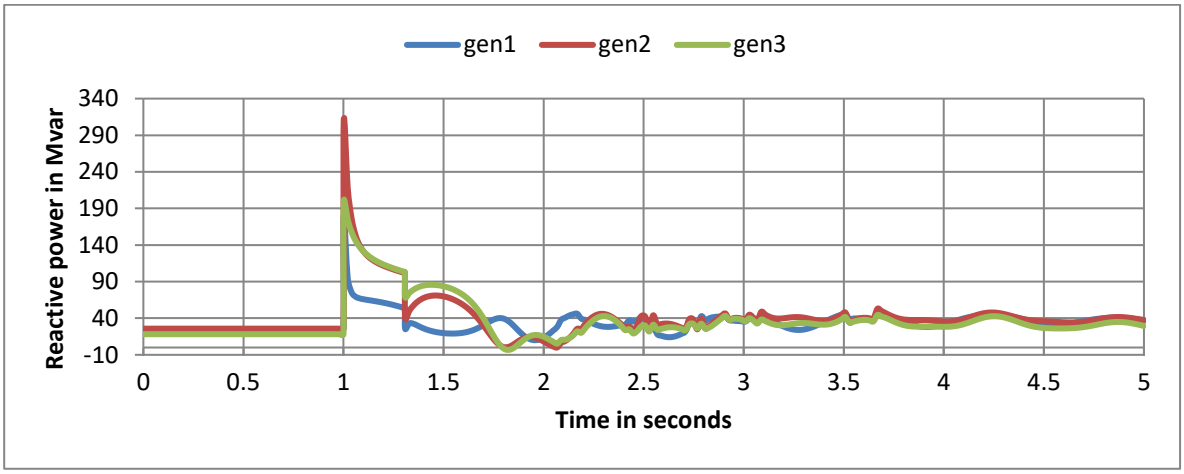
FIGURE.4. Generators status during contingency without clearing the fault, (a) generators MVAR, (b) generators MW, (c) generators relative power angles

From figure (4-a), before second one, all of the generators were producing MVARs and the system were stable. After second one, all of the three generators increase the production of the reactive power especially generator 1 (the swing generator) in order to support system's voltage collapse during the contingency. About the second three, the system lost synchronism and became unstable.

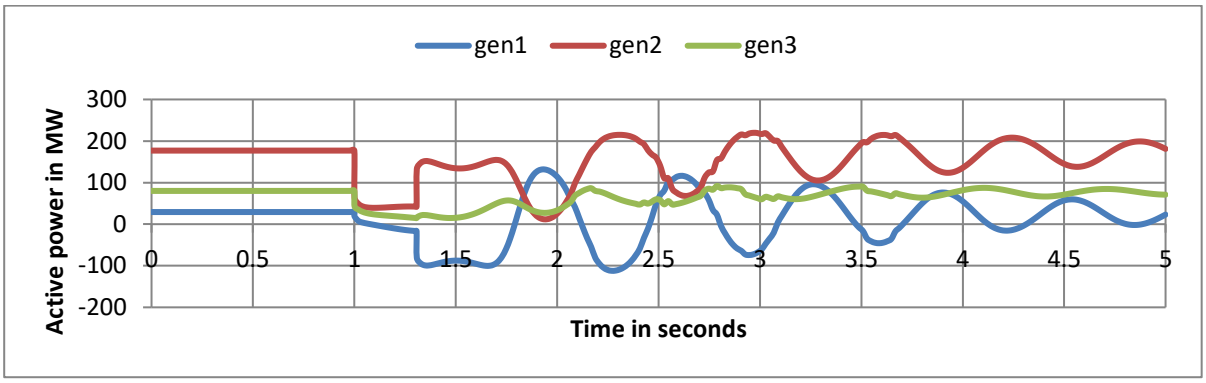
From figure (4-b), after one second, the active powers of the generators began to oscillates and at three seconds, the system lost synchronism and all active powers became zero.

As shown in figure (4-c), the relative power angles of the generators become to oscillate between 200 and -200 after one second which indicate that the system became unstable.

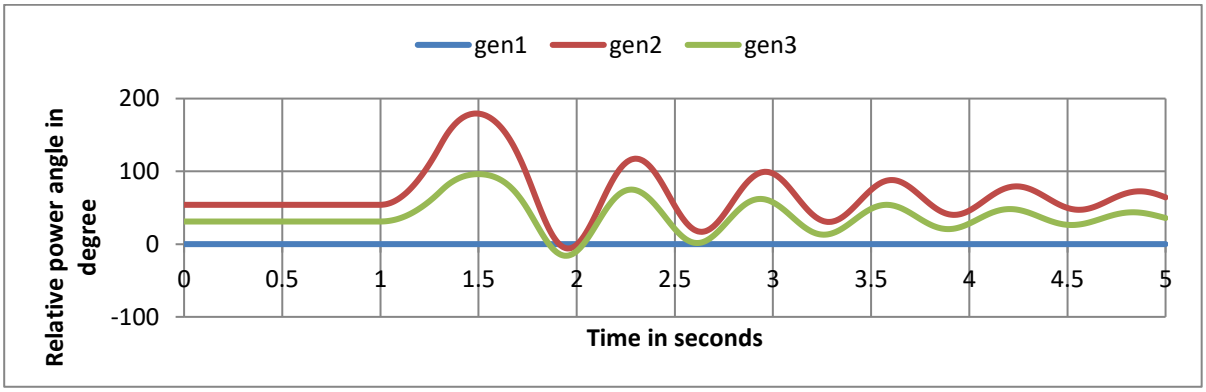
After that, the critical clearing time of the system was calculated based on the swing equation and the equal area criteria. The critical clearing time of the system was found to be 307 ms. The fault was cleared at the critical clearing time of the system. Figure (5) shows the generators MWs, MVARs, and relative power angles after the fault is cleared at 1.307 sec.



(a)



(b)



(c)

FIGURE.5. Generators status during contingency with clearing of the fault at 1.307 sec, (a) generators MVAR, (b) generators MW, (c) generators relative power angles

As shown in figure (5-a), the reactive powers of the generators increased at 1 sec, and after the fault is cleared, the reactive powers came back to the steady-state operating values as before. From figure (5-b), the huge oscillations in the active powers at 1 sec can be noticed, but, after the fault is cleared, the active powers came back to the steady-state operating values as before. As shown in figure (5-c), the power angles of the generators oscillate at 1 sec, then, the oscillation is decreased due to the fault clearance, and the power angles came back to the initial steady-state operating values.

3.2. Adding wind turbine to the system

A 20 MW wind turbine was added to bus 4 in the system. The power flow analysis for this system is shown in figure (6). Bus 1, bus 2, and bus 3 are working on 100% of their voltage. From bus 3 to bus 9 the percentage of the operating voltages ranges between 99% and 96%. The power flow from the generating units to the loads is seem to be very good. Hence, it is verified that the system is working correctly without any problem.

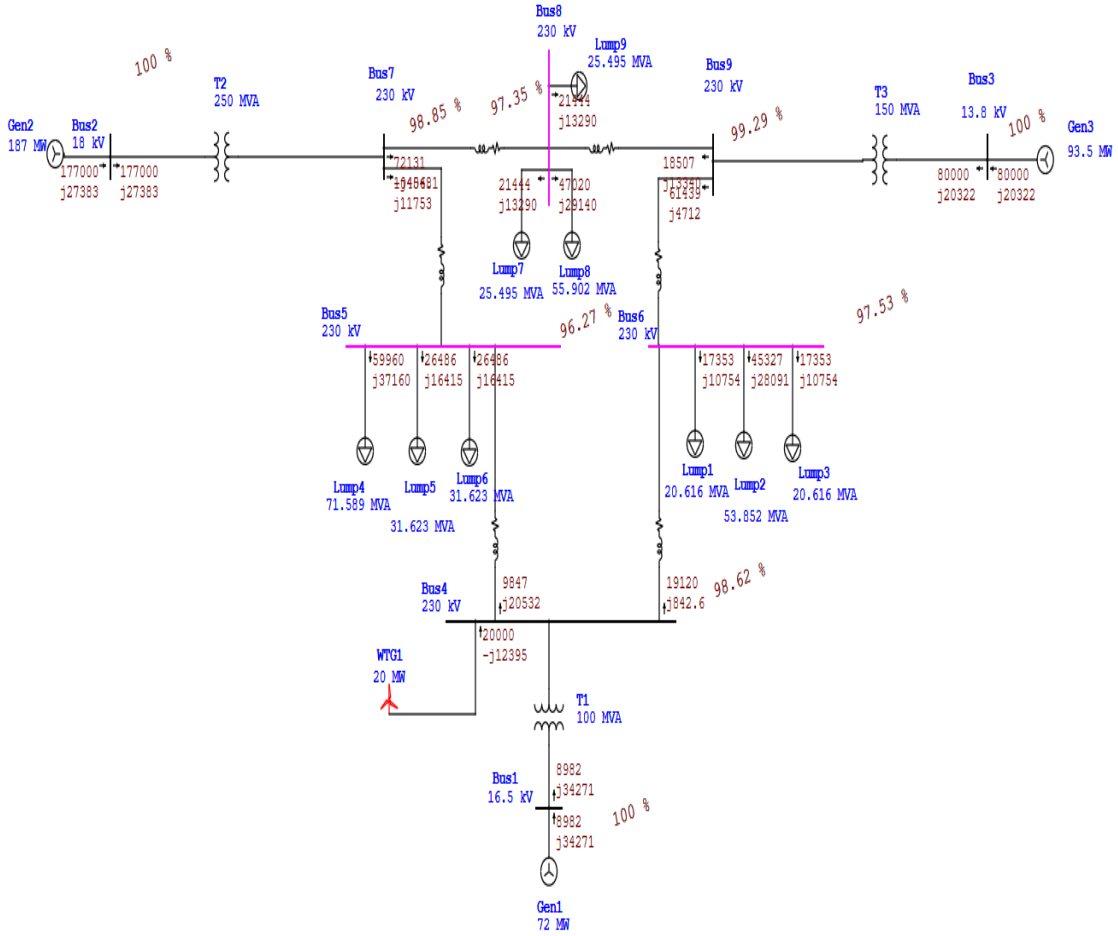
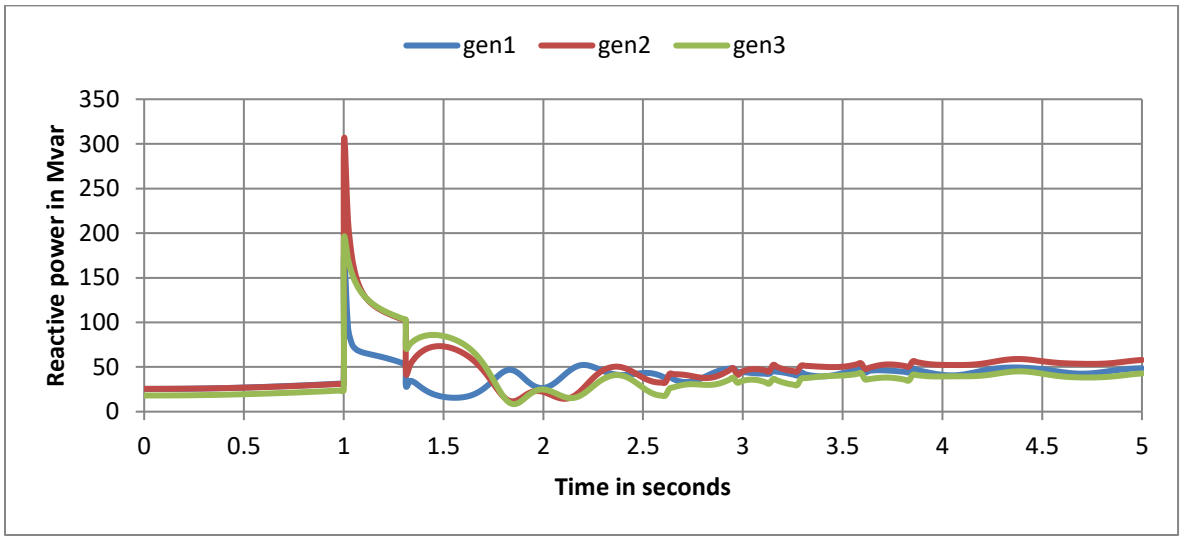
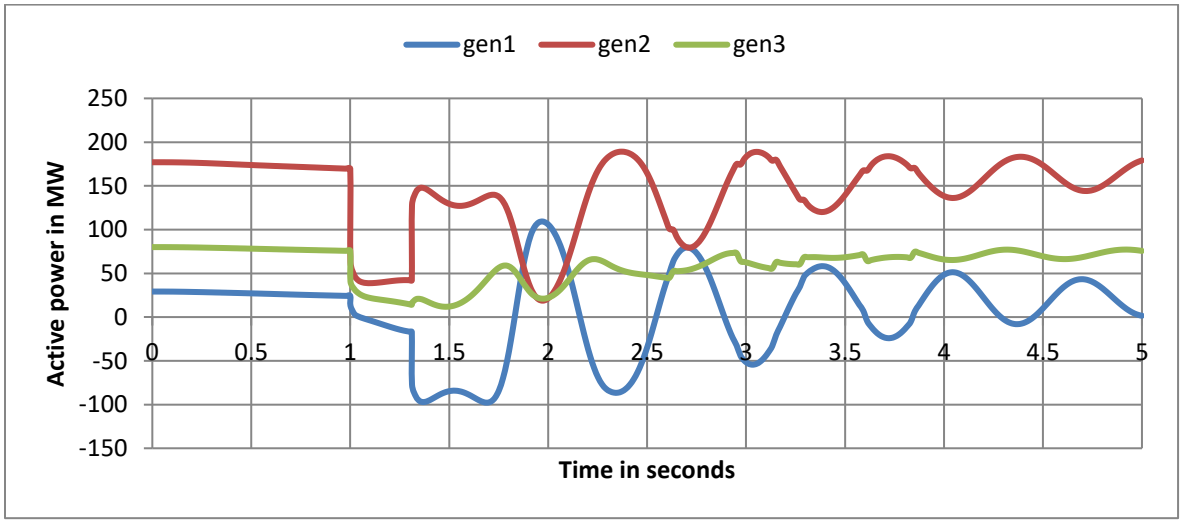


FIGURE.6. Power flow analysis for the system with wind turbine

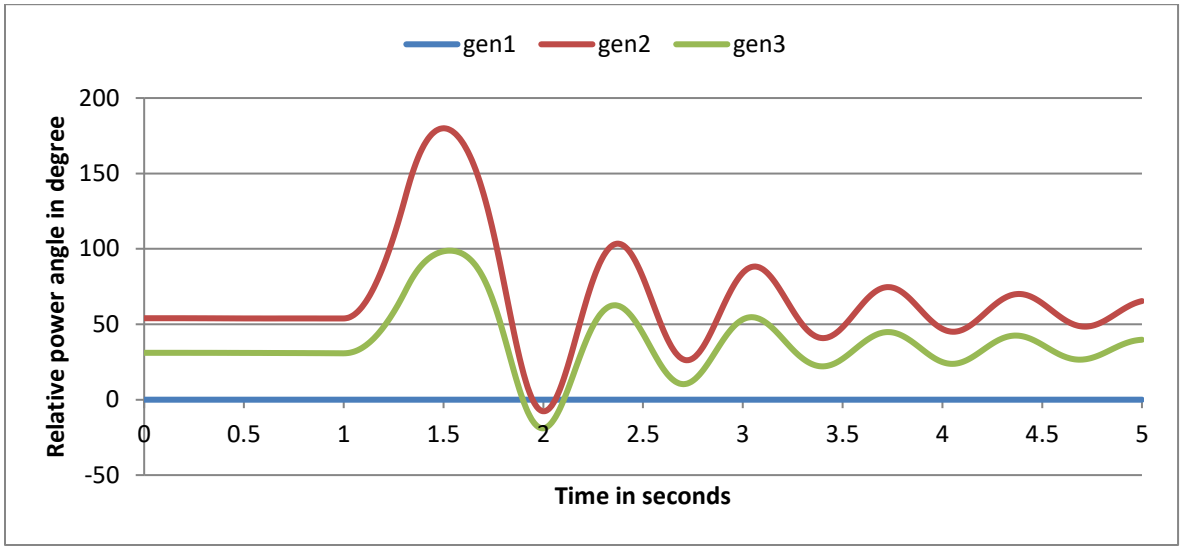
The same contingency case was added to this system (three-phase fault on bus 5 at 1 sec). The critical clearing time for this system was calculated based on the swing equation and the equal area criteria and it was found to be 311 ms. The fault was cleared at this CCT. The generators active powers (MW), reactive powers (MVARs), and relative power angles (degrees) are shown in figure (7). The wind turbine's active power (MW), reactive power (MVAR), and mechanical power (MW) are shown in figure (8).



(a)



(b)

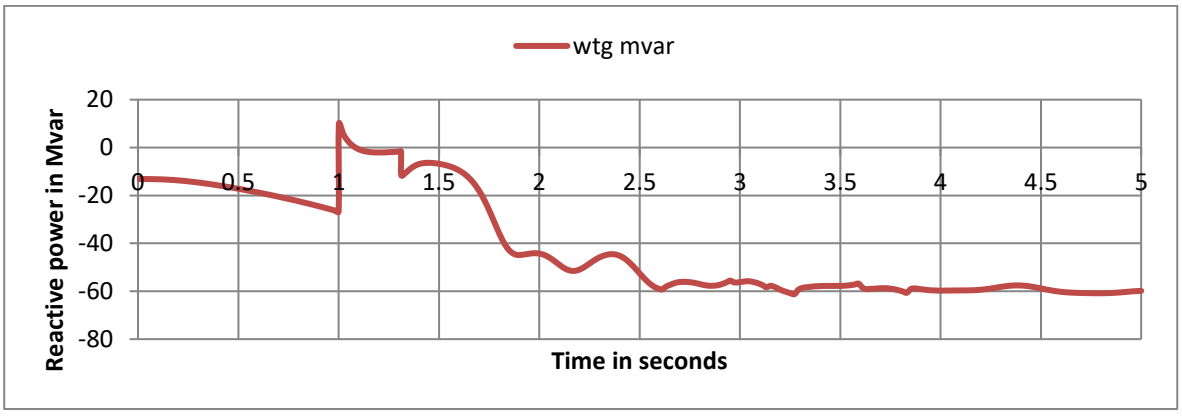


(c)

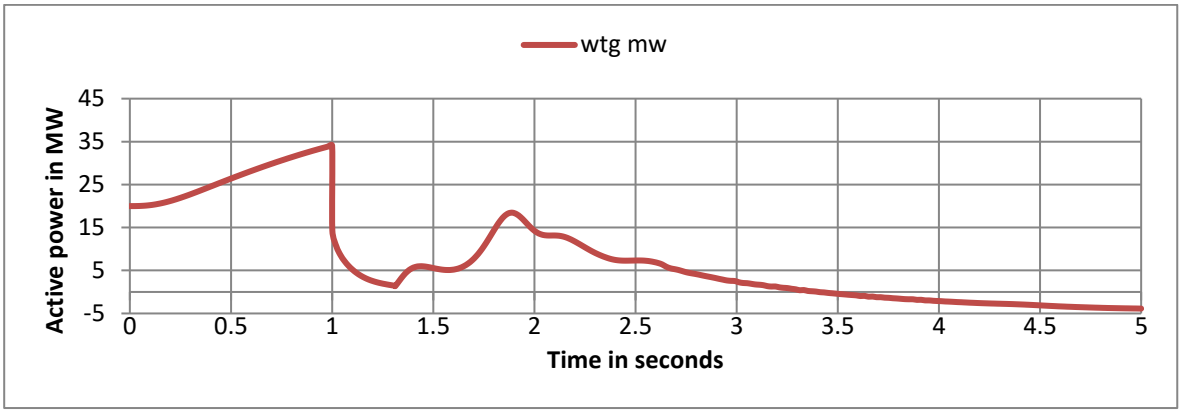
FIGURE.7. Generators status during contingency with clearing of the fault at 1.311 sec, (a) generators MVAR, (b) generators MW, (c) generators relative power angles

From figure (7), the generators MVARs in this system increased at 1 sec and came back to the normal operating values just like the normal system, but, the difference here is that there is a small increasing in the generators MVARs before 1 sec (during the steady-state).

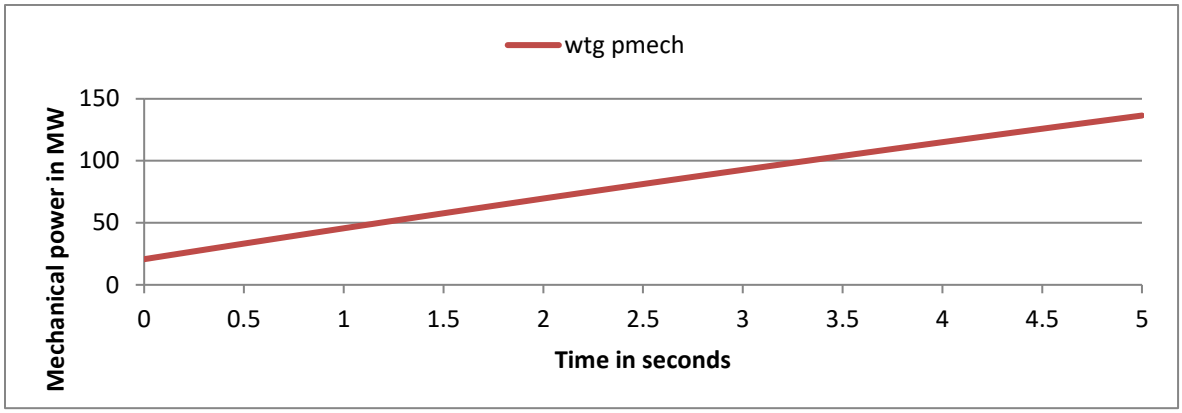
The generators MWs acts just like the normal system's performance, but, the difference here is that there is a slight decreasing in the MWs during the steady-state operation (before 1 sec). the relative power angles acts like the ones in the normal system; they oscillate at 1 sec, then came back to the normal steady-state initial values.



(a)



(b)



(c)

FIGURE.8. WTG status during contingency with clearing of the fault at 1.311 sec, (a) WTG MVAR, (b) WTG MW, (c) WTG mechanical power

From figure (8), the wind turbine generator (WTG) performance during the transient contingency summarized in supporting the system with MVARs when a transient disturbance occurs in order to stay connected to the system as long as possible. Figure (8-a) shows that the wind turbine producing MVARs at 1 sec instead of consuming it, and after the fault is cleared, the WTG came back to consume even more MVARs from the system.

Figure (8-b) shows that the WTG increase the production of active power during the steady-state operation (before 1 sec), and when the fault occurs, the active power decreased from 35 MW to 1 MW, and after the fault is cleared, the active power increased again to 19 MW at 1.9 sec, then, start to decreasing (i.e. it oscillates in order to find the new stable conditions).

Figure (8-c) shows the mechanical power of the wind turbine generator, this power starts at 20 MW (initial value) and continue to increase during the next 5 seconds (as expected).

3.3 Adding PV station to the system

A 3.6 MW PV station was added to the system through bus 4. Figure (9) shows the power flow analysis of the system.

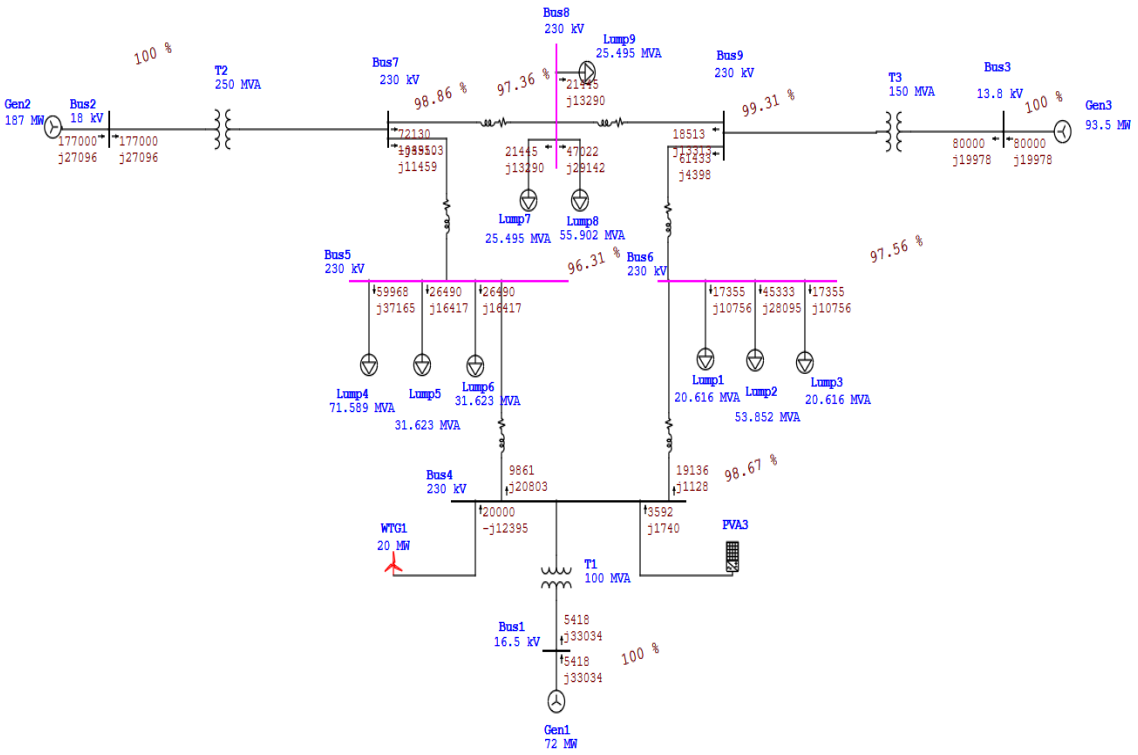
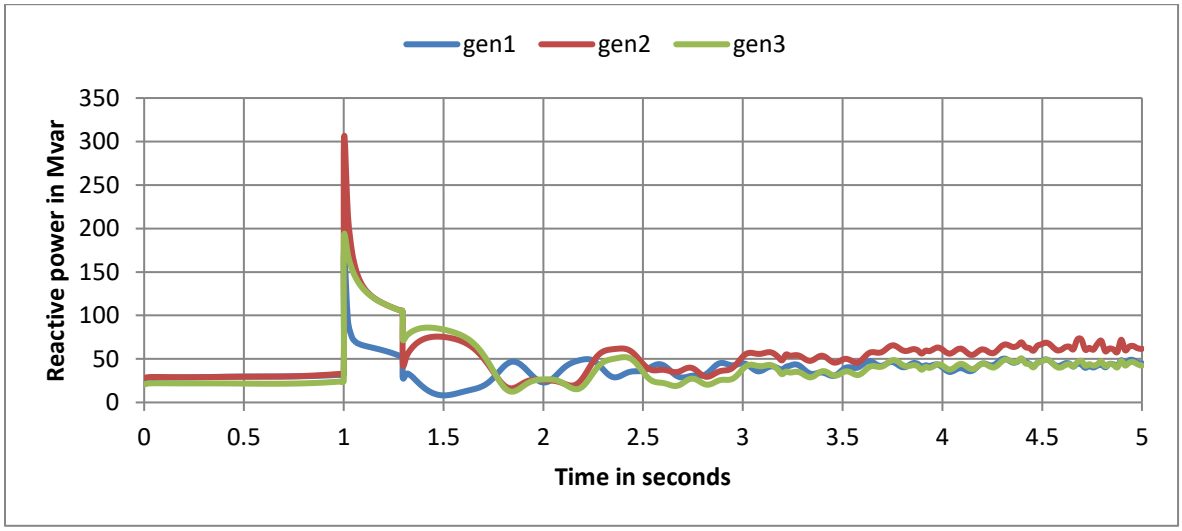


FIGURE.9. Power flow analysis for the system with PV and wind

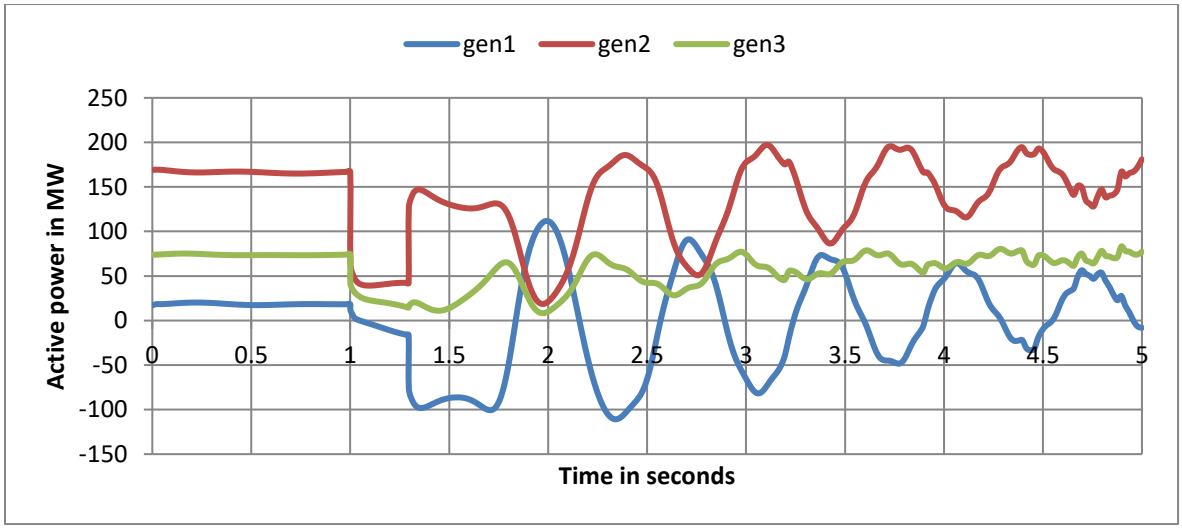
Bus 1, bus 2, and bus 3 are working on 100% of their voltage. From bus 3 to bus 9 the percentage of the operating voltages ranges between 99% and 96%. The power flow from the generating units to the loads is seem to be very good. Hence, it is verified that the system is working correctly without any problem.

The same contingency case was added to this system (three-phase fault on bus 5 at 1 sec). The critical clearing time for this system was calculated based on the swing equation and the equal area criteria and it was found to be 295 ms. The fault was cleared at this CCT.

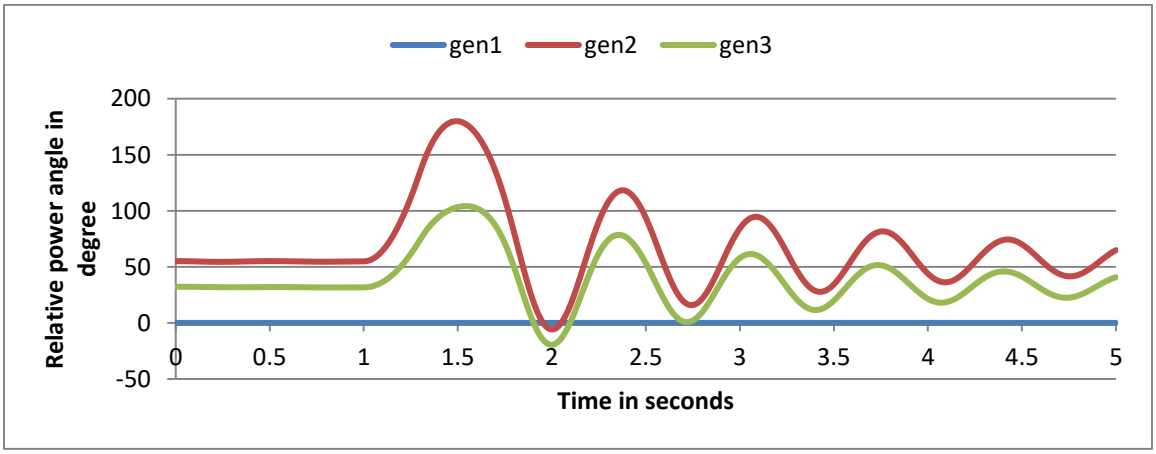
The generators active powers (MW), reactive powers (MVAR), and relative power angles (degrees) are shown in figure (10). The wind turbine's active power (MW), reactive power (MVAR), and mechanical power (MW) are shown in figure (11).



(a)



(b)



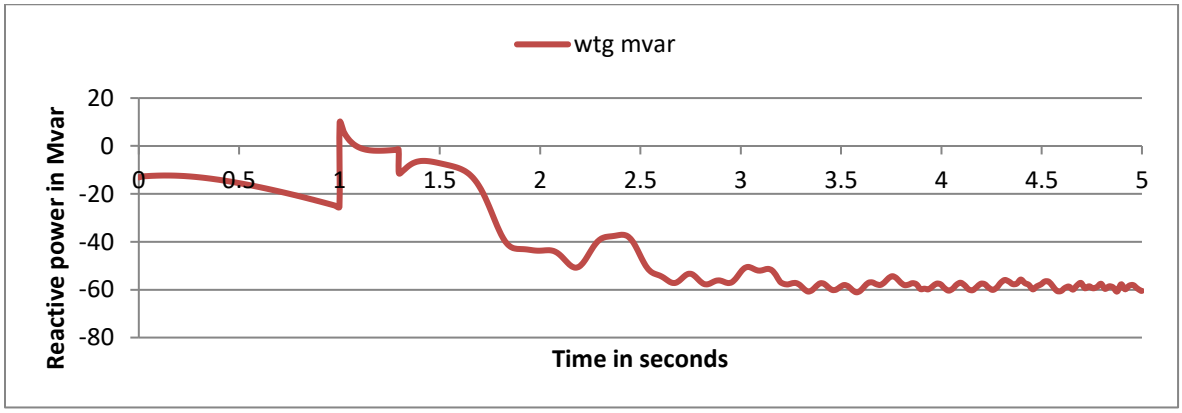
(c)

FIGURE.10. Generators status during contingency with clearing of the fault at 1.295 sec, (a) generators MVAR, (b) generators MW, (c) generators relative power angles

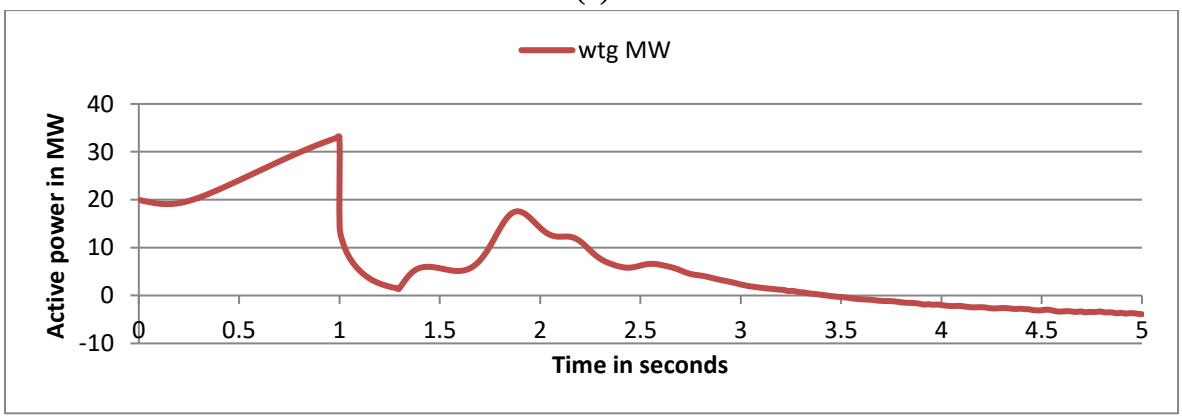
As shown in figure (10-a), the reactive powers of the generators increased at 1 sec to support the system's voltage, but the difference here is that after the fault is cleared, the MVARs return to steady-state values but with a noticeable oscillations around these values.
The same effect appears at figure (10-b), the generators active powers start to oscillate at 1 sec, and after the fault is cleared, an extra oscillations appear on the generators MWs when they try to reach a new steady-state operating values.

From figure (10-c), the relative power angles oscillations of the generators do not affected by the installation of the PV panels in the system. The relative power angles starts to oscillate at 1 sec, and after the fault is cleared, the oscillation of these angles decreased in order to reach an new steady-state operating values.

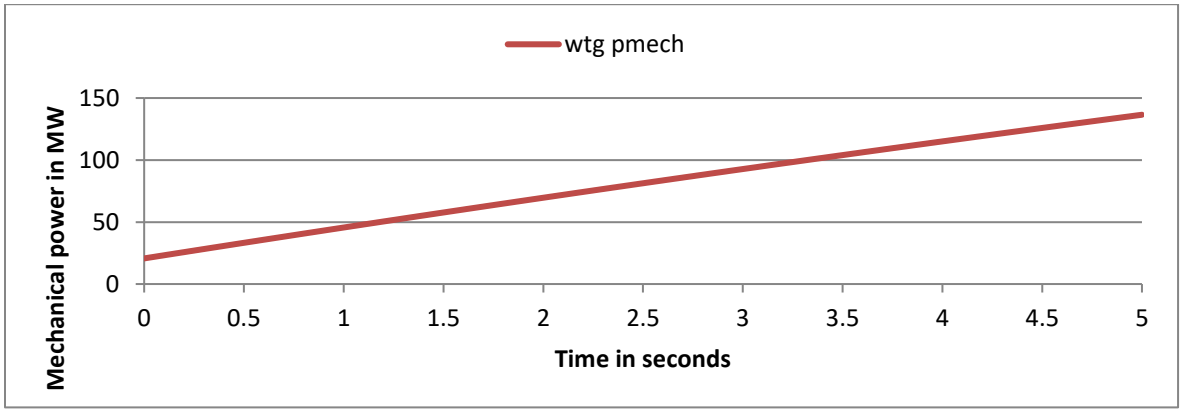
Hence, it can be noticed that the addition of photo voltaic panels in the system affects both of the reactive and active powers of the real synchronous generators by adding extra oscillation to the signals after the fault is cleared. This result appears due to the absence of rotational masses in the conventional inverter-based photovoltaic panels which will make the overall moment of inertia in the system, and the transient stability margins to be decreased.



(a)



(b)



(c)

FIGURE.11. WTG status during contingency with clearing of the fault at 1.295 sec, (a) WTG MVAR, (b) WTG MW, (c) WTG mechanical power

As shown in figure (11-a), the wind turbine generator start producing reactive power to the system at 1 sec instead of consuming it to support the system voltage during the contingency, and to stay connected with the grid. This behavior of WTG is similar to the one that obtained in the previous system (system with only WTG), but, the difference here is that the installation of PV panels in the system affects the MVAR behavior of the WTG after clearing the fault. This effect appears as an extra oscillations of the MVARS at around 3 sec.

From figure (11-b), the active power decreased to almost zero at 1 sec, then, it starts to increase after the fault is cleared just like the previous system. Hence, the PV station does not affect the MW behavior of the WTG.

As shown in figure (11-c), the mechanical power of the wind turbine generator starts at 20 MW (initial value) and continue to increase during the next 5 seconds (as expected). Hence, the PV station does not affect the mechanical power behavior of the WTG.

3.4 Comparison of the three systems

From the above results it can be noticed that the critical clearing time changed for each of the three systems; normal system, system with only wind turbine, and system with PV and WTG. The CCT of the normal system was 307 ms. When only wind turbine was added to the system, the CCT increased to 311 ms. But, when the PV station was added to the system, the CCT decreased to 295 ms. This means that the wind turbine has a small positive impact on the system stability compared to the large negative impact of PV panels. This is due to the absence of rotational masses (moment of inertia) in the stationary PV panels and the small inertia in the wind turbines.

By comparing the two systems; system with only WTG, and system with both PV and WTG, it can be noticed that the impact of adding PV panels on the wind turbine performance is small. The PV panels do not affect the MVAR behavior during the fault period. It affect the behavior after the fault is cleared by producing an extra oscillations on the MVAR signal when it tries to

reach stability after the disturbance diminishes. This is due to the lack of inertia in the stationary PV panels.

4. Conclusion

Based on the above results and discussion, it can be concluded that:

- The impact of PV panels on the wind turbine performance during transient contingencies appears in the reactive power signal of the wind turbine generator. It does not affect the reactive power behavior during the fault period, however, it affects the behavior of the reactive power after the fault is cleared by introducing extra oscillations to the signal.
- The WTG slightly increase the critical clearing time of the system whereas the PV panels significantly decrease it. This is because the WTG support the system's voltage by producing reactive power.

REFERENCES

[1] Glover, J., D., Sarma, M., S., and T., J., Overbye, (2010), "Power System Analysis and Design", 5th edn., US, Cengage Learning.

[2] Kundur, P., (1994), "Power System Stability and Control", US, McGraw-Hill.

[3] Eftekharnejad, S., Vittal, V., Heydt, G., Keel, B., and J., Loehr, (2013, May), "Impact of Increased Penetration of Photovoltaic Generation on Power Systems", IEEE Transaction on Power Systems, Vol.28, No.2, 893-901.

[4] Munkhchuluun, E., and L., Meegahapola, (2017, December), "Impact of the Solar Photovoltaic (PV) Generation on Long-Term Voltage Stability of a Power Network", 2017 IEEE Innovative Smart Grid Technologies - Asia (ISGT-Asia) conference, IEEE, 1-6.

[5] Tamimi, B., Cañizares, C., and K. Bhattacharya, (2013, July), "System Stability Impact of Large-Scale and Distributed Solar Photovoltaic Generation: The Case of Ontario, Canada", IEEE TRANSACTIONS ON SUSTAINABLE ENERGY, Vol.4, No.3, 680-688.

[6] Achilles, S., Schramm, S., and J., Bebic, (2008, February), "Transmission System Performance Analysis for High-Penetration Photovoltaics", National Renewable Energy Laboratory-Subcontract Report, 1-50.

[7] Acharya, S., and M., Ramezani, (2020, February), "Transient stability assessment for generators and DER integration into the IEEE 9 Bus system", 2020 IEEE Texas Power and Energy Conference (TPEC), IEEE, 1-6.

[8] Mohammad M. Almomani, Abdullah Al-Odienat, "The Impact of Wind Generation on Low Frequency Oscillation in Power Systems". *2021 IEEE PES/IAS PowerAfrica*, *August* 23-28, 2021.

[9] Nunes, M., et al., (2004, December), "Influence of the Variable-Speed Wind Generators in Transient Stability Margin of the Conventional Generators Integrated in Electrical Grids", IEEE TRANSACTIONS ON ENERGY CONVERSION, Vol.19, No.4, 692-701.

[10] Meegahapola, L., et al., (2008, September), "Transient Stability Analysis of a Power System with High Wind Penetration", 2008 43rd International Universities Power Engineering Conference, IEEE, 1-5.

[11] Gautam, D., et al., (2009, August), "Impact of Increased Penetration of DFIG-Based Wind Turbine Generators on Transient and Small Signal Stability of Power Systems", IEEE TRANSACTIONS ON POWER SYSTEMS, Vol.24, No.3, 1426-1434.

[12] B. T. Alkhamis and A. Al-Odienat, "The Application of Synchronverter for the Enhancement of Power System Stability," 2023 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 2023, pp. 44-49, doi: 10.1109/JEEIT58638.2023.10185786.

[13] T. M. Al-Jaafreh and A. Al-Odienat, "The Application of Deep Learning Techniques for Solar Power Forecasting," 2022 13th International Conference on Information and Communication Systems (ICICS), 2022, pp. 214-219, Irbid, Jordan, June 21-23, 2022.

Jordan Journal of Energy
Volume, Number, 2022

ISSN (Online): 2790-7678
ISSN (Print): 2790-766X

Jordan Journal of Energy (JJE)
Journal Homepage: http://dsr.mutah.edu.jo/index.php/jje
JEE an official peer review journal of Mutah University,

Future Low Inertia Power Systems: A Comprehensive Review of Virtual Inertia Emulation Techniques and Inertia Estimation Methods

Tamdher M. Al-Momani[1]*, Mohammad M. Al-Momani[2]
*[1]Electrical Engineering, Al-Balqa Applied University, Jordan
[1]tamaduralmomani@bau.edu.jo
[2]NEPCO, Jordan
[2]monqedmohammad@gmail.com

Received 17th June 2023; Accepted 19th August 2023
*Corresponding Author Email: **tamaduralmomani@bau.edu.jo**

ABSTRACT. *This review paper provides a comprehensive analysis of future low inertia power systems, focusing on the challenges posed by increased renewable energy penetration. The impact of low inertia on frequency response and system stability is examined, along with the critical penetration limit for renewable energy sources. The paper reviews various virtual inertia emulation techniques, including virtual synchronous machines, virtual induction machines, and inertia emulation in wind turbines and solar PV panels. Additionally, it explores specific methods such as VISMA, virtual synchronous generator, synchronverter, power synchronization control, and cascade virtual synchronous machine. The review also covers inertia algorithms in wind turbines, encompassing droop control, hidden inertia emulation, fast power reserve, over speed control, and pitch angle control. Furthermore, the paper discusses inertia estimation techniques, including both model-based and measurement-based approaches. The insights provided in this review will assist researchers and practitioners in developing effective solutions for addressing low inertia challenges in future power systems with high renewable energy integration*.

Keywords: Future low inertia power systems, Renewable energy penetration, Frequency response, Virtual inertia emulation, Virtual synchronous machine, Virtual induction machine, Wind turbine inertia algorithm, Inertia estimation, Model-based techniques, Measurement-based technique, VISMA.

1. Introduction. The motivation behind this paper is the increasing integration of renewable energy sources and the reduction of synchronous generators in modern power systems. These changes lead to a decrease in system inertia, which can compromise system stability and result in operational challenges. Therefore, the paper seeks to address this issue by reviewing various virtual inertia emulation techniques and inertia estimation methods that can be employed to compensate for the loss of system inertia. The goal is to provide a comprehensive examination of these techniques, evaluate their advantages and limitations, and highlight their suitability for different system configurations. By doing so, the paper aims to contribute to the development of reliable and efficient future low inertia power systems.

The literature review for this paper provides an overview of research on virtual inertia emulation techniques and inertia estimation methods in power systems. Several studies have been conducted on these topics, which are summarized below:

Control strategies for virtual inertia emulation: Several studies have proposed control strategies for emulating virtual inertia in power systems. For instance, [1] proposed a control strategy based on state feedback and adaptive backstepping to emulate virtual inertia in a grid-connected wind power system.

Energy storage systems for inertia emulation: Energy storage systems, such as batteries and supercapacitors, have been proposed as a means of emulating virtual inertia in power systems. [2] proposed a battery energy storage system (BESS) to emulate virtual inertia in a grid-connected PV system.

Frequency response analysis for inertia estimation: Frequency response analysis (FRA) has been proposed as a method for inertia estimation in power systems. For example, [3] proposed an FRA-based method for inertia estimation in a wind power system.

Kalman filter-based inertia estimation: Kalman filter-based methods have been proposed for inertia estimation in power systems. For instance, [4] proposed a Kalman filter-based method for inertia estimation in a microgrid. Similarly, [5] proposed a virtual inertia control strategy for a grid-connected photovoltaic (PV) system. [6] proposed a supercapacitor energy storage system for virtual inertia emulation in a microgrid.

For example, [7] proposed a multi-model approach for inertia estimation in a grid-connected wind power system. Model predictive control for virtual inertia emulation: Model predictive control (MPC) has been proposed as a control strategy for virtual inertia emulation in power systems [8] proposed an MPC-based control strategy for virtual inertia emulation in a grid-connected wind power system.

Optimal control strategies for virtual inertia emulation: Some studies have focused on developing optimal control strategies for virtual inertia emulation in power systems. For instance [9] proposed an optimal control strategy for virtual inertia emulation in a grid-connected PV system. Several studies have proposed advanced modelling approaches for inertia estimation in power, while [10] proposed a state observer-based approach for inertia estimation in microgrids.

Machine learning-based control strategies have been proposed for virtual inertia emulation in power systems. For example, [11] proposed a deep reinforcement learning-based control strategy for virtual inertia emulation in a wind power system. Machine learning techniques, such as artificial neural networks and support vector machines, have been proposed for inertia estimation in power systems. For example, [12] proposed a support vector machine-based method for inertia estimation in a microgrid.
Hybrid energy storage systems for virtual inertia emulation: Hybrid energy storage systems, such as batteries and supercapacitors, have been proposed for virtual inertia emulation in power

systems. For example, [13] proposed a hybrid energy storage system for virtual inertia emulation in a wind power system. Hybrid approaches: Some studies have proposed hybrid approaches that combine multiple techniques for virtual inertia emulation and inertia estimation. For instance, [14] proposed a hybrid approach that combines a proportional-integral-derivative (PID) controller and MPC for virtual inertia emulation in a grid-connected PV system.

Data-driven approaches for inertia estimation: Data-driven approaches, such as data clustering and pattern recognition, have been proposed for inertia estimation in power systems. For example, [15] proposed a data-driven approach for inertia estimation in a microgrid.

Adaptive control strategies for virtual inertia emulation: Adaptive control strategies, which can adjust the control parameters in real-time, have been proposed for virtual inertia emulation in power systems. For example, [16] proposed an adaptive control strategy for virtual inertia emulation in a grid-connected wind power system.

Now, we give some potential study gaps to consider:

Limited research on specific virtual inertia emulation techniques: While the concept of virtual inertia emulation is gaining attention, there may be a gap in specific studies comparing and evaluating different techniques. Further research could focus on the effectiveness, efficiency, and scalability of various virtual inertia emulation techniques in different power system scenarios.

Lack of comparative analysis: It may be beneficial to have more studies that compare the performance of different inertia estimation methods. Comparative analysis can help identify the strengths, limitations, and applicability of different methods in varying system conditions.

Need for practical implementation studies: Many studies focus on theoretical aspects of virtual inertia emulation and inertia estimation methods. However, there may be a gap in practical implementation studies that explore the challenges, limitations, and best practices for implementing these techniques in real-world power systems.

Limited consideration of economic aspects: While virtual inertia emulation and inertia estimation methods have the potential to improve power system operations, there may be gaps in research concerning the cost-effectiveness and economic viability of these approaches. Studies could explore the economic benefits and trade-offs associated with the adoption of such techniques.
Environmental impact assessment: Given the increasing importance of sustainability in power systems, research gaps may exist in assessing the environmental impact of virtual inertia emulation techniques and inertia estimation methods. Studies could incorporate environmental factors, such as carbon footprint reduction, into the evaluation of these approaches.

Integration challenges with renewable energy sources: As renewable energy penetration increases, there may be gaps in research addressing the specific challenges and opportunities

associated with integrating virtual inertia emulation techniques and inertia estimation methods in renewable energy-rich power systems.

2. FUTURE-LOW INERTIA POWER SYSTEM BACKGROUND

A. Power system inertia and renewable energy

Power system inertia refers to the ability of a power system to maintain its frequency in response to disturbances. Inertia is typically provided by synchronous generators, which are commonly used in conventional power systems. Synchronous generators are designed to operate at a constant speed and are connected to the power system through a mechanical shaft. When there is a disturbance in the system, the kinetic energy stored in the rotating mass of the generator provides a damping effect that helps to stabilize the system frequency.

Renewable energy sources, such as wind and solar, do not have the same inherent inertia as synchronous generators. This can make it more challenging to maintain system stability and prevent frequency fluctuations, particularly as the share of renewable energy in the power system increases.

Inverter-based generation, which includes solar PV and wind turbines with power electronics, operates differently from synchronous generators. Inverter-based systems convert DC power from the renewable energy source into AC power that can be integrated into the grid. Inverter-based systems can provide some level of synthetic inertia by adjusting their output in response to changes in system frequency. This can help to stabilize the system, but it is not as effective as the natural inertia provided by synchronous generators.

Wind generation is a significant source of renewable energy, and wind turbines are commonly used in power systems around the world. Wind turbines operate by converting the kinetic energy of the wind into mechanical energy that is used to drive a generator. The output of wind turbines can vary depending on the wind speed and direction, which can affect system frequency. To address this, wind turbines are typically equipped with power electronics that allow them to adjust their output in response to changes in system frequency. This can help to stabilize the system, but it is not as effective as the natural inertia provided by synchronous generators.

B. Frequency indices and critical RES

Frequency indices are measurements or parameters used to assess the stability and performance of a power system in terms of frequency deviation. These indices provide an indication of the system's ability to maintain a stable frequency under various operating conditions. Renewable Energy Sources (RES) play a crucial role in the power system, and their integration has an impact on frequency-related aspects. Some frequency indices and the criticality of RES integration are as follows:

Frequency Deviation: Frequency deviation is the difference between the actual frequency and the nominal frequency of the power system. This index is used to monitor the system stability. The integration of RES, especially large-scale wind and solar power plants, can affect frequency deviation due to their intermittent nature and variability in generation.

Rate of Change of Frequency (RoCoF): RoCoF measures the rate at which the system frequency is changing. It indicates the dynamic response of the system to disturbances. The integration of RES can impact RoCoF, particularly during sudden changes in renewable generation output or during the occurrence of faults in the system. RES with fast ramp rates can lead to significant RoCoF deviations.

Frequency Nadir: Frequency nadir represents the lowest frequency reached during a disturbance or event. It is an important indicator of the system's stability and the available margin for frequency control. The integration of RES can affect the frequency nadir, especially during high renewable penetration scenarios or when there is a lack of appropriate control measures.

Frequency Response: Frequency response refers to the ability of the power system to recover and return to its nominal frequency following a disturbance. The integration of RES can impact frequency response due to their limited or lack of inherent inertia. In systems with high RES penetration, additional measures such as grid-forming inverters or energy storage systems may be required to provide frequency response support. The criticality of RES integration lies in the need to maintain system stability and reliability while accommodating the variability and intermittency of renewable generation. As the share of RES in the power system increases, the challenges associated with frequency control and stability become more significant. Proper grid integration measures, advanced control strategies, and the deployment of energy storage systems can help mitigate these challenges and ensure the reliable and stable operation of the power system with a higher penetration of RES. It's important to note that the criticality and impact of RES integration on frequency indices may vary depending on the specific characteristics of the renewable technologies, their penetration levels, grid conditions, and the availability of appropriate control and mitigation measures.

3. REVIEW OF VIRTUAL INERTIA EMULATION METHODS

A. Virtual Synchronous Generator (VSG):

The Virtual Synchronous Generator (VSG) is a control strategy used to emulate the behaviour of synchronous generators in inverter-based systems, enabling the provision of synthetic inertia. Several implementations of VSG have been proposed and studied. Here are the key methods as shown in figure (1) [37]:

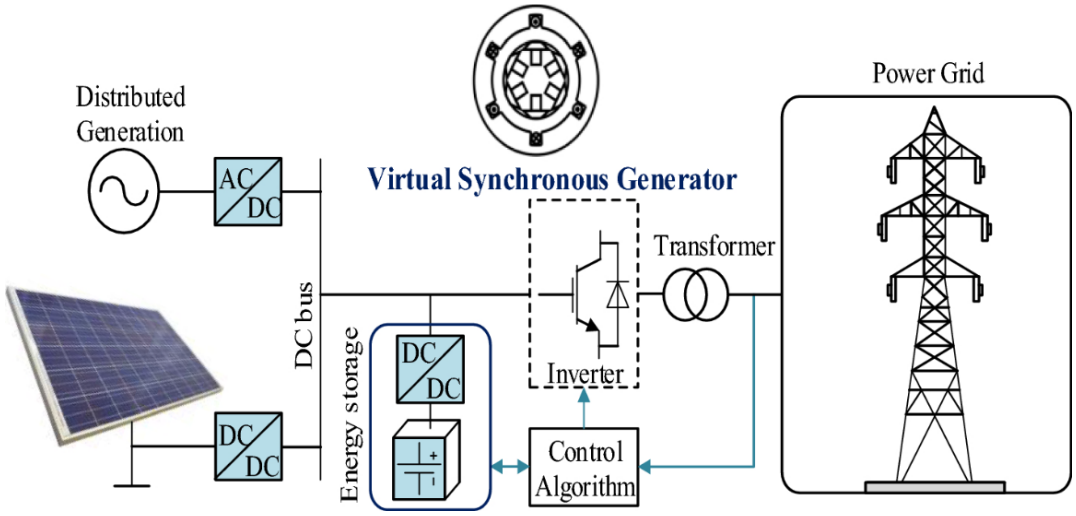


FIGURE 1. VSG concept

a. VISMA (Virtual Impedance and Synchronous Machine Algorithm):

VISMA combines virtual impedance control and synchronous machine emulation algorithms. It employs a virtual impedance loop to regulate the active and reactive power output of the inverter and a synchronous machine emulation algorithm to replicate the inertia and damping characteristics of a synchronous generator. VISMA has demonstrated stable frequency response and improved system stability as shown in figure (2). [38]

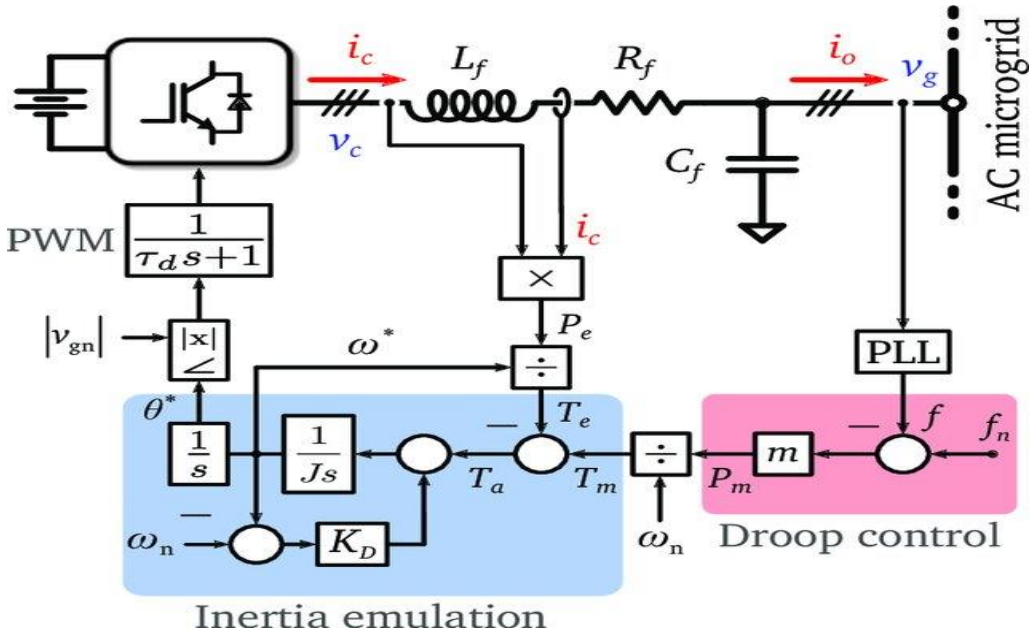


FIGURE 2. Current source based VISMA

b. Virtual Synchronous Generator:

The Virtual Synchronous Generator is a basic implementation that involves adjusting the inverter's control parameters to mimic a synchronous generator. By manipulating active and

reactive power setpoints, frequency and voltage droop characteristics, and phase-locked loop (PLL) parameters, the inverter can respond to changes in system frequency and voltage similar to a synchronous generator. This method has been widely investigated and applied in various studies. [18-19]

Synchronous generators are frequently subjected to various assumptions in order to cater to diverse research requirements, thereby rendering analysis and design more manageable. In light of the fact that the present article is solely concerned with the external features of synchronous generator inertia and damping characteristics, the second-order transient model of synchronous generators appears to be the most appropriate choice. This is evident from the Eq. (1) presented below, which is in conformity with the aforementioned model and is therefore deemed to be more suitable for the current research investigation. Consequently, it can be surmised that the adoption of this model would yield the most promising and efficacious results.

$$T_m - T_\varepsilon = \frac{P_m}{\omega} - \frac{P_\theta}{\omega} = J\frac{d\omega - \omega_0}{\omega} - D_p\omega - \omega_0 \qquad (1)$$

$$\omega = \frac{\mathrm{d}\theta}{\mathrm{dt}}$$

where J is the moment of inertia, D_p is the damping coefficient, ω is the angular frequency, and θ is the electrical angle; T_m is the mechanical torque and T_ε is the electromagnetic torque as shown Figure (3). [39]

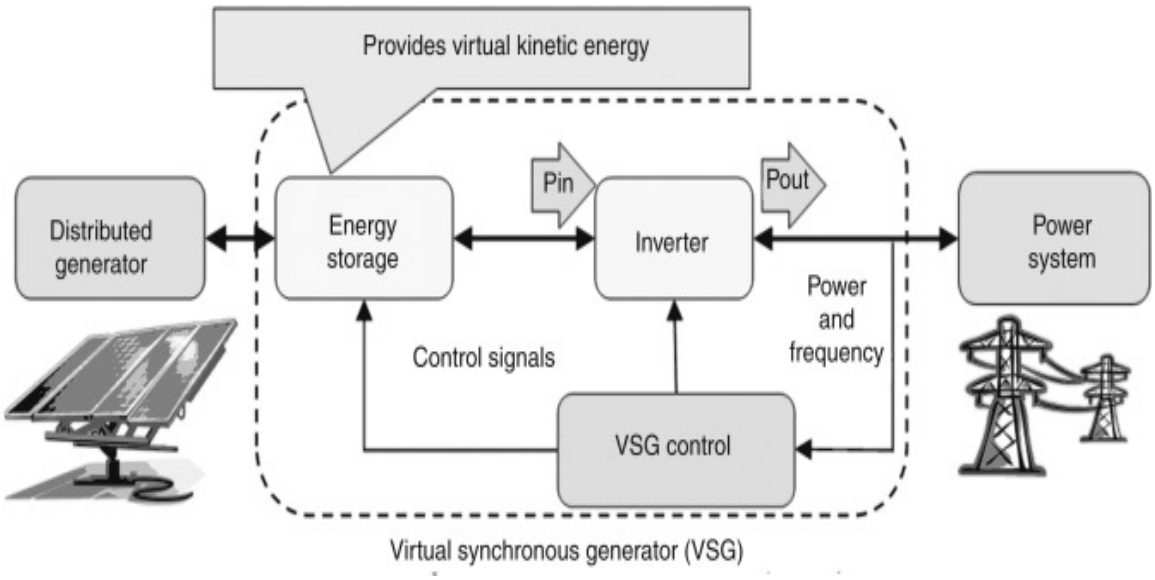


FIGURE 3. Virtual Synchronous Generator (VSG)

c. Synchronverter:

Synchronverter is another VSG implementation that relies on a combination of PLL and current control loops to synchronize the inverter output with the grid. By employing appropriate control algorithms, the Synchronverter can provide synthetic inertia and enhance system stability. This method has been examined in different research works as shown Figure (4). [36]

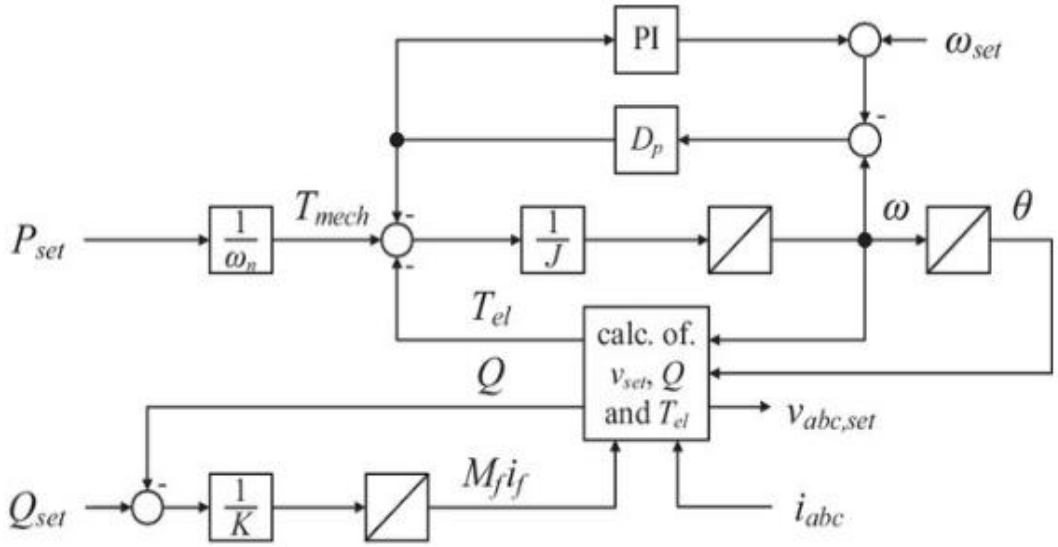


FIGURE 4. Synchronverter control

d. Power Synchronization Control:

Power Synchronization Control (PSC) focuses on achieving synchronization between the inverter output and the grid. It features a synchronization controller that adjusts the inverter's output frequency and phase angle based on the grid's frequency and voltage. PSC has been studied for its ability to provide virtual inertia and improve system stability. [22-23]

There is currently a proposed power-synchronization control law for VSCs.

$$\frac{d\Delta\theta}{dt} - k_p(f_{\text{ref}} - \rho') \qquad (2)$$

where P_{ref} is used as a reference for the active power, P is the measured active power output from the VSC, $k_p$is the controller gain, and $\Delta\theta$ is the output of the controller. $\Delta\theta$, as was already mentioned, directly supplies the synchronization for the VSC. During normal operation, a second PLL is obviously not needed. Similar to connected SMs, a VSC that uses power-synchronization control has a dynamic process. By moving the VSC's output voltage phasor forward or backward, the transmitted power can be increased or decreased. Section IV gives a thorough explanation of the power-synchronization loop's design as shown Figure (5). [22-23]

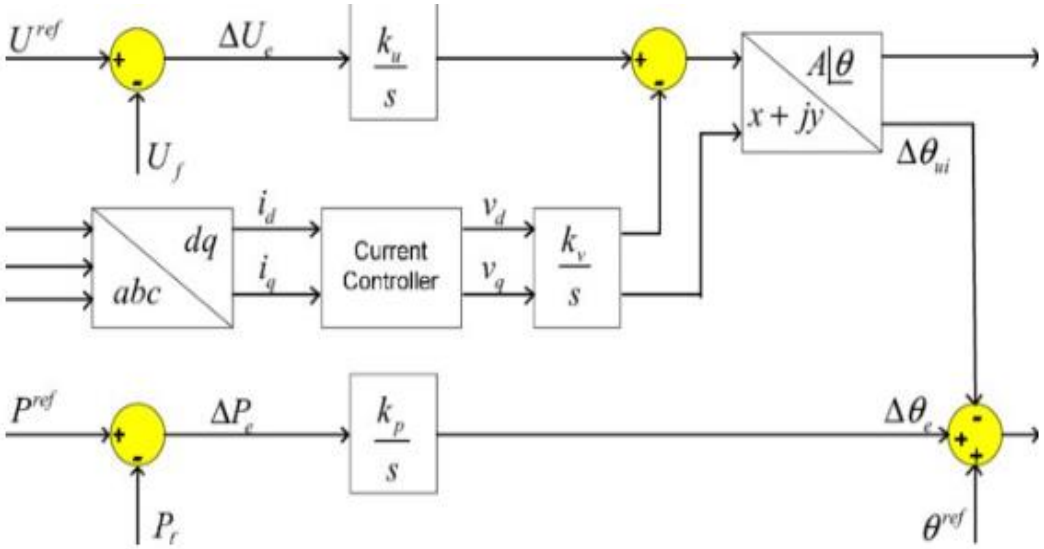


FIGURE 5. Power synchronization control

e. Cascade Virtual Synchronous Machine:

Cascade Virtual Synchronous Machine (VSM) uses a cascade control structure to emulate synchronous machine dynamics. It comprises an inner current control loop and an outer power control loop. The inner loop regulates inverter currents to emulate synchronous machine behaviour, while the outer loop adjusts active and reactive power setpoints based on system frequency deviation. Cascade VSM has been evaluated in various studies as shown Figure (6). [24-25]

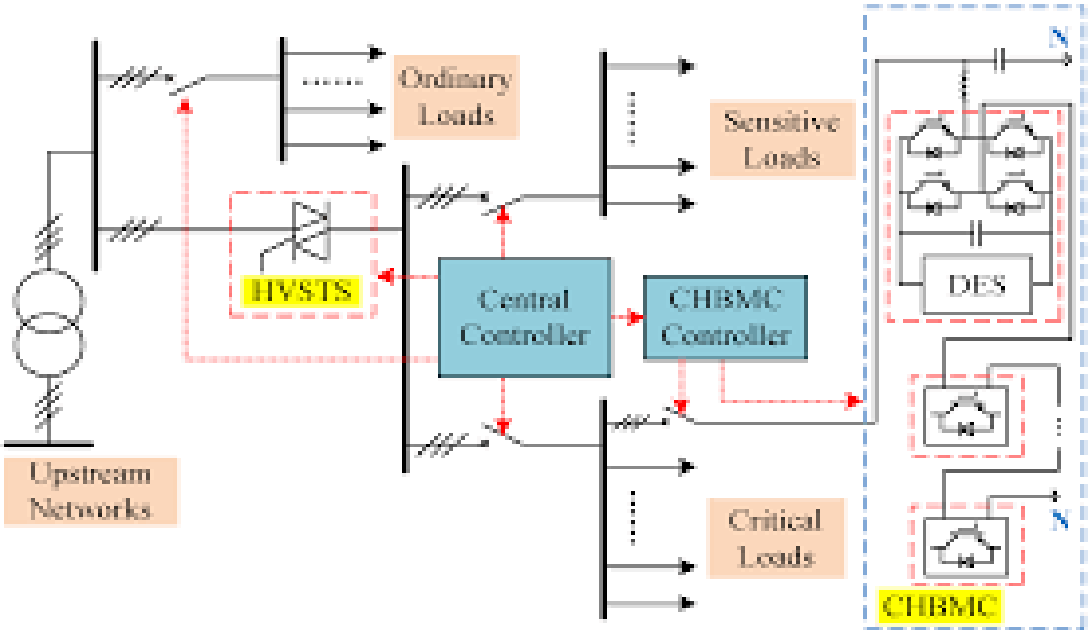


FIGURE 6. Cascade Virtual Synchronous Machine

These different implementations of VSG and virtual inertia emulation methods represent ongoing research and development efforts to enhance the integration of renewable energy sources (RES) into power systems. Each method has specific control algorithms and characteristics aimed at achieving stable frequency response, system stability, and improved RES grid integration. Continued advancements in these techniques are expected to optimize their performance and enable higher RES penetration.

Figure 7 summarizes the various methods discussed in literature for frequency regulation in the presence of RESs. [35]

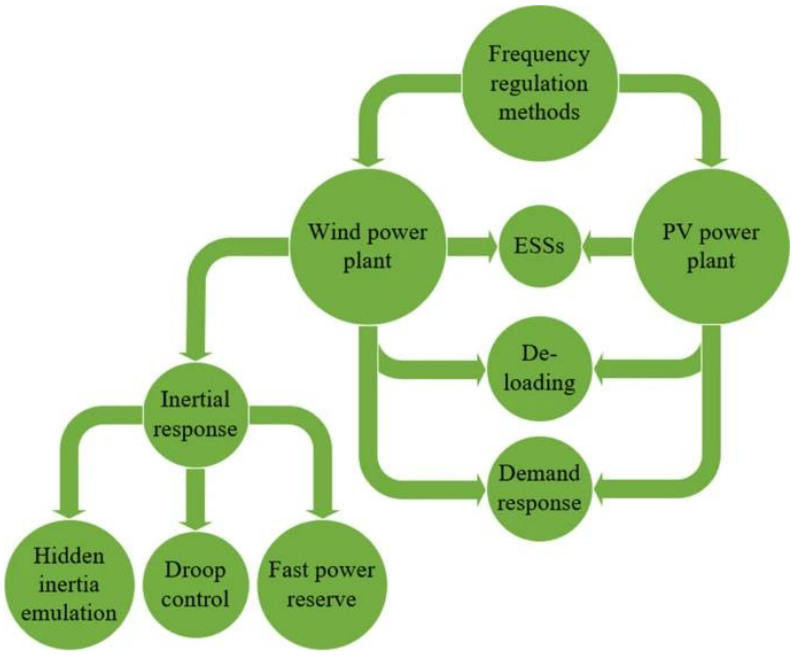


FIGURE 7. An overview of the frequency support techniques using RESs.

B. Induction emulation

Induction emulation, also known as virtual induction or virtual synchronous generator (VSG) emulation, is a control strategy used in grid-connected power electronic systems to provide dynamic response characteristics similar to those of a traditional synchronous generator or an induction machine. In power systems, synchronous generators with large rotating masses provide inertia, which helps stabilize the system during disturbances. However, in grid-connected power electronic systems such as renewable energy systems or microgrids, there may not be physical rotating machines with significant inertia. In such cases, induction emulation techniques are employed to mimic the behaviour of synchronous generators and provide virtual or synthetic inertia.

Induction emulation typically involves the implementation of control algorithms that regulate the power flow and dynamics of the power electronic converter by emulating the characteristics of an induction machine or a synchronous generator. These algorithms aim to replicate the inertial response and frequency stability of conventional generators, enhancing the stability and

reliability of the grid-connected system. The control algorithms used in induction emulation often incorporate virtual impedance and droop control methods. Virtual impedance control adjusts the output impedance of the power electronic converter to mimic the behaviour of an induction machine or synchronous generator. Droop control adjusts the power output in response to changes in system frequency, simulating the droop characteristics of synchronous generators. By implementing induction emulation techniques, grid-connected power electronic systems can provide stability support to the grid, enhance the system's ability to handle sudden changes in power demand or supply, and improve overall grid reliability and resilience.

C. Inertia emulation in wind technologies

The inertia emulation in wind technologies, including droop control, hidden inertia emulation, fast power reserve, over speed control, and pitch angle control:

a. Droop Control:

Droop control is a common method used in wind technologies for inertia emulation. It involves adjusting the output power of wind turbines based on changes in grid frequency. The control strategy is inspired by the droop characteristic of synchronous generators, where the output power is reduced as the grid frequency increases. By implementing droop control, wind turbines can contribute to grid stability by responding to frequency deviations. This control strategy allows wind turbines to emulate the inertial response of traditional generators, enhancing the system's ability to handle frequency variations.[26]

b. Hidden Inertia Emulation:

Hidden inertia emulation is a technique used in advanced wind turbine control systems to provide virtual inertia to the grid. It involves the use of advanced control algorithms to emulate the inertial response of conventional generators. The control system continuously monitors the grid frequency and adjusts the power output of the wind turbine accordingly, imitating the behaviour of synchronous generators. Hidden inertia emulation helps stabilize the grid during disturbances by providing an additional source of inertia.[27]

c. Fast Power Reserve:

Fast power reserve is a feature implemented in wind turbines to provide a quick response to frequency deviations in the grid. It involves the capability of wind turbines to rapidly increase or decrease their power output to support grid stability. Fast power reserve helps in maintaining grid frequency within acceptable limits during sudden changes in power demand or supply. By quickly adjusting their power output, wind turbines with fast power reserve contribute to inertia emulation and assist in grid stability.[28]

d. Over Speed Control:

Over speed control is a safety feature in wind turbines that limits the rotational speed of the turbine rotor. It is designed to prevent the turbine from operating at excessively high speeds, which can cause mechanical stress and damage to the turbine components. Over speed control systems monitor the rotational speed and adjust the pitch angle or break the turbine to limit the

speed within safe operating limits. By controlling the rotor speed, over speed control ensures the safe and reliable operation of wind turbines.[29]

e. Pitch Angle Control:

Pitch angle control is a commonly used control strategy in wind turbines to regulate the power output and maintain stable operation. It involves adjusting the angle of the turbine blades to optimize the capture of wind energy. By changing the pitch angle, wind turbines can control the aerodynamic forces acting on the blades and adjust the power output. Pitch angle control is essential for maintaining the turbine's power output within safe limits and optimizing the turbine's performance under varying wind conditions.[30]

4. REVIEW OF INERTIA ESTIMATION ALGORITHMS

Inertia estimation algorithms are used to estimate the inertia of power systems. Accurate estimation of inertia is important for system stability and control. There are several methods for inertia estimation, including model-based algorithms, data-driven algorithms, and hybrid algorithms. This review focuses on model-based algorithms for inertia estimation, which involve the use of mathematical models of the power system to estimate inertia. Model-based algorithms can be classified into two categories: single machine model and multi-machine model.

A. Model-Based Algorithms:

Model-based algorithms involve the use of mathematical models of the power system to estimate inertia. These algorithms are based on the fundamental physical principles of the power system and are generally more accurate than data-driven algorithms. Model-based algorithms can be further classified into two categories: single machine model and multi-machine model.

a. Single Machine Model:

Single machine model-based algorithms estimate the inertia of a power system using a mathematical model of a single machine. The algorithm estimates the inertia by measuring the response of the machine to a disturbance. The response is then used to calculate the machine's inertia. Single machine model-based algorithms are relatively simple and easy to implement, but they are limited to small power systems where the dynamics of the entire system can be approximated by a single machine.[31]

b. Multi-Machine Model:

Multi-machine model-based algorithms estimate the inertia of a power system using a mathematical model of multiple machines. The algorithm estimates the inertia by measuring the response of the machines to a disturbance. The response is then used to calculate the inertia of the entire system. Multi-machine model-based algorithms are more accurate than single machine model-based algorithms and can be used for larger power systems. However, they are

more complex and require detailed information about the system's topology and parameters.[32]

B. Measurement based algorithms

Measurement-based algorithms are used to estimate the inertia of power systems based on measurements from the system. These algorithms are based on the analysis of the system's response to disturbances or ambient data. Measurement-based algorithms can be further classified into two categories: ambient data-based estimation and large disturbance-based estimation.

a. Ambient Data-Based Estimation:

Ambient data-based estimation involves the use of measurements from the system under normal operating conditions to estimate the inertia. The algorithm analyses the frequency response of the system to ambient disturbances and uses this information to estimate the inertia. Ambient data-based estimation algorithms are relatively simple and do not require any additional disturbances to be introduced to the system. However, they are generally less accurate than large disturbance-based estimation algorithms.[33]

b. Large Disturbance-Based Estimation:

Large disturbance-based estimation involves the use of measurements from the system during large disturbances to estimate the inertia. The algorithm analyses the frequency response of the system to large disturbances and uses this information to estimate the inertia. Large disturbance-based estimation algorithms are more accurate than ambient data-based estimation algorithms but require the introduction of large disturbances to the system, which may not be practical in some cases.[34]

5. CONCLUSION

Inertia emulation is an important aspect of wind technologies that helps in stabilizing the grid during disturbances. Droop control, hidden inertia emulation, fast power reserve, over speed control, and pitch angle control are some of the common methods used for inertia emulation in wind turbines. These control strategies allow wind turbines to emulate the inertial response of traditional generators, enhancing the system's ability to handle frequency variations.
Inertia estimation algorithms are used to estimate the inertia of power systems, which is important for system stability and control. Model-based algorithms and measurement-based algorithms are two categories of inertia estimation algorithms. Model-based algorithms involve the use of mathematical models of the power system to estimate inertia, while measurement-based algorithms use measurements from the system to estimate inertia. Single machine model-based algorithms and multi-machine model-based algorithms are two types of model-based algorithms. Ambient data-based estimation and large disturbance-based estimation are two types of measurement-based algorithms.

In conclusion, the above topics highlight the importance of inertia emulation and estimation in power systems. The control strategies and algorithms discussed in the above topics play a crucial role in maintaining grid stability and ensuring reliable operation of power systems. These topics demonstrate the continuous efforts being made in the field of power systems to improve system stability and control.

There are some potential future works as follows:

1. Development of advanced control strategies for inertia emulation that can handle a wide range of operating conditions and disturbances.
2. Investigation of the impact of wind turbine control strategies on the stability and reliability of the grid.
3. Development of innovative methods for integrating wind power into power systems with increased reliability and stability.
4. Study of the influence of wind turbine parameters such as rotor size, blade pitch angle, and generator rating on the effectiveness of inertia emulation strategies.
5. Exploration of the potential for using renewable energy sources other than wind, such as solar and hydropower, for inertia emulation.
6. Development of hybrid algorithms that combine the strengths of both model-based and measurement-based algorithms for more accurate inertia estimation.
7. Investigation of the impact of communication delays and measurement errors on the accuracy of inertia estimation algorithms.
8. Exploration of the use of machine learning techniques for inertia estimation, such as deep learning and reinforcement learning.
9. Study of the impact of increasing renewable energy penetration on the accuracy of inertia estimation algorithms.
10. Development of real-time inertia estimation algorithms that can provide accurate estimates of inertia for fast-acting control strategies.

Acknowledgment. The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] B. Li, Y. Liu, and L. Chen, "Virtual inertia control for grid-connected wind power based on state feedback and adaptive backstepping," Energy Conversion and Management, vol. 158, pp. 164-174, 2018.

[2] L. Wang, Y. Li, and S. Wang, "Battery energy storage system for virtual inertia emulation and frequency control of grid-connected photovoltaic system," Renewable Energy, vol. 118, pp. 853-865, 2018.

[3] S. Huang, K. Kalsi, and J. Fuller, "Inertia estimation in wind power plants using frequency response analysis," IEEE Transactions on Sustainable Energy, vol. 9, no. 3, pp. 1419-1428, 2018.

[4] J. Chen, H. Xu, and Y. Mao, "Inertia estimation in microgrid based on Kalman filter," Journal of Modern Power Systems and Clean Energy, vol. 6, no. 4, pp. 708-715, 2018.

[5] J. Liu, J. Liu, and W. Qiao, "Virtual inertia control strategy for grid-connected photovoltaic system," Journal of Renewable and Sustainable Energy, vol. 11, no. 3, 033301, 2019.

[6] X. Li, M. Zhu, and H. Wang, "Supercapacitor energy storage system for virtual inertia emulation in microgrid," IEEE Transactions on Power Electronics, vol. 34, no. 3, pp. 2694-2707, 2019.

[7] X. Zhang, Y. Li, and X. Ma, "Multi-model-based inertia estimation for grid-connected wind power system," IEEE Transactions on Sustainable Energy, vol. 10, no. 2, pp. 871-880, 2019.

[8] S. Huang, K. Kalsi, and J. Fuller, "Model predictive control for virtual inertia emulation in wind power plants," IEEE Transactions on Sustainable Energy, vol. 10, no. 1, pp. 207-216, 2019.

[9] M. Cucuzzella, F. D'Ippolito, and R. Lamedica, "Optimal control strategy for virtual inertia emulation in grid-connected photovoltaic systems," Renewable Energy, vol. 139, pp. 1177-1188, 2019.

[10] Y. Chen, M. Chen, and X. He, "State observer-based inertia estimation for microgrids," IEEE Transactions on Smart Grid, vol. 11, no. 2, pp. 1296-1306, 2020.

[11] S. Huang, Y. Wu, and K. Kalsi, "Deep reinforcement learning-based control for virtual inertia emulation in wind power plants," IEEE Transactions on Sustainable Energy, vol. 11, no. 3, pp. 1595-1604, 2020.

[12] Y. Zhang, Z. Lu, and L. Zhao, "Inertia estimation for microgrid based on support vector machine," IEEE Access, vol. 8, pp. 123885-123894, 2020.

[13] J. Liu, H. Yang, and X. Wang, "Hybrid energy storage system for virtual inertia emulation in a wind power system," Journal of Modern Power Systems and Clean Energy, vol. 8, no. 3, pp. 594-603, 2020.

[14] S. Huang, Y. Wu, and K. Kalsi, "Hybrid control for virtual inertia emulation in grid-connected photovoltaic systems," Electric Power Systems Research, vol. 190, 106627, 2021.

[15] H. Li, J. Wang, and Y. Zhang, "A data-driven approach for inertia estimation in microgrid," Electric Power Systems Research, vol. 192, 106966, 2021.

[16] L. Yu, Y. Zhang, and X. Yin, "Adaptive control strategy of virtual inertia for grid-connected wind power system," Journal of Renewable and Sustainable Energy, vol. 13, no. 4, 043305, 2021.

[17] V. N. Mettananda, J. Ekanayake, and N. Jenkins, "Virtual Impedance and Synchronous Machine Algorithm for Inertia Emulation in Grid-Connected Converters," IEEE Transactions on Power Electronics, vol. 30, no. 11, pp. 6035-6044, Nov. 2015.

[18] J. M. Guerrero et al., "Virtual synchronous generators for integrating distributed generation into the grid," IEEE Industrial Electronics Magazine, vol. 9, no. 1, pp. 28-39, Mar. 2015.

[19] S. Liu, X. Zhang, and J. Wang, "Control strategies of virtual synchronous generator in microgrid," 2015 IEEE 15th International Conference on Environment and Electrical Engineering (EEEIC), pp. 1213-1218, Rome, Italy, Jun. 2015.

[20] S. Ghosh and A. M. Gole, "A New Control Strategy of Virtual Synchronous Generator for Grid-Connected Distributed Generation," IEEE Transactions on Energy Conversion, vol. 28, no. 2, pp. 392-401, Jun. 2013.

[21] S. Ghosh and A. M. Gole, "Virtual synchronous generator control of a grid-connected inverter for distributed generation," IEEE Transactions on Energy Conversion, vol. 27, no. 4, pp. 907-916, Dec. 2012.

[22] J. M. Guerrero et al., "Power synchronization control: A new active power decoupling method for power converters operating in parallel," IEEE Transactions on Power Electronics, vol. 19, no. 4, pp. 1025-1034, Jul. 2004.

[23] J. M. Guerrero et al., "Power-Synchronization Control of Distributed Power-Generation Systems," IEEE Transactions on Industrial Electronics, vol. 53, no. 5, pp. 1461-1470, Oct. 2006.

[24] X. Rong et al., "A novel control strategy based on cascade virtual synchronous machine for grid-connected inverters," IEEE Transactions on Industrial Electronics, vol. 64, no. 6, pp. 5077-5086, Jun. 2017.

[25] H. Li, Z. Chen, and S. Yang, "A Novel Virtual Synchronous Machine Control Strategy With Cascade Current and Power Loops," IEEE Transactions on Industrial Electronics, vol. 65, no. 5, pp. 4024-4035, May 2018.

[26] A. D. Hansen, C. P. Butterfield, "Pitch-controlled variable-speed wind turbine generation," in IEEE Transactions on Industry Applications, vol. 37, no. 1, pp. 240-246, Jan.-Feb. 2001.

[27] A. D. Hansen and P. Sørensen, "Hidden Markov model-based control of wind turbines for power system stability enhancement," in IEEE Transactions on Power Systems, vol. 27, no. 1, pp. 101-110, Feb. 2012.

[28] L. Gosselin and J. Morren, "Ancillary services from wind power plants: Field tests on up and down regulation and automatic generation control," in IEEE Transactions on Sustainable Energy, vol. 3, no. 4, pp. 796-805, Oct. 2012.

[29] J. D. Sørensen and A. M. Hansen, "Control of wind turbines: Past, present, and future," in IEEE Control Systems, vol. 32, no. 1, pp. 76-92, Feb. 2012.

[30] T. Burton, D. Sharpe, N. Jenkins and E. Bossanyi, "Wind energy handbook," John Wiley & Sons, 2011.

[31] M. Mohandes, A. Abido and S. Al-Hajjaji, "Robust decentralized power system stabilizer design using particle swarm optimization technique," in IEEE Transactions on Power Systems, vol. 20, no. 1, pp. 34-41, Feb. 2005.

[32] C. Jin, J. Chen, Y. Qi and Y. Liu, "A novel inertia estimation method for power system based on wide-area measurement system," in IEEE Transactions on Power Systems, vol. 33, no. 2, pp. 1868-1876, March 2018.

[33] H. Chen, X. Xu and X. Li, "Inertia estimation of power systems via ambient data," in IEEE Transactions on Power Systems, vol. 30, no. 2, pp. 1086-1094, March 2015.

[34] Y. Liu, C. Jin and B. Pal, "A new approach for online estimation of power system inertia," in IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 3040-3049, Aug. 2013.

Jordan Journal of Energy
Volume 1, Number 2, 2023

ISSN (Online): 2790-7678
ISSN (Print): 2790-766X

Jordan Journal of Energy (JJE)
Journal Homepage: http://dsr.mutah.edu.jo/index.php/jje
JEE an official peer review journal of Mutah University,

Adaptive Active Frequency Drift Islanding Detection for PV Inverters

Khaled Al-Maitah
Electricity Distribution Company (EDCO), Jordan
kmaitah@edco.jo

Received 15th June 2023; Accepted 17th August 2023

ABSTRACT. *The penetration level of renewable energy resources (RESs), such as photovoltaic (PV) plant and Wind plant (WP), in the power system is increasing exponentially, such plants connected with grid via inverter. This increasing rises from the attention about the undetected islanding operation. The islanding can be defined, according to IEEE std.1547, as a situation in which part of the power system becomes isolated from the rest of the system.*

Islanding detection methods (IDMs) are divided into passive and active IDM. Among active IDMs, active frequency drift (AFD) is the most IDM applied in the literatures. AFD bases on injecting a distortion waveform to the original waveform of inverter reference current, this to drift the inverter frequency during islanding event to be out of the nominal range. Due to the distortion waveform high harmonics will be injected to the system. Recently, to decrease this harmonic an improved active frequency drift (IAFD) was presented in the literature. IAFD uses a constant step change in in 2nd and 4th quarters of the inverter reference current. IAFD has lower total harmonic distortion (THD) injected to the system compared with conventional AFD.

Since the non-detection zone (NDZ) has been considered as a performance measure for any IDM. The IAFD method did not introduce any improvement in NDZ over the AFD method. Thus, in this paper an adaptive step change is proposed to improve the performance of IAFD method, where a positive feedback of voltage frequency is used in this work to vary the distortion factor of IAFD. The adaption manner of step change enhances in increasing of injected perturbations during islanding event only. Which, it will reduce the NDZ during islanding event and decrease the injected THD in steady state operation. The proposed method has been theoretically analyzed and modeled using MATLAB/Simulink environment. As a result, the proposed method improves the performance of IAFD regard to the non-detection zone (NDZ).

Keywords: Islanding detection, active frequency drift, non-detection zone, total harmonic distortionAdaptive protection,

1. Introduction. The penetration level of renewable energy resources (RESs), such as photovoltaic (PV) plant and Wind plant (WP), in the power system is increasing exponentially,

such plants connected with grid via inverter [1], [2]. This increasing rises from the attention about the undetected islanding operation [3]. The islanding can be defined, according to IEEE std.1547 [4], as a situation in which part of the power system becomes isolated from the rest of the system.

The islanding situation was divided into intentional islanding and unintentional islanding. The intentional islanding is doing by operators for urgent and routine maintenance. The unintentional islanding occurs due to fault in the network. If these situations are not detected, serious problems may occur such as manpower safety, protection, and power quality problems [5].

The IEEE Standard 929 [6] and Standard 1547 [4] restrict the normal operation parameters (voltage, frequency, and total harmonic distortion (THD), and specify the allowed time to detect the islanding situations. Additionally, the standards suggest steps and testbed system to test the islanding detection methods (IDM).

IDM for gride-tie inverter can be classified into remote and local methods. Remote methods are those methods which use the communication infrastructure and located at utility level. Remote methods are characterized by high reliability and depend on the communication system reliability, but its implementation is expensive and complex. On the other hand, the local methods are those methods that utilize the measured quantities in the local level and located inside each distributed generation (DG) unit or grid-tie inverter. In more details, the local IDM are further divided to passive and active IDM.

Passive IDM are utilizing the measured parameters (voltage, frequency, active and reactive power, THD, ...etc.), to detect the islanding events, by comparing the measured parameters with predefined threshold values. The under/over frequency (UOF), under/over voltage (UOV), active power variation IDMs were presented in [1], [7], [8]. IDM by reactive power was presented in [9]. Rate of change of frequency IDM was presented in [10]. Voltage with THD IDM was presented in [11]. Power factor variation with voltage IDM was presented in [12]. Although, these methods do not have any impact on the power quality, because there is no control action, it was characterized by large Non-detection zone (NDZ) [5]. NDZs are determinable conditions, IDM may fail to detect islanding situation at those conditions. NDZ has been considered as a performance measure for any IDM.

Active methods were proposed in the literatures to increase the performance of islanding detection. The active methods have lower NDZ compared with passive methods [13]. The operation principle of active methods based on injects a small distortion signal in the system to force at least one of the system parameters out of the normal operation limits during islanding events. Although, the injected distortion causes some of issues in power quality specially for THD, the active methods are the most methods among IDMs reported in the literatures, that because it is effective on the NDZ reducing.

The active IDMs further can be classified according to its target actions to active voltage drift (AVD) method and active frequency drift (AFD) method [14], [15]. In AVD IDM, the injected perturbation will be able to drift the voltage at the point of common coupling (PCC) to activate

the UOV protection relay during islanding events [1]. AFD IDM able to drift the frequency to activate the UOF protection relay during islanding events. AFD method was proposed in [16], [17]. Where, the AFD method has been mathematically analyzed, as a result the NDZ of AFD method highly depends on the load quality factor (Q) and zero conduction time (tz) in the distorted current waveform. The NDZ reduced with large tz. On the other hand, the large value of tz ¬is resulting higher THD. To reduce NDZ, an AFD with positive feedback (AFDPF), which aka as sandia frequency shift (SFS), was proposed in [18], [19]. SFS is expansion of the AFD method [14]. In SFS a positive feedback of frequency of the voltage at PCC is used to change the chopping fraction (Cf). Where, Cf is a function of the frequency deviation between the voltage frequency at PCC and the nominal frequency [18]. An improved active frequency drift (IAFD) with new distortion waveform, based on constant step change in 2nd and 4th quarters of the inverter reference current waveform, was proposed in [13], the IAFD injects 30% less THD compared with conventional AFD, but the authors limit their study in single PV grid connected inverter. To the best of our knowledge, the performance of using of positive feedback of voltage frequency with IAFD did not study in the literatures.

In this paper a modified IAFD method is proposed. The proposed method is extension of IAFD method, where a positive feedback of frequency of the voltage at PCC has been added to the IAFD. This modification enhances the performance of IAFD by further reducing the NDZ and further decreasing of the injected THD to the system at steady state operation. Where, the step change in 2nd and 4th quarters of the inverter reference current waveform will be a function of frequency deviation between the PCC voltage frequency and nominal frequency. The adaption manner of step change enhances in increasing of injected perturbations during islanding event only. Which, it will reduce the NDZ during islanding event and decrease the injected THD in steady state operation.

2. Review of Active Frequency Drift AFD:

For better understand the proposed method, an overview of conventional active frequency drift (AFD) and the improved active frequency drift (IAFD) method were presented in this section. The main principle of conventional AFD bases on injecting a distortion waveform to the original waveform of inverter reference current, that to drift the inverter frequency during islanding event. The original, distorted, and AFD reference current waveforms are shown in Fig.1. By distorted waveform, a permanent drift will be produced to drift the operation frequency toward the resonance frequency of the load and force the frequency to be out of the normal operation limits.

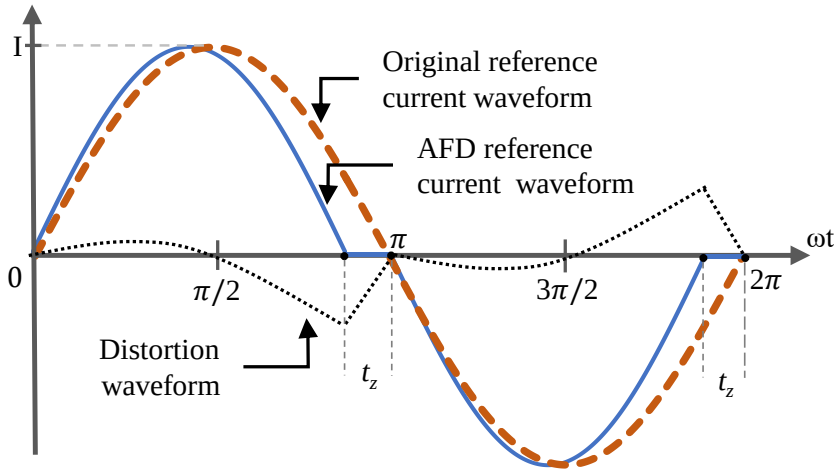


FIGURE.1 Original, AFD, and distortion waveform

The distortion level can be controlled by zero-conduction time (t_z) which can be expressed as chopping fraction (C_f) as in (1), where the greater t_z, the greater C_f hence a larger distortion will be introduced to the reference current.

$$C_f = \frac{t_z}{T} \tag{1}$$

Where, t_z is the zero-conduction time and T is the original signal period (2π). Thus, the reference current of AFD shown in Fig.1 can be expressed as in (2),

$$i_{AFD}(t) = \begin{cases} I\sin(\omega' t) & \rightarrow \quad 0 \le \omega t \le \pi - t_z \\ 0 & \rightarrow \quad \pi - t_z \le \omega t \le \pi \\ I\sin(\omega' t) & \rightarrow \quad \pi \le \omega t \le 2\pi - t_z \\ 0 & \rightarrow \quad 2\pi - t_z \le \omega t \le 2\pi \end{cases} \tag{2}$$

Where $\omega' = \omega\left(\frac{1}{1-C_f}\right)$

When grid-tie inverter connected with local parallel RLC load and an islanding event is occurred, the operation frequency will drift to the resonance frequency of the local load. Thus, phase angle criteria can be applied ($\theta_{load} = \theta_{AFD}$) as in (3), where $\theta_{AFD} = 0.5\pi C_f$ [16].

$$arg\,[R^{-1} + (j\omega L)^{-1} + j\omega C]^{-1} = 0.5\pi C_f \tag{3}$$

Where the operator arg determine the angle of local load in radian, C_f is the chopping fraction as given in (1). However, this method is effective, but it has a large NDZ for some RLC load combinations, and it injects high harmonics to the system. To overcome these issues a positive feedback was proposed in [16] to vary the chopping fraction (C_f) as in (4).

$$C_f = C_{f_o} + \beta(f_g - f) \tag{4}$$

Where, C_{f_o} is the initial value of chopping fraction, f is the nominal frequency (50 or 60 Hz), f_g is the grid frequency at PCC, and β is the acceleration rate. These improves the NDZ for different load types, but still effect on the power quality by introducing harmonic components. Where according to [20], in AFD, the THD $\approx Q/P \approx C_f$. To drive the frequency out of limit, a

large $\Delta Q/P$ is needed, consequence a large C_f is required, then high harmonics will be injected to the system [21-22].

To decrease the THD produced from AFD an IAFD, that uses different distortion signal, was proposed in [13]. IAFD uses a new distortion waveform, it bases on constant step change in 2nd and 4th quarters of the inverter reference current waveform. The waveforms of original, distorted and IAFD reference current waveforms are shown in Fig.2.

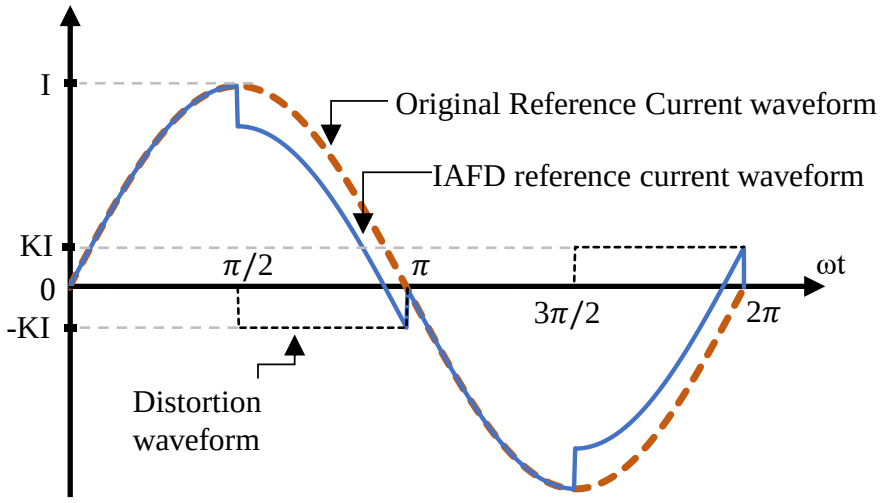


FIGURE.2 Original, IAFD, and distortion waveforms

The reference current waveform of IAFD can be expressed as,

$$i_{IAFD}(t)= \begin{cases} I\sin(\omega t) & \rightarrow \quad 0 \le \omega t \le \pi/2 \\ I\sin(\omega t) - KI & \rightarrow \quad \pi/2 \le \omega t \le \pi \\ I\sin(\omega t) & \rightarrow \quad \pi \le \omega t \le 3\pi/2 \\ I\sin(\omega t) + KI & \rightarrow \quad 3\pi/2 \le \omega t \le 2\pi \end{cases} \tag{5}$$

Where, K is a constant represents the detorsion factor. IAFD method decreases the injected THD to about 30% compared with AFD method. However, according to [13] the THD produced by IAFD is expressed as,

$$\mathrm{THD_{IAFD}} = \sqrt{\frac{K^2(\pi^2 - 8)}{\pi^2 - 4\pi K + 8K^2}} \tag{6}$$

In addition, the phase angle θ_1 of the fundamental IAFD reference current was expressed in [13] as in (7),

$$\theta_1 = tan^{-1}\left(\frac{2K}{\pi - 2K}\right) \tag{7}$$

Where, K is a constant represents the detorsion factor. Since the active power and reactive power of sinusoidal waveform are defined as in (8) and (9), respectively, the Q/P ratio can be expressed as in (10),

$$P = V \cdot I_1 \cdot \cos(\theta_1) \tag{8}$$

$$Q = V \cdot I_1 \cdot \sin(\theta_1) \tag{9}$$

$$\frac{Q}{P} = tan(\theta_1) = \frac{2K}{\pi - 2K} \quad (10)$$

Where, I_1 and θ_1 are the rms value and the phase angle of the fundamental reference current waveform. As a comparison between AFD and IAFD, THD ≈ *Q/P* for AFD, consequence the maximum allowable value of *Q/P* is (5%) that because THD limitation. On the other hand, based on (10) to produce *Q/P* = 5% in IAFD the distortion factor will be *K* = 0.075. Thus, based on (6) the THD will be about 3.4%. In other word, the IAFD success in decrease the THD as compared with conventional AFD.

Regarding to the NDZ, the IAFD method did not introduce any improvement in NDZ over the AFD method, Where the NDZ of IAFD approximately equal to the NDZ of AFD. This has motivated the present work to modify the IAFD to decrease NDZ.

3. The Proposed Method

As stated in the previous section, the distortion waveform in IAFD was a constant step change in 2nd and 4th quarters, where the distortion factor *K* in IAFD was constant. The proposed method in the present work, a positive feedback of the grid voltage frequency has been used to vary the distortion factor *K*. Consequently, the distortion factor *K* is a function of frequency deviation between the grid frequency f_g and nominal frequency *f*, this can be given as,

$$K(f) = K_o + \beta(f_g - f) \quad (11)$$

Where, K_o is the initial value of distortion factor, β is the accelerating factor of the proposed method, f_g is the grid frequency at PCC, and *f* is the nominal frequency (50 or 60 Hz). Thus, the phase angle θ_1 of the fundamental reference current will be as,

$$\theta_1 = tan^{-1}\left(\frac{2K(f)}{\pi - 2K(f)}\right) \quad (12)$$

Where, *K(f)* is the distortion factor as given in (11). The angle of local load can be calculated as,

$$\theta_{load} = tan^{-1}\left(Q_f\left[\frac{f_0}{f} - \frac{f}{f_0}\right]\right) \quad (13)$$

Where, Q_f is the load quality factor. f_0 is the resonance frequency of the load. To determine the NDZ of the proposed method, the phase angle criteria can be applied ($\theta_1 = \theta_{load}$) as,

$$tan^{-1}\left(\frac{2K(f)}{\pi - 2K(f)}\right) = tan^{-1}\left(Q_f\left[\frac{f_0}{f} - \frac{f}{f_0}\right]\right) \quad (14)$$

Thus, after reorganizing the equation (14), the NDZ of the proposed method can be determine by solve the following second order equation,

$$f_o^2 - \frac{2fK(f)}{Q_f(\pi - 2K(f))} f_o - f^2 = 0 \quad (15)$$

Where, $K(f)$ is the distortion factor as given in (11) and f_o is the resonance frequency of load. To calculate the NDZ of the proposed method, the islanding frequency f is first adjusted to a threshold frequency (f_{min} or f_{max}). Then the value of Q_f is varied, and finally the resonant frequency f_o of the load is calculated at the threshold of the NDZ.

In the proposed method the distortion factor K is continuously variated by the acceleration rate β. When the acceleration rate is zero the proposed method becomes an IAFD. However, the NDZ of the proposed IDM versus the quality factor Q_f, with distortion factor $K = 0.105$, nominal frequency $f = 60$ Hz, and difference acceleration rate β, is presented in Fig. 3.

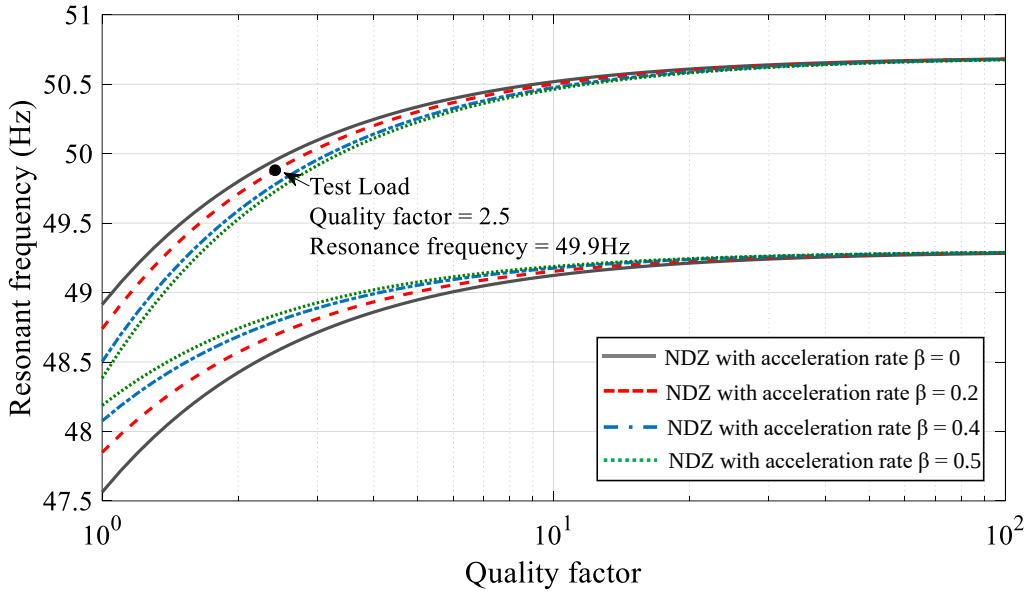


FIGURE. 3. NDZ for the proposed methods with K = 0.105 and difference acceleration rate β.

As seen in Fig.3, the more acceleration rate, the smaller NDZ. By using acceleration rate β zero the NDZ of the proposed method like as the NDZ in IAFD. Additionally, at steady state operation (grid frequency f_g equal to the nominal frequency f) the acceleration term in (11) will be zero, that is mean there no additional THD will be injected in the system. Once the frequency deviated away from the nominal frequency the distortion factor starts to vary in linear manner with frequency deviation, which decrease the NDZ to detect the island situation.

4. Simulation Results

To verify the proposed method, a grid connected single-phase inverter with parallel RLC load has been considered. The power circuit of the test model was presented in Fig.4. the system parameters are listed in Table I. The test model and the proposed method were modeled in MATLAB/Simulink. The inverter was modeled as H-bridge IGBT thyristor with PWM current control. The LCL filter was designed to limit ripple in the inverter output current and to limit the THD to be less than 5%.

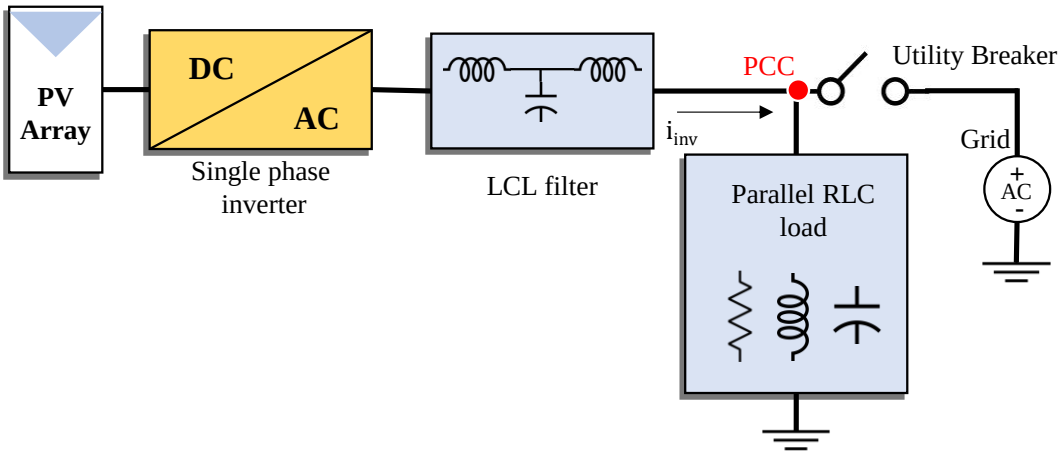


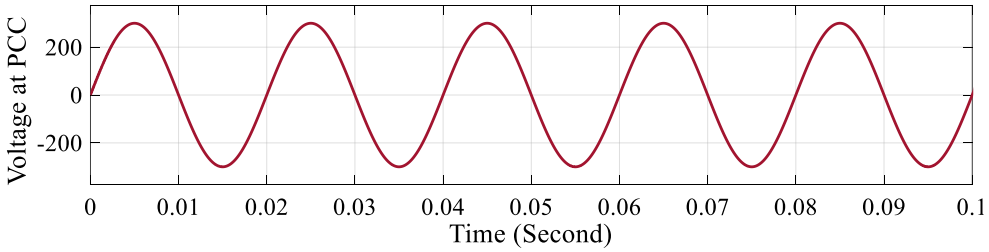
FIGURE. 4. Power circuit of the test model.

TABLE 1. SYSTEM PARAMETERS

Parameter	**Value**
DC Voltage	400 V
AC grid voltage	300 V
Grid frequency f	50 Hz
Switching frequency fs	10kHz
L_1 for LCL filter	4.06mH
L_2 for LCL filter	4.35mH
C for LCL filter	6.01µF
Initial distortion factor *Ko*	0.105
Accelerating factor β	0.05
Test load	f_o = 49.9Hz, Q_f = 2.5

The voltage waveform at PCC and inverter output current at normal operation (without islanding) are presented in Fig. 5 (a) and (b), respectively. It observed that the inverter output current is distorted based on the proposed method. Where, at normal operation the distortion factor *K* is equal to the initial distortion factor (K_o = 0.105), that because there is no deviation between the voltage frequency at PCC and the grid nominal frequency.

(a)



(b)

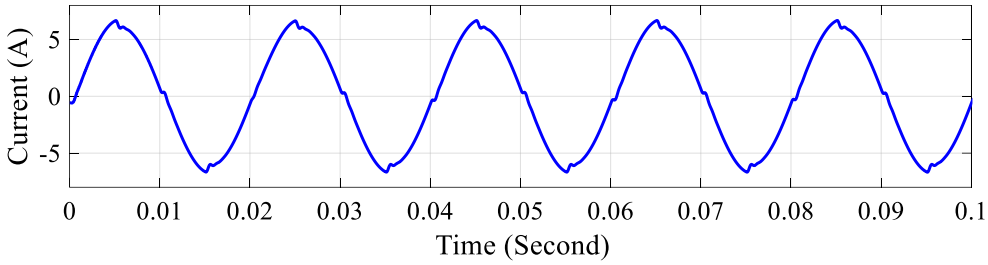


FIGURE. 5. Voltage and current at normal operation with proposed method: (a) voltage waveform at PCC (b) inverter output current.

The spectrum of inverter output current waveform is presented in Fig.6. It is observed that the THD was 4.9%, that because the used distortion factor was (0.105). However, the THD for various values of distortion factors K are presented in Fig.7. It is observed that, the maximum allowable initial distortion value is about 0.105, which produce THD about 5%.

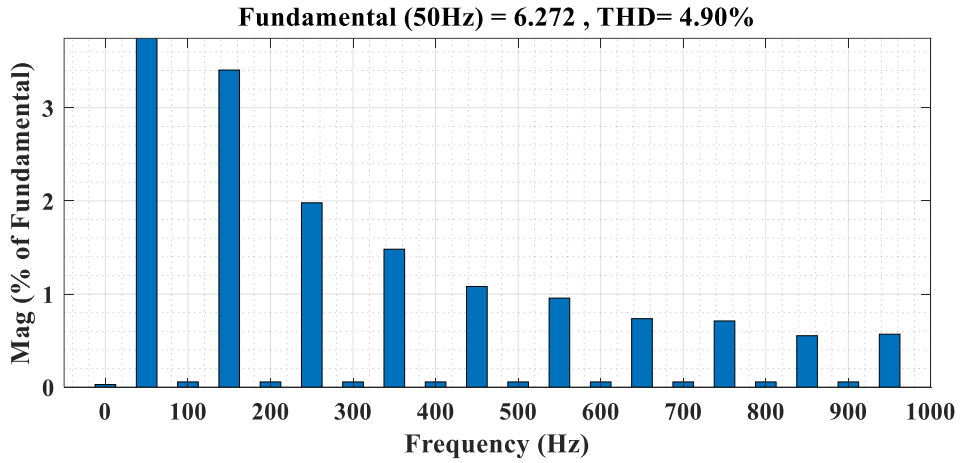


FIGURE. 6. spectrum of the inverter output current.

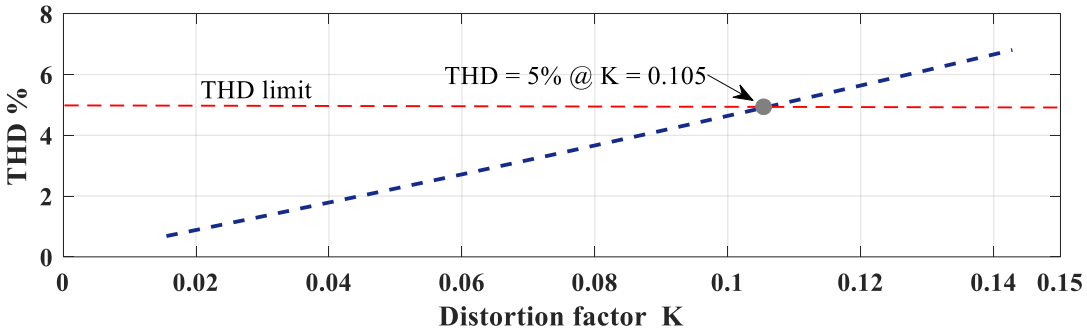


FIGURE. 7. THD for various versus the distortion factor.

To verify the NDZ of the proposed method, a test load with quality factor 2.5 and resonance frequency 49.9 Hz has been considered. As shown in Fig. 3, the test load is in the NDZ of the IAFD, and it is out of the NDZ of the proposed method.

An islanding situation is simulated at 0.2 second of the simulation time by open the utility breaker in Fig.4. The inverter output current, voltage at PCC, and the frequency of at the PCC

has been presented in Fig.8 (a), (b), and (c). it is observed the inverter current has small distortion due to the distortion signal of the proposed method. From Fig.4 (c), the frequency at PCC start to decrease at about 0.21 second due to the proposed method, and the frequency reached to the frequency limit (49.3 Hz) at about 0.25 second.

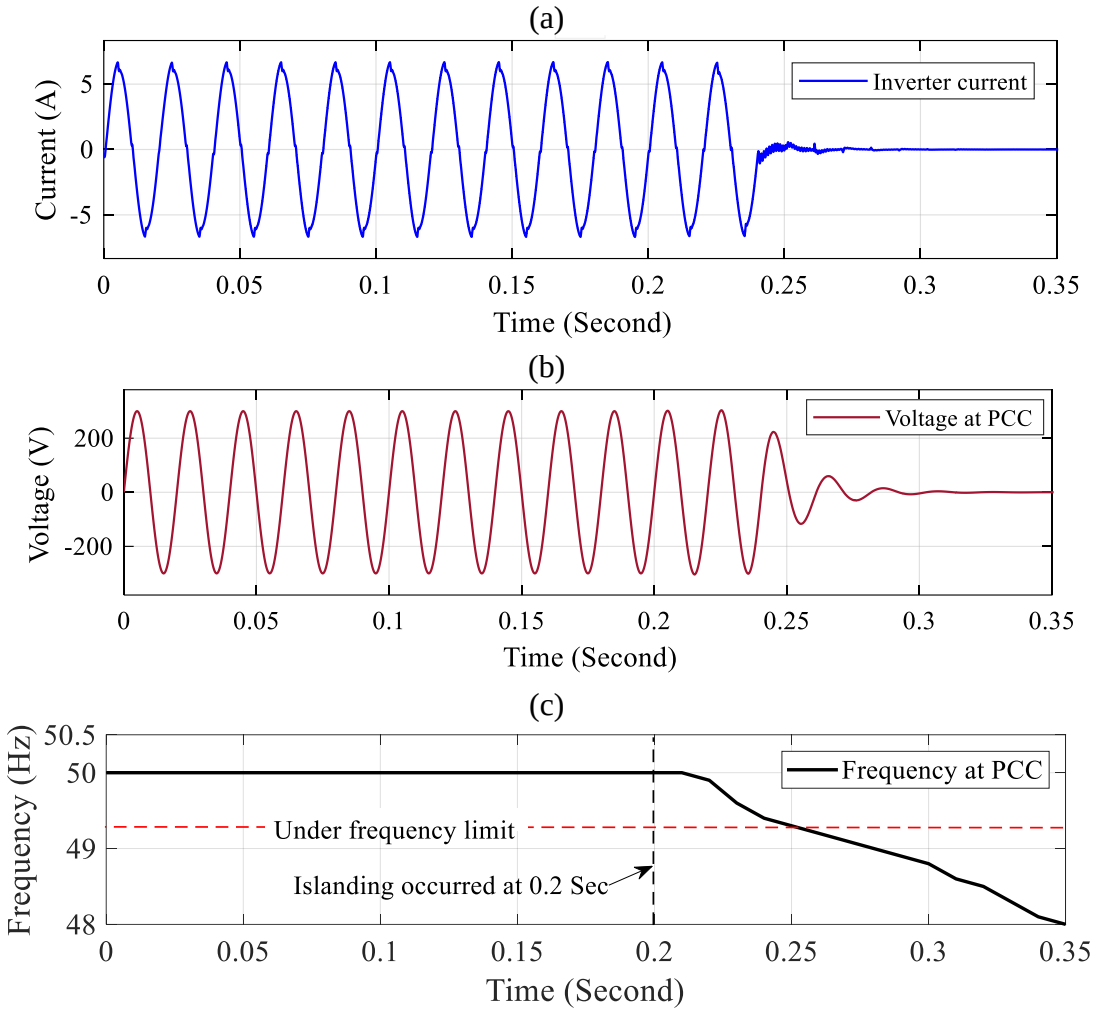


FIGURE. 8. (a) Inverter output current at islanding event. (b) voltage at PCC. (c) frequency at islanding event

From voltage and current measurements Fig (a) and (b), the islanding is properly detected by the proposed method. As a comparison between the proposed method and IAFD method, the test load located in the NDZ of the IAFD, that mean the IAFD unable to detect the islanding situation at that load. On the other hand, the proposed method able to detect the islanding at that load.

In the proposed method, the distortion factor is adaptive. The variation of distortion factor during the islanding event has been presented in Fig.9. It is observed that, the initial value of distortion factor was 0.105, and it starts varying at 0.2 second. Where, according to proposed method the distortion factor increases with frequency deviation.

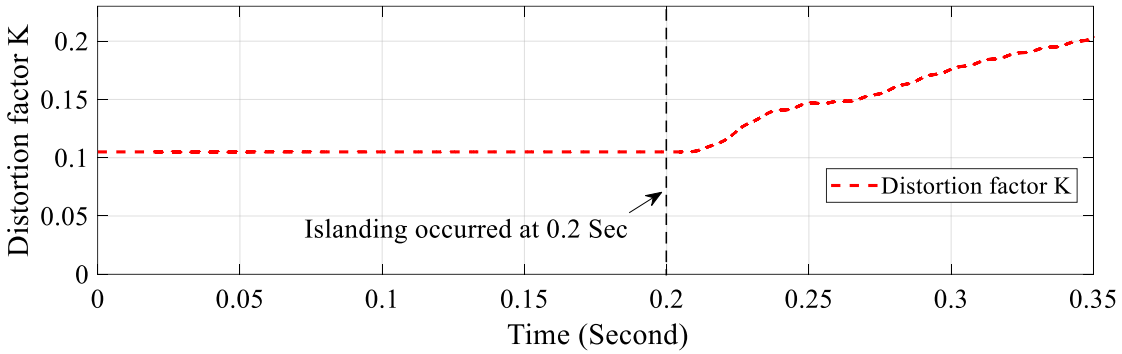


FIGURE. 9. The variation of distortion factor for proposed method.

Based on the simulation results, the proposed method successfully improved the performance of IAFD islanding detection method by decreasing the NDZ. Additionally, the proposed method does not inject any additional harmonics over the IAFD at steady state operation.

5. Conclusion

In this paper, a modified IAFD method was proposed. A positive feedback of frequency of the voltage at PCC was added to vary the injected perturbation, that to improve the performance of the IAFD. The adaption manner of distortion signal enhances in increasing the injected perturbations during islanding event only. Which reduced the NDZ during islanding event and decreased the injected THD in steady state operation. The proposed method was modeled in MATALB/Simulink environment, and it was tested in testbed system as suggested in IEEE Standard 929 [6] and Standard 1547 [4]. As a result, the proposed method successfully improved the performance of IAFD method by decreasing the NDZ. The proposed method could be enhanced farther by choosing the optimal values of initial distortion factor K_o and acceleration factor β, this could be as a future work of the presented study.

REFERENCES

[1] W. Bower and M. E. Ropp, “Evaluation of islanding detection methods for photovoltaic utility-interactive photovoltaic systems,” International Energy Agency, Paris, France, Tech. Rep. IEA-PVPS T5-09, 2002..

[2] H. Zeineldin, “A q-f droop curve for facilitating islanding detection of inverter-based distributed generation,” IEEE Trans. Power Electron., vol. 24, no. 3, pp. 665–673, Mar. 2009.

[3] J.-H. Kim, J.-G. Kim, Y.-H. Ji, Y.-C. Jung, and C.-Y. Won, “An islanding detection method for a grid-connected system based on the goertzel algorithm,” IEEE Trans. Power Electron., vol. 26, no. 4, pp. 1049–1055, Apr. 2011..

[4] IEEE Standard for Interconnecting Distributed Resources With Electric Power Systems, IEEE Standard 1547, Jul. 2003..

[5] A. S. Subhadra, P. L. Reddy, and S. B. Modi, “Islanding detection in a distribution system with modified DG interface controller,” Int. J. Appl. Power Eng., vol. 6, no. 3, pp. 135–143, Dec. 2017.

[6] IEEE Recommended Practice for Utility Interface of Photovoltaic (pv) Systems, IEEE Standard 929-2000.

[7] F. De Mango, M. Liserre, A. Aquila, and A. Pigazo, “Overview of antiislanding algorithms for PV systems. part i: Passive methods,” in Power Electronics and Motion Control Conference, 2006. EPE-PEMC 2006..

[8] A. Aljankawey, W. Morsi, L. Chang, and C. Diduch, “Passive methodbased islanding detection of renewable-based distributed generation: The issues,” in Electric Power and Energy Conference (EPEC), 2010 IEEE, aug. 2010, pp. 1 –8.

[9] M. Bakhshi, R. Noroozian, and G. Gharehpetian, “Passive anti-islanding scheme based on reactive power in the smart grids,” in Smart Grids (ICSG), 2012 2nd Iranian Conference on, may 2012, pp. 1 –7..

[10] S.-J. Huang and F.-S. Pai, “A new approach to islanding detection of dispersed generators with self-commutated static power converters,” IEEE Trans. Power Del., vol. 15, no. 2, pp. 500–507, Apr. 2000..

[11] S.-I. Jang and K.-H. Kim, “An islanding detection method for distributed generations using voltage unbalance and total harmonic distortion of current,” IEEE Trans. Power Del., vol. 19, no. 2, pp. 745–752, Apr. 2004..

[12] S. K. Salman, D. J. King, and G. Weller, “New loss of mains detection algorithm for embedded generation using rate of change of voltage and changes in power factors,” in Proc. 7th Int. Conf. Develop. Power Syst. Protect. (DPSP), 2001, pp. 82–85..

[13] A. Yafaoui, B. Wu and S. Kouro, "Improved Active Frequency Drift Anti-islanding Detection Method for Grid Connected Photovoltaic Systems," in *IEEE Transactions on Power Electronics*, vol. 27, no. 5, pp. 2367-2375, May 2012, doi: 10.1109/TPEL.2011.2171997..

[14] De Mango, F., Liserre, M. and Dell’Aquila, A., ‘Overview of Anti-islanding Algorithms for PV Systems. Part II: Active Methods’. In Proceedings of the 12th International Power Electronics and Motion Conference, August 2006, pp. 1884–1889..

[15] Petrone, G., Spagnuolo, G., Teodorescu, R., Veerachary, M. and Vitelli, M., ‘Reliability Issues in Photovoltaic Power Processing Systems’. IEEE Transactions on Industrial Electronics, vol. 55, no. 7, July 2008, 2569–2580..

[16] M. E. Ropp, M. Begovic, and A. Rohatgi, “Analysis and performance assessment of the active frequency drift method of islanding prevention,” IEEE Trans. Energy Conversion, vol. 14, no. 3, pp. 810–816, Sep. 1999..

[17] H. Sun “Performance Assessment of Islanding Detection Methods Using the Concept of Non-Detection Zones,” M.A.Sc. thesis, Dept. Elect. Comput. Eng., Concordia Univ., Montreal, QC, Canada, Jan. 2005..

[18] H. H. Zeineldin and S. Kennedy, “Sandia frequency-shift parameter selection to eliminate non-detection zones,” IEEE Trans. Power Del., vol. 24, no. 1, pp. 486–487, Feb. 2009..

[19] M. Khodaparastan, H. Vahedi, F. Khazaeli, and H. Oraee, “A novel hybrid islanding detection method for inverter-based DGs using SFS and ROCOF,” IEEE Trans. Power Del., vol. 32, no. 5, pp. 2162–2170.

[20] Estebanez, E. Moreno, V. Pigazo, A. Liserre and M. Dell’Aquila, ‘Performance of evaluation of active islanding detection algorithms in distributed generation photovoltaic systems: two inverter case’, IEEE Trans. Ind. Electron., 2010, vol. 99, no. 1, pp. 1-9.

[21] Abdullah Al-Odienat, Khaled Al-Maitah, Batool Al-Khraisat, “The enhancement of Frequency Stability of Low Inertia Interconnected Power System”. *2021 IEEE PES/IAS PowerAfrica*, August 23-28, 2021.

[22] A. Al-Odienat and K. Al-Maitah, "A modified Active Frequency Drift Method for Islanding Detection," *2021 12th International Renewable Engineering Conference (IREC)*, Amman, Jordan, 2021, pp. 1-6, doi: 10.1109/IREC51415.2021.9427796