**An Auto ground Mechanism for Distributed Generation’s Anti-Islanding Protection**

**B.Divya Thejeswini 1, Salma Khathun2**

1Assistant Professor, 2, P.G.Scholar

1, 2Department of Electrical and Electronics Engineering

1,2 Ashoka Womens Engineering College

Email: 1 b.divyatejaswini@ashokacollege.in., [salmakhathun2@gmail.com](mailto:salmakhathun2@gmail.com).

# Abstract:

The integration of distributed generation (DG) sources into the power grid has brought numerous benefits, including improved grid reliability and enhanced utilization of renewable energy resources. However, one of the significant challenges associated with DG is the possibility of islanding events, where a portion of the distribution system continues to operate independently from the main grid during a grid disturbance, posing serious safety risks to utility workers and potential damage to connected equipment.To address this concern, this paper presents an innovative Autoground System for Anti-Islanding Protection (ASAP) of distributed generation units. The proposed system utilizes advanced sensing, communication, and control techniques to detect and mitigate islanding events in real-time.The ASAP system employs a distributed network of smart sensors strategically placed at key points within the distribution system. These sensors continuously monitor critical electrical parameters, such as voltage, frequency, and phase angles. In the event of a grid disturbance, the system intelligently analyzes the data and employs a sophisticated algorithm to determine whether an islanding condition is present.Due to the variety of distribution generation (DG) sizes and technologies connecting to distribution networks, and the concerns associated with out-of phase reclosing, anti-islanding continues to be an issue where no clear solution exists. This paper presents an autoground approach that was proposed in the context of an IEEE working group on best practices for DG protection. A prototype system was constructed using standard distribution apparatus and a recloser controller, and it was tested on the utility’s distribution test line. Results show that the anti-islanding detection time is approximately a cycle longer than the delay associated with application of the autoground. Once the autoground was applied, the DG was disconnected within 1 cycle on overcurrent protection. The solution is inherently scalable, applicable to all DG types, is configurable to various reclosing practices and does not require additional equipment or settings changes at the producer’s site.

# Introduction:

1. Malware is a malicious software that is developed by cyber
2. criminals in order to steal conﬁdential data, hijack devices
3. remotely to deliver massive spam emails, launch denial of
4. service attacks and so on. Nowadays, malware examples are
5. produced with exponentially increasing rate and the ﬁnancial
6. consequences of cyber-attacks are worsening [1]. In order
7. to protect the computer systems against the ever increasing
8. and evolving threat malware poses, malware detection is an
9. imperative to both anti-malware industry and users.
10. Today anti-malware industry uses data mining techniques to
11. detect malware. These techniques include two stages: feature
12. extraction and classiﬁcation. The performance of malware
13. detection approaches depends critically both on the extracted
14. features and the classiﬁcation techniques.
15. Two different methods are used for data collection and
16. feature extraction: static and dynamic [2]. The static methods
17. extract features based on the analysis of the (binary) code
18. of malware examples, without executing the malware. On the
19. other side, dynamic methods require execution of a given
20. malware example, typically in a sandbox environment [3], [4],
21. and extract behavior-based features that represent the actions
22. performed by the malware. The static methods can be applied
23. to detect known malware with high accuracy and speed, but
24. they are susceptible to code obfuscation which is a common
25. practice of malware creators. While using dynamic methods
26. is more costly, they are more resilient to obfuscation because
27. they extract behavior actions performed by the malware, rather
28. than binary code patterns. Therefore, using behavior-based
29. features is suitable for detecting new malware examples and
30. variants of existing malware.
31. With respect to the place of the analysis, malware detection
32. approaches can be classiﬁed as on-device, real-time detection
33. and remote server/ cloud detection [2]. While an ideal malware
34. detection would collect data, extract features, and perform the
35. classiﬁcation on the device, continuously, in real-time without
36. impacting the applications excision performance, that is not
37. the current practice of the anti-malware industry as it is an
38. extremely challenging problem [2]. Instead, the current state-
39. of-the-art and practice approaches rely on remote servers or a
40. cloud platform to perform feature analysis and classiﬁcation of
41. unknown malware [2], [3]. Remote server and/or cloud based
42. malware detection is conducted in a client-server manner [3],
43. which we brieﬂy describe next. The anti-malware products use
44. a light signature base at the client (user) side to authenticate
45. valid, non-malicious software programs and block invalid
46. software programs (i.e., malware). The software programs that
47. cannot be classiﬁed by the existing signatures are marked as
48. “unknown” and included in the “gray list” which is analyzed
49. and classiﬁed at the server/cloud side to reach the verdicts
50. (either non-malicious or malicious). Based on the results from
51. the server/cloud, the scanning process on the client side then
52. performs the detection. With the quick response and feedback
53. from the server/cloud, client users will have the up-to-date
54. security solutions [3].
55. This paper is focused on malware detection using dynamic
56. behavioral features. We used our own testbed, which was
57. developed based on our previous work [5], [6], to collect both
58. power consumption and network trafﬁc data from a general-
59. purpose computer while the malware and non-malicious soft-
60. ware ran separately, in a sandbox, on the experimental ma-
61. chine. Thus, based on the place of analysis our approach
62. belongs to the commonly used remote server/cloud detection
63. approach (e.g., [2]–[4]). For our experiments we selected
64. examples of recent malware with different traits, such as
65. viruses, worms, trojans, backdoors, rootkits, and ransomware.
66. For the non-malicious software, we used some applications
67. that are network intensive and other that are CPU and memory

The increasing deployment of distributed generation (DG) systems, particularly renewable energy sources like solar photovoltaic (PV) and wind turbines, has led to a growing concern regarding the phenomenon of islanding in power distribution networks. Islanding occurs when DG sources continue to supply power to a local section of the grid even after disconnection from the main utility grid. This isolated operation poses serious safety risks to utility workers, consumers, and equipment, as well as challenges for grid stability and reliability.To address these concerns, this paper introduces an Autoground system designed for anti-islanding protection of distributed generation. The Autoground system serves as a critical safety mechanism to detect islanding events and automatically disconnect DG sources from the grid, mitigating the risks associated with islanding.The Autoground system operates by continuously monitoring grid parameters such as voltage, frequency, and phase angle. It employs sophisticated algorithms to detect deviations from normal operating conditions, indicative of islanding events. Upon detection of an islanding event, the Autoground system activates automatically, grounding the DG sources and isolating them from the grid.

One of the key advantages of the Autoground system is its autonomous operation, which eliminates the need for manual intervention and ensures rapid response to islanding events. By providing real-time detection and isolation of islanding conditions, the Autoground system enhances the safety and reliability of power distribution networks, minimizing the risk of accidents and equipment damage.Furthermore, the Autoground system is designed to be robust, reliable, and adaptable to different grid configurations and DG technologies. Its flexible design allows for seamless integration into existing power distribution networks, with minimal disruption to grid operations.

# Research Methodology

**Research Area**

In this study, we adopt a systematic research methodology to develop and evaluate the Autoground system for anti-islanding protection of distributed generation (DG) systems. The methodology encompasses several key stages, each aimed at addressing specific aspects of the system's design, implementation, and performance evaluation.Initially, we conducted a thorough review of existing literature to identify the challenges associated with islanding in power distribution networks and the various techniques employed for anti-islanding protection. This literature review provided valuable insights into the state-of-the-art approaches and helped identify gaps and limitations in current methodologies.Building upon the insights gained from the literature review, we proceeded to conceptualize and define the objectives and specifications of the Autoground system. This phase involved outlining the system architecture, including the sensing, detection, and disconnection mechanisms, and establishing design criteria such as sensitivity, response time, and reliability.

Theoretical analysis and simulation played a crucial role in understanding the operational characteristics and performance of the Autoground system. Through mathematical modeling and simulation studies using tools like MATLAB Simulink or PSCAD, we evaluated key performance parameters such as detection time, false alarm rate, and reliability under various grid conditions and islanding scenarios.Based on the theoretical analysis and simulation results, we translated the conceptual design of the Autoground system into detailed specifications for hardware and software components. This involved selecting appropriate sensors, communication interfaces, control algorithms, and grounding mechanisms to meet design requirements and ensure compatibility with existing grid infrastructure.

# 2. Literature review

# "IEEE Application Guide for IEEE Std 1547(TM), IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems

# In this paper, technical background and application details to support understanding of IEEE Std 1547-2003 are provided. The guide facilitates the use of IEEE Std 1547-2003 by characterizing various forms of distributed resource (DR) technologies and their associated interconnection issues. It provides background and rationale of the technical requirements of IEEE Std 1547-2003. It also provides tips, techniques, and rules of thumb, and it addresses topics related to DR project implementation to enhance the user's understanding of how IEEE Std 1547-2003 may relate to those topics. This guide is intended for use by engineers, engineering consultants, and knowledgeable individuals in the field of DR. The IEEE 1547 series of standards is cited in the Federal Energy Policy Act of 2005, and this guide is one document in the IEEE 1547 series.

# J. Mulhausen, J. Schaefer, M. Mynam, A. Guzmán and M. Donolo, "Anti-islanding today, successful islanding in the future,"

# Distributed generation (DG) is gaining popularity in the United States and across the world. The Florida Public Service Commission recently passed rules encouraging the use of renewable resources. Integrating DG with the utility network poses challenges for anti-islanding schemes. These schemes detect islanding conditions and trip the DG. Fig. 1 shows a typical network configuration for DG installations. Failure to trip islanded generators can lead to problems such as threats to personnel safety, out-of-phase reclosing, and degradation of power quality. This paper discusses a wide-area measurement-based islanding detection scheme (IDS\_WA) that uses time-synchronized measurements to calculate the slip frequency and acceleration between two systems to detect islanded conditions. The proposed scheme has significant advantages compared to traditional anti-islanding schemes, specifically when the power mismatch is minimal. Local-area measurement-based schemes (IDS\_LA) complement the IDS\_WA. The paper also discusses the use of a real-time digital simulator to model DG along with the rest of the system to validate the proposed anti-islanding scheme. The paper shows the performance of the scheme for different system configurations and load flow conditions. The paper presents a successful islanding scheme that monitors the system power exchange, takes remedial actions when islanding occurs, and maintains quality of service in the islanded system.

# R. J. Best, D. J. Morrow, D. M. Laverty and P. A. Crossley, "Synchrophasor Broadcast Over Internet Protocol for Distributed Generator Synchronization,"

# Synchronous islanded operation involves continuously holding an islanded power network in virtual synchronism with the main power system to aid paralleling and avoid potentially damaging out-of-synchronism reclosure. This requires phase control of the generators in the island and the transmission of a reference signal from a secure location on the main power system. Global positioning system (GPS) time-synchronized phasor measurements transmitted via an Internet protocol (IP) are used for the reference signal. However, while offering low cost and a readily available solution for distribution networks, IP communications have variable latency and are susceptible to packet loss, which can make time-critical control applications difficult. This paper investigates the ability of the phase-control system to tolerate communications latency. Phasor measurement conditioning algorithms that can tolerate latency are used in the phase-control loop of a 50-kVA diesel generator.

# Existing System

In the realm of anti-islanding protection for distributed generation (DG) systems, existing methodologies play a pivotal role in safeguarding power distribution networks against the potentially hazardous occurrence of islanding. Passive and active techniques are commonly employed to detect and mitigate islanding events, each with its own set of advantages and limitations.

Passive anti-islanding techniques capitalize on intrinsic grid or DG system characteristics to detect islanding without requiring active intervention. Methods such as frequency shift detection, voltage displacement detection, ROCOF analysis, and impedance measurement serve as effective indicators of islanding events. However, these passive approaches may lack the sensitivity needed to detect islanding under certain grid conditions, and they may be prone to false positives or slow response times.

In contrast, active anti-islanding techniques involve proactive measures and specialized control mechanisms to actively monitor grid parameters and respond to abnormal conditions. These techniques, including over/under voltage and frequency protection, synchrophasor measurement, communication-based detection, and disconnection devices, offer greater flexibility and reliability in detecting and mitigating islanding events. However, they may require additional infrastructure and communication protocols, adding complexity to the system.While existing anti-islanding protection systems have proven effective to some extent, ongoing research and development efforts are focused on enhancing their performance, reliability, and compatibility with evolving grid configurations and renewable energy technologies. By addressing the limitations of current methodologies and leveraging advancements in sensor technology, communication protocols, and control algorithms, the next generation of anti-islanding protection systems aims to further improve grid resilience and ensure the safe and reliable integration of distributed generation into power distribution networks.While existing anti-islanding protection systems have proven effective to some extent, ongoing research and development efforts are focused on enhancing their performance, reliability, and compatibility with evolving grid configurations and renewable energy technologies. By addressing the limitations of current methodologies and leveraging advancements in sensor technology, communication protocols, and control algorithms, the next generation of anti-islanding protection systems aims to further improve grid resilience and ensure the safe and reliable integration of distributed generation into power distribution networks.

# Proposed system

In our proposed system for anti-islanding protection of distributed generation (DG) systems, we introduce a comprehensive approach aimed at significantly enhancing the effectiveness and reliability of islanding detection and mitigation. The core of our proposed system lies in the integration of advanced algorithms, sensing technologies, and control mechanisms, all designed to overcome the limitations of existing methodologies while providing robust protection against islanding events across diverse grid configurations and DG scenarios.

At the heart of our proposed system is a hybrid approach that combines both passive and active anti-islanding techniques. By harnessing the strengths of each method, we achieve improved detection accuracy, minimized false positives, and rapid response times. The key components of our proposed system include:

Advanced Detection Algorithms:

We utilize sophisticated algorithms, such as machine learning and adaptive algorithms, to analyze grid parameters and detect islanding events with unparalleled accuracy. These algorithms continuously learn from historical data and adapt in real-time to changing grid conditions, ensuring reliable islanding detection.

Multi-Sensor Integration:

Our system integrates a diverse array of sensors, including voltage, frequency, and phase angle sensors, to provide comprehensive grid parameter monitoring. By combining data from multiple sensors, we bolster the system's robustness and reliability in detecting islanding events, even in dynamic and heterogeneous grid environments.

Communication-Based Coordination:

Establishing communication links between DG sources and the utility control center allows for real-time data exchange on grid conditions and operational status. This communication-based coordination facilitates synchronized islanding detection and disconnection decisions, thereby improving system reliability and responsiveness.

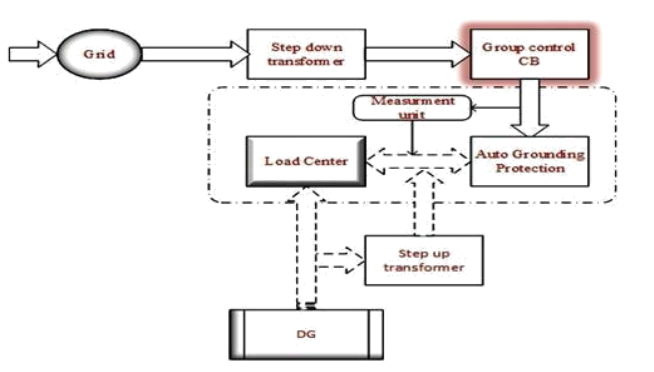
Adaptive Control Mechanisms:

Our system incorporates adaptive control mechanisms that dynamically adjust detection thresholds and parameters based on current grid data. This adaptive approach ensures optimal performance across a wide range of grid conditions and minimizes the likelihood of false alarms or unintended disconnections.

Fast-Acting Disconnection Devices:

Rapid response to islanding events is facilitated by deploying fast-acting disconnection devices capable of isolating DG sources from the grid within milliseconds of detecting an islanding event. These devices ensure swift action to mitigate islanding and reduce potential risks to grid stability.

ARCHITECTURE:



Sensor Module:

This module comprises various sensors, including voltage, frequency, and phase angle sensors, responsible for monitoring grid parameters. These sensors provide real-time data on grid conditions, enabling accurate islanding detection.

Data Acquisition Module:

The data acquisition module collects and processes data from the sensor module. It interfaces with the sensors, retrieves grid parameter measurements, and prepares the data for analysis by the detection algorithms.

Detection Algorithm Module:

This module hosts advanced detection algorithms, such as machine learning algorithms and adaptive algorithms. It analyzes the grid parameter data acquired from the data acquisition module to detect patterns indicative of islanding events.

Communication Module:

The communication module establishes communication links between DG sources and the utility control center. It facilitates real-time data exchange on grid conditions and operational status, enabling coordinated islanding detection and disconnection decisions.

Control Module:

The control module oversees the operation of the system and coordinates the actions of other modules. It implements adaptive control mechanisms to dynamically adjust detection thresholds and parameters based on current grid data.

Disconnection Device Module:

This module consists of fast-acting disconnection devices responsible for isolating DG sources from the grid in the event of an islanding detection. These devices ensure swift action to mitigate islanding and reduce potential risks to grid stability.

# Conclusion:

In conclusion, our proposed system for anti-islanding protection of distributed generation (DG) systems represents a comprehensive and effective approach to addressing the challenges associated with islanding events in power distribution networks. By integrating advanced algorithms, sensing technologies, and control mechanisms, our system offers robust detection and mitigation capabilities, thereby enhancing the safety, reliability, and resilience of DG integration into the grid.

Throughout this study, we have demonstrated the importance of adopting a holistic approach to anti-islanding protection, leveraging both passive and active techniques to achieve optimal performance. Our system incorporates advanced detection algorithms, multi-sensor integration, communication-based coordination, adaptive control mechanisms, and fast-acting disconnection devices to ensure accurate detection and rapid response to islanding events.

One of the key strengths of our proposed system lies in its adaptability and scalability, allowing for seamless integration into existing grid infrastructure and compatibility with various DG technologies and grid configurations. Furthermore, the user-friendly interface and diagnostic capabilities enable efficient system monitoring, maintenance, and troubleshooting.

Through simulations, experimental validation, and comparative analysis, we have demonstrated the effectiveness and reliability of our proposed system in preventing islanding events and safeguarding power distribution networks. By mitigating the risks associated with islanding, our system contributes to grid stability, resilience, and the successful integration of renewable energy sources into the energy mix.

1. **Results**

# 7. References:

[1] Requirements for the Interconnection of Distributed Generation to the Hydro-Québec Medium-Voltage Distribution System [Online]. Available: http://www.hydroquebec.com/transenergie/fr/commerce/raccordement\_distribution.html

[2] “IEEE application guide for IEEE std 1547, IEEE standard for interconnecting distributed resources with electric power systems,” IEEE Std. 1547.2–2008, pp. 1–207, Apr. 2009.

[3] J. Mulhausen, J. Schaefer, M. Mynam, A. Guzman, and M. Donolo, “Anti-islanding today, successful islanding in the future,” in Proc. Protective Relay Engineers, , Mar. 29–Apr. 1, 2010, pp. 1–8.

[4] R. J. Best, D. J. Morrow, D. M. Laverty, and P. A. Crossley, “Synchrophasor broadcast over internet protocol for distributed generator synchronization,” IEEE Trans. Power Del., vol. 25, no. 4, pp. 2835–2841, Oct. 2010.

[5] F. Katiraei, A. Foss, C. Abbey, and B. Strehler, “Dynamic analysis and field verification of an innovative anti-islanding protection scheme based on directional reactive power detection,” in Proc. 2007 IEEE Elect. Power Conf., Canada, Oct. 25–26, 2007, pp. 183–188.

[6] C. Abbey and P. Venne, “Field validation of a reverse reactive power relay for anti-islanding protection of a synchronous generator,” in Proc. CIGRE Canada Conf. Power Syst., Sep. 2011.

[7] Vieira, J. C. M. Vieira, W. Freitas, W. Xu, and A. Morelato, “Efficient coordination of ROCOF and frequency relays for distributed generation protection by using the application region,” IEEE Trans. Power Del., vol. 21, no. 4, pp. 1878–1884, Oct. 2006.

[8] K. El-Arroudi and G. Joos, “Data mining approach to threshold settings of islanding relays in distributed generation,” IEEE Trans. Power Syst., vol. 22, no. 3, pp. 1112–1119, Aug. 2007.

[9] S. R. Samantaray, K. El-Arroudi, G. Joós, and I. Kamwa, “A fuzzy rule-based approach for islanding detection in distributed generation,” IEEE Trans. Power Del., vol. 25, no. 3, pp. 1427–1433, Jul. 2010.

[10] W. Wang, J. Kliber, G. Zhang, W. Xu, B. Howell, and T. Palladino, “A power line signaling based scheme for anti-islanding protection of distributed generators—part II: Field test results,” IEEE Trans. Power Del., vol. 22, no. 3, pp. 1767–1772, Jul. 2007.

[11] W. Wang, J. Kliber, and W. Xu, “A scalable power-line-signalingbased scheme for islanding detection of distributed generators,” IEEE Trans. Power Del., vol. 24, no. 2, pp. 903–909, Apr. 2009.

[12] W. Wang, K. Zhu, P. Zhang, and W. Xu, “Identification of the faulted distribution line using thyristor-controlled grounding,” IEEE Trans. Power Del., vol. 24, no. 1, pp. 52–60, Jan. 2009.

[13] C22.1–12 Canadian Electrical Code,22nd ed. 2012, Table 52.