energies

MDPI

Editorial

Fault-Tolerant Control for Microgrids—Recent Developments and Future Directions

Mehdi Hosseinzadeh

School of Mechanical and Materials Engineering, Washington State University, Pullman, WA 99164, USA; mehdi.hosseinzadeh@wsu.edu

1. Introduction

Microgrids are defined as a cluster of loads, distributed energy resources, and storage devices, and they are receiving worldwide attention due to the increasing rate of consumption of nuclear and fossil fuels and the community demand for reducing pollutant emission in electricity generation fields. The control functional requirements of a microgrid are as follows: (i) the regulation of voltage and frequency within limits; (ii) active and reactive power balance and proper communication among resources; (iii) seamless transition between grid-connected and islanded modes of operation; (iv) economic dispatch of the resources; and (v) power-flow control among microgrid components. Although many schemes and approaches have been proposed for each of the above-mentioned functions, possible faults and failures in any of the components of microgrids can severely affect the performance, applicability, optimality, and robustness of the proposed schemes such that they are no longer suitable or even feasible/admissible. This means that the control schemes must be adapted appropriately to treat faults and failures in the components of microgrids.

The Special Issue "Microgrids and Fault-Tolerant Control" aims at presenting the latest developments, trends, research solutions, and applications of fault-tolerant control to engineering problems in the implementation and utilization of microgrids. This Special Issue includes three original research articles and two review articles, which will be briefly discussed in the next section.

2. Special Issue Articles

Table 1 summarizes the published articles in the Special Issue "Microgrids and Fault-Tolerant Control". The review article [1], which is authored by M. Hosseinzadeh and F. R. Salmasi, provides an overview of islanding fault detection in microgrids. Islanding fault is a condition in which the microgrid become disconnected from the utility grid unintentionally due to any fault in the utility grid. Islanding fault poses the following drawbacks: (i) It is a hazard for personnel, as they may consider the systems as inactive while the generation units are feeding power to the loads; (ii) the voltage and frequency may not be maintained at a standard acceptable level; (iii) circuit reclosers reconnect the disconnected microgrid to the utility grid when out of phase. Review article [1] surveys the extensive literature concerning the development of islanding fault detection techniques (see Figure 1), which can be classified into remote and local techniques, where the local techniques can be further classified as passive, active, and hybrid. In [1], various detection methods in each class are studied, and advantages and disadvantages of each method are discussed.

Review article [2], authored by F. Nejabatkhah, Y. Wei, H. Liang, and R. R. Ahrabi, discusses cyber-security of smart microgrids. Since cyber system and physical process are tightly coupled in microgrids (see Figure 2), any cyber incidents can have economic and physical impacts on the operation of microgrids. Review article [2] discusses cyber-attacks on data availability, integrity, and confidentiality. In particular, ref. [2] investigates the false data injection (FDI) attack as one of the most challenging threats for smart microgrids, where the attacker compromises the data integrity in the cyber/communication network.

check for updates

Citation: Hosseinzadeh, M. Fault-Tolerant Control for Microgrids—Recent Developments and Future Directions. *Energies* **2022**, *15*, 8522. https://doi.org/10.3390/en15228522

Received: 6 September 2022
Accepted: 9 September 2022
Published: 15 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Moreover, ref. [2] provides implementation examples of FDI attacks' construction and detection/mitigation in smart microgrids and presents samples of recent cyber-security projects in the world and critical cyber-security standards of smart grids.

Table 1. Summary of the Special Issue articles.

Work	Summary
[1] *	Provides an overview of islanding fault detection in microgrids.
[2] *	Discusses cyber-security in smart microgrids.
[3]	Designs and implements a novel inverter configuration called impedance (Z)-source inverter to obtain high voltage output with single-stage power conversion. Moreover, it develops a fault-tolerant strategy to improve the reliability and efficiency of the designed configuration.
[4]	Designs and implements two novel fault-tolerant schemes based on fuzzy logic and model predictive controls to control AC/DC pulse-width modulation power electronic converters in the presence of microgrid faults.
[5]	Designs and implements two novel fault detection schemes based on sliding mode techniques to detect current and voltage sensor faults in DC microgrids.

* Review article.

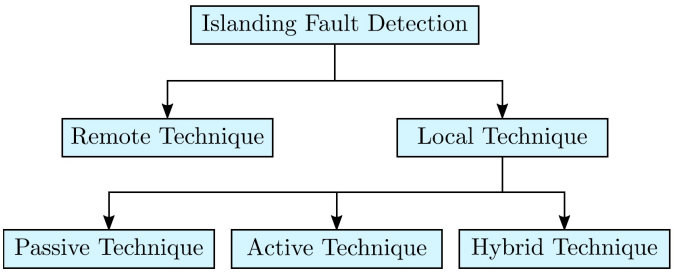

Figure 1. Islanding fault-detection techniques [1].

In [3], V. Sharma, M. J. Hossain, S. M. Nawazish Ali, and M. Kashif proposed an inverter configuration, called Impedance (Z)-source inverter, to obtain high-voltage outputs with single-stage power conversion; the proposed configuration is particularly suitable for irrigation applications. Moreover, ref. [3] develops a fault-tolerant strategy to improve reliability and efficiency of the proposed inverter configuration. Underlying the utilized fault-tolerant strategy is the incorporation of an additional redundant leg with an improved control strategy that facilitates the fault-tolerant operation. The developed fault-tolerant circuit is capable of handling open- and short-circuit faults. See Figure 3 for a general structure of the scheme proposed in [3].

The authors of [4] focused on the control of AC/DC pulse-width modulation power electronic converter, which is crucial to ensure efficient power flow between AC and DC subgrids in hybrid AC/DC microgrids. Two passive fault-tolerant control schemes, based on fuzzy logic and model predictive control techniques, are designed and compared in [4]. Both schemes have the capability of tolerating fault effects due to power-loss faults in solar systems in the presence of unknown uncertainties and load variations (see Figure 4 for an overview of the considered fault scenario), which prevents adverse impacts on the quality of power flow and the stability of microgrid as a whole.

Finally, D. Narzary and K. C. Veluvolu focused on current and voltage sensor faults in DC microgrids in [5]. They designed and implemented two high-order sliding mode observers to estimate the voltage and current and to generate residuals for detecting faulty sensors. Moreoveer, they have designed a hierarchical controller to ensure the equal sharing of currents among the distributed generation units of the DC microgrid and to stabilize the system. See Figure 5 for a functional block diagram of the designed controller and observer.

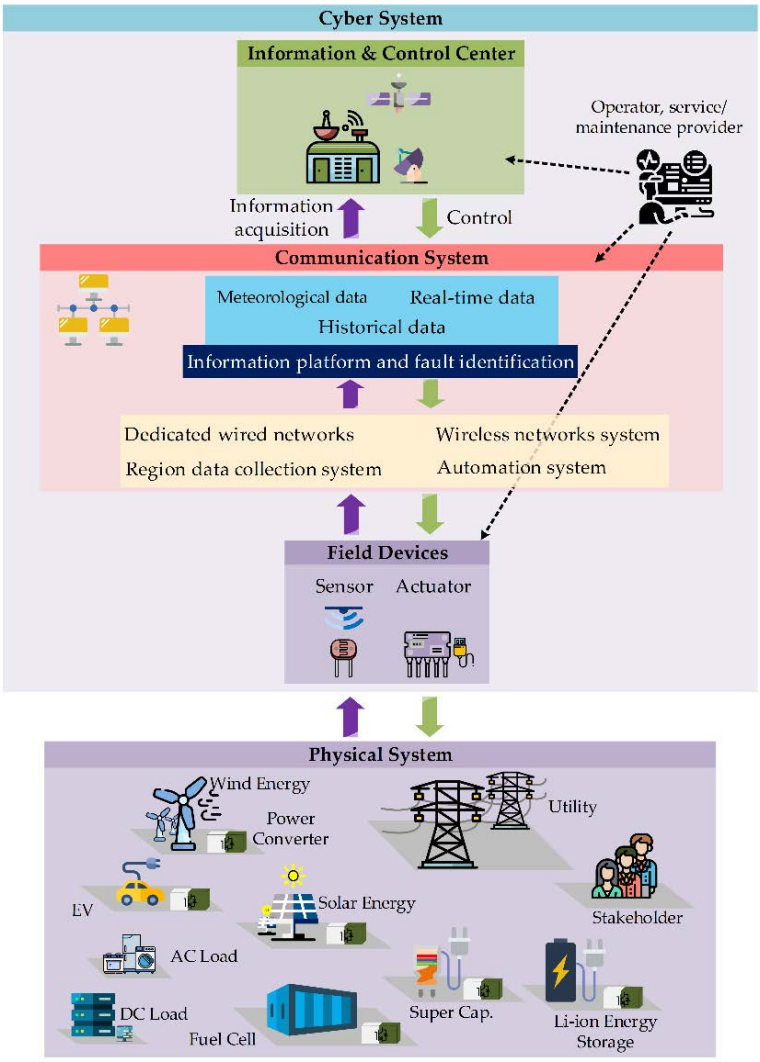

Figure 2. A typical smart microgrid with cyber-physical systems [2].

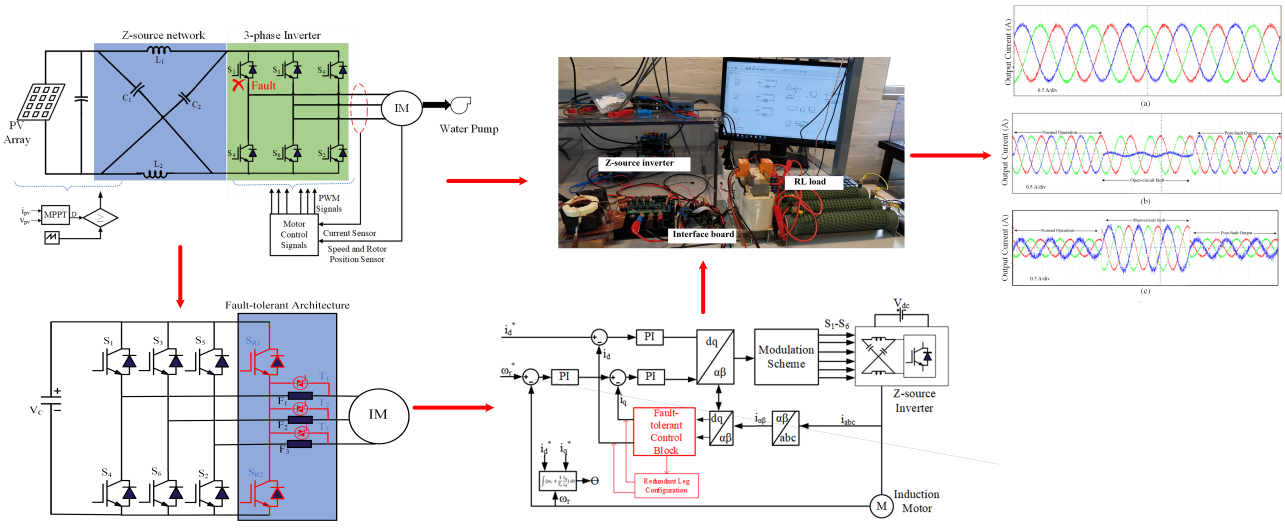

Figure 3. General structure of the scheme proposed in [3].

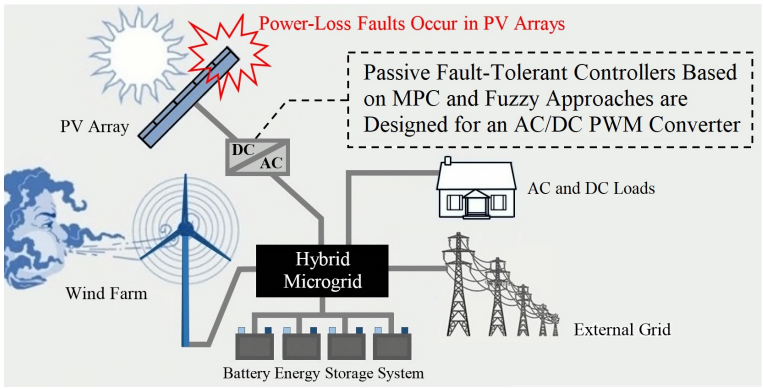

Figure 4. An overview of the fault scenario considered in [4].

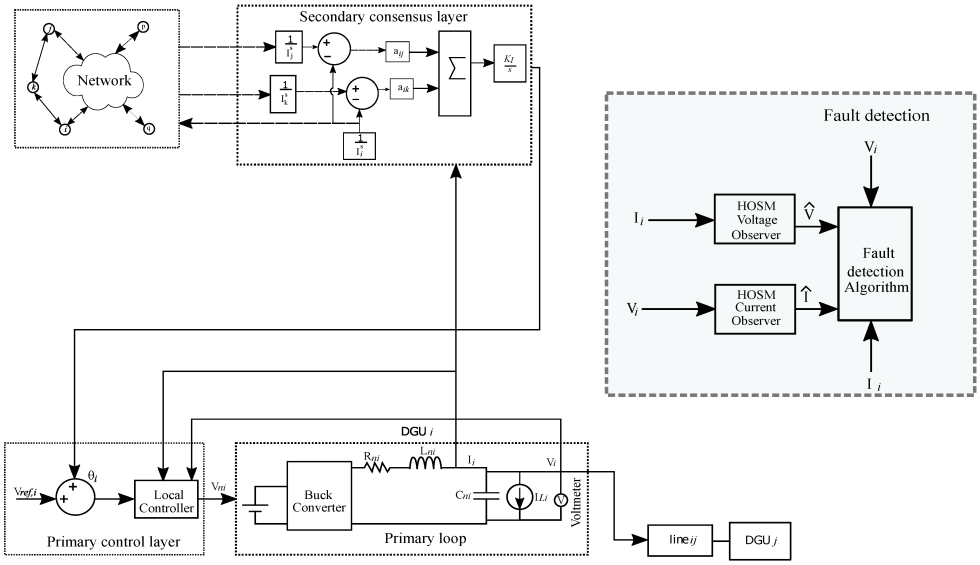

Figure 5. Functional block diagram of the *i*th distributed generation units with controllers and higher order sliding mode observers [5].

3. Future Directions

Regarding the islanding fault detection, [1] suggests three future research topics: (i) synergistic combinations of different detection techniques to build new hybrid techniques with reduced non-detection zone, reduced false alarm rate, and improved detection performance; (ii) utilizing the available signal processing techniques and learning algorithms to compute the parameters of islanding fault detection techniques (e.g., threshold value); and (iii) investigating the applicability and practicality of islanding fault detection techniques in future smart grids.

Review article [2] provides a wide range of directions that can be pursued to improve cyber-security in microgrids. In particular, [2] suggests the following research topics: (i) state estimation under cyber attacks; (ii) frequency and voltage control under cyber attacks; (iii) cyber-security of electric vehicles and charging stations; (iv) applications of blockchain technology in microgrids; and (v) utilizing software-defined networking technologies to improve cyber-security of microgrids.

Even though different fault-detection and fault-tolerant control schemes have been designed and implemented in [3–5], their real-time implementation and their robustness against model uncertainties and external disturbances remain as future research topics. Moreover, distinguishing faults from cyber attacks is a very important research topic that needs to be investigated in future. This is a very challenging task as there is a brain behind each cyber attack; that is, the attacker can conduct an attack such that the system behaves as

a faulty system. To the best of our knowledge, there is no systematic method for detecting and isolating faults from cyber attacks.

4. Conclusions

The Special Issue "Microgrids and Fault-Tolerant Control" comprises five articles (two review articles and three original research articles) with various topics and methodologies in fault-tolerant control for microgrids. This editorial briefly summarized the details of each study and provided future directions to further pursue the subjects. The editorial team would like to thank all contributors, reviewers, and journal staff for their efforts.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Hosseinzadeh, M.; Salmasi, F.R. Islanding Fault Detection in Microgrids—A Survey. *Energies* **2020**, *13*, 3479. [CrossRef]
2. Nejabatkhah, F.; Wei, Y.; Liang, H.; Ahrabi, R.R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2021**, *14*, 27. [CrossRef]
3. Sharma, V.; Hossain, M.J.; Ali, S.M.N.; Kashif, M. A Photovoltaic-Fed Z-Source Inverter Motor Drive with Fault-Tolerant Capability for Rural Irrigation. *Energies* **2020**, *13*, 4630. [CrossRef]
4. Jadidi, S.; Badihi, H.; Zhang, Y. Passive Fault-Tolerant Control Strategies for Power Converter in a Hybrid Microgrid. *Energies* **2020**, *13*, 5625. [CrossRef]
5. Narzary, D.; Veluvolu, K.C. Higher Order Sliding Mode Observer-Based Sensor Fault Detection in DC Microgrid's Buck Converter. *Energies* **2021**, *14*, 1586. [CrossRef]

Short Biography of Authors

Mehdi Hosseinzadeh received his Ph.D. degree from the University of Tehran, Iran, in 2016. From 2017 to 2019, he was a postdoctoral researcher at the Université Libre de Bruxelles, Brussels, Belgium. From October 2018 to December 2018, he was a visiting researcher at the University of British Columbia, Vancouver, Canada. From 2019 to 2022, he was a postdoctoral research associate at the Washington University in St. Louis, MO, USA. Currently, he is an assistant professor in the School of Mechanical and Materials Engineering at the Washington State University, WA, USA. His research focuses on safety, resilience, and long-term autonomy of autonomous systems, with applications to autonomous robots, autonomous vehicles, energy systems, video streaming, and drug delivery systems.