Scientia Iranica D (2022) 29(5), 2552–2565

SCIENTIA IRANICA

Sharif University of Technology
Scientia Iranica
Transactions D: Computer Science & Engineering and Electrical Engineering
http://scientiairanica.sharif.edu

Research Note

Smart microgrid educational laboratory: An integrated electric and communications infrastructure platform

M. Abedini[*], **T. Vahabzadeh, S.-A. Ahmadi, M.-H. Karimi, H. Manoochehri, A.-H. Nazeri, M. Karami, M. Arani, F. Aminifar, and M. Sanaye-Pasand**

School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran.

Received 11 May 2020; received in revised form 29 August 2020; accepted 18 October 2020

KEYWORDS
Communication infrastructure;
Microgrid automation;
Renewable energy integration.

Abstract. Microgrids as local area power systems are changing the power system landscape due to their potential to offer a viable solution for integrating renewable energy resources into the main grid. From the operational point of view, microgrids should have appropriate power electronic interfaces, control schemes, and monitoring and automation infrastructure to provide the required flexibility and meet the related IEEE 1547 standard requirements. This study describes some of the efforts made at the smart microgrid educational laboratory to provide such facilities and create real-world conditions needed to conduct research and teach the related courses. Laboratory works not only increase the practical skills of the students but also can motivate them to pursue theoretical courses with a strong passion. The introduced facilities are somehow unique for the integration of both electric and communication infrastructures which can resolve the problem of disregard for data transfer challenges in the studies. Complete hardware design of power plant components and incorporation of solar photovoltaic (PV) and two types of wind turbine generations are some of the efforts made to bring the real-world conditions into the laboratory.

1. Introduction

Engineering education is incomplete without practical skills and university as an important institution in training the required engineers of the industry should appropriately respond to this need. In this way, the effective role of the laboratory cannot be denied [1]. Laboratory works not only increase the practical skills of the students but also can motivate them to pursue theoretical courses with a stronger passion. In addition to the educational purposes of the laboratory, they can be used to conduct the experimental tests needed in science researches. In the laboratory tests, various real phenomena can be observed in a controlled environment which provide an opportunity to develop new theories and evaluate new ideas. From a generic point of view, laboratory work can have the following advantages [2]:

- Better illustration of the scientific phenomena;
- Understanding the way of implementing theories in practice;
- Practicing the way of presenting observations and concluding the results;
- Becoming familiar with the equipment and how to use them.

Smart Microgrid Laboratory of University of Tehran (SMLUT) is funded to achieve the aforementioned goals and also, to provide a real-world situation to conduct experimental tests needed in academic or

[*]. *Corresponding author.*
E-mail address: m.abedini@ut.ac.ir (M. Abedini)

doi: 10.24200/sci.2020.55942.4483

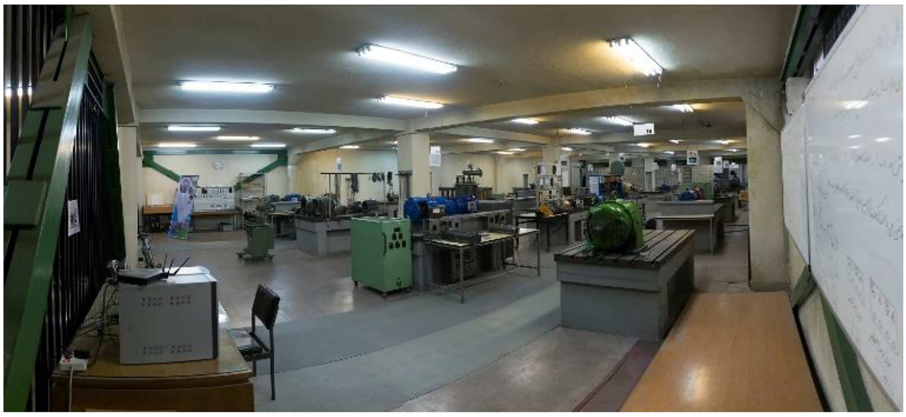


Figure 1. Main hall of the SMLUT.

industrial research. Hardware implementation of different parts of a power network and energy resources offers a real situation to analyze all possible scenarios that may happen in practice. For example, there are some power system instabilities that originate from data communication delay, which cannot be observed in the computer simulation environment [3]. However, in a hardware-based laboratory, all of the real-world shortcomings are considered and more accurate results can be obtained. A report on the SMLUT including its facilities and application areas is given in this paper. It is worth mentioning that besides the knowledge of power systems, several areas due to multi-dispensary nature of the power system including communications, controls, instruments, Information Technology (IT), and cyber-attack should be considered in the power system educations. The main educational outcomes of the SMLUT are:

- Understanding fundamentals of power system operation;
- Understanding important contemporary issues due to the integration of DG, technical challenges, benefits, and perspectives;
- Realizing automation and monitoring concept in power systems and its vulnerability against cyber-attacks;
- Familiarization with hardware components including measurement, protective relay, and control.

The authors of this study wish that reflecting these experiences would motivate and guide scholars and engineers across the world to establish and promote such activities.

The rest of the paper is organized as follows. Section 2 describes the laboratory facilities in summary and Section 3 reflects their applications. Section 4 provides some experimental tests to demonstrate the applicability of the SMLUT. Section 5 concludes the paper.

2. Educational laboratory facilities

The SMLUT has a variety of equipment and facilities to conduct educational and research programs. The main hall of the laboratory is shown in Figure 1 and its overall diagram including the designed facilities is depicted in Figure 2. Each of the laboratory parts with their implemented hardware is described below.

2.1. Synchronous based generating unit emulator

The actual model of the power plant is crucial to most of the power system studies. For example, in the case of system dynamic studies, accurate behaviors of different power plant parts including prime mover, governor, Automatic Voltage Regulator (AVR), and Power System Stabilizer (PSS) are important to truly observe system transients, voltage variations, and frequency disturbances [4–8]. There are various models in the computer simulation software to represent the dynamic properties of the power plant components [9–11]. However, since all of the computer simulations are conducted in ideal conditions, they cannot represent the actual characteristics of the power plant during disturbances. To tackle this drawback and perform real-time and close-to-reality simulations, a hardware-based synchronous generating unit emulator is designed in the SMLUT.

The designed power plant emulator includes two sets of DC motor coupled with a synchronous generator (T-G1 and T-G2). The DC motor is a separately excited one that is used to simulate the behavior of generator prime mover and generates the needed mechanical power of the turbine. Field windings of the DC motor and synchronous generator are independently controlled to regulate the output speed and voltage of power plants, respectively. The developed emulator setup is shown in Figure 3(b).

For the frequency control, the hardware is designed to adjust the input field current of the DC motor, which models the operation of the governor and

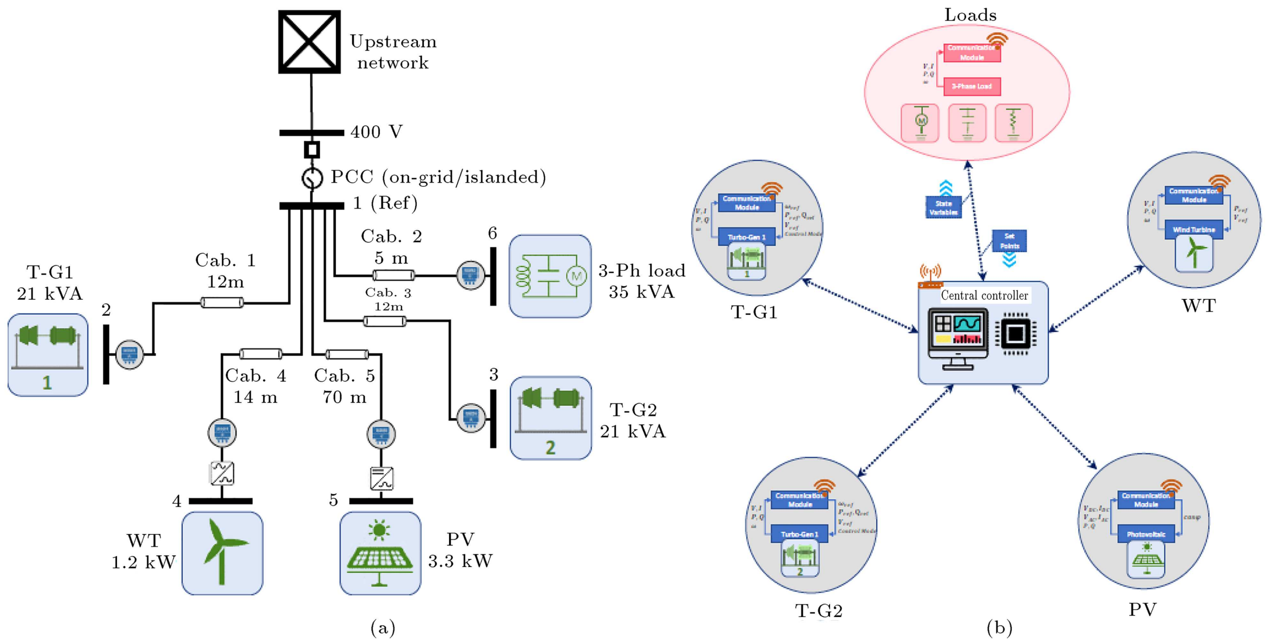


Figure 2. SMLUT: (a) Electric mimic diagram including turbine-generator, wind turbine and PV and (b) communication schematic diagram.

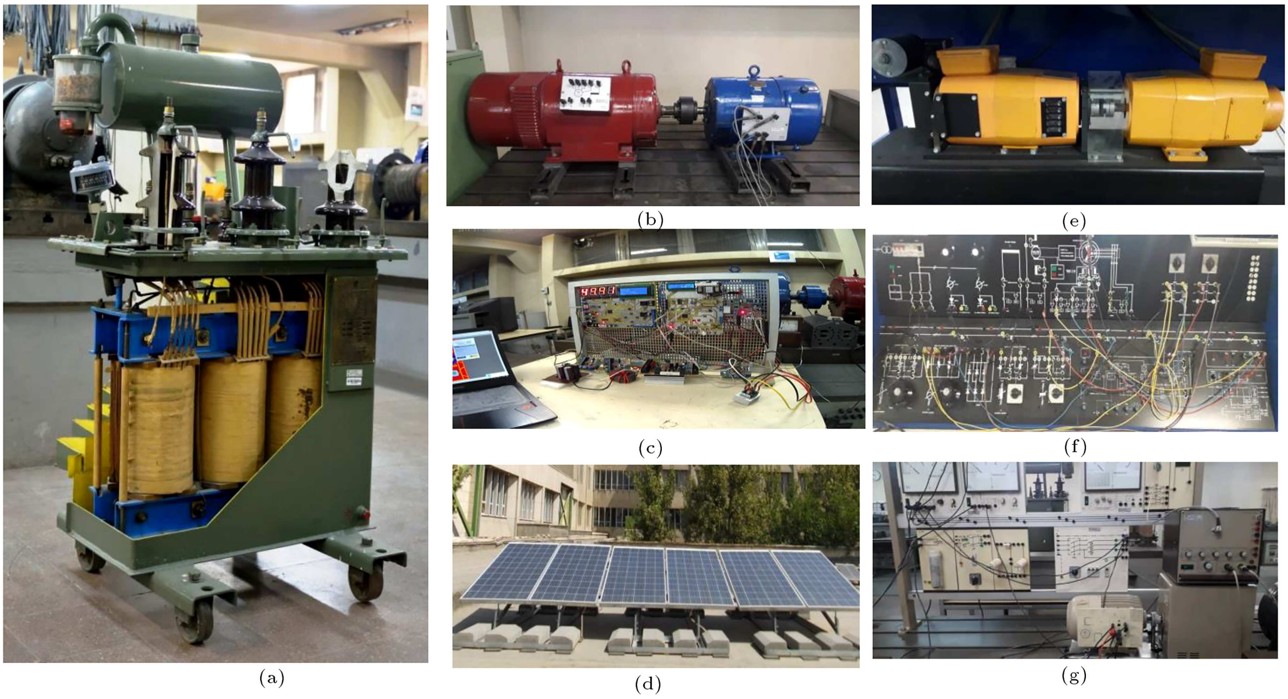


Figure 3. Some of the SMLUT facilities: (a) Transformer, (b) generating unit emulator, (c) governor, AVR and PSS control circuits, (d) PV panels, (e) wind turbine emulator, (f) control board of the wind turbine emulator, and (g) motor test setup.

adjusts the input mechanical power of the generator, thereby controlling the frequency. To locally monitor the governor behavior, a governor monitoring module is also embedded in the setup. In addition, several protection considerations such as field failure, over speed, and temperature measurement are implemented.

The governor hardware is designed such that various control strategies used in a real power plant can be implemented in this hardware including:

i) Constant output power;

ii) Isochronous frequency control;

iii) Droop control.

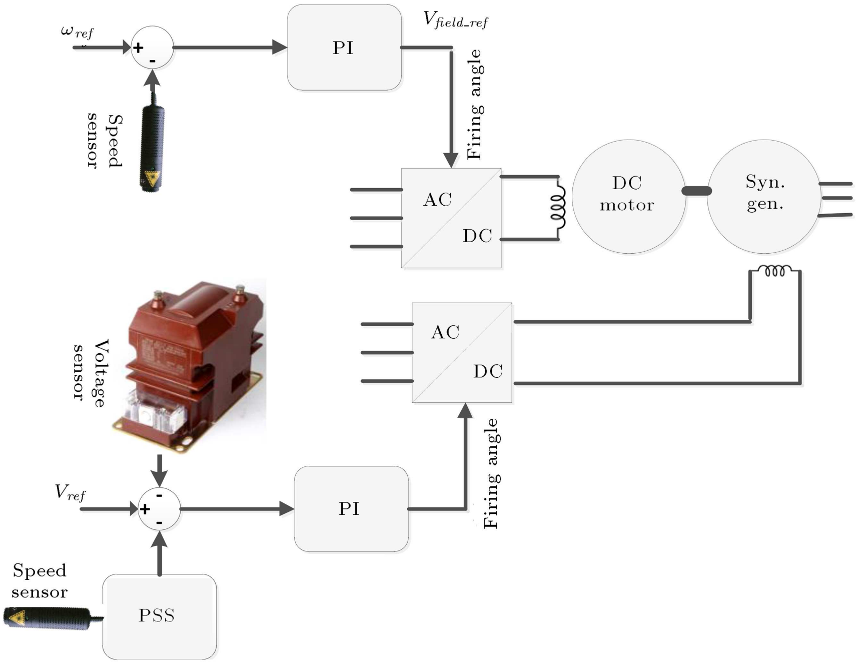


Figure 4. Control part of the power plant emulator.

To do so, state spaces of the aforementioned control modes are implemented and executed in a real-time manner. The power plant emulator setups can operate in both islanded and grid-connected modes, as well. In the islanded condition, the overall laboratory network is an independent microgrid. Since one synchronous generator should play the role of slack generator and take over the task of frequency control during the islanded operation, an automatic control mode switching scheme is designed to ensure the frequency stability of the islanded microgrid for the mentioned condition.

For the voltage control, field winding current of the generator is controlled through designed hardware which acts as AVR. Since there are different types of excitation systems, modular architecture is used and the hardware is designed such that the inner control system can be adapted to the users' needs by changing the state equations written in the software. Using this architecture, various control strategies such as: i) voltage, ii) reactive power, iii) power factor, iv) droop, and v) manual control can be implemented. When the generators are connected to the upstream network, to preserve stability of the microgrid, the excitation system works in the power factor or droop control modes. Immediately after islanding the microgrid, the control mode of one generator is switched to the voltage control mode to prevent voltage instability, while others can have any other modes. In a real power plant, high-speed AVR improves the transient stability, while it reduces the ability of the generator to damp the system electromechanical oscillations, i.e., dynamic stability. The practical solution to compensate this shortcoming is the use of PSS. The designed hardware for performing the AVR task is accordingly equipped with an integrated PSS to truly emulate the behavior of the power plant. The implemented hardware of the control part is shown in Figure 3(c) and its schematic diagram is depicted in Figure 4.

2.2. Small-scale solar photovoltaic (PV) power plant

There are many incentives for the development of solar PV power generations due to their positive environmental impacts and no need for fossil fuels. Future electric networks are highly penetrated with PV panels [12,13]. To provide the facilities needed to train and conduct researches on the behavior of PV interconnection to the network in different conditions, a single-phase grid-connected 3.3 kW solar PV power plant setup is installed at the SMLUT. Figure 3(d) shows installed PV panels.

2.3. Wind turbine emulator

Among different types of renewable energy generations, wind turbines attract greater attention due to their lower net cost [14]. The wind turbine emulator replicates the static and dynamic behaviors of a real wind turbine and provides real-time hardware-based simulations [15,16]. Upon using this emulator, the performance of wind energy conversion and also, operation of control schemes can be analyzed without the need for a controlled environment in terms of wind profiles and other environmental conditions.

This emulator consists of a 1.2 kW DC motor coupled with an induction generator along with a computer software interface to take the desired wind

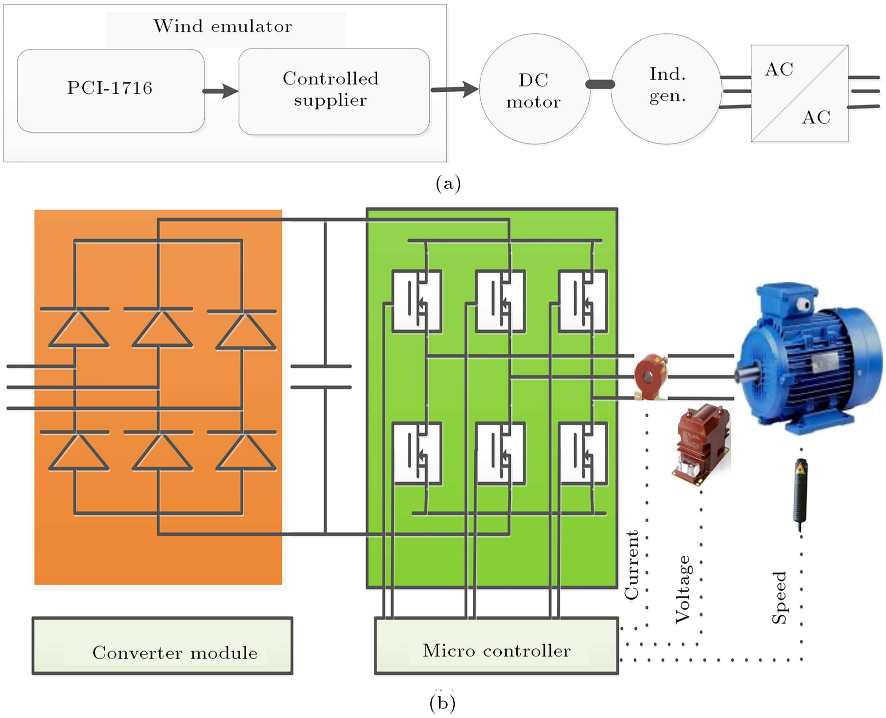


Figure 5. (a) Conceptual design of the wind turbine emulator. (b) Grid-side power electronics interface.

profile from the user. Figure 5 shows the conceptual design of this emulator and the grid-side power electronics interface, and Figure 3(e) and (f) shows the implemented setup and control board. In order to calculate the operating point of DC motor corresponding to the input data of wind profile, a computer software control system using Real-Time Windows Target Toolbox of the MATLAB/Simulink software and PCI-1716 multifunction data acquisition card is designed to inject the required reference signals into the DC motor and control the induction generator. At the time of writing this manuscript, only Types I and II of the wind turbines are modeled using this emulator, while our future work is to model other types of wind turbines feasible using this emulator. The adopted control strategy for the developed wind turbine in the islanded mode is V/F control. It should be noted that the V/F controlled converter emulates the behavior of a synchronous machine and thus, it can control both voltage and frequency of the AC system. The inverter acts as a voltage source with the magnitude and frequency of the output voltage being controlled.

2.4. Intelligent Electronic Device (IED)

IEDs are vital requirements in any electrical equipment and systems to guarantee proper operation and prevent the propagation of disturbances. Nowadays, digital microprocessor-based IEDs have become integrated terminals with various modules to play key roles in different functionalities which can be classified into the following groups:

- **Protection:** This functionality covers all protection functions to protect a generator, motor, transformer, or feeder;
- **Control functions and logics:** These functions may be control loops in voltage regulators, control logics in circuit breakers, etc.;
- **Metering:** This function is used for metering values including line voltages, phase currents and voltages, frequency, power and energy, harmonics, and disturbance recording;
- **Serial communication:** This function supports protocols like Modbus RTU, Modbus TCP, Profibus, etc. in order to enable interoperation of IEDs from different vendors.

Various IED types are installed at the SMLUT which can support the aforementioned functionality and thus, enhance the reliability and security of the Lab. In addition, these IEDs can be used for educational purposes.

2.5. Automation infrastructure

Smart networks are two-way interconnected networks in which automation infrastructure plays a fundamental role in the data transfer procedure [17]. Automation infrastructure for transmitting information and receiving remote commands requires high-speed communication technology and capability to collect and process electric signals [18]. To have such a smart network, various advanced technologies including smart metering devices, monitoring facilities, com-

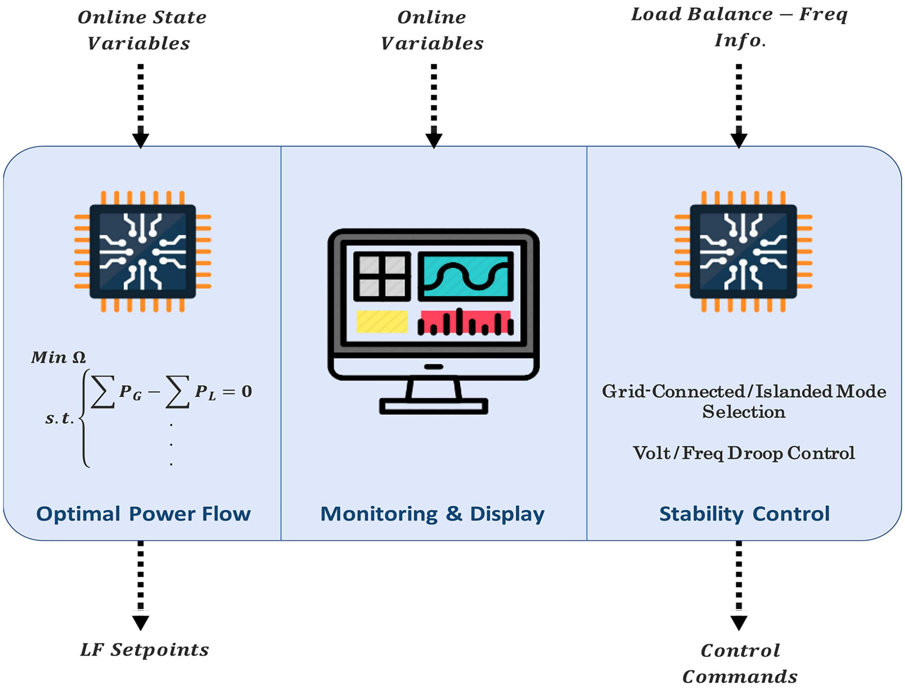


Figure 6. Different features of dispatching software.

munication infrastructures, supervisory control, and data acquisition systems are needed. In order to equip the SMLUT with these technologies, much effort has been made. In doing so, all of the laboratory setups are equipped with smart industrial meters to gather local information. The collected information is then sent to an Xbee module to be transmitted to the area operating center, which is a Raspberry Pi single-board computer. In addition to the implemented area operating center, a computer-based upstream control system with developed dispatching software is designed to monitor the overall network and deliver the users' commands for supervisory controlling of different network parts.

The local communication protocol of the smart meters is a common and easy-to-implement Modbus serial protocol of RS-485 [19]. In the XBee module, the received data are read based on this protocol and then, they are sent to the Raspberry Pi board through ZigBee protocol, which is the common protocol of power networks [20]. The communication link between the Raspberry Pi area control center and the computer-based central control system is the Universal Asynchronous Receiver-Transmitter (UART) serial protocol. Generally, various data communication protocols are implemented at the SMLUT to make the infrastructure ready for conducting research based on all data communication protocols. In addition to the hardware infrastructure of the automation system, monitoring and control dispatching software is developed to display the collected data of the setups and to receive the users' command. Different features of this software that demonstrate its capabilities are graphically shown in Figure 6.

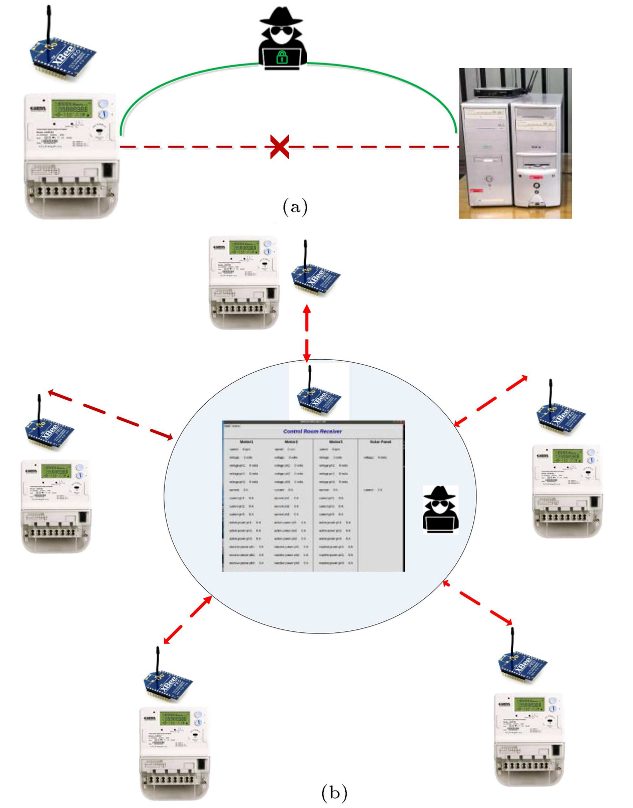
2.6. Man-in-the-middle cyber-attack interface

The automation infrastructure in the power network and integration of different communication protocols, along with all of the opportunities and advantages brought to the system, make it vulnerable against cyber-attacks. The increased growth of cyber-attacks in today's electric networks has raised serious concerns and proves the necessity of security. Accordingly, a controlled environment to apply cyber-attacks and examine their impact on the network is established to develop an approach to detecting and preventing them. Cyber attackers are always looking for new methods to access various parts of the network and apply malicious operations hidden to the control center.

In SMLUT, a cyber-attacker computer interface based on the concept of man-in-the-middle attack depicted in Figure 7 is developed. Using this interface, all of the obtained data from different testbeds before entering the control center are monitored and controlled. Accordingly, any data change needed to apply a cyber-attack can be performed. The developed interface enables applying different kinds of cyber-attacks in the laboratory network based on the False Data Injection Attack (FDIA) method.

3. Application area and users

The provided facilities at the SMLUT can be used by a vast community of people for a variety of educational,



(a)

(b)

Figure 7. Developed man-in-the-middle attack interface concept.

research, and industrial purposes. In addition to the undergraduate students using laboratory facilities for educational intents, different groups of users including master students, PhD candidates, post-doctoral researchers, industry specialists, visiting scientists, etc. can conduct their experimental studies or industry projects inside the laboratory. A list of some laboratory applications with the current under-study research topics is reported in the following.

3.1. Monitoring, control, and automation in smart networks

Having procured the automation infrastructure consisting of smart metering devices, communication systems, data processing, and control centers, which enables real-time condition monitoring and remote controlling of the grid, a series of studies on the monitoring, automation, and control of the smart networks can be conducted. One of the most fundamental technologies developing in this category of research is the well-known Wide-Area Monitoring, Protection, and Control (WAMPAC) system [21–23]. It uses the system-wide information transmitted to the control center from the selected locations to decide about the system condition and prevent the propagation of large disturbances in case of emergencies. WAMPAC technology aims to reduce the number of catastrophic blackouts and improve the security and reliability of the network. It can predict the voltage and frequency instabilities and suggest the required remedial actions to prevent them. Almost all of the required infrastructures used in conducting experimental studies on this area are provided at the SMLUT. The developed automation infrastructure facilitates evaluating new hierarchical control strategies before their real implementation [24].

3.2. Power system and microgrid dynamic studies

Nowadays, transmission networks are required to be ready for more flexible interchange transactions. This provides a condition where the power system operates close to its dynamic thermal limit [25]. In this condition, the dynamic analysis of the power system becomes more important. At the design and implementation stages of the SMLUT, much effort has been made to accurately model the dynamic behavior of all setups. This brings about an opportunity to conduct dynamic studies in near-reality conditions and to observe more phenomena than the studies conducted in the simulation environment.

By means of this laboratory, various experimental studies including dynamic model validation, stability analysis, load shedding schemes, inter-area oscillation damping, etc. can be conducted. In addition to the mentioned classic studies, other recent challenges in the dynamic field can be studied at the founded laboratory. For example, increased penetration of inverter-based generations and low-inertia synchronous generators make the microgrid and the overall network more vulnerable to the transient instability [26,27]. Generally, different dynamic behaviors of inverter-based and low-inertia generations including their fast response are changing the previous paradigms in dynamic studies. Provided facilities at the laboratory, mainly renewable generation setups, provide an opportunity to conduct experimental studies on such emerging issues.

3.3. Cybersecurity of networks

Since the 1970s, the structure of power network control centers has changed from a closed uniform framework to an open interactive one. In the emerging concept of smart networks, the use of Internet Protocol (IP) based equipment is growing because utilities enjoy the advantages of remote controlling and wide-area applications [28]. Philosophy of these networks is tied with information transfer between integrated distributed computing systems through communication links, which can be whether a dedicated line, microwave communication, or the internet. In this situation, unauthorized access to the Supervisory Control and Data Acquisition (SCADA) system and the Wide-Area Measurement System (WAMS) becomes possible [29].

According to IEC 62351 standard [30], the fundamental causes that make the power network vulnerable against cyber-attacks are mentioned. Some of these causes are listed below:

- Weakness or absence of login permission authentication;
- Use of open international standards such as IEC 60870, IEC 61850, and IEC 61970;
- Accessibility to world-wide public networks;
- Lack of personal knowledge about cyber threats;
- Absence of cybersecurity requirements in the design and development of equipment and software;
- Outdated software and insufficient firewalls to protect the power network against hacking.

The abovementioned reasons attenuate the cybersecurity of power system and make it vulnerable to the targeted attacks. These attacks can cause varying levels of severity, but the most destructive one is launching control actions through the SCADA environment after gaining access to the supervisory control center. In such scenarios, the cyber attackers can lead the system to collapse or hazardous conditions [31–34].

At the SMLUT, all of the facilities required to conduct experimental tests for cybersecurity studies are provided. Industrial communication and automation infrastructures, area operating, and supervisory control centers along with the dispatching software are developed to emulate the cyber-physical infrastructure of a real power system. Inside this laboratory, not only may malicious faults and contingencies be applied but also FDIAs based on the man-in-the-middle technique to change the power system state estimation are modeled. Of note, state estimation software should be robust against FDIA. One of the practical solutions to ensure this security is defining an index to detect FDIA referred to as the largest normalized residual (LNR) as follows:

$$LNR = \left\| Z - H\widehat{X} \right\|, \tag{1}$$

where "‖" indicates the norm of the vector. In addition, Z is the matrix of the measured values and X represents the system variables. The function H indicates mathematical notation of the variables to the measurements. During the normal condition, LNR value is almost equal to zero. However, in the event of cyber-attack, it can be skyrocketed. It is assumed that bad data A is added to the measured value as an FDIA; thus, we have:

$$Z_{bad} = Z + A, \tag{2}$$

$$X_{bad} = X + C, \tag{3}$$

$$\begin{aligned}\widehat{X}_{bad} &= \left(H^T W H\right)^{-1} H^T W Z_{bad} \\ &= \left(H^T W H\right)^{-1} H^T W (Z + A) \\ &= \widehat{X} + \left(H^T W H\right)^{-1} H^T W A = \widehat{X} + C,\end{aligned} \tag{4}$$

where C is the deviation vector of the state variables from the original value and W is the covariance matrix of the network measurements. LNR index is calculated as follows:

$$\begin{aligned} LNR_{bad} &= \left\| Z_{bad} - H\widehat{X}_{bad} \right\| \\ &= \left\| Z + A - H\left(\widehat{X} + \left(H^T W H\right)^{-1} H^T W A\right) \right\| \\ &= \left\| Z + A - H\widehat{X} + (AH(H^T W H)^{-1} H^T W A) \right\| \\ &= \left\| Z - H\widehat{X} + (A - HC) \right\|. \end{aligned} \tag{5}$$

Based on Eq. (5), if $A = HC$ is fulfilled, this attack is undetectable. Overall, based on the above explanations, there are five possible attacks applied to the man-in-the-middle computer interface of the laboratory as follows:

i) **Implement a valid FDIA without any restrictions:** It is assumed that the attacker has all the configuration information of the system (the H-matrix) and can attack all meters;

ii) **Implement a valid FDIA under certain restrictions:** The attacker has H-matrix with a limited ability to hack the meters due to the physical protection of the measurements. In such a scenario, choosing a measurement with the highest impact is important for the attacker;

iii) **Implement a valid FDIA with incomplete H-matrix information:** It is assumed that the structure of the power system is secret and not accessible;

iv) **Implement a valid FDIA with distorted topology:** In this type of attack, it is assumed that the attacker can manipulate not only the continuous data (measurements of smart meters) but also the discrete data (the indication of open/close state of power circuits), reflecting the topology of the power network;

v) **Implement a valid FDIA on the control system of power plants:** In this case, the attacker changes the control parameters of the power plant and this measure leads to severe blackout in the power system.

3.4. Protection studies

Designing a reliable protection scheme for microgrids is challenging, since the short-circuit current levels keep changing when the DG units are connected/islanded [35,36]. Each DG's contribution is based on its location, size, and generator type. The fault current contribution of the microgrids with synchronous DGs is much greater than the ones with inverter-based DGs [37]. As a result, the contribution from multiple DGs will affect the settings and coordination of protective devices [38]. To overcome these protection problems, the application of adaptive protection relays is a promising solution due to their flexibility online to modify both relay settings and characteristics using external signals.

At the SMLUT, programmable compact hardware with output switching modules has been developed to easily implement the protection algorithms. Besides, various specially designed equipment pieces are provided at the laboratory to conduct protection and fault analysis studies. For example, by using the designed transformer with internal fault capability, real-fault signals can be generated which is very useful for testing the transformer relays and also, performance evaluation of protection algorithms. The same studies can be conducted using other existing equipment such as generators and motors.

For generator protection studies, the available facilities can be used to test the protection algorithm, which is proposed to detect abnormal operating conditions such as loss of field, over-excitation, etc. [39]. The setup of renewable energy resources at the laboratory provides an opportunity to investigate protection issues on the inverter-based systems. Since the output voltage and current of these systems are controlled via the inverter modules, previous protection schemes cannot properly detect their faults. Therefore, new protection techniques should be proposed for fault detection in these systems. Another important issue in such systems is the detection of islanding events. These events should be rapidly detected to enable an appropriate action [40,41]. To do so, passive methods are used and a protective relay including the following functions is installed at the Point of Common Coupling (PCC):

- **Over/under voltage:** Monitors whether or not the grid voltage goes out of the limits established by the relevant standards;
- **Over/under frequency:** Monitors whether or not the grid frequency goes out of the limits imposed by the relevant standards;
- Monitoring Rate of Change Of Frequency (ROCOF) and Voltage (ROCOV);
- **Phase monitoring:** Monitors fast jumps of grid voltage phase angle.

At the SMLUT, the required facilities to conduct such research studies are provided. Besides, the existing infrastructures at the laboratory are sufficient to perform power system protection studies such as wide-area protection schemes. For example, faster-than-real-time approaches to predicting instability are of recent studies ongoing at the laboratory [41].

3.5. Studies related to the rotating machines and transformers

The rotating machine setups at the laboratory are well equipped such that most of the studies related to the rotating machines can be conducted. The modeling, design, operation testing, condition monitoring, and control issues associated with rotating machines are some of the research topics that are now being followed at the laboratory [42,43]. In addition to the pure rotating machines studies, another type of research on the effect of applying motor-type inductive loads to the network can be conducted. These types of studies focus on the interaction between electric machines and the power network. For example, unexpected delay in the recovery of voltage due to the removal of an external fault, which is known as Fault Induced Delayed Voltage Recovery (FIDVR) phenomenon, can be easily observed and studied using inductive motors at the laboratory [44,45].

In addition, at the SMLUT, educational transformers are designed such that their inner parts containing their cores, windings, connections, etc. can be easily observed. Besides, a testbed is provided to teach and practice the way of laminating the core and winding the transformer. These handmade transformers are then simulated in finite element 3D software to improve the ability of students to design and analyze the transformers in simulation environments. In addition to the educational tools, there are various facilities to conduct research on the transformer studies. A transformer with the capability of applying internal faults is designed for transformer protection studies. Various fault types including turn-to-ground, turn-to-turn, etc. can be modeled using this equipment.

3.6. Integration of renewable energy resources into the network

Traditional sources of power generation are rapidly being replaced with renewable energy ones. It can be predicted that in near future, a high percentage of the required energy will be supplied by them. Integration of renewable energy resources into the network provides some new challenges for the network operators. Since the generated power of these resources is not fixed and depends on the environmental conditions, weather, and season, secure use of them in the network is not easy and requires comprehensive studies [46]. The small-scale PV power-plant and the wind turbine emulator of the SMLUT enable the required studies to utilize renewable energy resources in the network. Optimal scheduling of renewable microgrids dealing with the stochastic and uncertain amount of renewable power generation, etc. is part of the research areas that can be studied at the laboratory.

Besides, connecting the renewables to the grid exposes the system to some new security and protection challenges, which compel the network operators to establish new grid codes for preventing insecure conditions. For example, the low voltage ride through (LVRT) requirement is one of them which indicates the necessity of continuing operation and not disconnecting the renewables from the upstream network during low-voltage conditions [47–50]. The mentioned challenges can be analyzed at the laboratory and proper solutions for overcoming them can be proposed. Besides, new grid codes can be comprehensively evaluated at the laboratory in a near-reality condition before applying them to the network.

4. Some of experimental study results

In the previous sections, the SMLUT facilities and their application areas were presented. To demonstrate the laboratory applications, some experimental studies have been carried out. However, given the page limitation, only a summary of two of these studies is provided in this section.

4.1. Performance of the governor during the islanded operation

Performance of the implemented governor is evaluated in this section. To this end, it is assumed that the microgrid operates in the islanded mode and the synchronous generator (T-G1) loading is about 30% and operates in both voltage and frequency control modes. Other DGs are in service and operate in active power and reactive power constant modes. Suddenly, resistive load corresponding to 50% of the T-G1 is connected to the microgrid and is rejected again after about 4 s. Figure 8 shows the behavior of the implemented governor. Since T-G1 operates as the slack machine, it seeks to keep the frequency system within the permissible range. To do so, when the load is connected to the microgrid, T-G1 injects more current into the system and when the load is disconnected, T-G1 participation is reduced. It can be concluded that the generator speed is appropriately recovered to the nominal speed for both increment and decrement loads.

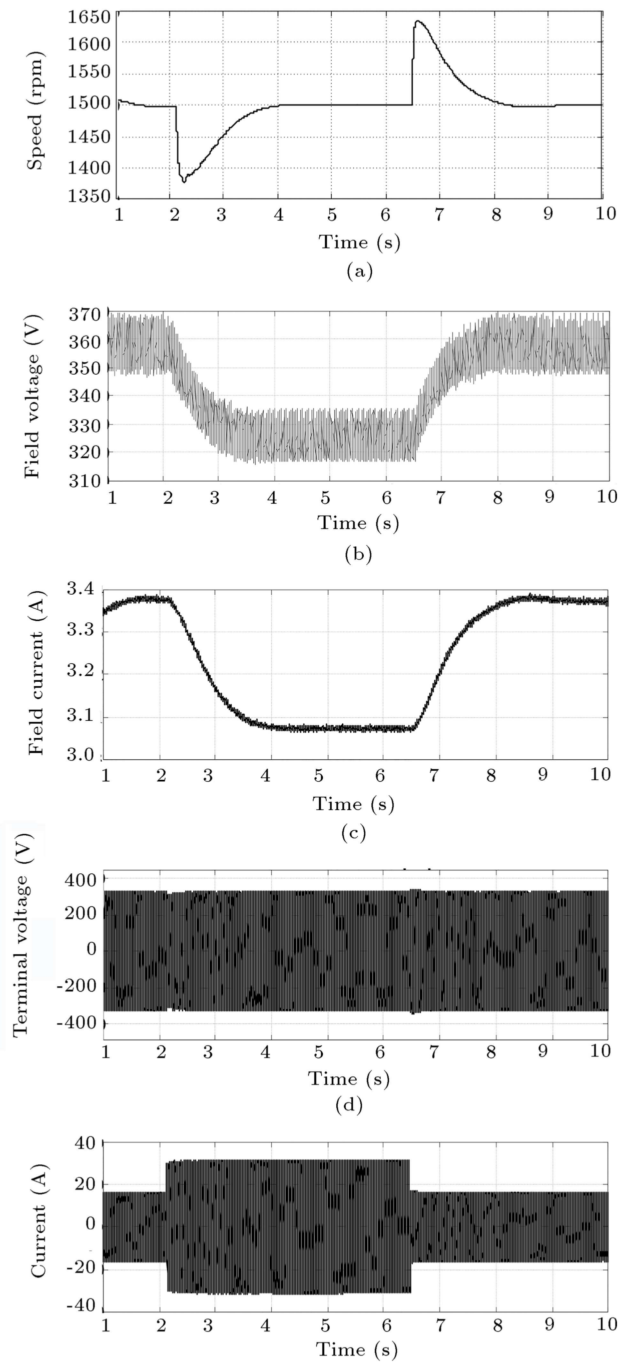


Figure 8. Governor behavior for the load changes: (a) Speed, (b) field voltage of the DC motor, (c) field current of the DC motor, (d) terminal voltage of the generator, and (e) terminal current of the generator.

4.2. FDIA to the control system of the power plant

As presented before, the man-in-the-middle attack interface is able to apply 5 different attacking scenarios. These types of attacks can be categorized into two major groups of static and dynamic attacks. The first four of them are static ones where the changes are reflected in the load flow results. However, in the 5th scenario when the attacker changes a control parameter, nothing is reflected in the static parameters of the load flow; thus, the dispatching operators cannot observe any abnormal condition in the network. This type of attack, which represents the dynamic cyber-attack in this paper, is the most destructive scenario.

To illustrate the impact of this type of attack, the following test study is designed.

In this test, to prevent destructive damages, it is assumed that only one turbine-generator (T-G1) is in-service and 7 kW resistive load is connected to it. In addition, the microgrid operates in the islanded mode. It is assumed that the attacker changes the speed reference of the governor system periodically based on FDIA and through the man-in-the-middle cyber-attack interface. Before the attack, the speed reference is set to 1 pu. This parameter is changed into 1.01 and 0.99 pu with a period of 4 s in a step change manner.

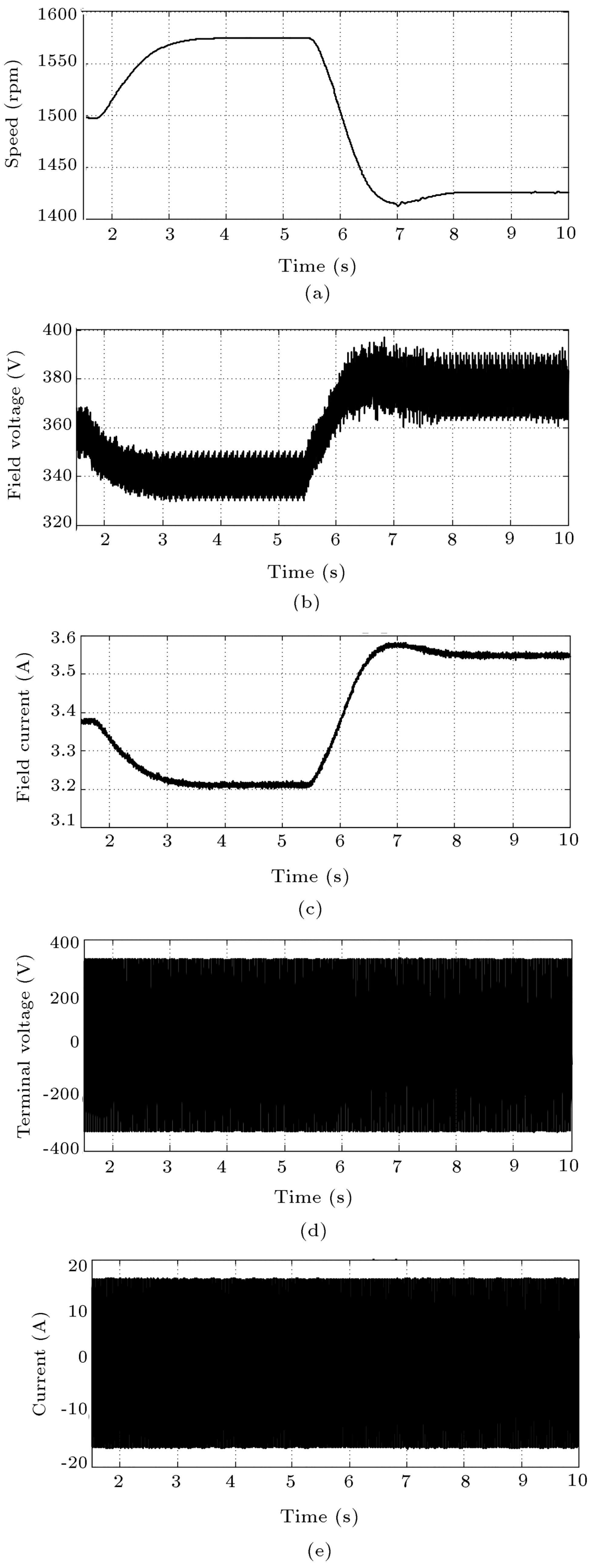
Figure 9 shows the behavior of the T-G1 signals. As can be observed, the output voltage and current signals which are monitored in the dispatching centers are not changed, while the internal parameters such as generator speed and field voltage are changed. Figure 9(a) shows the deviation of the mechanical speed from the nominal speed to follow the speed reference. If this action keeps on happening for a long time, the machine experiences severe damage and results in blackout, as well.

Nearly all of the conducted studies in the field of cyber-security assessment of power system only consider the static attack. However, the results of this test show the destructive effect of dynamic attacks. Highlighting their impact and proposing solutions to detect and prevent them will be handled in the future works of the laboratory.

5. Conclusion

This study presented a Smart Microgrid Laboratory of University of Tehran (SMULT). The focus here was on microgrid modeling, control, automation, and protection, which were developed and implemented completely at this university. Different sections of the model were addressed and some of its applications were explained. It is true that although different software platforms can teach engineering concepts to students, the importance and impact of the practical laboratories should not be ignored. It is important for the students to see and work with real power apparatuses, and this purpose can be achieved with the help of laboratories. SMULT provides this opportunity to promote students' understanding and skill as in the following:

- Analysis of the structure of the rotating machines and transformers;
- Analysis and understanding of control concepts of the centralized/decentralized DGs for the operation of microgrid with emphasis on the requirements of performance balancing, robustness, reliability, and resiliency in a realistic condition;
- Contribution of DGs during short-circuit events by considering different dynamic behaviors;



(a)

(b)

(c)

(d)

(e)

Figure 9. Governor behavior for the load changes: (a) Speed, (b) field voltage of the DC motor, (c) field current of the DC motor, (d) terminal voltage of the generator, and (e) terminal current of the generator.

- Implementation of appropriate protection schemes for microgrids operating in different control modes and different type resources;
- Programming on different platforms that would be interfaced with the traditional substation elements to monitor different signals and status;
- Discussion, implementation, and analysis of network-based communication technologies including Supervisory Control and Data Acquisition (SCADA) protocols;
- Discussion and evaluation of the threats against vulnerable system components and application of information security.

References

1. Boud, D., Dunn, J., and Hegarty, E., *Teaching in Laboratories*, In Society for Research into Higher Education & NFER-Nelson (1986).
2. Jervis, L., *Laboratory Work in Science Education: An Evaluation with Case Studies*, in Plymouth, UK: University of Plymouth (1999).
3. Milano, F. and Anghel, M. "Impact of time delays on power system stability", In *IEEE Transactions on Circuits and Systems I: Regular Papers*, **59**(4), pp. 889–900 (April 2012).
4. Parizad, S., Mohamadian, M., Iranian, E., et al. "Power system real-time emulation: a practical virtual instrumentation to complete electric power system modeling", In *IEEE Transactions on Industrial Informatics*, **15**(2), pp. 889–900 (Feb. 2019).
5. Akhavan, A. and Mohammadi, H.R. "A new control method for grid-connected quasi-Z-source multilevel inverter based photovoltaic system", *Scientia Iranica, Transactions D: Computer Science & Engineering, Electrical*, **22**(6), p. 2505 (2015).
6. Akhbari, A. and Rahimi, M. "Performance and stability analysis of grid connected single phase inverters used in solar photovoltaic systems", *Scientia Iranica, Transactions D: Computer Science & Engineering, Electrical*, **22**(6), pp. 2505–2515 (2015).
7. Farahani, H.F., Khalili, M., Rabiee, A., et al. "On the application of plug-in hybrid electric vehicle to compensate network harmonics: A multiobjective approach", *Scientia Iranica. Transactions D: Computer Science and Engineering, Electrical*, **21**(6), pp. 2177–2185. (2014).
8. Asad, R. and Kazemi, A. "A novel practical fair nodal price for DC microgrids and distribution systems", *Scientia Iranica, Transactions D: Computer Science & Engineering, Electrical*, **21**(6), pp. 2232–2242 (2014).
9. Darabi, A., Tindall, C., and Ferguson, S. "Finite-element time-step coupled generator, load, AVR, and brushless exciter modeling", In *IEEE Transactions on Energy Conversion*, **19**(2), pp. 258–264 (June 2004).
10. Kunitomi, K., Kurita, A., Tada, Y., et al. "Modeling combined-cycle power plant for simulation of frequency excursions", In *IEEE Transactions on Power Systems*, **18**(2), pp. 724–729 (May 2003).
11. Nicolet, C., Greiveldinger, B., Herou, J.J., et al. "High-order modeling of hydraulic power plant in islanded power network", In *IEEE Transactions on Power Systems*, **22**(4), pp. 1870–1880 (Nov. 2007).
12. Alam, N., Chakrabarti, S., and Ghosh, A. "Networked microgrids: state-of-the-art and future perspectives", In *IEEE Transactions on Industrial Informatics*, **15**(3), pp. 1238–1250 (March 2019).
13. Selvakumar, S., Madhusmita, M., Koodalsamy, C., et al. "High-speed maximum power point tracking module for PV systems", In *IEEE Transactions on Industrial Electronics*, **66**(2), pp. 1119–1129 (Feb. 2019).
14. Corbus, D., Lew, D., Jordan, G., et al. "Up with wind", In *IEEE Power and Energy Magazine*, **7**(6), pp. 36–46 (November-Dec. 2009).
15. Moness, M. and Moustafa, A.M. "Real-time switched model predictive control for a cyber-physical wind turbine emulator", In *IEEE Transactions on Industrial Informatics*, **16**(6), pp. 3807–3817 (2020). DOI: 10.1109/TII.2019.2937549
16. Moness, M., Mahmoud, M.O., and Moustafa, A.M. "A real-time heterogeneous emulator of a high-fidelity utility-scale variable-speed variable-pitch wind turbine", In *IEEE Transactions on Industrial Informatics*, **14**(2), pp. 437–447 (Feb. 2018).
17. Lu, X., Wang, W., and Ma, J. "An empirical study of communication infrastructures towards the smart grid: design, implementation, and evaluation", In *IEEE Transactions on Smart Grid*, **4**(1), pp. 170–183 (March 2013).
18. Gungor, V.C., Sahin, D., Kocak, T., et al. "A survey on smart grid potential applications and communication requirements", In *IEEE Transactions on Industrial Informatics*, **9**(1), pp. 28–42 (Feb. 2013).
19. Xunwen, S., Shaoping, W., Dongmei, Z., et al. "RS-485 serial port pseudo-full-duplex communication research and application", In *2010 Prognostics and System Health Management Conference*, Macao, pp. 1–5 (2010).
20. de Almeida Oliveira, T. and Godoy, E.P. "ZigBee wireless dynamic sensor networks: feasibility analysis and implementation guide", In *IEEE Sensors Journal*, **16**(11), pp. 4614-4621 (June 2016).
21. Liu, Z., Chen, Z., Sun, H., et al. "Multiagent system-based wide-area protection and control scheme against cascading events", In *IEEE Transactions on Power Delivery*, **30**(4), pp. 1651–1662 (Aug. 2015).
22. Adamiak, M.G., Apostolov, A.P., Begovic, M.M., et al. "Wide area protection-technology and infrastructures", In *IEEE Transactions on Power Delivery*, **21**(2), pp. 601–609 (April 2006).

23. Salehi, V., Mohamed, A., Mazloomzadeh, A., et al. "Laboratory-based smart power system, Part II: control, monitoring, and protection", In *IEEE Transactions on Smart Grid*, **3**(3), pp. 1405–1417 (Sept. 2012).

24. Paudyal, P., Munankarmi, P., Ni, Z., et al. "A hierarchical control framework with a novel bidding scheme for residential community energy optimization", In *IEEE Transactions on Smart Grid*, **11**(1), pp. 710–719 (Jan 2020). DOI: 10.1109/TSG.2019.2927928

25. Ahmadi, S., Vahidinasab, V., Ghazizadeh, M.S., et al. "Co-optimising distribution network adequacy and security by simultaneous utilization of network reconfiguration and distributed energy resources", In *IET Generation, Transmission & Distribution*, **13**(20), pp. 4747–4755 (2019).

26. Razzaghi, R., Davarpanah, M., and Sanaye-Pasand, M. "A novel protective scheme to protect small-Scale synchronous generators against transient instability", In *IEEE Transactions on Industrial Electronics*, **60**(4), pp. 1659–1667 (April 2013).

27. Mohamed, A.I. and El-Saadany, E.F. "Adaptive decentralized droop controller to preserve power sharing stability of paralleled inverters in distributed generation microgrids", In *IEEE Transactions on Power Electronics*, **23**(6), pp. 2806–2816 (Nov. 2008).

28. Chan, A.C. and Zhou, J. "On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628", In *IEEE Communications Magazine*, **51**(1), pp. 58–65 (January 2013).

29. Wei, D., Lu, Y., Jafari, M., et al. "Protecting smart grid automation systems against cyberattacks", In *IEEE Transactions on Smart Grid*, **2**(4), pp. 782–795 (Dec. 2011).

30. Power systems management and associated information exchange - Data and communications security, IEC 62351:2018 (2018).

31. Giani, A., Bitar, E., Garcia, M., et al. "Smart grid data integrity attacks", In *IEEE Transactions on Smart Grid*, **4**(3), pp. 1244–1253 (Sept. 2013).

32. Liu, X. and Li, Z. "Local topology attacks in smart grids", In *IEEE Transactions on Smart Grid*, **8**(6), pp. 2617–2626 (Nov. 2017).

33. Liu, X., Li, Z., Liu, X., et al. "Masking transmission line outages via false data injection attacks", In *IEEE Transactions on Information Forensics and Security*, **11**(7), pp. 1592–1602 (July 2016).

34. Che, L., Liu, X., Shuai, Z., et al. "Cyber cascades screening considering the impacts of false data injection attacks", In *IEEE Transactions on Power Systems*, **33**(6), pp. 6545–6556 (Nov. 2018).

35. Ahmadi, S., Sanaye-Pasand, M., and Davarpanah, M. "Preventing maloperation of distance protection due to CCVT transients", In *IET Generation, Transmission & Distribution*, **13**(13), pp. 2828–2835 (2019).

36. Orji, U., Schantz, C., Leeb, S.B., et al. "Adaptive zonal protection for ring microgrids", In *IEEE Transactions on Smart Grid*, **8**(4), pp. 1843–1851 (July 2017).

37. Zarei, F. and Parniani, M. "A comprehensive digital protection scheme for low-voltage microgrids with inverter-based and conventional distributed generations", In *IEEE Transactions on Power Delivery*, **32**(1), pp. 441–452 (Feb. 2017).

38. Sharaf, M., Zeineldin, H.H., and El-Saadany, E. "Protection coordination for microgrids with grid-connected and islanded capabilities using communication assisted dual setting directional overcurrent relays", In *IEEE Transactions on Smart Grid*, **9**(1), pp. 143–151 (Jan. 2018).

39. Abedini, M., Sanaye-Pasand, M., and Davarpanah, M. "An analytical approach to detect generator loss of excitation based on internal voltage calculation", In *IEEE Transactions on Power Delivery*, **32**(5), pp. 2329–2338 (Oct. 2017).

40. Bakhshi, M., Noroozian, R., and Gharehpetian, G.B. "Novel islanding detection method for multiple DGs based on forced Helmholtz oscillator", In *IEEE Transactions on Smart Grid*, **9**(6), pp. 6448–6460 (Nov. 2018).

41. Makwana, M. and Bhalja, B.R. "Experimental performance of an islanding detection scheme based on modal components", In *IEEE Transactions on Smart Grid*, **10**(1), pp. 1025–1035 (Jan. 2019).

42. Betta, G., Liguori, C., Paolillo, A., et al. "A DSP-based FFT-analyzer for the fault diagnosis of rotating machine based on vibration analysis", In *IEEE Transactions on Instrumentation and Measurement*, **51**(6), pp. 1316–1322 (Dec. 2002).

43. Ostojic, P., Banerjee, A., Patel, D.C., et al. "Advanced motor monitoring and diagnostics", In *IEEE Transactions on Industry Applications*, **50**(5), pp. 3120–3127 (Sept.-Oct. 2014).

44. Hajipour, E., Saber, H., Farzin, N., et al. "An improved aggregated model of residential air conditioners for FIDVR studies", In *IEEE Transactions on Power Systems*, **35**(2), pp. 909–919 (March 2020). DOI: 10.1109/TPWRS.2019.2940596

45. Wang, W., Diaz-Aguiló, M., Mak, K.B., et al. "Time series power flow framework for the analysis of FIDVR using linear regression", In *IEEE Transactions on Power Delivery*, **33**(6), pp. 2946–2955 (Dec. 2018).

46. Naghdalian, S., Amraee, T., Kamali, S., et al. "Stochastic network constrained unit commitment to determine flexible ramp reserve for handling wind power and demand uncertainties", In *IEEE Transactions on Industrial Informatics*, **16**(7), pp. 4580–4591 (July 2020). DOI: 10.1109/TII.2019.2944234.

47. Xie, D., Xu, Z., Yang, L., et al. "A comprehensive LVRT control strategy for DFIG wind turbines with enhanced reactive power support", In *IEEE Transactions on Power Systems*, **28**(3), pp. 3302–3310 (Aug. 2013).

48. Li, X., Zhang, X., Lin, Z., et al. "An improved flux magnitude and angle control with LVRT capability for DFIGs", In *IEEE Transactions on Power Systems*, **33**(4), pp. 3845–3853 (July 2018).

49. "IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces", In *IEEE Std. 1547-2018 (Revision of IEEE Std. 1547-2003)*, pp. 1–138 (6 April 2018).

50. Abedini, M., Davarpanah, M., Sanaye-Pasand, M., et al. "Generator out-of-step prediction based on faster-than-real-time analysis: concepts and applications", In *IEEE Transactions on Power Systems*, **33**(4), pp. 4563–4573 (July 2018).

Biographies

Moein Abedini received the BSc and MSc degrees in Electrical Engineering from the University of Tehran, Tehran, Iran in 2011 and 2013, respectively. Currently, he is an Assistant Professor at the School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran. His research interests include power system dynamic, control, and transients.

Taleb Vahabzaded received the BSc degree from the University of Tehran, Tehran, Iran in 2020. His research interests include power system protection, control, and communication.

Seyed-Alireza Ahmadi received BSc and MSc degrees in Electrical Engineering from the University of Beheshti, Tehran, Iran in 2014 and 2017, respectively, where he is currently pursuing the PhD degree in the mentioned major. His research interests include power system protection problems and stability studies.

Mohammad-Hasan Karimi received the BSc degree from the University of Tehran, Tehran, Iran in 2020. His research interests include power system protection, control, and communication.

Hamid Manoochehri received the BSc and MSc degrees in Electrical Engineering from the University of Khaje Nasir Toosi, Tehran, Iran in 2014 and 2017, respectively. His research interests include power system protection problems and stability studies.

Amir-Hossein Nazeri received the BSc degree from the University of Tehran, Tehran, Iran in 2020. His research interests include power system protection, control, and communication.

Mahyar Karami received the BSc degree from the University of Tehran, Tehran, Iran in 2020. His research interests include power system protection, control, and communication.

Mohammadreza Arani received the BSc degree from the University of Tehran, Tehran, Iran in 2020. His research interests include power system protection, control, and communication.

Farrokh Aminifar (S'07–M'11–SM'15) has been with the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, IL, USA since 2009. He is currently an Assistant Professor at the School of Electrical and Computer Engineering, University of Tehran, Tehran. His research interests include wide area measurement systems, power system expansion planning and reliability assessment, and smart grid initiatives.

Majid Sanaye-Pasand (M'98–SM'05) received the BSc degree in Electrical Engineering from The University of Tehran, Tehran, Iran, and the MSc and PhD degrees from The University of Calgary, Calgary, AB, Canada. Currently, he is a Professor at the School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran. His research interests include power system protection, control, and transients. He is also an editor of IEEE Transactions on Power Delivery.