Abstract— Microgrids as the local area power systems are changing the power system landscape due to their potential of offering a viable solution for integrating renewable energy resources into the main grid. From the operational point of view, microgrids should have the appropriate power electronic interfaces, control schemes, as well as monitoring and automation infrastructures to provide the required flexibility and meet the related IEEE 1547 standard requirements. This paper describes some of the efforts made in the smart microgrid educational laboratory to provide these facilities and create a real-world conditions needed to conduct researches 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 more passion. The introduced facilities are somehow unique for the integration of both electric and communication infrastructures which overcome the shortcomings of not considering 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 in the laboratory. In the load-related side, dynamic behaviors of the various types of motors are modeled. To demonstrate some of the laboratory applications, some experimental studies have been carried out. The results show that this laboratory model is useful to provide insightful perspectives about the microgrid future.

Index Terms— Communication infrastructure, microgrid automation, renewable energy integration.

I. INTRODUCTION

Engineering education is incomplete without practical skills, and the 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 more passion. In addition to the educational purposes of the laboratory, they can be used to conduct the experimental tests needed in scientific researches. In the laboratory tests,
various real phenomena can be observed in a controlled environment, which brings the opportunity of developing new theories and also evaluating new ideas. From a generic point of view, laboratory work can have the following advantages [2]:

- A 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 the University of Tehran (SMLUT) is funded to achieve the aforementioned goals and also provide a real-world situation to conduct experimental tests needed in academic or industrial researches. Hardware implementation of the different parts of a power network and energy resources offers a real situation to analyze all possible scenarios that may happen in practice. As an example, there are some power system instabilities that originated 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, are given in this paper.

It is worth mentioning that besides the knowledge of power systems, several areas due to the 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 the 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 system and also its vulnerability against cyber-attacks.
- Familiarization with hardware components including measurement, protective relay and control.

It is hoped that reflecting these experiences motivates and guides the scholars and engineers across the world to establish and promote related activities. The rest of the paper is organized as follows. Section II describes the laboratory facilities in summary and its applications are reflected in Section III. Section IV provides some experimental tests to show the applicability of the SMLUT. Section V concludes the paper.
II. 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 Fig. 1 and its overall diagram, including the designed facilities, are depicted in Fig. 2. Each of the laboratory parts with their implemented hardware is described below.

A. Synchronous based generating unit emulator

The actual model of the power plant is crucial for most of the power system studies. As an example, for system dynamic studies, accurate behavior of power plant different 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 computer simulations are conducted in the ideal conditions, they cannot represent the actual characteristics of the power plant during disturbances. To tackle this drawback and perform a real simulation, a hardware-based synchronous based generating unit emulator is designed in the SMLUT.

The designed power plant emulator includes two sets of coupled DC motor to the synchronous generator (T-G1 and T-G2). The DC motor is a separately excited one and is used to simulate the behavior of the 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 Fig. 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 adjusts the input mechanical power of the generator, thereby controlling the frequency. To locally monitor the governor’s behavior, a governor monitoring module is also embedded in the setup. In addition, several protection logics such as field failure, over speed, and temperature measuring are implemented as well.

The governor hardware is designed in a way 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, and iii) droop control. To do this, state spaces of the aforementioned control modes are implemented and executed in the 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 during the islanded operation, one synchronous generator should play the role of a slack generator and take over the task of frequency control, 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 various types of excitation systems, modular architecture is used, and the hardware is designed in a way 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 the 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 the others can have any other modes. In a real power plant, high-speed AVR improves transient stability, on the other side, it reduces the ability of generator in damping the system electromechanical oscillations, i.e., dynamic stability. The practical solution to compensate for this shortcoming is the use of PSS. The designed hardware for performing the AVR task is accordingly equipped with an integrated PSS to emulate the power plant behavior truly. The implemented hardware of the control part is shown in Fig. 3 (c) and its schematic diagram is depicted in Fig. 4.

B. 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 in the SMLUT. Installed PV panels and the collected profile of injected power for one day are depicted in Fig. 3 (d) and Fig. 5, respectively.

C. Wind turbine emulator

Among various types of renewable energy generations, wind turbines attract more attention due to their lower net cost [14]. The wind turbine emulator replicates the static and dynamic behavior of a real wind turbine and provides
the real-time hardware-based simulations [15-16]. The performance of wind energy conversion, and the 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 profile from the user. The conceptual design of this emulator and the grid-side power electronics interface is shown in Fig. 6, and the implemented setup and control board are depicted in Fig. 3 (e) and (f). 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 to the DC motor and control the induction generator. Up to the time of writing this manuscript, only Types I and II of the wind turbines are modeled using this emulator, while our future works are to make modeling other types of wind turbines feasible using this emulator. The adopted control strategy for the developed wind turbine for 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.

D. The intelligent electronic device (IED)

IEDs are vital requirements in any electrical equipment and systems to guarantee the proper operation and preventing the propagation of disturbances. Nowadays, digital microprocessor-based IEDs become integrated terminals with various modules to play further key roles in different functionalities that 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 support protocols like Modbus RTU, Modbus TCP, Profibus, etc., in order to enable interoperation of IEDs from different vendors.
Various types of IEDs are installed at the SMLUT that can support the aforementioned functionality and thus enhance the reliability and security of the Lab. Besides, these IEDs can be used for educational purposes as well.

E. Automation infrastructure

Smart networks are two-way interconnected networks in which the 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 the capability of collecting and processing the electric signals [18]. To have a smart network, various advanced technologies, including smart metering devices, monitoring facilities, communication infrastructures, supervisory control and data acquisition systems are needed. In order to equip the SMLUT with these technologies, lots of efforts have been made. In this way, 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 a developed dispatching software is designed to monitor the overall network and deliver the users’ commands for supervisory control of different network parts.

The local communication protocol of the smart meters is common and yet easy to implement the 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 in the SMLUT to make the infrastructure ready for conducting researches under all data communication protocols. In addition to the hardware infrastructure of the automation system, a monitoring and control dispatching software is developed to display the measured data. Different features of this software and its capabilities are graphically illustrated in Fig. 7. In addition, part of the monitoring system is shown in Fig. 8. Based on this figure, the measured data, e.g., voltage, current and active power of the different buses can be easily monitored by the operator in real-time.
F. 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, makes it vulnerable against cyber-attacks. The increasing growth of cyber-attacks in today’s electric networks has raised serious concerns and proves the necessity of security. Accordingly, in order to develop an approach for detecting and preventing cyber-attacks, establishing a controlled environment to apply them and examine their impact on the network is essential. 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 Fig. 9 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 various kinds of cyber-attacks in the laboratory network based on the false data injection attack (FDIA) method.

III. Application Area and Users

A vast community of people can use the provided facilities in the SMLUT for a variety of educational, research, and industrial purposes. In addition to the undergraduate students who use the laboratory facilities for educational intents, different groups of the users, including master students, Ph.D. 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 at the following.

A. Monitoring, control, and automation in smart networks

One of the most fundamental technologies which are 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 is aimed at reducing 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 necessary
infrastructure to conduct experimental studies on this area is provided in the SMLUT. The developed automation infrastructure enables the studies on the evaluation of new hierarchical control strategies before their real implementation [24].

B. Power system and microgrid dynamic studies

Nowadays, transmission networks are required to be ready for more flexible interchange transactions. This leads to the operation of the power system near 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, lots of efforts have been made to model the dynamic behavior of all setups accurately. This brings the opportunity of conducting dynamic studies in near-reality conditions and observe more phenomena than the studies conducted in the simulation environment.

Utilizing 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 also be studied in the founded laboratory. For example, increasing penetration of inverter-based generations and also low-inertia synchronous generators make the microgrid and the overall network more vulnerable to the transient instability [26-27]. Generally, the different dynamic behavior of inverter-based and low-inertia generations, such as their fast response, is changing the previous paradigms in dynamic studies. Provided facilities in the laboratory, mainly the renewable generation setups, bring the opportunity of conducting experimental studies on these emerging issues.

C. Cybersecurity of networks

Since the 1970s, the structure of the power network control center has been 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 increasing due to the interest of utilities in taking 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 also the wide-area measurement system (WAMS) becomes possible [29].
In 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 from world-wide public networks;
- Lack of personnel’s 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 decrease the cybersecurity of the power system and make it vulnerable to the targeted attacks. These attacks can have different severity, but the most destructive one is launching control actions through the SCADA environment after gaining access to the supervisory control center. In these scenarios, the cyber attackers can lead the system to collapse or hazardous conditions [31-34].

In the SMLUT, all of the required facilities 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 malicious faults and contingencies can be applied but also FDIAAs based on the man-in-the-middle technique to change the power system state estimation is modeled. State estimation software should be robust against FDIA. One of the practical solution to provide this security is defining an index to detect FDIA. This index is the largest normalized residual ($LNR$) and is as the following [33]:

\[
LNR = \left\| Z - HX \right\|
\]

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, at the event of cyber-attack, it can be skyrocket. It is assumed that bad data \(A\) is added to the measured value as an FDIA, then:

\[
Z_{bad} = Z + A
\]

\[
X_{bad} = X + C
\]
\[ X_{bad} = (H^T WH)^{-1} H^T W Z_{bad} \]
\[ = (H^T WH)^{-1} H^T W (Z + A) \]
\[ = X + (H^T WH)^{-1} H^T WA = X + C \]  \hspace{1cm} (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 can be calculated as follows

\[ LNR_{bad} = \left\| Z_{bad} - H X_{bad} \right\| \]
\[ = \left\| Z + A - H (X + (H^T WH)^{-1} H^T WA) \right\| \]
\[ = \left\| Z + A - H X + (AH (H^T WH)^{-1} H^T WA) \right\| \]
\[ = \left\| Z - H X + (A - HC) \right\| \]  \hspace{1cm} (5)

Based on (5), If \( A=HC \) is fulfilled, this attack will be undetectable. Overall, based on the above explanations, there are five possible attacks which are implemented in 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 to all meters.

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

iii) Implement a valid FDIA with incomplete H-Matrix information: It is assumed that the structure of 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), which reflects the topology of power network.

v) Implement a valid FDIA to the control system of power plants: In this case, the attacker changes the control parameters of the power plant and this action results in imposing severe blackout in the power system.

D. 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-based DGs is much higher 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, adaptive protection relaying is a promising solution due to its flexibility in online modifying both relay settings and characteristics using external signals.

In the SMLUT, programmable compact hardware with output switching modules has been developed to implement the protection algorithms easily. Besides, various specially designed equipment is provided in the laboratory to conduct protection and fault analysis studies. For example, 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 in the laboratory brings the opportunity of investigating 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 these systems is the islanding events detection. These events should be rapidly detected to enable an appropriate action [40-41]. 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 the grid voltage phase angle.

In the SMLUT, the required facilities to conduct these researches are provided. Besides, the existed infrastructures in the laboratory are sufficient to perform power system protection studies such as wide-area protection schemes. For
example, faster than real-time approaches to predict the instability condition are of the recent studies ongoing in the laboratory [41].

E. Studies related to the rotating machines and transformers

The rotating machines setups in the laboratory are well equipped in a way that most of the studies related to the rotating machines can be conducted. The rotating machines modeling, design, operation testing, condition monitoring, and control issues are some of the researches which are carried out in the laboratory [42-43]. In addition to the pure rotating machines studies, researches on the effect of presenting motor type inductive loads in the network can be carried out. These types of studies focus on the interaction of electric machines with the power network. For example, the unexpected delay in the recovery of voltage due to removing an external fault which is known as fault induced delayed voltage recovery (FIDVR) phenomenon, can be easily observed and studied using the inductive motors in the laboratory [44-45].

In addition, in the SMLUT, educational transformers are designed in a way 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 students' ability to design and analyzing the transformers in the simulation environments. In addition to the educational tools, there are various facilities to conduct researches 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.

F. Integration of renewable energy resources into the network

Traditional sources of power generation are rapidly replacing with renewable energy ones. It can be predicted that in the near future, a high percentage of the required energy will be supplied by them. Integration of renewable energy resources into the network, bring 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 needed to utilize the renewable energy resources in the network.
Optimal scheduling of renewable microgrids, coping with the stochastic and uncertain amount of renewables power generation, etc. are some of the research areas that can be studied in 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 in the laboratory, and proper solutions for overcoming them can be proposed. Besides, the new grid codes can be comprehensively evaluated in the laboratory in a near reality condition before applying them to the network.

IV. SOME OF EXPERIMENTAL STUDY RESULTS

In the previous sections, the SMLUT facilities and their application areas have been presented. Some experimental studies have been carried out to demonstrate the laboratory applications, but due to the page limitation, only the summary of two of them are provided in this section.

A. Performance of the governor during islanded operation

The performance of the implemented governor is evaluated in this section. Therefore, it is assumed that the microgrid is utilized in the islanded mode, and the synchronous generator (T-G1) loading is about 30% and operated in both voltage and frequency control modes. Other DGs are in service and operate in active power and reactive power constant modes. Suddenly, a resistive load corresponds to 50% of the T-G1 is connected to the microgrid. And approximately after 4 s it is rejected again. Fig. 10 shows the behavior of the implemented governor. Since T-G1 operates as the slack machine, it wants to keep the frequency system at the permissible range. Thus, when the load is connected to the microgrid, T-G1 injects more current to the system, and when the load is disconnected, T-G1 participation would be decreased. It can be concluded that the generator speed is appropriately recovered to the nominal speed for both increment and decrement loads.

B. FDIA to the control system of the power plant

As presented before, the man-in-the-middle attack interface can apply 5 different attacking scenarios. These types of attacks can be categorized into two major groups of static and dynamic attacks. The first 4 of them are static ones
where the changes are reflected in the load flow results. However, in the 5-th scenario, when the attacker changes a control parameter, nothing is reflected in the static parameters of the load flow. So the dispatching operators cannot observe any abnormal condition in the network. This type of attack, which is represented as the dynamic cyber-attack in this paper, is the most destructive scenario. To show 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. Also, the microgrid is operated at 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 to 1.01 and 0.99 pu with a period of 4 s in a step change manner. Fig. 11 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. Fig. 11 (a) demonstrates that the mechanical speed deviates from the nominal speed to follow the speed reference. If this action keeps on for a long time, the machine experiences a severe damage and results in a 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 are of the future works of the laboratory. The designed laboratory is somehow unique for the integration of both electric and communication infrastructures which overcome the shortcomings of not considering data transfer challenges in the studies. The existing laboratories such as the ones introduced in [51-53], only take the advantages of electric equipment such as PV panels, wind turbine generators, etc. However, in the SMLUT, communication infrastructures are also integrated with the electric parts. Since the existing time-synchronization and communication technologies make the remote connection and integration possible, the future plan for laboratory extension contains the study on the possibility of multiple microgrid integration and their challenges.

V. CONCLUSION

This paper presents the smart microgrid laboratory of the University of Tehran (SMLUT). The main focus of the paper is on the microgrid modeling, control, automation, and protection, which was developed and implemented
completely in this university. Different sections of the model were addressed, and some applications of the model are explained. Different software platforms can indeed teach engineering concepts to the students, however, the importance and impact of the practical laboratories should not be ignored. The students need 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 the understanding and skill of students in summary as follows:

- Analyze the structure of the rotating machines and transformers;
- Analyze and understand control concepts of the centralized/decentralized DGs for the operation of microgrid by considering 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;
- Implementation of appropriate protection schemes for microgrids operated 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.
- Discuss, implement, and analyze network-based communication technologies, including SCADA protocols.
- Discuss and evaluate the threats against vulnerable system components and apply information security.

REFERENCES

[1] D. Boud, J. Dunn, and E. Hegarty-Hazel, “Teaching in laboratories” in Society for Research into Higher Education & NFER-Nelson, 1986.

[2] L. Jervis, “Laboratory work in science education: An evaluation with case studies” in Plymouth, UK: University of Plymouth, 1999.

[3] F. Yang, J. He, and D. Wang, “New stability criteria of delayed load frequency control systems via infinite-series-based inequality,” in Industrial Informatics IEEE Transactions on, vol. 14, no. 1, pp. 231-240, 2018.

[4] A. Parizad, S. Mohamadian, M. E. Iranian, and J. M. Guerrero, “Power system real-time emulation: a practical virtual instrumentation to complete electric power system modeling,” in IEEE Transactions on Industrial Informatics, vol. 15, no. 2, pp. 889-900, Feb. 2019.

[5] M. Mahmoudian, M. Bian, and M. Gitizadeh. “High accuracy power sharing in parallel inverters in an islanded microgrid using modified sliding mode control approach,”, in Scientia Iranica. Transactions D: Computer Science & Engineering, Electrical, 2019. doi: 10.24200/sci.2019.51162.203.
[6] A. Akhbari, and M. Rahimi, “Performance and stability analysis of grid connected single phase inverters used in solar photovoltaic systems,” in *Scientia Iranica. Transactions D: Computer Science & Engineering, Electrical*, vol. 26, no. 3, pp. 1637-1651, June 2019.

[7] H.F. Farahani, M. Khalili, A. Rabiee, et al. “On the application of plug-in hybrid electric vehicle to compensate network harmonics: A multiobjective approach,” in *Scientia Iranica. Transactions D: Computer Science and Engineering, Electrical*, vol. 21, no. 6, pp. 2177-2185. Dec. 2014.

[8] R. Asad, and A. Kazemi, “A novel practical fair nodal price for DC microgrids and distribution systems,” in *Scientia Iranica. Transactions D: Computer Science & Engineering, Electrical*, vol. 21, no. 6, pp. 2232-2242, Dec. 2014.

[9] A. Darabi, C. Tindall, and S. Ferguson, “Finite-element time-step coupled generator, load, AVR, and brushless exciter modeling,” in *IEEE Transactions on Energy Conversion*, vol. 19, no. 2, pp. 258-264, June 2004.

[10] C. Luo, J. Yang, and Y. Sun, "Risk assessment of power system considering frequency dynamics and cascading process," in *Energies*, vol. 11, pp. 422, 2018.

[11] W. Yang, P. Norrlund, J. Bladh, J. Yang, and U. Lundin, "Hydraulic damping mechanism of low frequency oscillations in power systems: Quantitative analysis using a nonlinear model of hydropower plants," in *Applied Energy*, vol. 212, pp. 1138, 2018.

[12] M. N. Alam, S. Chakrabarti, and A. Ghosh, “Networked microgrids: state-of-the-art and future perspectives,” in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1238-1250, March 2019.

[13] S. Selvakumar, M. Madhusmita, C. Koodalsamy, S. P. Simon, and Y. R. Sood, “High-speed maximum power point tracking module for PV systems,” in *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1119-1129, Feb. 2019.

[14] H. Bitaraf, and S. Rahman, "Reducing curtailed wind energy through energy storage and demand response," in *IEEE Transactions on Sustainable Energy*, vol. 9, no. 1, pp. 228-236, Jan. 2018.

[15] M. Moness and A. M. Moustafa, “Real-time switched model predictive control for a cyber-physical wind turbine emulator,” in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 3807-3817, June 2020.

[16] M. Moness, M. O. Mahmoud, and A. M. Moustafa, “A real-time heterogeneous emulator of a high-fidelity utility-scale variable-speed variable-pitch wind turbine,” in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 437-447, Feb. 2018.

[17] X. Lu, W. Wang, and J. Ma, “An empirical study of communication infrastructures towards the smart grid: design, implementation, and evaluation,” in *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 170-183, March 2013.

[18] V. C. Gungor et al., “A survey on smart grid potential applications and communication requirements,” in *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 28-42, Feb. 2013.

[19] S. Xunwen, W. Shaoping, Z. Dongmei and Q. Zhu, “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] T. de Almeida Oliveira, and E. P. Godoy, “ZigBee wireless dynamic sensor networks: feasibility analysis and implementation guide,” in *IEEE Sensors Journal*, vol. 16, no. 11, pp. 4614-4621, June, 2016.

[21] Z. Liu, Z. Chen, H. Sun, and Y. Hu, “Multiagent system-based wide-area protection and control scheme against cascading events,” in *IEEE Transactions on Power Delivery*, vol. 30, no. 4, pp. 1651-1662, Aug. 2015.
[22] M. G. Adamiak, et al., “Wide area protection—technology and infrastructures,” in IEEE Transactions on Power Delivery, vol. 21, no. 2, pp. 601-609, April 2006.

[23] V. Salehi, A. Mohamed, A. Mazloomzadeh, and O. A. Mohammed, “Laboratory-based smart power system, Part II: control, monitoring, and protection,” in IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1405-1417, Sept. 2012.

[24] P. Paudyal, P. Munankarmi, Z. Ni, and T. M. Hansen, “A hierarchical control framework with a novel bidding scheme for residential community energy optimization,” in IEEE Transactions on Smart Grid, vol. 11, no. 1, pp. 710-719, Jan. 2020.

[25] S. Ahmadi, V. Vahidinasab, M. S. Ghazizadeh, K. Mehran, D. Giaouris, and P. Taylor, “Co-optimising distribution network adequacy and security by simultaneous utilization of network reconfiguration and distributed energy resources,” in IET Generation, Transmission & Distribution, vol. 13, no. 20, pp. 4747-4755, 2019.

[26] M. Abedini, M. Davarpanah, A. Sepehr, and F. B. Ajaei, “Shunt capacitor bank: Transient issues and analytical solutions,” in International Journal of Electrical Power & Energy Systems, vol. 120, pp. 106-025, Sep. 2020.

[27] Y. A. I. Mohamed, and E. F. El-Saadany, “Adaptive decentralized droop controller to preserve power sharing stability of paralleled inverters in distributed generation microgrids,” in IEEE Transactions on Power Electronics, vol. 23, no. 6, pp. 2806-2816, Nov. 2008.

[28] A. C. Chan, and J. Zhou, “On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628,” in IEEE Communications Magazine, vol. 51, no. 1, pp. 58-65, January 2013.

[29] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, “Protecting smart grid automation systems against cyberattacks,” in IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 782-795, Dec. 2011.

[30] Power systems management and associated information exchange – Data and communications security, IEC 62351:2018, 2018.

[31] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, “Smart grid data integrity attacks,” in IEEE Transactions on Smart Grid, vol. 4, no. 3, pp. 1244-1253, Sept. 2013.

[32] X. Liu, and Z. Li, "Local topology attacks in smart grids,” in IEEE Transactions on Smart Grid, vol. 8, no. 6, pp. 2617-2626, Nov. 2017.

[33] X. Liu, Z. Li, X. Liu, and Z. Li, “Masking transmission line outages via false data injection attacks,” in IEEE Transactions on Information Forensics and Security, vol. 11, no. 7, pp. 1592-1602, July 2016.

[34] L. Che, X. Liu, Z. Shuai, Z. Li and Y. Wen, "Cyber cascades screening considering the impacts of false data injection attacks,” in IEEE Transactions on Power Systems, vol. 33, no. 6, pp. 6545-6556, Nov. 2018.

[35] M. Abedini, M. Sanaye-Pasand, M. Davarpanah, H. Lesani, and M. Shahidehpour “A predictive auto-reclosure approach to enhance Transient stability of grid-connected DGs,” in IET Generation, Transmission & Distribution, vol. 19, no. 9, pp. 943–954, 2019.

[36] M. Abedini, M. Davarpanah, and M. Sanaye-Pasand, “Appropriate grounding system for grid-connected small-scale synchronous generators,” in IEEE Trans. on Industry Applications, doi: 10.1109/TIA.2015.2422814.

[37] S. F. Zarei, and M. Parniani, “A comprehensive digital protection scheme for low-voltage microgrids with inverter-based and conventional distributed generations,” in IEEE Transactions on Power Delivery, vol. 32, no. 1, pp. 441-452, Feb. 2017.

[38] H. M. Sharaf, H. H. Zeineldin, and E. El-Saadany, “Protection coordination for microgrids with grid-connected and islanded capabilities using communication assisted dual setting directional overcurrent relays,” in IEEE Transactions on Smart Grid, vol. 9, no. 1, pp. 143-151, Jan. 2018.
[39] M. Abedini, M. Sanaye-Pasand, and M. Davarpanah, "An analytical approach to detect generator loss of excitation based on internal voltage calculation," in IEEE Transactions on Power Delivery, vol. 32, no. 5, pp. 2329-2338, Oct. 2017.

[40] M. Bakhshi, R. Noroozian, and G. B. Gharehpetian, "Novel islanding detection method for multiple DGs based on forced helmholtz oscillator," in IEEE Transactions on Smart Grid, vol. 9, no. 6, pp. 6448-6460, Nov. 2018.

[41] Y. M. Makwana, and B. R. Bhalja, "Experimental performance of an islanding detection scheme based on modal components," in IEEE Transactions on Smart Grid, vol. 10, no. 1, pp. 3125-3137, Jan. 2019.

[42] G. Betta, C. Liguori, A. Paolillo, and A. Pietrosanto, "A DSP-based FFT-analyzer for the fault diagnosis of rotating machine based on vibration analysis," in IEEE Transactions on Instrumentation and Measurement, vol. 51, no. 6, pp. 1316-1322, Dec. 2002.

[43] P. Ostojic, A. Banerjee, D. C. Patel, W. Basu, and S. Ali, "Advanced motor monitoring and diagnostics," in IEEE Transactions on Industry Applications, vol. 50, no. 5, pp. 3120-3127, Sept.-Oct. 2014.

[44] M. Abedini, M. Sanaye-Pasand, and S. Azizi “An adaptive load shedding scheme to preserve the power system stability following large disturbances,” in IET Generation, Transmission & Distribution, vol. 8, no. 12, pp. 2124–2133, 2019.

[45] W. Wang, M. Diaz-Aguiló, K. B. Mak, F. de León, D. Czarkowski and R. E. Uosef, "Time series power flow framework for the analysis of FIDVR using linear regression," in IEEE Transactions on Power Delivery, vol. 33, no. 6, pp. 2946-2955, Dec. 2018.

[46] M. Abedini, M. Sanaye-Pasand, and M. Davarpanah, “Flux linkage estimation based loss of excitation relay for synchronous generator,” in IET Generation, Transmission & Distribution, vol. 11, pp. 280–288(8), Jan. 2017.

[47] M. Abedini, M. Sanaye-Pasand, M. Davarpanah, and R. Iravani, “A loss-of-field detection relay based on rotor signals estimation,” in IEEE Transactions on Power Delivery, vol. 33, no. 2, pp. 779–788, April 2018.

[48] X. Li, X. Zhang, Z. Linm and Y. Niu, “An improved flux magnitude and angle control with LVRT capability for DFIGs," in IEEE Transactions on Power Systems, vol. 33, no. 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] M. Abedini, M. Davarpanah, M. Sanaye-Pasand, S. M. Hashemi, and R. Iravani, “Generator out-of-step prediction based on faster-than-real-time analysis: concepts and applications,” in IEEE Transactions on Power Systems, vol. 33, no. 4, pp. 4563-4573, July 2018.

[51] C. Patrascu, N. Muntean, O. Cornea, and A. Hedes, "Microgrid laboratory for educational and research purposes," in IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), Florence, 2016, pp. 1-6.

[52] B. Blackstone, C. Hicks, O. Gonzalez, and Y. Baghzouz, "Development of an outdoor diesel generator – PV microgrid for education and research," in IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, 2018, pp. 1-5.

[53] M. Prodanovic, A. Rodríguez-Cabero, M. Jiménez-Carrizosa, and J. Roldán-Pérez, "A rapid prototyping environment for DC and AC microgrids: Smart energy integration Lab (SEIL)," in 2017 IEEE Second International Conference on DC Microgrids (ICDCM), Nuremberg, 2017, pp. 421-427.
Fig. 1. Main hall of the SMLUT
Fig. 2. SMLUT (a) electric mimic diagram including turbine-generator, wind turbine and PV, (b) communication schematic diagram
Fig. 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, g) motor test setup
Fig. 4. Control part of the power plant emulator
Fig. 5. Profile of the injected power of the solar PV
Fig. 6. (a) Conceptual design of the wind turbine emulator, (b) Grid-side power electronics interface
Fig. 7. Dispatching software different features.
Fig. 8. Monitoring and display features of the developed software.
Fig. 9. Developed man-in-the-middle attack interface concept
Fig. 10. 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, (e) terminal current of the generator
Fig. 11. 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, (e) terminal current of the generator.