INVITED PAPER

Cybersecurity in Distributed Power Systems

This paper addresses cybersecurity issues in distributed power systems, in particular, microgrids.

By Zhiyi Li, *Student Member IEEE*, Mohammad Shahidehpour, *Fellow IEEE*, and Farrokh Aminifar, *Senior Member* IEEE

ABSTRACT | This paper presents the application of cybersecurity to the operation and control of distributed electric power systems. In particular, the paper emphasizes the role of cybersecurity in the operation of microgrids and analyzes the dependencies of microgrid control and operation on information and communication technologies for cybersecurity. The paper discusses common cyber vulnerabilities in distributed electric power systems and presents the implications of cyber incidents on physical processes in microgrids. The paper examines the impacts of potential risks attributed to cyberattacks on microgrids and presents the affordable technologies for mitigating such risks. In addition, the paper presents a minimax-regret approach for minimizing the impending risks in managing microgrids. The paper also presents the opportunities provided by software-defined networking technologies to enhance the security of microgrid operations. It is concluded that cybersecurity could play a significant role in managing microgrid operations as microgrids strive for a higher degree of resilience as they supply power services to customers.

KEYWORDS | Cyber–physical systems, cybersecurity, defense-in-depth strategy, microgrid-based distributed electric power systems, risk assessment and mitigation, software-defined networking

I. INTRODUCTION

Reliability and resilience are two indispensable dimensions of contemporary electric power system operations, which highlight the migration of electric energy infrastructure toward the smart grid implementation. The traditional electric power systems designed with conventional reliability requirements are not inherently resilient. Such systems are often designated as being robust for managing "highly probable with low impact" disturbances (e.g., $N-1$ contingencies) but potentially vulnerable to "high impact with low probability" disruptions (e.g., $N-k$ contingencies). Catastrophic power outages in the wake of Hurricane Sandy, which left nearly 7.5 million people without electricity for several days after striking a large portion of the eastern United States in October 2012, represented a clear example of the lack of resilience in contemporary electric power systems. Given a growing number of extreme weather events often attributed to global warming, resilience is increasingly valued in the supply of power services to customers.

The emergence of distributed energy resources (DERs) has given rise to an intense interest in the development and implementation of distributed electric power systems. Such distributed systems can support and gradually replace traditionally centralized electric power systems as the localized power generation and consumption continue to reduce inefficiencies and vulnerabilities embedded in the long-distance power delivery, particularly in troubled regions of the world.

Microgrids are viewed as a powerful platform for building distributed electric power systems that are efficient, secure, sustainable, reliable, and resilient. The deployment of microgrids with enhanced and hierarchical control systems is identified as a clear solution to realizing the significant merits of dispersed and variable DERs [1]. Microgrids can also play a role in mitigating the impact of electric power system disturbances under unexpected but catastrophic events like natural disasters and cyberattacks. When the operation of bulk power systems is disrupted by a natural disaster, microgrids are able to function as self-contained entities while

Manuscript received November 6, 2016; revised January 25, 2017; accepted March 2, 2017. Date of publication May 23, 2017; date of current version June 16, 2017. The funding for this project titled, "MERGE: Microgrids for Economics and Resiliency of the Grid Enterprise," was provided by the NSTIP Strategic Technologies Program in the Kingdom of Saudi Arabia—Project No. 13-ENE2411-03. *(Corresponding author: Mohammad Shahidehpour.)*

Z. Li is with the Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, IL 60616 USA (e-mail: zhiyi.li@hawk.iit.edu).
M. Shahidehpour is with the Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, IL 60616 USA, and also with the Renewable Energy Research Group, King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: ms@iit.edu).
F. Aminifar is with the School of Electrical and Computer Engineering, College of Engineering, University of Tehran, 11365-4563, Iran (e-mail: faminifar@ut.ac.ir).

Digital Object Identifier: 10.1109/JPROC.2017.2687865

0018-9219 © 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

Table 1 Power Outages Related to Cyber Incidents

Event	Cause	Consequence
2003 Northeast Blackout	Alarm system failure due to a software bug	More than 50 million customers lost electricity
2003 Italy Blackout	Cascading failures between power and communication infrastructures	About 56 million people across Italy were affected
2007 Arizona Blackout	Unexpected activation of the load shedding program	About 100,000 customers lost 400 MW load
2008 Florida Blackout	Disabled relay protection during a diagnostic process	About 1 million customers lost 3,650 MW load
2011 Southwest Blackout	Monitoring equipment failure at a substation	Around 2.7 million customers lost electricity
2015 Ukraine Blackout	Remote cyber intrusions after the malware installation	Approximately 225,000 customers lost electricity

guaranteeing the survivability and the continuity of power supplies to local and critically positioned loads. Through the strategic management of onsite resources (both DERs and controllable loads), microgrids can further offer ancillary services (e.g., black start) to restore electric power services in territories that are located outside microgrids. Accordingly, the increased penetration of microgrids at the power distribution level can potentially make a significant contribution to strengthening the resilience of electric power system operations [2]–[5].

Meanwhile, with the extensive use of information and communication technologies (ICTs), electric power systems have evolved as cyber–physical systems in which the functions of cyber and power components are tightly coupled in their operations. ICTs can improve the operational performance of electric power systems, but may also unintentionally expose electric power systems to cyber threats when there is a lack of proper security management. Cyber incidents can even give rise to catastrophic impacts on electric power system operations. In the simulated Erebos Cyber Blackout Scenario [6], a group of hackers successfully manipulated 50 generators remotely after their control systems were infected with a malware known as Erebos Trojan. The generators were forced to be overloaded and finally burned out, which led to the collapse of the regional electric power system in the northeastern part of the United States. This viable scenario has successfully aroused public awareness to the potential physical damages on electric power systems by cyber means.

Table 1 lists the massive electric power outages resulting from cyber incidents [7]–[9] which demonstrate that cyberattacks can potentially trigger a widespread blackout in practical electric power systems. Specifically, attackers switched off breakers remotely in the Ukrainian electric power system with the help of a malware named BlackEnergy Trojan on December 23, 2015, which left more than 30 substations disconnected and approximately 225 000 customers without power for about 6 h. It is believed that cyberattacks can further magnify the implications of physical disruptions when electric power system operations are severely disrupted by extreme events. As the number of cyberattacks aimed at disrupting electric power supplies tends to increase globally, electric power systems have to face a new frontier for managing resilience in their operations.

Although microgrids pose significant potentials in sustaining local power services under emergency operating conditions, they are also subjected to cyber incidents. It is thus of significance to identify cyber vulnerabilities in microgrid operations and deploy effective measures to address cyber threats. Also, it is critical to pay further attention to strengthening the capabilities of microgrids for sustaining power services in the event of cyber incidents and protect local customers when cyber-induced power outages occur. In this context, cybersecure microgrid operations will be particularly eminent to maintain highly reliable and resilient power supplies.

The rest of the paper is organized as follows. Section II introduces the composition and operation of microgrids by incorporating both cyber and physical characteristics. Section III presents the general cybersecurity requirements for microgrid operations, as well as the most common cyber incidents in contemporary microgrids. Section IV discusses the implications of cyber incidents on microgrid operations. Section V provides a risk-based framework for addressing cybersecurity concerns. Section VI develops a defense-in-depth approach to enhance microgrids' cybersecurity based on software-defined networking technologies. Section VII concludes the paper.

II. MICROGRIDS AS CYBER–PHYSICAL SYSTEMS

Microgrid operations are increasingly reliant on ICTs for the full observability and the direct controllability of onsite resources. Accordingly, a dependable cyber system is integral to each microgrid for achieving adequate functionalities in satisfying local customers.

A. Microgrids as Distributed Electric Power Systems

A microgrid is a small-scale power system clustering DERs and loads within a local area. DERs include renewable-energy-based generation units (e.g., photovoltaic systems, wind turbines, biofuel systems), energy storage devices (e.g., battery storage systems, thermal storage systems, flywheels), conventional generators (e.g., cogeneration systems, diesel generators), and plug-in electric vehicles that support vehicle-to-grid (V2G) services. In accordance with the specific characteristics of DERs and loads, the localized electric power system can be implemented and operated as a full alternating current (ac) [10], full direct current (dc) [11], or hybrid ac/dc microgrid [12].

Microgrids can be located at residential, commercial, and industrial customer sites. A microgrid is commonly connected to an existing power distribution system (i.e., main grid) via the point of common coupling (PCC). Additionally, microgrids that are geographically close to each other can

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

be networked to gain additional opportunities of supplying satisfactory power services to their customers [13]–[17]. Through strategically controlling the connection to PCC, a microgrid can be operated in harmony with the main grid, neighboring microgrids, or as a self-contained entity by relying on local DERs to retain power services within its territory. On the one hand, microgrids can facilitate fine-grained strategies to take full advantage of cheap, local, and sustainable renewable energy generation, while managing and controlling its DERs and loads in close coordination. On the other hand, microgrids can actively interact with adjoining power distribution systems by exchanging flexible energy and ancillary services for attaining a global sustainability in electric power system infrastructure.

B. Microgrid Cyber System

Microgrids are increasingly utilizing ICTs in the process of energy generation, delivery, and consumption within their territories. Accordingly, microgrid operations integrate the physical process with the computation, communication, and control functionalities that are realized by a cyber system. The microgrid cyber system is typically composed of a control center, a multitude of sensors and actuators embedded in dispersed field devices, and the associated communication infrastructure. Fig. 1 presents the typical microgrid architecture from the cyber–physical perspective.

The control center normally comprises an application server, a historian, together with a human–machine interface (HMI). The historian is a database that logs the process information of microgrid operations, while the HMI provides an interface for visualizing real-time or historical operating conditions, and configuring operational functionalities. The application server is equipped with the supervisory control and data acquisition (SCADA) system and the energy management system (EMS). The EMS works in concert with the SCADA system. The SCADA system acts as the front–end interface to interact with field devices, whereas the EMS is the back–end processor with decision-making capabilities.

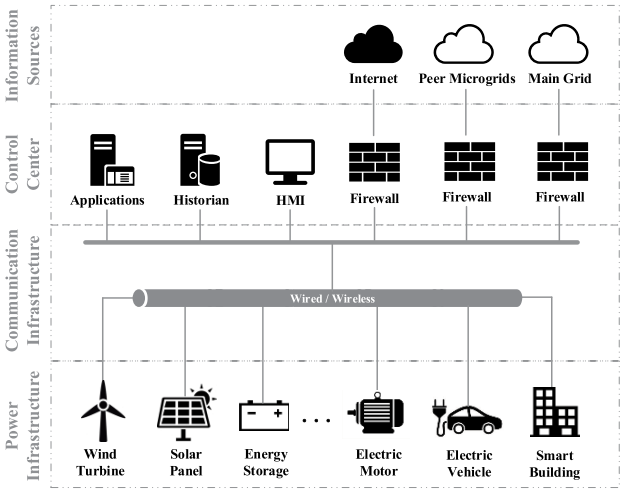

Fig. 1. ***Typical microgrid architecture.***

The SCADA system acquires real-time measurements from and issues supervisory control commands to field devices. Based on real-time measurements gathered by the SCADA system, the EMS runs a collection of functions to maintain security, reliability, economics, resilience, sustainability, and efficiency of microgrid operations. Should there be a mandate to change microgrid operating conditions, the EMS will request modifications to the functions prescribed to field devices through the SCADA system.

Sensors and actuators inside field devices are the interfaces between the cyber system and power components (e.g., DERs, load entities, feeders, transformers, capacitor banks, power converters) involved in physical processes. Sensors are installed for monitoring and metering the physical processes in real time, which facilitate the improved situational awareness for guiding microgrid operations, and the timely detection of malfunctions or failures of power components. Sensors cover various types of measuring instruments such as phasor measurement units (PMUs) and smart meters. PMUs allow the observation and the measurement of electric power system dynamics, while smart meters are installed at customer sites for recording the electricity usage. In contrast, actuators directly affect a physical process by implementing the supervisory control commands issued by the SCADA system. Actuators are extensively involved in microgrid control and protection applications, which can come in the form of protective relays, tap changers, capacitor bank switches, recloser controllers, voltage regulators, etc.

The communication network may be a heterogeneous amalgamation of wired systems such as fiber-optics and cables, and wireless media such as microwave and infrared technologies. In addition to communications with onsite field devices, the control center is commonly connected to external information sources including the Internet and other control centers for gaining more support concerning accurate load forecasts and cooperative operations with external electric power systems in its critical decision-making processes. Firewalls are often deployed to separate internal communications from external networks. Firewalls are configured with stringent rules to only allow permissible data to flow into the microgrid cyber system while blocking potentially harmful data stemmed from unidentified external sources.

C. General Control Loop of Microgrid Operations

A microgrid is theoretically a networked control system, where the control center continuously exchanges information with field devices using dedicated protocols over the communication network. Dispersed sensors continuously take measurements pertaining to the physical processes in order to monitor the microgrid operating state (e.g. voltage, current, frequency) and ambient conditions

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

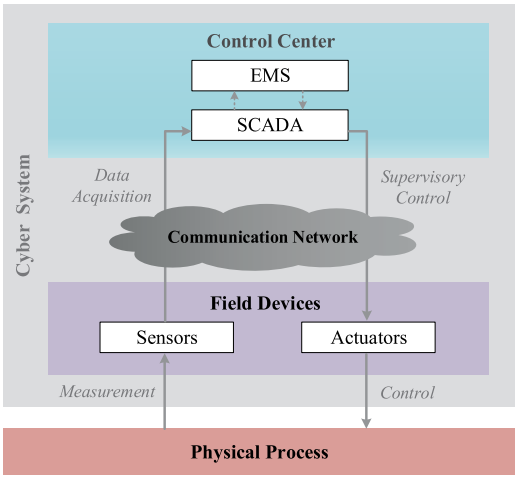

Fig. 2. ***General control loop of microgrid operations.***

(e.g., temperature, humidity). The control center periodically polls sensors via the SCADA system and then processes the real-time measurements using a set of microgrid EMS applications (e.g., state estimation, economic dispatch, demand-side management). By executing these applications, the control center manages to optimize the generation schedules of DERs, maintain frequency and voltage stabilities, and provide high-quality power services to local customers under any operating condition. After making operational decisions, the control center sends out supervisory control signals (e.g., opening/closing line switches, adjusting power output settings of DERs, demand response signals) via the SCADA system to instruct the functions of field devices. These instructions are implemented by actuators in the physical process.

Fig. 2 describes the operational management as a microgrid closed-loop control system, where cyber and physical system processes interact. Notably, intelligent electronic devices (IEDs), programmable logic controllers (PLCs), and other electronic devices with microprocessors can directly monitor and control the physical process in a decentralized manner. For example, IEDs can automatically issue control commands to trip switches when detecting overcurrents, or adjust DERs' power outputs when discerning frequency or voltage abnormalities. These devices that can act as local controllers are supervised and configured by the control center. Such layered control hierarchy enhances the observability and controllability of the physical process, while requiring a much lower bandwidth for communication links between field devices and the control center.

III. CYBER THREATS IN MICROGRIDS

Although the application of advanced ICTs helps improve the operational flexibility and effectiveness, it can also be the Achilles heel of microgrid operations. In fact, microgrids are continuously subject to a variety of cyber threats due to the potentially increasing vulnerabilities in their cyber systems.

A. Cybersecurity Requirements

The microgrid cyber system collects, transmits, processes, displays, and stores the information on microgrid operations through data flows. Data appear in the form of monitoring and metering information, control commands, as well as microgrid configurations (e.g., network layout, communication protocol, device settings). Clearly, efficient and reliable data flows are essential for governing the continuous physical process.

In terms of the data pertaining to the cyber system, cybersecurity of microgrid operations ought to meet three fundamental requirements [18]: availability, integrity, and confidentiality, as stated below.

- Availability refers to guaranteeing that data are accessible and timely. It is vital to ensure a continued access to necessary data for making operational decisions so as to adapt swiftly to dynamic conditions in critical circumstances. Due to the time-sensitive nature of data, any latency or loss of synchronization may hamper the situational awareness and impact the operational performance of microgrids. Table 2 lists the maximum latency allowed for multiple data types [19].
- Integrity refers to assuring that data are trustworthy and accurate. The authenticity and consistency of data should be retained over their entire lifecycle, including collection by sensors, transmission via wired or wireless media, analysis in application servers, HMI visualization, and storage in the historian. Meanwhile, data should always represent the actual information under all operating conditions. In particular, any data alterations by unauthorized parties need to be thwarted, which otherwise tend to incur adverse effects on microgrid functionalities.
- Confidentiality refers to protecting data from being accessed and comprehended by unauthorized parties. Any unexpected disclosure may reveal sensitive information with devastating outcomes on microgrid operations and customer behaviors.

The above cybersecurity requirements are differentiated from those in the traditional information technology (IT) domain. The IT security is encumbered with

Table 2 Time Latency Requirements in Microgrids

Max Latency	Data Type
4ms	Protective relaying
Sub-seconds	PMU-based situational awareness monitoring
Seconds	Supervisory control and data acquisition
Minutes	Microgrid energy management
Hours	Smart meter reading

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

the burden of ensuring anonymity and confidentiality for preserving user privacy, whereas the primary focus of cybersecurity in microgrids is to retain the quality and the continuity of power supplies for keeping the lights on. Accordingly, availability and integrity are usually prioritized over confidentiality in order to maintain timely and reliable data flows for authorized applications that govern microgrid operations.

B. Cyber Vulnerabilities

Cyber vulnerabilities are flaws or weaknesses of a system that is exposed to cyber threats. Cyber vulnerabilities may exist across a microgrid cyber system, ranging from the application software, to the communication network, to field devices. Table 3 summarizes the most common cyber vulnerabilities. As cyber–physical systems, microgrids not only inherit common vulnerabilities from the IT domain, but also have to face unique vulnerabilities specific to their operational characteristics. In practice, communication technologies and networking components retain the same vulnerabilities as those used in the IT domain. However, field devices and software applications have their specific vulnerabilities which depend on the microgrid design and configuration.

Microgrids tend to be susceptible to an increasing number of cyber vulnerabilities that result from the following trends.

- Growing complexity in communication technologies. Wireless communication options (e.g., Zigbee [20], Wi-Fi [21]) are gaining popularity in interconnecting field devices that are scattered in a microgrid [22]. The potential coexistence of wired and wireless communication technologies complicates the enforcement of a robust and uniform policy for cybersecurity. In particular, pervasive access points in a wireless network enlarge potential exposures to cyber threats. If wireless connections lack strict access controls, attackers can gain a direct route to the microgrid cyber system and hypothetically disrupt microgrid operations in real time. Meanwhile, field devices may exchange information with each other and the control center based on diverse communication protocols. In addition to disparate proprietary protocols, microgrids are adopting open standard protocols (e.g., DNP3 [23], IEC 61850 [24]) that facilitate interoperability among various vendor products. The inherent vulnerabilities of these communication protocols collectively result in a larger number of cyber threats against microgrid operations.
- Greater exposure to external networks. The microgrid control center is commonly in contact with grid operators (e.g., distribution system operators) in the main grid for improving the overall performance of power distribution system operations. External links to the Internet offer ancillary information (e.g., weather forecasts, fuel prices) to optimize microgrid-wide energy management. Communications among peer microgrid control centers in support of information sharing are also becoming increasingly frequent, especially when microgrids are interconnected as clusters. These external connections present microgrids with additional vulnerabilities to cyber threats permeating from outside intruders. In other words, attackers can gain extra chances to influence the operation of a microgrid through any compromised network that is connected with the microgrid cyber system. Particularly, Internet connections amplify cyber vulnerabilities since the Internet itself has given birth to a myriad of cyber threats [25].
- Increasingly extensive internal communications. A growing number of field devices are included in a microgrid. DERs are increasingly deployed for realizing the benefits of local renewable energy generation, while smart meters are increasingly installed at customer sites for facilitating demand-side management. These distributed components continually interact with the control center via pervasive communication links, which results in a higher possibility of malicious attacks and unintentional errors. In particular, each component represents an exploitable entry point for infiltrating the microgrid cyber system. Without inherent security designs, these components may be compromised or even counterfeited by attackers. For example, smart meters are tempting targets for attackers to compromise. Additionally, malware inside an infected component may quickly propagate and overwhelm the entire cyber system due primarily to the ubiquitous connectivity, which magnifies the implications of cyber incidents on microgrid operations.

Table 3 Most Common Cyber Vulnerabilities in Microgrids

Domain	Common Vulnerability
Application Software	Poor Code Quality
	Inadequate Configuration Management
	Poor Permissions and Access Management
	Inadequate Patch Management
	Inadequate Data Integrity Checking
	Inadequate Error Handling
	Inadequate Database Protection
Communication Network	Inadequate Segregation and Segmentation
	Inadequate Access Control
	Weak Intrusion Detection and Prevention
	Weak Encryption Mechanism
	Inadequate Sensitive Data Protection
	Inadequate Network Monitoring and Auditing
	Inadequate Anomaly Tracking
Field Devices	Unprotected Physical Access
	Improper Device Configuration
	Inadequate Firmware Protection
	Lack of Tamper-resistance Hardware
	Weak Authentication and Authorization

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

Cyber vulnerabilities are potentially exploited by attackers to gain an unauthorized means to a microgrid cyber system for compromising microgrid operations. A larger number of cyber vulnerabilities indicate a higher possibility for the microgrid to confront cyberattacks, since attackers might only need to make use of most easily exploitable vulnerabilities for achieving their malicious goals. In particular, zero-day vulnerabilities in software or hardware designs, which have not become generally recognized but have been known by attackers, leave few opportunities for microgrid operators to perceive the resulting cyber threats.

C. Cyberattack Vectors

An attack vector is a path that attackers can take to gain access to the targeted cyber system. Given an attack vector, attackers are ready to intrude into the system. Attackers may gain unauthorized access by directly compromising an unsecured or poorly secured cyber component. For example, networking devices are often configured with default or even hardcoded passwords. Even as protected with intricate passwords, these components are at the risk of a brute-force attack. Additionally, wireless communication technologies provide attackers with pervasive avenues to crack communication networks. For example, an attacker within an unsecured wireless network can masquerade as a legitimate device by spoofing the media access control address.

Besides the aforementioned local means, attackers may even intrude into cyber systems from remote sites via backdoors opened by Trojan horses [26]. A Trojan horse is a malicious program that can be embedded inside either software applications or hardware devices to provide attackers with a very effective means of bypassing security perimeters. For example, Trojan horses enable attackers to gain a sustained access to an infected system simply by retrieving login credentials, especially those with administrative privileges. BlackEnergy, Havex, and Sandworm are recent examples of Trojan horses targeting monitoring and control systems.

Generally, Trojan horses can infect a microgrid cyber system by the following means.

- Phishing attacks. Phishing attacks, especially Spear Phishing attacks [27], are performed through fraudulent e-mails that are tailored to look authentic. Microgrid operators could inadvertently open contaminated e-mail attachments that will allow Trojan horses to be installed and executed automatically.
- Infected external hardware. Removable media such as flash drives used for file transfers as well as shared laptops used for repairs and maintenance can easily reproduce and distribute the contained Trojan horses as soon as they are connected to the microgrid cyber system.
- Infected external networks. Once an external network is contaminated with Trojan horse, the connected microgrid cyber system may be the next victim. Notably, the Internet is an unintended carrier of Trojan horses. When a microgrid operator accidently opens an Internet website contaminated with a malicious software, the microgrid cyber system could also be afflicted with Trojan horses.
- Compromised supply chain. Apart from Trojan horses existing in the software applications, a serious concern is that hardware-based Trojan horses would be deliberately embedded in field devices that are manufactured by untrusted entities [28]. Since microgrid components are commonly procured from various vendors, attackers are likely to insert Trojan horses during the hardware/software development and manufacturing process.

The attack vectors listed above can be employed together for launching particular attacks. Upon successful intrusion, attackers can further explore the microgrid cyber system and exploit the vulnerabilities to execute subsequent attacks.

D. Cyber Incidents

A cyber incident is a realization of cyber threats that actually or potentially jeopardize the data flows for microgrid operations. Cyber incidents usually result from deliberate attacks, inadvertent human errors, defective equipment or software, and natural disasters. Noticeably, deliberate attacks may be launched by outsiders (e.g., hackers, terrorists) and/or insiders (e.g., operators, legitimate users) with various motivations (e.g., financial gain, political action, revenge, entertainment). With intimate knowledge and authorized access, insiders can easily circumvent security measures and perform insidious actions to cause considerable consequences, which is particularly difficult to prevent. In addition, cyberattacks can be launched by physical (e.g., locally sabotage cyber components) and/or logical (e.g., remotely manipulate data flows) means. Malware (e.g., worms, spyware, viruses) installed on either hardware devices or in software applications can also assist attackers in achieving the attack goal (e.g., affecting performance or availability of devices or services, sniffing sensitive information).

In general, the most likely forms of cyber incidents are classified into: communication inefficiency, information distortion, secrecy leakage, device malfunction, and software misconfiguration, as discussed below.

- Communication inefficiency usually results from denial of service (DoS) attacks. DoS attacks could culminate in the unavailability or overload of any component in the communication network (e.g., servers, routers, communication links), which prevents or impairs normal authorized functions and thus lead to interruptions or significant delays in legitimate services (e.g., transmitting monitoring data, issuing control commands). Attackers can perpetrate DoS attacks with the aid of worms which are

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

malicious programs designed for spreading rapidly and automatically in the microgrid cyber system so that DoS attacks could be launched in a distributed manner to disable microgrid functionalities (e.g., by sending a flood of fake requests) through manipulating dispersed compromised sources (e.g., smart meters, PMUs, IEDs) [29]. Wireless networks are especially vulnerable to DoS attacks [30], where attackers have additional means of launching DoS attacks including emitting radio frequency signals to jam legitimate traffics and counterfeiting a networking device to mislead the traffics.

- Information distortion refers to the violation of in-transit data integrity, which usually occurs after attackers assume a direct control over data flows in a communication network. Without necessarily knowing the content, attackers can simply reroute the data flow to a different destination or retransmit a previously-captured data flow (i.e., replay attacks [31]) on relevant communication links. Attackers can also corrupt data flows in such a manner that critical information (e.g., real-time monitoring data, supervisory control signals) in transition may be intercepted and modified to spurious values that are in accordance with the attack goals. Additionally, attackers can forge data flows to falsify nonexisting communications.
- Secrecy leakage may be caused by insiders who intentionally or inadvertently provide the critical information to potential attackers. More frequently, attackers acquire sensitive information by eavesdropping data flows through communication links. Attackers can perform network reconnaissance and covert traffic analysis through sniffing and collecting network traffics. For example, attackers can utilize traffic analysis tools to identify valuable information, extract privileged credentials, and even reverse-engineer communication protocols. Attackers possessing more sophisticated tools (e.g., spyware) can continuously eavesdrop for an extended period of time and retrieve the sensitive information without detection.
- Device malfunction often occurs once the device is reconfigured and manipulated in an unauthorized manner. If a device is compromised, attackers can leverage control over the device and hinder the normal functions of the associated sensors and/or actuators (e.g., altering the data that will be reported to the control center, denying the implementation of supervisory control commands).
- Application misconfiguration assists attackers in gaining unauthorized access, escalating illegitimate privileges and taking control of the cyber system. In addition to operators' unintended errors, software applications are potentially corrupted and modified by viruses hidden in the servers' operating systems.

Table 4 Violation of Cybersecurity Caused by Cyber Incidents

Cyber Incident	Availability	Integrity	Confidentiality
Communication Inefficiency	×		
Information Distortion		×	
Secrecy Leakage			×
Device Malfunction	×	×	×
Application Misconfiguration	×	×	×

Cyber incidents may exist over the entire data lifecycle and their impacts on each dimension of cybersecurity is shown in Table 4. Additionally, multiple cyber incidents may happen concurrently or sequentially in cases of sophisticated cyberattacks.

IV. IMPACT OF CYBER INCIDENTS ON MICROGRID OPERATIONS

Considering the complex cyber–physical interdependencies, cyber incidents cannot be viewed solely as IT activities. Any violation of availability, integrity, or confidentiality has the potential to impact the physical process. Sophisticated cyberattacks can even drive the operation of microgrids to collapse, resulting in substantial equipment damage and prolonged power outages.

A. Classification of Microgrid Operating Conditions

The complex interactions of the physical process and the cyber system introduce new security concerns in microgrid operations. In fact, threats either in the physical process or in the cyber system may have adverse effects on power supplies in a microgrid. In addition to the well-studied physical security [51]–[53], cybersecurity is also essential for a microgrid to fulfill its primary mission, that is, to sustain desired power supplies to local customers. Hence, it is necessary to expand the perception of the security of microgrid operations to include both physical security and cybersecurity.

Physical security pertains to the reliability of the physical process. Microgrid operations are physically secure only when power-related operating states (e.g., frequency, voltages, currents) are all within stability limits. Meanwhile, cybersecurity indicates the operational reliability of the cyber system. Microgrid operations are cybersecure only when the operational performance of the cyber system meets the requirements of availability, integrity and confidentiality for all the data. Lack of physical security in electric power systems results from physical disruptions, whereas cyber incidents give rise to cyber insecurity.

As depicted in Fig. 3, the possible operating conditions of a microgrid with pervasive cyber–physical interactions can be classified into the four following states.

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

Fig. 3. ***Characterization of microgrid operating conditions.***

- Secure state. Both cybersecurity and physical system security are maintained. Microgrids are required to be operated in this state in normal circumstances.
- Alert state. Physical security is maintained but cybersecurity is violated. For example, microgrids will be operated in this state when supervisory control commands are blocked and field devices manage to stabilize the physical process by using their default settings.
- Emergency state. Cybersecurity is maintained but physical security is violated. For example, microgrids will be operated in this state when line flows exceed their thermal limits for an extended period under certain weather conditions.
- Extreme state. Cybersecurity and physical security are violated simultaneously. For example, microgrids will be operated in this state when a natural disaster destroys both the physical equipment and the communication network simultaneously.

With the occurrence of subsequent physical disruptions or cyber incidents, microgrid operations continue to suffer the degradation of the security state. Conceptually, there are four types of reactive actions for transferring the operating state from one to another in order to restore the security of microgrid operations, as listed below.

- Preventive control. It recovers the secure state from the alert state to by restoring the cybersecurity and maintaining the physical security in microgrid.
- Corrective control. It recovers the secure state from the emergency state by restoring the physical security and maintaining the cybersecurity.
- Remedial control. It recovers the emergency state from the extreme state by eliminating cyber insecurity and preventing the further degradation of physical security.
- Restorative control. It recovers the alert state from the extreme state by eliminating any issues with physical security and preventing the further degradation of cyber insecurity.

The continuity and the quality of power supplies principally hinge on the physical process, which means microgrid operations should guarantee physical security all the time. However, cybersecurity is critical for a microgrid to maintain physical security. Basically, cyber insecurity can result in physical disruptions that transcend the cyber realm, either directly [54] or indirectly [55], and eventually endanger physical security. Particularly, cyber incidents may hinder the observability or the controllability of the physical process. A clear example is that attackers can disconnect a generator by remotely altering the associated relay status so as to force microgrid operations outside the stability limits. Cyber incidents may also cause hidden failures of power components under specific conditions. For example, a sensor failure may not alter the physical process but hinder the observation of a physical disruption, thereby deteriorating the operating condition. In addition, compromised settings of protective devices may be overlooked until the occurrence of a local fault aggravates physical disruptions.

Meanwhile, physical security is also a critical prerequisite for cybersecurity due to the fact that functional cyber systems rely on uninterrupted high-quality supplies of power. Any lack of physical security which results in disruptions or degradations of power supplies may lead to the breakdown of cyber components, and thus will have an opportunity to impact cybersecurity. Accordingly, ties between physical disruptions and cyber incidents may result in cascading failures of cyber and physical infrastructures, which can pose serious challenges on the performance of microgrid operations.

Microgrids are thus required to withstand any cyber and physical disturbances while sustaining satisfactory services to local customers. Although microgrids are commonly designed to survive physical disruptions, they should also be in a position to mitigate physical implications of cyber incidents.

B. Physical Implications of Cyber Incidents

Due to tight couplings of the cyber system and the physical process in a microgrid, it is impractical to comprehend the impact of cyber incidents solely based on IT theories. Notably, cyber incidents, either deliberate or inadvertent, have the potential to inflict physical implications on microgrid operations. Each microgrid is heavily dependent on efficient and reliable data flows to maintain the observability and controllability of the physical process, whereas delayed

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

or corrupted data flows may hamper the smooth functioning of field devices. In particular, attackers can remotely intrude into a microgrid cyber system, elevate their privileges, and perform unauthorized actions to block or manipulate data flows so as to make microgrid operations unobservable or uncontrollable, thereby jeopardizing the stability, safety, or efficiency of power supplies to local customers.

The time-critical operational characteristics render microgrids especially susceptive to DoS-type attacks. The delivery of both monitoring measurements and control commands should meet strict requirements of timeliness, especially under emergency conditions due to extreme events. On the one hand, any delay or loss of measurements could hamper the microgrid-wide situational awareness, which means the control center can hardly have a complete and correct understanding of the present operating condition. Accordingly, it is rather difficult for the control center to make timely and effective operational decisions that are adaptive to highly dynamic conditions. For example, the control center would become blind to any malfunction or failure of power components whose associated sensors were destroyed by severe weather, and cannot take prompt actions to repair or restore these components, potentially resulting in more damaging physical consequences. On the other hand, DoS attacks could block or defer the issued control signals to take effect in the physical process. In consequence, the physical process cannot be directly controlled and thus the containment of operating condition's deterioration is unavoidable to fail. For example, time latency could nullify an IED's directional overcurrent protection function, and impede the mitigation of local faults, leading to the propagation of power outages.

Meanwhile, attackers may poison the data critical to making operational decisions. Attackers with direct access to the database or field devices can even modify the microgrid configuration (e.g., line ratings, DERs' characteristics, protective settings [32]–[34]) for inflicting physical consequences on microgrid operations. Besides, attackers are likely to manipulate the real-time measurements so as to tempt the control center to make the inappropriate decisions or force the field devices to autonomously trigger unnecessary control actions. Even without specific power engineering knowledge, attackers can attempt to destabilize a microgrid merely by a replay attack. The Stuxnet incident [35] is a clear example of replay attacks that could result in severe physical consequences. In this incident, attackers successfully induced excessive vibrations or distortions to destroy the fast-spinning centrifuges by retransmitting to the controller the recorded measurements in past operating conditions. Sophisticated attackers may also launch data integrity attacks like false data injection (as will be detailed in Section IV-C) to influence the accuracy and validity of state estimation results, which potentially leads to misguided microgrid operations causing degradation and even interruption of power services.

Additionally, attackers may compromise the in-transit control commands or fabricate unauthorized commands in order to remotely manipulate the equipment critical in the physical process. Such violations of data integrity can directly alter the operating condition of a microgrid. Notably, microgrids are subject to aurora vulnerability [36], [37], whereby attackers could stealthily manipulate the PCC switch to drive a microgrid out of synchronization with the main grid. In order to achieve this malicious goal, attackers continually send malicious control signals to open and close the PCC switch in a rapid fashion. When the PCC switch is (re)closed, the microgrid is forced to be connected and synchronized with the main grid. When the PCC switch is (re)opened, the microgrid suffers a loss of synchronization. Eventually, the continuous changes of the switch status would result in a significant difference in phase angle, frequency, or voltage magnitude between two sides of the PCC at the moment of resynchronization. The resulting strong power flow immediately would pose a critical physical stress on the PCC switch as well as other equipment inside the microgrid, causing catastrophic device destructions and power outages. Fig. 4 illustrates the impacts of cyberattacks on microgrid operations.

Cyber incidents compromising availability or integrity tend to incur adverse effects on microgrid operations. These incidents may not only impact the efficiency and the economics of microgrid operations, but also threaten the continuity and the quality of power supplies. Although any violations of confidentiality might not pose direct physical consequences, they would help attackers prepare for subsequent attacks causing violations of availability or integrity. For example, eavesdropping network traffics will not directly result in any physical consequences, but might lead to the disclosure of present operating states

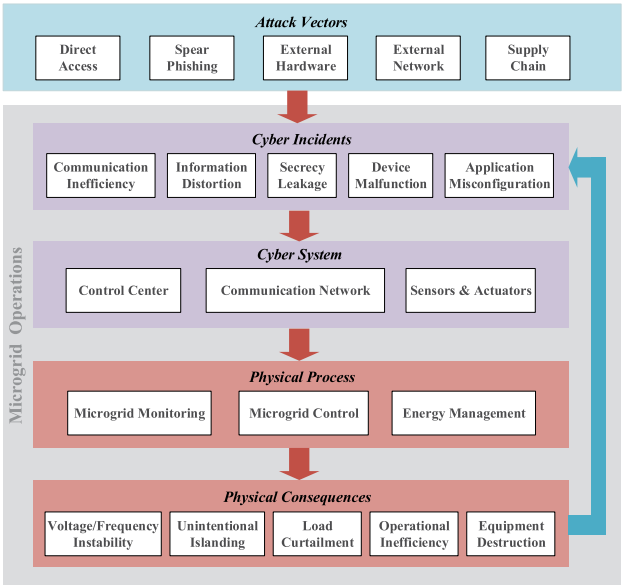

Fig. 4. ***Impacts of cyberattacks on microgrid operations.***

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

(e.g., voltage, frequency, power flow) and control strategies (e.g., setpoints of DER power generation) that are fundamental for perpetrating potential attacks to destabilize the microgrid. Furthermore, physical disruptions resulting from cyber incidents may in turn cause subsequent failures or malfunctions in the cyber system (e.g., failing to supply power to networking devices), thereby leading to cascading failures between cyber and physical domains of microgrid operations.

C. Potential Cyberattacks on Microgrid Operations

This section takes the example of false data injection to illustrate the way cyberattacks potentially affect microgrid operations. False data injection, as a type of cyberattacks against data integrity, is a rapidly growing concern in electric power system operations [38]–[40]. With a sufficient knowledge of the electric power system configuration, attackers can introduce arbitrary errors in state estimation results by conducting false data injection [41]. Since the false data are seemingly valid according to physical laws, conventional techniques for bad data detection can hardly distinguish the false data from normal measurements. Accordingly, state estimation results are stealthily perturbed as if the system is actually operating under the operating condition represented by the false data.

False data injection can be easily realized by a man-in-the-middle attack [42] that intercepts and modifies the data in transit. Given the widespread deployment of meters and sensors in a microgrid, attackers can easily get access to compromise the measurements in order to manipulate the state estimation results. In particular, attacks can physically compromise a field device due to the lack of tamper-resistant hardware. Since microgrid applications (e.g., frequency/voltage regulation, fault diagnosis, contingency analysis) rely heavily on state estimation results, microgrid operations are particularly vulnerable to collected measurements that are false but hardly detectable.

In the following, we analyze two types of false data injection, namely, load redistribution attack (LRA) and topology preserving attack (TPA), which might potentially disturb microgrid operations even when attackers possess a limited knowledge of microgrid configurations [47]–[49].

The LRA could make loads seemingly redistributed in a microgrid [43], [44]. In principle, it keeps the total amount of loads unchanged while altering load measurements at some buses. Additionally, all relevant power flow measurements are modified in order to accommodate changes in load measurements so that the adjusted power flow distribution seems consistent with the redistributed loads. Accordingly, these compromised measurements collectively misguide the state estimation results while bypassing the conventional bad data detection. The LRA can be launched to lower the operational efficiency of microgrids and cause economic losses. For example, attackers can make up false loading conditions to induce the microgrid control center to make uneconomical dispatch decisions. Attackers can also employ the LRA to cover up severe loading conditions that can directly impact the security and stability of microgrid operations.

Fig. 5 presents an example of the LRA on a five-bus microgrid where the lines are assumed to have the same impedances. Fig. 5(a) shows the original operating condition where the cogeneration system at bus 3 and the photovoltaic system at bus 5 supply 6 and 2 MW to three building loads at buses 1 (3 MW), 2 (3 MW), and 4 (2 MW), respectively. Fig. 5(b) shows the false operating condition caused by LRA where false measurements are presented in italic. The load measurements at buses 1, 2, and 4 are altered to 3.5, 2.75, and 1.75 MW, respectively, while the total amount of building loads is kept at 8 MW. The line flow measurements are also adjusted to match the redistribution of building loads. Accordingly, the state estimation results will be corrupted to represent the false operating conditions. Note that only a subset of the measurements (i.e., three out of five load measurements and two out of five line flow measurements) need to be modified, which alleviates the burden of attackers to realize the LRA to affect microgrid operations.

The TPA could be launched for masking the topology change of a microgrid due to line outages that are caused

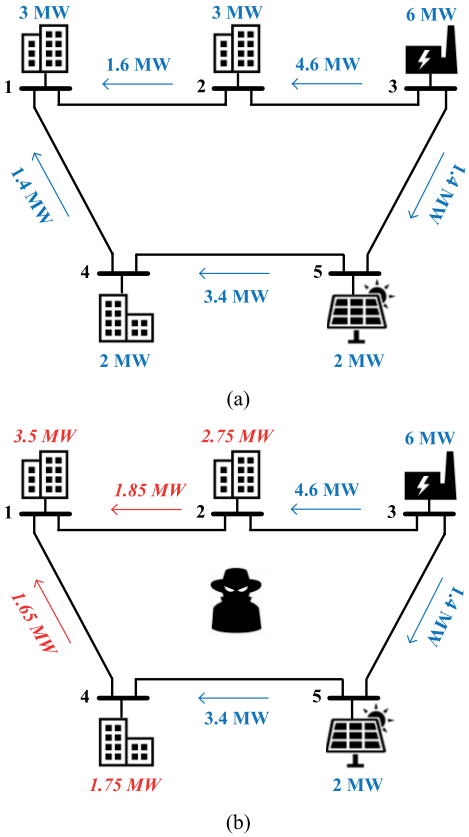

Fig. 5. ***Load redistribution attack. (a) Original operating condition; (b) False operating condition.***

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

by either physical disruptions or cyber incidents [45], [46]. The TPA forges power flow measurements of the disrupted lines and modifies load measurements at certain buses (if necessary) in order to preserve the state estimation results after line outages. If the false measurements are carefully fabricated, the lines on outage would seem to remain in service as represented by the state estimation results. Accordingly, the TPA impedes the detection of line outages, thereby deteriorating the operating conditions and causing an extended service disruption.

Fig. 6 illustrates the TPA on the five-bus microgrid that is originally operated under the same condition as that in Fig. 5(a). Fig. 6(a) depicts the actual operating condition after line 1-2 is intentionally disconnected by an undetected cyberattack (e.g., stealthily manipulating the line switch). Straightforwardly, the line outage could be masked by the TPA that simply alters all the line measurements back to the values prior to the outage, as depicted in Fig. 6(b). The resulting state estimation results will not reveal the change in microgrid topology, and thus the line outage will not be detected until significant transients in the physical process are observed. Besides, the LRA can be coordinated with the TPA to mask line outages in a sophisticated manner [46], [50].

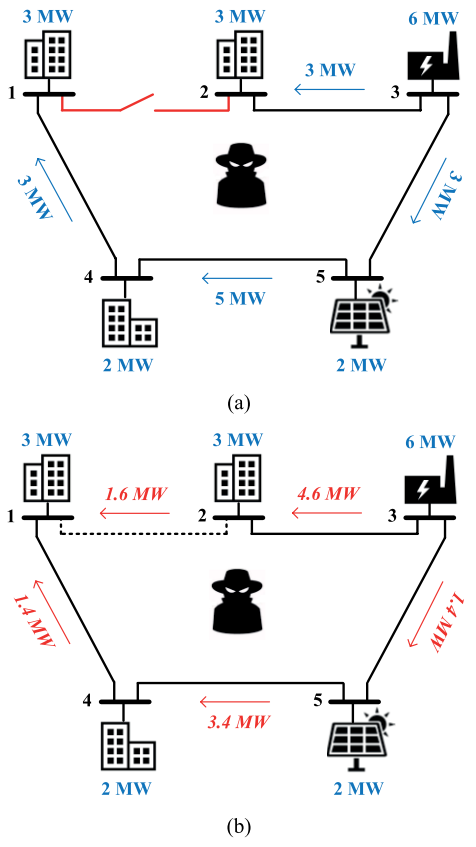

Fig. 6. ***Topology preserving attack. (a) Switch status alteration; (b) False data injection.***

V. CYBER RISK MANAGEMENT IN MICROGRIDS

It is essential to address cybersecurity concerns in microgrids without posing any adverse effects on local power services. Cyber risk assessment presents human operators with a profound understanding of the role of cybersecurity, and supports their objectives in prioritizing and deploying defensive measures for mitigating the cyber threats against microgrid operations.

A. Cyber Risk Assessment

In light of the growing frequency of cyber incidents, microgrid operators should be on alert to gain a clear consciousness of cybersecurity concerns in microgrid operations and then determine effective countermeasures. Cyber risk assessment, which manages to translate cybersecurity in a quantifiable term, is a systematic and repeatable approach to the evaluation of potential consequences of exploiting cyber vulnerabilities [56]–[58]. The assessment results not only facilitate the perception of the cybersecurity posture of a microgrid, but also pave the way for mitigating the risk of potential incidents in the microgrid cyber system. Accordingly, the cyber risk in microgrid operations should be continually assessed for meeting the challenges posed by a variety of ever-evolving cyber threats.

In order to assess the cyber risk in microgrid operations, cyber contingencies [59], [60], which are defined as the most likely cyber incidents, should be identified. Since it is impractical to enumerate all possible cyber incidents, the selection of cyber contingencies is accomplished through vulnerability analyses like attack tree analyses. As an integral part of the EMS, the existing contingency analyses are performed to deal with potential physical disruptions in a microgrid. However, both physical security and cybersecurity play a role in microgrid operations. Hence, contingency analyses need to be expanded to incorporate cyber contingencies emanating from the exploitation of vulnerabilities in the microgrid cyber system.

Given a set of postulated cyber contingencies under a certain operating condition, the cyber risk can be assessed as

$$Risk = \sum_{\text{Contingencies}} Likelihood \times Severity \ \forall \ Conditions$$

Clearly, the likelihood of each cyber contingency and the severity of the resulting implications on microgrid operations are two key factors in cyber risk assessment. The former relies on both vulnerabilities of the cyber system and capabilities of attackers, which is calculated after probability-based attack tree analyses (see Section V-B), whereas the latter is evaluated for each contingency by performing the cyber–physical cosimulation (see Section V-C).

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

B. Attack Tree Analysis

An attack tree is a hierarchical logical diagram for visualizing the paths for realizing cyber incidents in a system, which reflects the cyber system's inherent capabilities against malicious cyberattacks [61]. In an attack tree, the attack goal is the root node at the top and the subgoals attackers may have to achieve during the process of realizing the ultimate goal are represented as the subordinate nodes. The sequential connection of subgoals showing how attackers prepare and execute the attack forms an attack path. Along the attack paths, attackers climb up the attack tree step by step starting from the realization of initial subgoals located at the bottom (i.e., leaf nodes). The subgoals that are achievable within the same step are arranged at a single level of the attack tree. There are two types of logical connections among the subgoals including "AND" and "OR". Here, "AND" means union and "OR" indicates alternatives. More specifically, lower level subgoals leading to "AND" need to be achieved in order to perform the subsequent action at the upper level, whereas any realization of the subgoals leading to "OR" is sufficient to launch the subsequent action. Additionally, each attack goal possesses a separate tree, despite the fact that subtrees and nodes may be shared among multiple attack trees.

Generally, the procedures of launching a successful cyberattack involves three stages: penetration, preparation, and execution. First, attackers penetrate into a microgrid cyber system either directly or via backdoors provided by Trojan horses. Subsequently, they explore the cyber system to escalate unauthorized privileges and engage in studying the principles of microgrid communication and control. When adequately prepared, attackers perform malicious actions to impact the physical process. Attack trees therefore provide an effective means to model the sequences among attackers' potential actions against microgrid operations.

Fig. 7 shows a simplified attack tree against the availability of a sensor's measurement to the control center. Notably, either device malfunction or communication interruption may make the measurement unavailable. In order to make the field device dysfunctional, attackers can either install malware inside the device or physically compromise the device. In order to cause communication interruption, attackers can choose to launch a DoS attack by cyber means or conduct a physical damage on the communication links. However, a successful execution of the DoS attack is dependent on two prerequisites, including sufficient resources for attackers (i.e., infected field devices), and attackers' knowledge of the targets (i.e., communication links that are to be blocked). In sum, there are four separate paths in total to achieving the attack goal.

Accordingly, attack tree analysis provides a formal methodology for analyzing and addressing the vulnerabilities of a microgrid cyber system. In fact, each attack path indicates how attackers can achieve their ultimate goal at each step

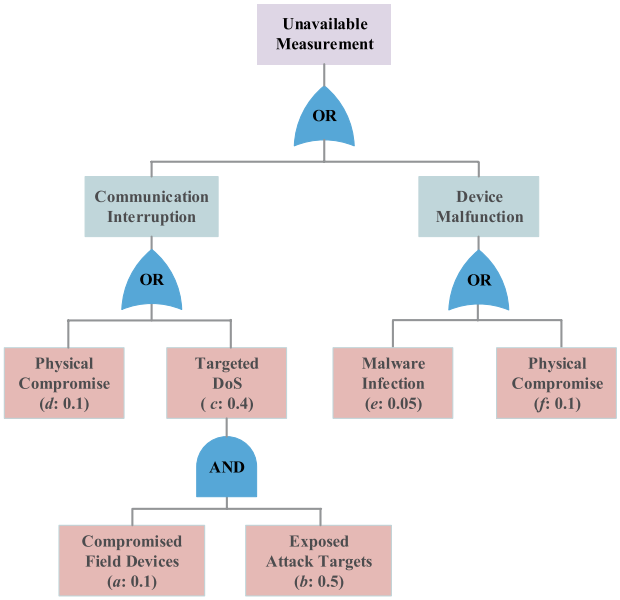

Fig. 7. ***Simplified attack tree diagram.***

through sequential exploitations of cyber vulnerabilities. However, an attack path is feasible only when attackers can successfully exploit the discovered vulnerabilities to fulfill their subgoals at each step along the path. An attack path is therefore seen as infeasible either when there is no cyber vulnerability exposed to attackers at any step, or when attackers are incapable of exploiting the vulnerabilities at any step. Attack tree analysis raises the awareness of vulnerabilities and their interdependencies by deductively delineating cyberattacks, which helps identify potential cyberattacks according to the perceived vulnerabilities. Accordingly, attack tree analysis guides the deployment of security measures for eliminating vulnerabilities that may incur damaging cyberattacks on microgrid operations. If all possible attack paths are thwarted, microgrid operations are adequately protected against a variety of cyberattacks.

Attack trees can also be modeled in a probabilistic manner [62], which provides a higher comprehensibility for implications of cyber vulnerabilities and the likelihood of potential cyberattacks. Probabilistic values can be assigned to subordinate nodes where attackers exploit the discovered vulnerabilities for achieving subgoals. In principle, these values indicating the probabilities of successful exploitations depend on the accessibility (either physical or logical) and exploitability of cyber vulnerabilities, as well as on attackers' capabilities and budgets (either concrete like financial cost or abstract like time). Hence, the reachability of the attack goal can be quantified after a necessary probabilistic reasoning. For the example depicted in Fig. 7, corresponding probabilities of successful exploitations are assigned to six subordinate nodes related to the exposure of vulnerabilities a–cf. Note that the exploitation

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

of vulnerability c is conditioned on joint exploitations of vulnerabilities a and b; so the probability that attackers can achieve the subgoal is determined by

$$\Pr(\text{Targeted DoS}) = \Pr(\text{Exploit } c|\text{Exploit } a \,\&\, b) \cdot \Pr(\text{Exploit } a \,\&\, b) = 0.4 \cdot (0.1 \cdot 0.5) = 0.02.$$

Additionally, the probability of device malfunction is the sum of the probabilities of successfully exploiting vulnerabilities e and f, which means

$$\Pr(\text{Device Malfunction}) = \Pr(\text{Exploit } e) + \Pr(\text{Exploit } f) = 0.05 + 0.1 = 0.15.$$

Similarly, the probability of communication interruption is

$$\Pr(\text{Communication Interruption}) = 0.1 + 0.02 = 0.12.$$

Finally, the ultimate attack goal can be obtained with the probability of 0.27. The calculation of the reachability of attack goals is advantageous for refining cyber contingencies. Cyber contingencies can be ranked and selected according to the values of reachability when higher values indicate higher priorities.

C. Cyber–Physical Cosimulation

Once a postulated cyber contingency (e.g., bandwidth loss, data distortion, malware infection) occurs, the resulting cyber insecurity will inevitably hamper microgrid monitoring and control functions, potentially causing severe implications on the physical process. Hence, it is critical to quantify the extent and the degree of potential physical effects of cyber contingencies for refining the role of cybersecurity. Additionally, dynamics of microgrid operations rather than the static states should be taken into consideration so that the reactive measures to cyber incidents can be fully modeled. Hence, the comprehensive evaluation of cyber contingencies from the cyber–physical perspective needs to combine dynamics in the physical process and data-flow-related functions in the cyber system.

However, it is theoretically difficult to consider the physical process and the cyber system in a microgrid as an integrated model, primarily due to the operational heterogeneity between physical and cyber components. In principle, the physical process is continuously governed by certain principles such as Kirchhoff's laws, whereas the cyber system is intrinsically driven by discrete events with much fewer limitations. Table 5 compares the modeling of the physical process and the cyber system.

As an alternative to the complicated analytical models, we can resort to high-fidelity simulation tools. In terms of microgrid operations, the physical process at the power distribution level can be simulated using commercially available software packages such as PSCAD/EMTDC [68], PowerWorld [69], and DIgSILENT PowerFactory [70], whereas data flows in the communication network can be simulated using ns-2/ns-3 [71], Riverbed SteelCentral (OPNET) [72] and OMNeT++ [73]. Furthermore, microgrid applications such as SCADA and EMS can be either configured in existing simulators or coded in external platforms such as Python [74] and Matlab [75].

Table 5 Modeling Details of Microgrid Operations

Property	Microgrid Modelling	
	Physical Process	Cyber System
State Variable	Voltage, Current, Frequency, Harmonics	Latency, Error Rate, Jitter, Throughput, Packet Loss
Driving Mode	Continuous-time	Discrete-event
Physical Principle	Kirchhoff's Laws	None
Static Model	Power Flow Equations	Data Flow Equations
Dynamic Model	Differential-algebraic Equations	Finite-state Machine, Queuing Theories

Since one-sided simulators are sufficient for explicitly representing cyber–physical interactions, a cosimulation approach should be considered to exploit the existing capabilities of cyber and physical simulators. This approach will retain the simulation processes embedded in individual simulators and coordinate them under a common framework, while bridging the gap between time-continuous and event-driven simulation by realizing strict time synchronization and efficient data exchanges [63]–[65]. The cosimulation approach facilitates the investigation of potential effects of one system's malfunction on the other system's dynamics, and streamlines the understanding of cascading failures between the two systems. The cosimulation approach can also be extended to include physical devices as hardware-in-the-loop simulation [66], [67] for enhancing the simulation quality and flexibility.

Fig. 8 shows the common framework for quantifying the physical implications resulting from cyber contingencies. Given the selected cyber contingencies, the cyber–physical cosimulation is conducted for identifying and recording the dynamics of the physical process in a microgrid. Obviously, cyber contingencies cause various consequences on microgrid operations, while incurring specific reactive actions. Hence, quantitative indices should be defined to measure the severity of cyber contingencies and to reflect the microgrid's ability to cope with these contingencies so that the resulting physical consequences can be evaluated from specific practical angles. For instance, the measure can identify local load interruption levels in contingency cases and how fast the steady-state physical process can be recovered.

D. Minimax-Regret Cyber Risk Mitigation

Mitigating the cyber risk in microgrid operations is critical for maintaining reliable and resilient supplies of power to local customers. Although the cyber risk cannot be eliminated completely, it can be strategically marginalized.

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

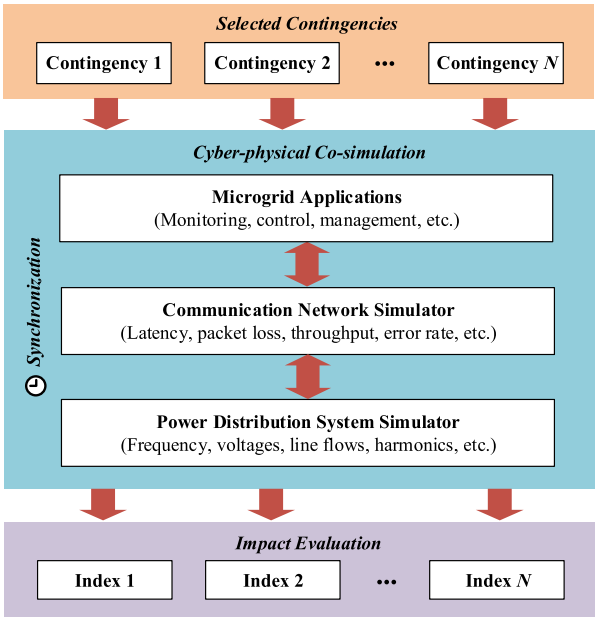

Fig. 8. ***Cyber–physical cosimulation framework.***

In essence, the cyber risk can be mitigated in two ways, namely, lowering the probability of occurrence of cyber contingencies, and reducing their physical impacts on microgrid operations.

Fig. 9 shows the procedures for microgrid operators to mitigate cyber risks on an ongoing basis. In the detection phase, microgrid operators utilize monitoring tools and detective measures to identify anomalous behaviors and enable early warnings for cyber incidents. In the restriction and restoration phases, microgrid operators respond quickly, by curbing and eliminating the implications of cyber incidents, to preserve and restore the operational performance of microgrids. In the adaptation and prevention phases, microgrid operators derive lessons from cyber incidents by postmortem analyses for minimizing the risk of similar attacks, while implementing defensive measures to prepare adequately for addressing ever-evolving cyber threats. These phases collectively form a closed-loop structure for improving the cybersecurity of microgrid operations.

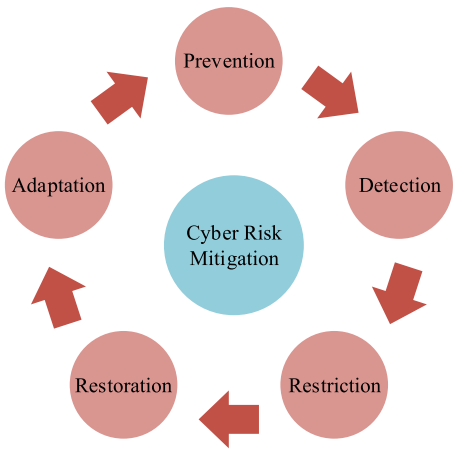

Fig. 9. ***Cyber risk mitigation phases.***

Generally, security measures for mitigating the cyber risk can be selected and implemented by considering the characteristics of microgrid operations, as well as the specific properties of hardware devices and software applications. In addition to staff training and physical protection policies, the following measures are usually considered to enhance cybersecurity in a microgrid [76]–[78]:

- deploying firewalls, antivirus software and intrusion detection systems to fend off malware;
- creating demilitarized zones to provide additional security;
- using dedicated, wired connections for critical applications;
- monitoring both remote and local access to critical cyber components;
- enabling multiple-factor authentication for access control;
- disabling unnecessary components and applications that could potentially enlarge the attack surface;
- retrofitting communication protocols with enhanced security mechanisms;
- encrypting sensitive data with sophisticated cryptography;
- fixing the flaws in applications and operating systems;
- perfecting incident response and recovery plans.

Note that traditional security solutions in the IT domain may introduce adverse effects on microgrid operations, degrading or even disrupting power supplies. For example, intricate cryptography can significantly enhance the confidentiality of data flows, but may inevitably cause unacceptable time latency and influence the performance of time-critical functionalities. Hence, security measures need to be tailored for microgrids conforming to their unique cyber–physical characteristics so that the availability and the integrity of data flows can always be assured. Moreover, microgrid operators should consider certain tradeoffs between performance (e.g., security, usability) and cost (e.g., development time, purchasing expense), as well as between proactive (i.e., protection) and reactive measures (i.e., response and recovery) in order to guarantee the effectiveness of deployed security measures in various operating conditions.

A popular subjective decision rule, labeled as the minimax regret criterion [79]–[81], is defined as

$$\text{Minimax Regret} = \min_{\text{Measures}} \left(\max_{\text{Conditions}} \text{Regret} \right)$$

which can be utilized to measure the effectiveness of security measures. With this criterion, microgrid operators are

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

Table 6 Illustration of the Minimax-Regret Criterion

Indices		Set A	Set B	Set C
Risk (MWh)	Scenario 1	16	18	17
	Scenario 2	13	12	14
	Scenario 3	8	7	8
Regret (MWh)	Scenario 1	0	2	1
	Scenario 2	1	0	2
	Scenario 3	1	0	1
Maximum Regret (MWh)		1	2	2

able to prioritize and implement security measures that minimize the worst case regret (i.e., maximum regret) over all possible operating conditions. Under a certain operating condition, regret stands for an incremental value between the lowest possible risk and the risk after implementing the selected set of security measures, which is stated as

$$\text{Regret} = \text{Risk} - \min_{\text{Measures}} \text{Risk} \ \forall \ \text{Conditions} \ \forall \text{Measures}.$$

Thus, the worst case regret can be quantified for each candidate set of security measures over all the possible operating conditions, and the set with the minimum value is selected for implementation. Reasonably, the implemented measures manage to guard microgrid operations against various cyber threats.

Table 6 illustrates the minimax regret criterion for enhancing cybersecurity in a microgrid, where the cyber risk is measured in terms of the expected energy not supplied over all the associated cyber contingencies. In this example, the microgrid's operating conditions are characterized as three representative scenarios (i.e., scenarios 1, 2, and 3) with equal probabilities of occurrence, while operators have three candidate sets of security measures (i.e., sets A, B, and C). The cyber risk varies with the implementation of security measures in different scenarios. In scenario 1, the implementation of set A corresponds to the lowest risk, so the regrets of sets B and C are 2 and 1 MWh, respectively. Instead, the lowest risk set in scenario 2 is set B and thus the regrets of sets A and C are 1 and 2 MWh, respectively. Similarly, in scenario 3, the regrets of sets A and C are both 1 MWh. Hence, the worst case regrets of three sets are 1, 2, and 2 MWh, which means set A as the minimum worst case regret excels in performance.

VI. DEFENSE-IN-DEPTH FRAMEWORK ENABLED BY SDN TECHNOLOGIES

As cyberattacks manifest themselves with an increasing level of sophistication, microgrids are in need of a layered defense framework consisting of robust cyber systems against malicious intrusions and fault-tolerant applications for governing power processes to maintain physical security in faulty cyber systems. Meanwhile, the emergence of software-defined networking (SDN) technologies opens up a wider range of opportunities for enhancing the cybersecurity of microgrid operations.

A. Software-Defined Networking

SDN is a novel communication paradigm that introduces a logically centralized controller (i.e., SDN controller) to make high-level decisions for guiding underlying switches to handle data flows throughout the communication network [82]. The switches communicate with the SDN controller for decision support using the OpenFlow protocol [83]. The network control capabilities are thus separated from the switches that are supervised by the SDN controller. Once the centralized SDN controller is protected from malfunction or failures, the functionalities of the communication network can always be preserved. The dynamic behaviors of SDN-enabled communication networks can be simulated in ns-3 or emulated in Mininet [84].

SDN breaks the conventional vertical integration and makes the communication network globally visible and directly programmable to the SDN controller. Given the global visibility, the SDN controller is capable of optimizing network-wide data flows more efficiently. Given the runtime programmability, the SDN controller manages to reroute data flows in a timely manner. Hence, SDN can continually monitor and reconfigure the communication network so as to sustain its satisfactory performance under dynamic conditions. Moreover, SDN introduces unprecedented capabilities to guard the communication network adequately against cyber incidents. On the one hand, SDN offers the per-flow micromanagement capability that is especially useful for checking the integrity of data while ensuring the timeliness of data transmission. On the other hand, SDN facilitates the implementation of network-wide security policy like access control.

When applied to microgrids, SDN technologies promise to overcome the limitations of existing communication infrastructure. SDN technologies not only simplify the data flow management to meet stringent quality-of-service requirements for microgrid applications, but also spur the development of microgrid-specific measures to make microgrid operations resistant to cyber incidents. In particular, the SDN controller can be deployed in the application server inside a microgrid control center [85]. Fig. 10 depicts the microgrid architecture with SDN-based communication technologies. Given the long lifespan of microgrid communication infrastructures, SDN technologies are also advantageous in refining and incorporating evolving communication technologies to meet future network management requirements.

B. Defense-in-Depth Approach

Traditional security measures performing well in the IT domain may not be adequate to protect microgrid operations

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

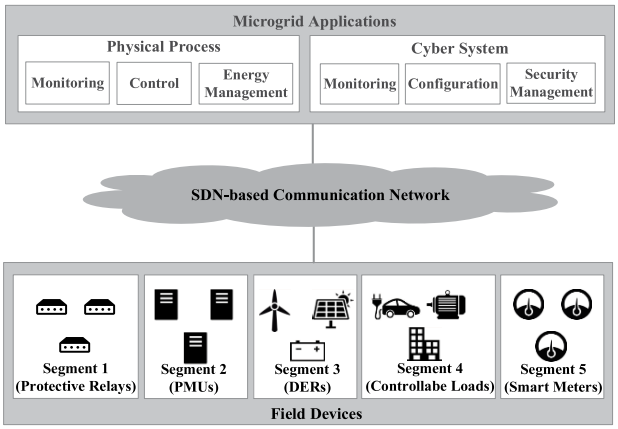

Fig. 10. ***SDN-enabled microgrid architecture.***

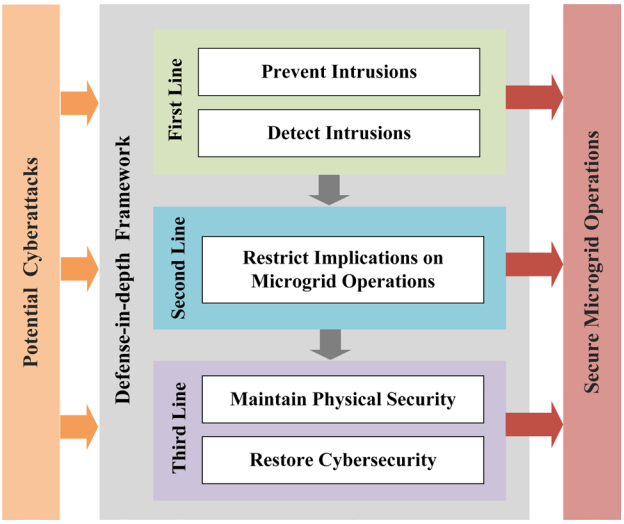

Fig. 11. ***Three lines of defense***

from potential realizations of cyber threats with continuously growing in complexity. For instance, the standard perimeter-hardening techniques such as firewalls and antivirus software can neither prevent exploitations of zero-day vulnerabilities, nor continue to counter cyberattacks once they are bypassed. Hence, an adaptive and holistic solution is critical to enhance the cybersecurity of microgrid operations.

Considering that microgrids are cyber–physical systems, cyberattacks also have the potential to endanger microgrid operations. In order to sustain the safety and the efficiency of power supplies, additional security measures specific to microgrid features should be designed and implemented by tightly integrating the efforts from both IT and power domains. On the one hand, cyber systems should be hardened to limit attackers' ability to penetrate and manipulate critical components, while detecting and mitigating cyberattacks effectively and promptly. On the other hand, control applications that regulate the physical process should continue to perform correctly when the operation of the cyber system is disrupted. In this sense, microgrid operations will be less susceptible to cyberattacks.

By taking full advantage of SDN technologies, a defense-in-depth approach can be developed to address the urgent security concerns in microgrid operations. In order to achieve the defense-in-depth goal, three lines of defense are deployed to fend off potential cyberattacks on microgrid operations. Fig. 11 presents the role of each defense line in accordance with the principles of mitigating the cyber risks presented in Fig. 9.

The first line of defense aims at preventing and detecting cyber intrusions so as to deter attackers from executing subsequently attacks on microgrid operations. The second line of defense is designed to thwart attackers from achieving the goals even if their intrusions into the cyber system are successful, so that the implications of cyberattacks on microgrid operations are restricted. The third line of defense is deployed to restore cybersecurity while preserving physical security, if microgrid operations are inevitably disrupted by cyberattacks. These three lines take effect in sequence, which means a line of defense starts to confront cyberattacks only when the preceding line fails to achieve the security of microgrid operations.

The defense-in-depth approach is effective in identifying, misdirecting, and disappointing potential attackers, thereby providing sufficient assurance for microgrids' secure operations. Representative defensive measures deployed at each defense line are illustrated in Fig. 12. Specifically, measures acting as the first line include the application-based segmentation and the real-time monitoring and verification (see Section VI-C); the measures realizing the moving-target defense and the defensive deception are deployed at the second line (see Section VI-D); the third

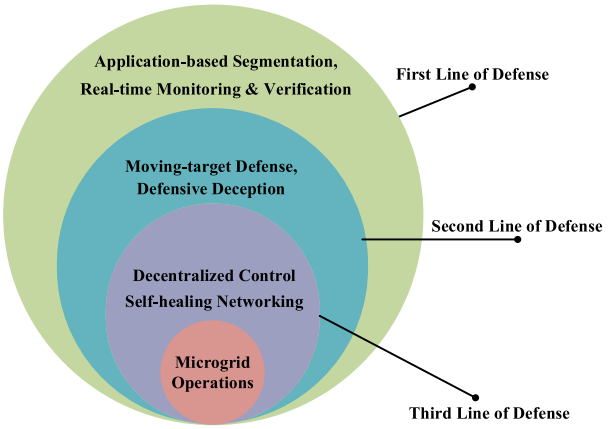

Fig. 12. ***Defense-in-depth security measures***

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

line comprises measures such as the decentralized power control and the self-healing communication networking (see Section VI-E). Note that additional defensive measures can be implemented in an adaptive manner for meeting the challenges of increasingly sophisticated cyberattacks.

C. First Line of Defense

1) Application-Based Segmentation: Application-based segmentation is a viable solution to building attack-resistive capabilities in microgrid operations, which introduces noticeable benefits in reducing the attack surface and enforcing security policies. In order to restrict communications in each segment, cyber components functioning in the same power application are grouped together and isolated from the rest of the communication network. Accordingly, network traffic and mutual interactions within each segment become more manageable, while the control center can track and respond to cyberattacks more efficiently. In particular, segmentation contains the propagation of cyber incidents because attackers are prohibited from accessing and contaminating the rest of the communication network via the compromised segment.

The application-based segmentation can be accomplished either physically or in a logical sense. Compared with the costly and complicated physical realization, SDN technologies facilitate the division of virtual segments without changing the physical communication network. Notably, cyber components within the same virtual segment are not necessarily close to each other, while all the virtual segments may share the same SDN controller. For the SDN-enabled microgrid shown in Fig. 10, the communication network is sliced to five virtual segments in accordance with power applications. Accordingly, protective relays, PMUs, DERs, controllable loads, and smart meters belong to separate segments, and therefore the control center can control and manage them more conveniently. In each virtual segment, the SDN controller manages to obtain finer grained traffic monitoring and management capabilities while only responding to requests from whitelisted cyber components (i.e., those with a particular privilege, service, mobility, access, or recognition). Particularly, data flows are secured by a flexible cryptographic encapsulation according to the time-critical requirements of power applications.

2) Real-Time Monitoring and Verification: SDN technologies provide the global visibility of communication network performance in real time, thereby facilitating the monitoring and verification of cyber intrusions. The SDN controller continuously watches network-wide data flows especially those initiated from the possible entry points of attackers while checking whether or not there exist any abnormal communications or suspicious connections. The standardized programmability provided by SDN enables straightforward implementations of existing verification techniques like the cross-layer semantics analysis [86]. In order to detect the presence of anomalies, the SDN controller may perform timing analyses and content inspection for each data flow by considering the spatiotemporal correlation of network traffics. Suspicious data flows can even be marked for subsequent forensic analyses to track and identify deliberate actions of attackers.

SDN technologies also make it easier to develop specification-based intrusion detection techniques. Specifications stipulating the characteristics of legitimate behaviors are defined uniquely for individual power applications. In comparison with conventional signature-based and anomaly-based techniques, specifications are advantageous in detecting previously unknown attacks with a reduced level of false-negative and false-positive errors [87]. For example, specifications largely improve the efficiency of identifying bad data in various electric power system applications. Furthermore, the SDN controller can even conduct complete semantics analyses for an application running in a virtual segment so as to detect and prevent any execution of inauthentic applications (e.g., possibly induced by the malware in application servers).

Through active monitoring and verification at runtime, the microgrid control center will obtain accurate security consciousness, and prepare for a rapid response to potential cyber incidents. For example, if there is a field device compromised by attackers, the control center will identify its appearance by observing its malicious behaviors in a timely manner. In particular, the SDN controller can even place temporary restrictions on the network connectivity of that device by prohibiting all associated data exchanges so as to prevent the propagation of cyber incidents.

D. Second Line of Defense

1) Moving Target Defense: Moving target defense presents attackers with a varying attack surface, thereby increasing the apparent complexity of achieving their goals [88]. In essence, moving target defense introduces unpredictability and diversification to system functionalities so that attackers lack a sufficient information to execute a successful attack.

With unprecedented network reconfiguration capabilities, SDN technologies can easily effectuate moving target defense in microgrid operations. First, the SDN controller can frequently change the IP addresses and traffic routing rules of connected field devices without hampering the configuration integrity or increasing the operation overhead [89]. Second, the SDN controller can dynamically control the connectivity of field devices to the control center [85]. Without any implication on physical functions, field devices are enforced to not always be accessible to the control center. Instead, they are periodically put in the idle state from the view of the cyber system and routes will be automatically established to enable data exchanges only when necessary.

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

Meanwhile, attackers will inadvertently expose their actions when manipulating the devices in the idle state. Third, the SDN controller can randomly select the partial information that is sufficient for power applications from abundant measurements so as to filter out unwanted and potentially malicious data. Therefore, in the face of moving target defense, attackers can hardly execute effective attacks to incur implications on microgrid operations.

Fig. 13 illustrates the application of moving target defense in the process of microgrid state estimation, where solid and dashed lines indicate measurements that are selected and not selected, respectively. The control center can utilize the measurements from any three of the five meters to conduct accurate state estimation, conforming to the fact that electric power systems commonly have enough measurement redundancy for achieving the full observability [90]. Accordingly, the control center can randomly change the combination of engaged measurements, which clearly increases the complexity of false data injection as compromised measurements are not necessarily used for state estimation.

2) Defensive Deception: Defensive deception is a way to "fight fire with fire," which is especially effective in fighting off targeted cyberattacks. Principally, defensive deception

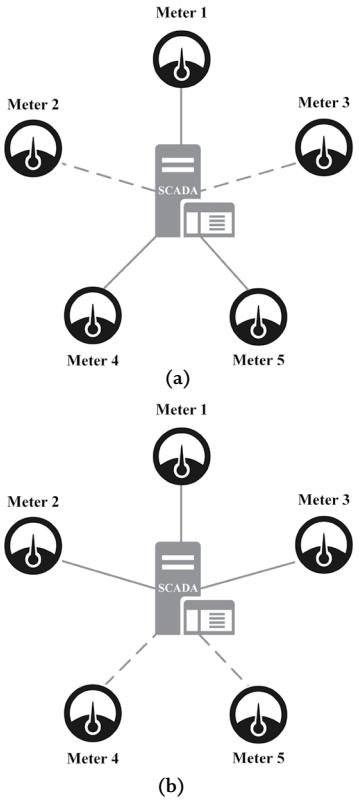

Fig. 13. ***Moving-target defense for microgrid state estimation. (a) One feasible combination; (b) Another feasible combination.***

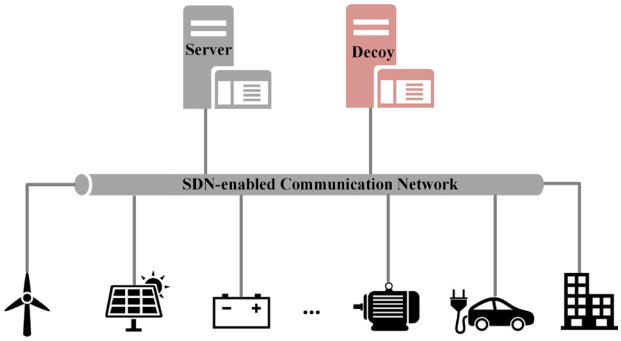

Fig. 14. ***Deployment of a decoy server.***

can obfuscate any critical information of microgrid operations (e.g., control command, communication protocol, power application, network connectivity) so that it manages to distort attackers' knowledge about the cyber system and make it more difficult for them to discover vulnerabilities.

In particular, system information can be camouflaged to imitate the complexity of realistic cases without reflecting their actual characteristics. SDN technologies are especially useful camouflaging the network traffics. For example, the SDN controller can command the switches to report nonexisting measurements on behalf of the connected field devices. Accordingly, even if attackers manage to invade the cyber system, they will be misguided by the camouflaged information and can hardly execute successful attacks against microgrid operations.

Similar to the well-known "Honeypot" in the IT domain [91], camouflaged traps can be inserted into the microgrid cyber system. These traps can mimic the smooth functioning of cyber components and intentionally expose exploitable vulnerabilities as decoys to potential attackers. Once attackers engage the decoy, the control center will be immediately notified to respond to their malicious activities. Fig. 14 shows the deployment of a decoy server for trapping attackers, where the data flows from and to this decoy can be forged using SDN technologies. Since there is no reason for legitimate devices to directly communicate with the decoy, the attempts made by attackers can be easily identified.

E. Third Line of Defense

1) Decentralized Power Control: Microgrids should remain functional and sustain high-quality power services to local customers even in the presence of cyberattacks impacting the normal operations. The control center, as the hub for microgrid operations, can suffer the single point failure. Any malfunction or failure of the control center may lead to degraded services or even power outages in the local area served by the microgrid. Thus, field devices, especially DERs, should possess the ability of operating properly in the absence of supervisory control from the microgrid control center.

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

The hierarchical control architecture [92], [93], shown in Fig. 15, provides microgrid operations with the distinguished flexibility against cyber incidents. This architecture combines the benefits of centralized and decentralized control mechanisms. On the one hand, DERs possess local controllers which allow them to function properly as autonomous control entities independent of the control center. Accordingly, these DERs can be controlled in a decentralized manner when the functionalities of the communication network or the control center are degraded or disrupted by cyberattacks. On the other hand, a functional control center provides dispersed DERs with optimal output settings to improve the efficiency of microgrid operations in normal conditions.

In order to implement the hierarchical control, DERs can be controlled as voltage sources to regulate the frequency and voltages in the microgrid according to their respective droop characteristics. Using local measurements, droops enable the power imbalance initiated by cyberattacks to be proportionally shared among DERs, as reflected in primary control. Secondary control aims at mitigating regulation errors introduced by primary control. Both primary and secondary control are performed locally at the DER level. Tertiary control is performed centrally at the control center for optimizing the microgrid-wide energy management. After the execution of secondary control, microgrids can maintain the nominal values for frequency and voltages even in the absence of tertiary control. Accordingly, microgrids can rely on the decentralized power control to sustain physical security while mitigating the implications of cyberattacks.

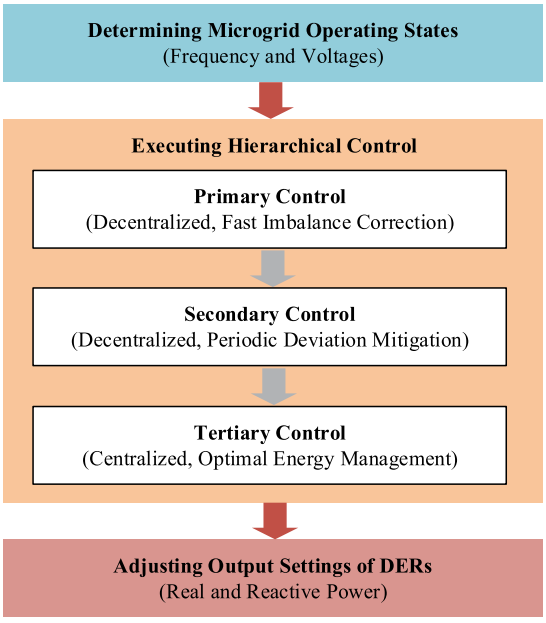

Fig. 15. ***Fault-tolerant power control flowchart.***

2) Self-Healing Communication Networking: SDN technologies are advantageous in incorporating self-healing capabilities in communication networks in order to ride through cyber incidents [94]. Once microgrid operations are influenced, the SDN controller can perform postmortem forensic analyses to locate compromised sources that initiated the attacks and isolate them from the communication network as a necessary step for normal operations. After the identification of compromised sources and disrupted components, the SDN controller dynamically reconfigures the communication network to curb the propagation of cyber incidents by strategically resetting switches and reestablishing the routing rules.

The self-healing networking capability takes effect in the form of fast failover, which can be achieved in two stages, as shown in Fig. 16. The first stage is in charge of determining the optimal failover schemes against postulated cyber contingencies with the consideration of uncertain network traffics. The first-stage problem with user-specified operation limitations can therefore be solved by robust optimization [95] or stochastic optimization [96] techniques in an offline fashion. After the realization of a cyber contingency, the SDN controller automatically reconfigures the network after looking up the failover tables specified at the first stage. Meanwhile, it optimizes the routes for data transmission to time-critical microgrid applications based on the real-time monitoring results of network traffics. Eventually, the SDN controller enables the configuration of newly optimized routes in the communication network at runtime.

VII. CONCLUSION

Microgrids play a significant role in achieving the goals of energy efficiency, sustainability, security, reliability, and resilience in electric power system operations. With the development and implementation of microgrids, electric

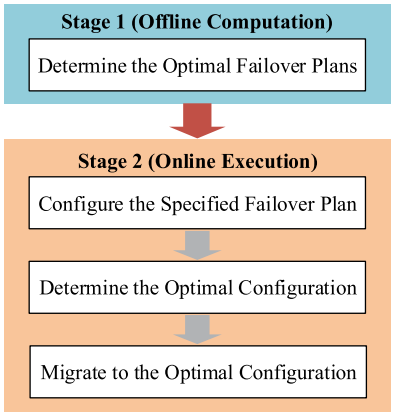

Fig. 16. ***Two-stage self-healing framework***

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

power systems have been transitioning from large-scale centralized systems to small-scale distributed systems. Microgrids, in essence, are typical cyber–physical systems where physical processes increasingly rely on advanced ICTs. While ICTs facilitate the control and management of onsite resources, they introduce a wide range of cyber threats to microgrid operations. Cybersecurity concerns are also spreading beyond the IT domain, since an insecure microgrid cyber system tends to incur inexplicable physical implications in the microgrid.

Cybersecurity plays a key role in maintaining the observability and controllability of physical processes, which necessitates the mitigation of cyber threats in microgrids for ensuring satisfactory power supplies to serve customers. Compared with the principles of mitigating physical vulnerabilities, ever-evolving cyber threats are considered more challenging. Microgrids adequately hardened against physical disruptions may remain unexpectedly vulnerable to cyberattacks. Accordingly, it is crucial to treat cybersecurity issues seriously and address them proactively so that the cyber risk in microgrid operations is reasonably reduced. Microgrids should also respond positively to and recover rapidly from cyber incidents in order to fulfill their critical mission of keeping the lights on.

A microgrid is also a promising platform for incorporating multiple local energy carriers (e.g., natural gas, heat, water) as an energy hub [97]–[99], which intertwines the generation, delivery, and consumption of multiple energy forms. In this context, microgrids are also subject to cyber threats in other energy infrastructures when a single cyber incident tends to cause severe physical consequences across several interdependent infrastructures. In order to provide reliable and resilient public services, microgrids need to enhance their cybersecurity holistically throughout the associated energy infrastructures, calling for close collaborations among industry, academia, and government. ■

Acknowledgement

The authors would like to thank the Science and Technology Unit at King Abdulaziz University for technical support.

REFERENCES

[1] M. Shahidehpour and J. F. Clair, "A functional microgrid for enhancing reliability, sustainability, and energy efficiency," *Electr. J.*, vol. 25, no. 8, pp. 21–28, Oct. 2012.

[2] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Bie, "Microgrids for enhancing the power grid resilience in extreme conditions," *IEEE Trans. Smart Grid*, to be published.

[3] L. Che, M. Khodayar, and M. Shahidehpour, "Only connect: Microgrids for distribution system restoration," *IEEE Power Energy Mag.*, vol. 12, no. 1, pp. 70–81, Feb. 2014.

[4] C. Abbey *et al.*, "Powering through the storm: Microgrids operation for more efficient disaster recovery," *IEEE Power Energy Mag.*, vol. 12, no. 3, pp. 67–76, May 2014.

[5] C. Marnay, H. Aki, K. Hirose, A. Kwasinski, S. Ogura, and T. Shinji, "Japan's pivot to resilience: How two microgrids fared after the 2011 earthquake," *IEEE Power Energy Mag.*, vol. 13, no. 3, pp. 44–57, Jun. 2015.

[6] E. Smith, S. Corzine, D. Racey, D. Patrick, H. Colin, and J. Weiss, "Going beyond cybersecurity compliance," *IEEE Power Energy Mag.*, vol. 14, no. 5, pp. 48–56, Sep. 2016.

[7] E. Bompard, T. Huang, Y. Wu, and M. Cremenescu, "Classification and trend analysis of threats origins to the security of power systems," *Int. J. Electr. Power Energy Syst.*, vol. 50, no. 1, pp. 50–64,Sep. 2013.

[8] Lloyd's, "Business blackout: The insurance implications of a cyber attack on the US power grid," 2015.

[9] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, pp. 1025–1028, Apr. 2010.

[10] M. Shahidehpour and M. Khodayar, "Cutting campus energy costs with hierarchical control: The economical and reliable operation of a microgrid," *IEEE Electrific. Mag.*, vol. 1, no. 1, pp. 40–56, Sep. 2013.

[11] L. Che and M. Shahidehpour, "DC microgrids: Economic operation and enhancement of resilience by hierarchical control," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2517–2526, Sep. 2014.

[12] X. Liu, P. Wang, and P. C. Loh, "A hybrid AC/DC microgrid and its coordination control," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 278–286, Jun. 2011.

[13] H. Farzin, M. Fotuhi-Firuzabad, and M. Moeini-Aghtaie, "Enhancing power system resilience through hierarchical outage management in multi-microgrids," *IEEE Trans. Smart Grid*, to be published.

[14] Z. Wang, B. Chen, J. Wang, and C. Chen, "Networked microgrids for self-healing power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 310–319, Jan. 2016.

[15] Z. Wang, B. Chen, J. Wang, M. M. Begovic, and C. Chen, "Coordinated energy management of networked microgrids in distribution systems," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 45–53, Jan. 2015.

[16] L. Che, M. Shahidehpour, A. Alabdulwahab, and Y. Al-Turki, "Hierarchical coordination of a community microgrid with AC and DC microgrids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3042–3051, Nov. 2015.

[17] X. Lu, S. Bahramirad, J. Wang, and C. Chen, "Bronzeville community microgrids: A reliable, resilient and sustainable solution for integrated energy management with distribution systems," *Electr. J.*, vol. 28, no. 10, Dec. 2015.

[18] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[19] *NISTIR 7628: Guidelines for Smart Grid Cyber Security: Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*, The Smart Grid Interoperability Panel–Cyber Security Working Group, 2010.

[20] *The ZigBee Alliance |Control your World.* [Online]. Available: http://www.zigbee.org

[21] *Wi-Fi Alliance.* [Online]. Available: https://www.wi-fi.org

[22] H. Wu and M. Shahidehpour, "Applications of wireless sensor networks for area coverage in microgrids," *IEEE Trans. Smart Grid*, to be published.

[23] *DNP—Overview of the DNP3 Protocol—DNP Users Group.* [Online]. Available: www.dnp.org/pages/aboutdefault.aspx

[24] A. Ruiz-Alvarez, A. Colet-Subirachs, F. Alvarez-Cuevas Figuerola, O. Gomis-Bellmunt, and A. Sudria-Andreu, "Operation of a utility connected microgrid using an IEC 61850-based multi-level management system," *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 858–865, Jun. 2012.

[25] J. Zittrain, *The Future of the Internet—and How to Stop It.* New Haven, CT, USA: Yale Univ. Press, 2008.

[26] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[27] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear phishing: Exploring embedded training and awareness," *IEEE Secur. Privacy*, vol. 12, no. 1, pp. 28–38, Feb. 2014.

[28] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan attacks: Threat analysis and countermeasures," *Proc. IEEE*, vol. 102, no. 8, pp. 1229–1247, Aug. 2014.

[29] R. K. C. Chang, "Defending against flooding-based distributed denial-of-service attacks: A tutorial," *IEEE Commun. Mag.*, vol. 40, no. 10, pp. 42–51, Oct. 2002.

[30] D. R. Raymond, S. F. Midkiff, A. Wood, and J. Stankovic, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive. Comput.*, vol. 7, no. 1, pp. 74–81, Mar. 2008.

[31] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, Jul. 2014.

[32] H. Ye, Y. Ge, X. Liu, and Z. Li, "Transmission line rating attack in two-settlement electricity markets," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1346–1355, May 2016.

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

[33] D.-H. Choi and L. Xie, "Ramp-induced data attacks on look-ahead dispatch in real-time power markets," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1235–1243, Sep. 2013.

[34] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Trans. Smart Grid*, to be published.

[35] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.

[36] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 235–244, Mar. 2013.

[37] M. Zeller, "Myth or reality—Does the Aurora vulnerability pose a risk to my generator?" in *Proc. 64th Annu. Conf. Prot. Relay Eng.*, Apr. 2011, pp. 130–136.

[38] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1244–1253, Sep. 2013.

[39] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Trans. Smart Grid*, to be published.

[40] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.

[41] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011.

[42] W. Gao, T. Morris, B. Reaves, and D. Richey, "On SCADA control system command and response injection and intrusion detection," in *Proc. Gen. Members Meet. eCrime Res. Summit, eCrime*, 2010.

[43] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[44] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.

[45] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, Jul. 2013.

[46] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sep. 2016.

[47] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.

[48] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced requirement on network information," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1686–1696, Jul. 2015.

[49] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid*, to be published.

[50] Z. Li, M. Shahidehpour, A. Abdulwhab, and A. Abusorrah, "Analyzing locally coordinated cyber-physical attacks for undetectable line outages," *IEEE Trans. Smart Grid*, to be published.

[51] A. Khodaei, S. Bahramirad, and M. Shahidehpour, "Microgrid planning under uncertainty," *IEEE Trans. Power Syst.*, vol. 30, no. 5, pp. 2417–2425, Sep. 2015.

[52] A. Gholami, T. Shekari, F. Aminifar, and M. Shahidehpour, "Microgrid scheduling with uncertainty: The quest for resilience," *IEEE Trans. Smart Grid*, to be published.

[53] A. Khodaei, "Resiliency-oriented microgrid optimal scheduling," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1584–1591, Jul. 2014.

[54] B. Falahati, Y. Fu, and L. Wu, "Reliability assessment of smart grid considering direct cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1515–1524, Sep. 2012.

[55] B. Falahati and Y. Fu, "Reliability assessment of smart grids considering indirect cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1677–1685, Jul. 2014.

[56] D. J. Landoll and D. Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. CRC Press, 2005.

[57] T. R. Peltier, *Information Security Risk Analysis*. Boca Raton, FL, USA: CRC Press, 2005.

[58] J. A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington, DC, USA: Center Strategic Int. Stud., 2002.

[59] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2375–2385, Sep. 2015.

[60] C.-W. Ten, A. Ginter, and R. Bulbul, "Cyber-based contingency analysis," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 3040–3050, Jul. 2016.

[61] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst. Man, Cybern. A Syst. Humans*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[62] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power system reliability evaluation with SCADA cybersecurity considerations," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1707–1721, Jul. 2015.

[63] Y. Zheng, D. M. Nicol, D. Jin, and N. Tanaka, "A virtual time system for virtualization-based network emulations and simulations," *J. Simul.*, no. 6, no. 3, pp. 205–213, Aug. 2012.

[64] C. Hannon, J. Yan, and D. Jin, "DSSnet: A smart grid modeling platform combining electrical power distribution system simulation and software defined networking emulation," in *Proc. Annu. ACM Conf. SIGSIM Principles Adv. Discrete Simulation (SIGSIM-PADS)*, 2016, pp. 131–142.

[65] H. Lin, S. S. Veda, S. S. Shukla, L. Mili, and J. Thorp, "GECO: Global event-driven co-simulation framework for interconnected power system and communication network," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1444–1456, Sep. 2012.

[66] L. Ren, Y. Qin, B. Wang, P. Zhang, P. B. Luh, and R. Jin, "Enabling resilient microgrid through programmable network," *IEEE Trans. Smart Grid*, to be published.

[67] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847–855, Jun. 2013.

[68] *PSCAD Home |PSCAD-Manitoba HVDC Research Centre*. [Online]. Available: https://hvdc.ca/pscad/

[69] PowerWorld. *The Visual Approach to Electric Power Systems*. [Online]. Available: http://www.powerworld.com/

[70] *PowerFactory-DIgSILENT Germany*. [Online]. Available: http://www.digsilent.de/index.php/products-powerfactory.html

[71] (2016). *ns-3*. [Online]. Available: https://www.nsnam.org/

[72] *OPNET Technologies-Network Simulator |Riverbed*. [Online]. Available: www.riverbed.com/products/steelcentral

[73] *OMNeT++ Discrete Event Simulator-Home*. [Online]. Available: https://omnetpp.org/

[74] *Welcome to Python.org*. [Online]. Available: https://www.pyt-hon.org/

[75] *MATLAB-MathWorks*. [Online]. Available: https://www.mathworks.com/products/matlab/

[76] G. N. Ericsson, "Cyber security and power system communication—Essential parts of a smart grid infrastructure," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1501–1507, Jul. 2010.

[77] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," *Comput. Secur.*, vol. 25, no. 7, pp. 498–506, Oct. 2006.

[78] W. T. Shaw, *Cybersecurity for SCADA Systems*. Tulsa, OK, USA: Pennwell Books, 2006.

[79] R. Jiang, J. Wang, M. Zhang, and Y. Guan, "Two-stage minimax regret robust unit commitment," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2271–2282, Aug. 2013.

[80] B. Chen, J. Wang, L. Wang, Y. He, and Z. Wang, "Robust optimization for transmission expansion planning: Minimax cost vs. minimax regret," *IEEE Trans. Power Syst.*, vol. 29, no. 6, pp. 3069–3077, Nov. 2014.

[81] L. Fan, J. Wang, R. Jiang, and Y. Guan, "Min-max regret bidding strategy for thermal generator considering price uncertainty," *IEEE Trans. Power Syst.*, vol. 29, no. 5, pp. 2169–2179, Sep. 2014.

[82] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[83] N. McKeown *et al.*, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Apr. 2008.

[84] *Mininet: An Instant Virtual Network on your Laptop (or other PC)-Mininet*. [Online]. Available: http://mininet.org/

[85] X. Dong, H. Lin, and R. Tan, "Software-defined networking for smart grid resilience: Opportunities and challenges [Position Paper]," in *Proc. 1st ACM Workshop Cyber-Phys. Syst. Secur. (CPSS)*, 2015, pp. 61–68.

[86] H. Lin, A. Slagell, Z. Kalbarczyk, P. Sauer, and R. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Trans. Smart Grid*, to be published.

[87] S. Goel, S. F. Bush, and B. David, *IEEE Vision for Smart Grid Communications: 2030 and Beyond*. New York, NY, USA: Inst. Elect. Electron. Eng., 2013.

[88] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threat*. Springer, 2011.

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.

[89] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: Transparent moving target defense using software defined networking," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.*, 2012, pp. 127–132.

[90] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Iimplementation*. Boca Raton, FL, USA: CRC Press, 2004.

[91] N. Provos, "A virtual honeypot framework," in *Proc. USENIX Secur. Symp.*, 2004, p. 173.

[92] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control system," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1963–1976, Dec. 2012.

[93] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization," *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 158–172, Jan. 2011.

[94] H. Lin *et al.*, "Self-healing attack-resilient PMU network for power system operation," *IEEE Trans. Smart Grid*, to be published.

[95] A. Ben-Tal, L. El Ghaoui, and A. Nemirovski, *Robust Optimization*. Princeton, NJ, USA: Princeton Univ. Press, 2009.

[96] D. P. Heyman and M. J. Sobel, *Stochastic Models in Operations Research: Stochastic Optimization*, vol. 2. Courier Corporation, 2003.

[97] M. Geidl, G. Koeppel, P. Favre-Perrod, B. Klockl, G. Andersson, and K. Frohlich, "Energy hubs for the future," *IEEE Power Energy Mag.*, vol. 5, no. 1, pp. 24–30, Feb. 2007.

[98] S. D. Manshadi and M. E. Khodayar, "Resilient operation of multiple energy carrier microgrids," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2283–2292, Sep. 2015.

[99] X. Zhang, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Optimal expansion planning of energy hub with multiple energy infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2302–2311, Sep. 2015.

ABOUT THE AUTHORS

Zhiyi Li (Student Member, IEEE) received the B.S. degree from Xi'an Jiaotong University, Xi'an, China, in 2011 and the M.S. degree from Zhejiang University, China, in 2014. He is currently working toward the Ph.D. degree in the Electrical and Computer Engineering Department, Illinois Institute of Technology, Chicago, IL, USA.

His research interests include large-scale system optimization and cyber–physical security in smart grids.

Mohammad Shahidehpour (Fellow, IEEE) received the Honorary Doctorate degree in electrical engineering from the Polytechnic University of Bucharest, Bucharest, Romania.

He is the Bodine Chair Professor and the Director with the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, IL, USA and a Research Professor with King Abdulaziz University, Jeddah, Saudi Arabia. He is a member of the US National Academy of Engineering and a Fellow of the American Association for the Advancement of Science (AAAS).

Farrokh Aminifar (Senior Member, IEEE) has been collaborating with the Robert W. Galvin Center for Electricity Innovation with the Illinois Institute of Technology, Chicago, IL, USA, since March 2009. He is currently an Assistant Professor with the School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran. His research interests include wide-area measurement systems, power system expansion planning and reliability assessment, and smart grid initiatives.

Dr. Aminifar is serving the IEEE Transactions on Sustainability and the IEEE Power Engineering Letters as the editor. He received the 2011 IEEE Iran Section Best Ph.D. Dissertation Award, the 2013 IEEE/PSO Transactions Prize Paper Award, and the 2015 IEEE Iran Section Young Investigator Award.

Authorized licensed use limited to: Illinois Institute of Technology. Downloaded on December 06,2025 at 11:46:02 UTC from IEEE Xplore. Restrictions apply.