Cyber Security of HVDC Systems

A Review of Cyber Threats, Defense, and Testbeds

Presekal, Alfan; Jorjani, Mohsen; Rajkumar, Vetrivel Subramaniam; Goyel, Himanshu; Cibin, Nicola; Semertzis, Ioannis; Stefanov, Alexandru; Palensky, Peter

DOI
10.1109/ACCESS.2024.3490605

Publication date
2024

Document Version
Final published version

Published in
IEEE Access

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 October 2024, accepted 24 October 2024, date of publication 4 November 2024, date of current version 18 November 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3490605

SURVEY

Cyber Security of HVDC Systems: A Review of Cyber Threats, Defense, and Testbeds

ALFAN PRESEKAL, (Member, IEEE), MOHSEN JORJANI, (Member, IEEE), VETRIVEL SUBRAMANIAM RAJKUMAR, (Graduate Student Member, IEEE), HIMANSHU GOYEL, (Graduate Student Member, IEEE), NICOLA CIBIN, (Graduate Student Member, IEEE), IOANNIS SEMERTZIS, (Graduate Student Member, IEEE), ALEXANDRU ŞTEFANOV, (Member, IEEE), AND PETER PALENSKY, (Senior Member, IEEE)

Department Electrical Sustainable Energy, Delft University of Technology, 2628CD Delft, The Netherlands

Corresponding author: Alfan Presekal (A.Presekal@tudelft.nl)

This work was supported by in part by the HVDC-WISE Project, in part by HVDC-WISE funded by European Union's Horizon Europe Program under Agreement 101075424, and in part by the U.K. Research and Innovation funding for HVDC-WISE is provided under the U.K. Government's Horizon Europe funding guarantee under Grant 10041877 and Grant 10051113.

ABSTRACT High Voltage Direct Current (HVDC) technology is one of the key enablers of the energy transition, especially for offshore wind energy systems. While extensive research on cyber security of High Voltage Alternating Current (HVAC) systems has been conducted, limited research exists on cyber security aspects of HVDC systems. These systems exhibit unique attributes, in comparison to HVAC systems, such as longer transmission line distances and increased volume of data samples for wide-area monitoring, control, and protection applications. These factors lead to a higher vulnerability of HVDC systems to cyber attacks. Existing state-of-the-art HVDC surveys, however, are primarily focused on HVDC physical components and exclude cyber security elements. Therefore, this paper presents the first detailed survey on the cyber security of HVDC Cyber-Physical Systems (CPS). We present a comprehensive review of the state-of-the-art HVDC systems, with a special focus on cyber threats and vulnerabilities, defense and mitigation strategies, and testbeds. Based on the review and analysis, insights and recommendations on future research directions to address the research gaps in this field of study are provided. Future research on cyber security for HVDC systems should prioritize the integration of cyber and physical system data and focus on early-stage detection to mitigate the potentially severe impacts of cyber attacks on HVDC grids.

INDEX TERMS Cyber attack, cyber defense, cyber security, HVDC, power system, testbeds, vulnerability.

I. INTRODUCTION

Power systems are undergoing fundamental changes in terms of digitalization, decarbonization, and decentralization. The realization of these trends has necessitated the widespread adoption of novel digital technologies, resulting in cyber security concerns [1]. Hence, power grids are now more susceptible to cyber attacks as a direct result of their growing reliance on digital technologies and equipment. Attacks on the power grid can potentially lead to devastating consequences for public safety, national security, and economic stability. Therefore, the cyber security of power grids has emerged as a critical issue that is being widely investigated in academic research [2].

Existing state-of-the-art research has examined cyber vulnerabilities of new prominent technologies being integrated into power grids, assessing the impact of cyber attacks on their operation, and creating defense strategies to protect them from attacks. The research includes state estimation and automatic generation control [3], [4], optimal power

The associate editor coordinating the review of this manuscript and approving it for publication was Dragan Jovcic.

flow [5], [6], cyber security for Phasor Measurement Units (PMU) [7], [8], [9], and power system communication protocols [10], [11]. Among them, research on the cyber security of High-Voltage Direct Current (HVDC) systems has become increasingly popular [12]. While extensive research on cyber security of High Voltage Alternating Current (HVAC) systems has been conducted, limited research exists on cyber security aspects of HVDC systems. These systems exhibit unique attributes, in comparison to HVAC systems, such as longer transmission line distances and increased volume of data samples for wide-area monitoring, control, and protection applications. These factors lead to a higher vulnerability of HVDC systems to cyber attacks, owing to their reliance on high-availability communication channels. The existing state-of-the-art HVDC surveys, however, are primarily focused on HVDC physical components and exclude cyber security elements. Therefore, this paper presents the first detailed survey on the cyber security of HVDC Cyber-Physical Systems (CPS). In the following subsections, we present the shift towards HVDC systems, survey methodology and related surveys, and contributions.

A. SHIFT TOWARD HVDC SYSTEMS

In recent years, HVDC systems and their applications in power grids have received lots of attention in the literature. This is due to the inherent advantages that HVDC systems provide in achieving ambitious climate neutrality targets [13]. To pave the path of reaching this target, renewable energy resources, e.g., wind, solar, and other clean, CO2 emission-free energy sources are being widely integrated into the power system.

The main advantages of HVDC systems are the lower power losses and greater capacities for transporting electricity over long distances, in comparison to High-Voltage Alternating Current (HVAC) systems [14]. Additionally, HVDC systems provide a number of important secondary and tertiary services for grid operation and control. These include, but are not limited to functionalities such as active power, voltage, and frequency control [15], [16], [17], [18], power oscillation damping [19], [20], and black start restoration [21]. Owing to these versatile functionalities, HVDC systems are becoming an increasingly appealing choice over HVAC systems for future power system planning. This is further evidenced by the steady increase in the number of publications involving HVDC systems, as depicted in Fig. 1.

B. SURVEY METHODOLOGY

This review uses the systematic literature review guidelines as outlined in [22]. A bibliographic review was conducted to identify the primary areas of investigation, which resulted in the identification of relevant studies. The primary objective of this paper is to identify existing cyber security research on HVDC systems. We classified the objectives of the survey into three sub-categories, i.e.,

1) cyber threats and vulnerabilities,
2) cyber attack mitigation and defense,
3) HVDC system co-simulation testbeds and, cyber attack use cases.

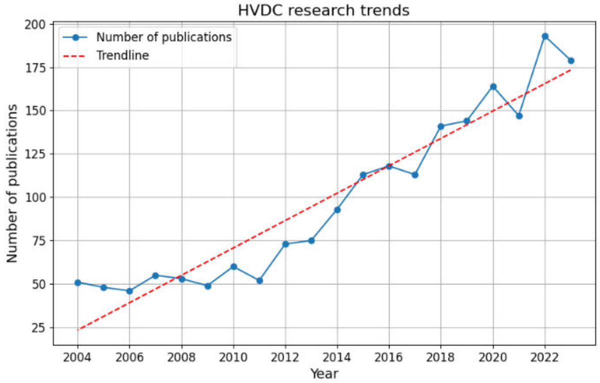

FIGURE 1. Trends of HVDC research from 2004-2023.

To identify the survey objectives, this review is guided by the following Research Questions (RQs):

- **RQ1**: *What are the cyber threats and vulnerabilities on HVDC systems?*
- **RQ2**: *What are the methods used to mitigate cyber attacks on HVDC systems?*
- **RQ3**: *What are the testbeds used to simulate and study cyber attacks on HVDC systems?*

A systematic literature review and bibliometric search of the relevant literature were performed to answer the RQs. The survey includes articles that were published in relevant digital libraries, i.e., *IEEEXplore and Scopus*. We limited the article categories primarily to journals and book chapters. Our survey uses the following Text Search (TS) queries that are in line with the search objectives in order to identify relevant articles from the aforementioned digital libraries. Based on the query search, we found 46 articles and filtered into 34 articles after excluding the duplicates and non-related articles as indicated in Fig. 2.

TS Query: ((HVDC **OR** High Voltage DC **OR** High Voltage Direct Current) **AND** (Cyber Attack **OR** Cyber Security))

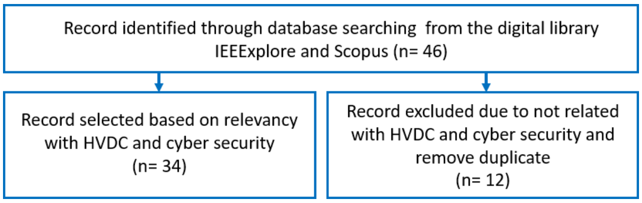
Record identified through database searching from the digital library IEEExplore and Scopus (n= 46)
Record selected based on relevancy with HVDC and cyber security (n= 34)
Record excluded due to not related with HVDC and cyber security and remove duplicate (n= 12)

FIGURE 2. Articles selection process.

C. RELATED SURVEYS AND CONTRIBUTIONS

Based on search queries on digital research libraries, we found 14 surveys and reviews related to HVDC and cyber security as reported in [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], and [35]. The majority of the

TABLE 1. Comparison of our survey with existing state-of-the-art surveys on HVDC systems.

Ref.	Year	Cyber Threats	Defenses	Testbeds	Remarks
Our survey	2024	✓	✓	✓	Review on cyber security on HVDC
[23]	2023	✗	✗	✗	Review on HVDC faults and protection system
[24]	2023	✗	✗	✗	Review of circuit breakers in HVDC systems
[25]	2022	✗	✗	✗	Review on the protection of multi-terminal HVDC grids
[26]	2021	✗	✗	✗	Review on fault protection methods in HVDC
[27]	2021	✗	✗	✗	Review on challenges of hybrid HVAC-HVDC
[28]	2021	✗	✗	✗	Review of HVDC stability assessment
[29]	2021	✗	✗	✗	Review of HVDC technologies
[30]	2021	✗	✓	✓	Review of protection systems for multi-terminal HVDC
[31]	2020	✗	✗	✗	Review on HVDC inductive fault current limiters
[32]	2020	✗	✗	✗	Survey on converter fault tolerance in MMC-HVDC
[33]	2019	✗	✗	✗	Review on HVDC technologies and market
[34]	2018	✗	✗	✗	Survey on inter-area oscillation damping control using HVDC
[35]	2017	✗	✗	✗	Review on MMC-based multi-terminal HVDC

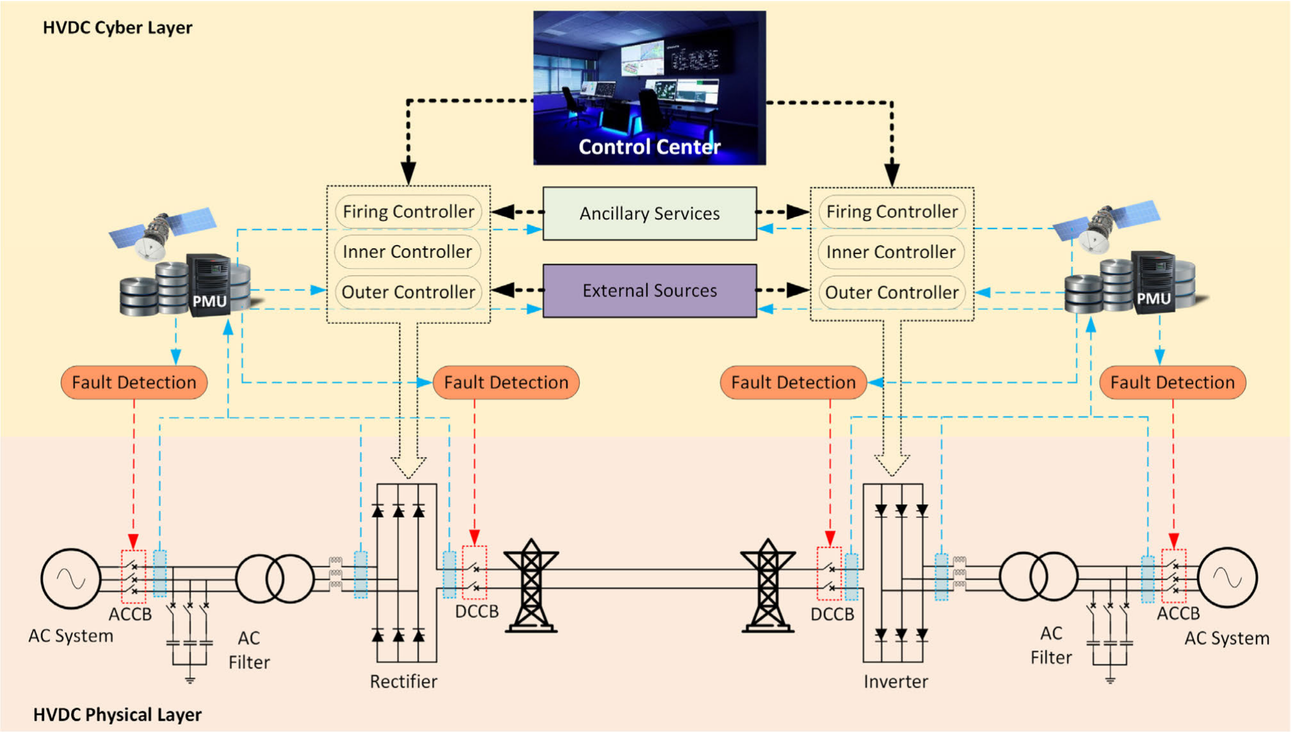

FIGURE 3. Cyber-physical HVDC system.

surveys focus on the physical components of the HVDC system, i.e., protection system, circuit breakers, Modular Multi-level Converter (MMC), etc. There are related surveys on cyber security of grid-connected power electronics as a component of HVDC systems in [36] and [37]. However, this study did not comprehensively cover the HVDC system as an integrated Cyber-Physical System (CPS); instead, it focuses more on the power electronic components. In [37], the survey primarily focused on cyber security from a component perspective, i.e., grid converters, power generation, transmission, and prosumers. However, our proposed survey provides a different angle from the threats, defense mechanisms, and co-simulation testbed perspective. Therefore, although there are some aspects that may intersect, we consider our survey to be novel based on the different angles of HVDC cyber security. The comparison of our survey with the existing surveys is shown in Table 1.

The main contributions of this paper are summarized as follows:

1) The state-of-the-art surveys on HVDC primarily focus on the physical aspects and exclude cyber security [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35]. Therefore, according to the systematic literature review, our survey paper is the first known comprehensive review of the cyber security on the HVDC cyber-physical systems. This survey contributes to identifying the research directions of cyber security

on HVDC systems, which differs from the predominant cyber security research focused on HVAC systems.

2) This survey identifies the potential cyber threats that can possibly target HVDC systems. The threats are categorized based on state-of-the-art research, i.e., False Data Injection Attack (FDIA), replay, and Denial of Service (DoS) attacks.
3) The survey provides a summary of the state-of-the-art cyber defense mechanisms against cyber attacks on HVDC systems. The defenses are classified into three categories, i.e., detection, mitigation, and resiliency.
4) The survey summarizes the state-of-the-art co-simulation testbeds for cyber security research on HVDC systems. It also identifies grid simulators and models used for HVDC simulations along with the cyber simulation tools.

The remaining sections of the paper are structured as follows. Section II is the state-of-the-art HVDC systems that cover HVDC cyber-physical systems, HVDC technologies, communications, and controllers. Section III describes the cyber security of HVDC systems, i.e., cyber threats, defense, and testbeds. Section IV provides the conclusion and recommendations.

II. HVDC SYSTEMS

In this section, a brief description of HVDC CPS is presented, elaborating on the foundation of HVDC CPS. This section also covers HVDC CPS components, including power transmission with digital control and communication. Furthermore, the state-of-the-art converter and communication technologies, alongside control aspects, are discussed.

A. HVDC CYBER-PHYSICAL SYSTEMS

The conceptual design of the HVDC CPS is depicted in Fig. 3, and it consists of two layers, i.e., physical and cyber. The physical layer is comprised of the following components [33]:

1) **Converter station:** This element serves as the backbone of an HVDC system and is responsible for converting AC voltage to DC voltage, i.e., rectifier mode, or vice-versa, i.e., inverter mode. Line Commuted Converters (LCCs) and Voltage-Source Converters (VSCs) are the two most widely adopted technologies for HVDC converter stations. Nevertheless, in recent years, MMC-based converter stations have become increasingly attractive due to their modular design and superior performance.
2) **Converter transformer:** It acts as an interface between the AC and DC systems, while also providing the isolation for the converters from possible short circuits/faults on the AC side. Moreover, different AC filters and reactors are typically installed at HVDC stations to reduce harmonics. As for protection, various AC circuit breakers and, prospectively, DC circuit breakers are also used on the AC/DC side of the converters. Different HVDC transmission configurations, e.g., monopolar and bipolar, are commonly used.

It should be noted that the selection between these configurations and other physical component specifications is mainly dependent on the specific needs and requirements of particular HVDC projects.

In the cyber layer, high-speed synchronized samples of different measurements (such as AC and DC side voltages, currents, and powers) are gathered from the system using PMU devices. The measurements gathered from each HVDC station are used by the relevant HVDC terminal controllers to generate appropriate firing angles for the respective converters. The control algorithms and theory are described more in-depth in the following Subsection II-D.

HVDC systems can also provide some ancillary services for the power grid, such as power oscillation damping, frequency regulation, etc. [15], [16], [17], [18], [19], [20], [21]. To do so, the PMU measurements from both HVDC stations are used by different algorithms, and proper control actions are then sent to the terminal controllers. The PMU measurements and ancillary service targets are also delivered to the power grid control center or DC substation, which controls the converter substation. Subsequently, the information is processed to make corrective decisions to optimize the overall performance of the power grid are adopted by processing them. These decisions are communicated to the HVDC terminal controllers and ancillary services in different forms, such as power order commands. Some external sources, i.e., the Remedial Action Scheme (RAS), might also provide input data for the terminal controllers [38], [39].

The AC and DC circuit breakers are also operated by AC and DC fault location algorithms which process the PMU measurements to decide on the occurrence of faults in the system and send appropriate tripping signals to them. According to what is discussed above, cyber layer components play a vital role in the control and protection of HVDC systems. However, as is depicted in Fig. 3, different cyber layer components usually communicate with each other through different widely-used communication protocols such as IEC 60255, IEC 60834, IEC 61850, and IEC 61869, DNP3, IEC 60870-5-101/104, and IEC C37.118 [40], [41], which could have underlying vulnerabilities. Therefore, investigating cyber vulnerabilities of HVDC systems is crucial to maintaining their secure operation and control.

B. HVDC TECHNOLOGIES

Over the years, for the development and deployment of HVDC systems, certain technologies have been utilized for the conversion of AC voltage to adequate DC voltage, suitable for power transmission, and vice versa. As such, the design and operation of the converter stations are the most important features of an HVDC system. Currently, the two leading technologies most widely used in HVDC infrastructures are LCC and VSC. Additionally, utilizing topological modifications on the VSC structure, new types of converters have emerged, with the most prominent being MMC.

1) LINE COMMUTATED CONVERTERS (LCC)

LCCs, also known as current source converters, operate based on the parameters of the AC transmission line. The converter's switching frequency matches the AC line frequency, while control is achieved by utilizing the thyristor firing angles. The advantages of LCC are the low power losses, the capability to transfer increased amounts of power while being overloaded, and their lower costs. A significant drawback of this applied technology is the lack of AC fault ride-through and black-start capabilities, as the thyristor control depends on the AC line voltages [42]. This limitation was addressed using auxiliary synchronous condensers, which activate when an AC fault occurs.

2) VOLTAGE-SOURCE CONVERTER (VSC)

VSC technology gradually replaced the LCC, especially for offshore and power transmission applications. The reasons for this shift are that VSCs are self-commutated, i.e., they can operate in four quadrants and do not depend on AC line voltages. The reversal of the power flow is based on the reversal of the DC current direction, while the voltage polarity remains constant. Thus, VSCs can utilize advanced switching techniques, e.g., Pulse-Width-Modulation (PWM), enabling higher switching frequencies compared to LCCs. As a result, the harmonic filters needed are smaller and more economically viable. Furthermore, as these converters are self-commutated, they enable fault-ride through and black-start capabilities. Finally, the four-quadrant operation enables the independent control of active and reactive power.

3) MODULAR MULTI-LEVEL CONVERTER (MMC)

This converter technology relies on replacing the switching series semiconductor strings with equivalent IGBT/capacitor sub-modules (SMs), thus increasing the scalability of the converter, in addition to its fault tolerance. Increasing the number of SMs enables the MMC to generate sinusoidal AC voltages with limited harmonics, thus reducing the need for AC or DC filters. An increased number of SMs also decreases the stress per module while the switching losses are reduced. Typical configurations for MMC HVDC are Half-Bridge (HB) or Full-Bridge (FB). Currently, HB SMs are the dominant topology due to the reduced costs and losses. However, HB topology is limited in its ability to block fault currents on the AC side for a fault on the DC side. For that, other topologies, such as FB are proposed.

4) HVDC TOPOLOGIES

Typically, HVDC links can either be point-to-point (two terminals connected together) or multi-terminal (at least three terminals connected together). Fig. 4 depicts the typical HVDC topologies and polarities. The term "symmetrical" refers to one wire having a positive voltage and the other having a negative voltage, both with the same absolute value. Unlike an asymmetrical monopole, none of the poles are attached to the earth as depicted in Fig. 4. Despite having lower investment costs than bipolar topologies, this topology is not ideal for linking offshore hubs to the coast because of its low flexibility and redundancy. Furthermore, it has a lower transmission capacity compared to bipolar lines.

HVDC links with a bipolar topology, in which two MMCs are coupled on each side of the link, are increasingly being used because of the benefits they provide. This topology provides additional operational margin to ensure a certain transfer capacity: even if one pole fails, it is still possible to transfer half of the total rated capacity by using the other pole. For example, in the event of planned maintenance on one pole, this pole might be unloaded using a suitable control approach, allowing for cable separation without the usage of costly and bulky DC circuit breakers.

C. COMMUNICATION

HVDC is more cost-effective than HVAC for transmission distances greater than 600-800 kilometers. Therefore, it is more valuable to utilize HVDC for longer transmission distances. However, these long distances bring drawbacks from a communication perspective. Previous research has identified the challenges of HVDC communication that highly depend on the minimum communication delay [26], [30]. In this survey, we identify three characteristics of HVDC communications, as follows.

1) COMMUNICATION DISTANCE LIMITATIONS

Fiber optics is now known as the fastest and most reliable kind of communication [43], and state-of-the-art power system transmission protection utilizes it for data communication [44]. With a latency of 0.5 ms per 100 km, it is the most optimal technology choice that is currently available [30]. However, some studies suggest that the delay of fiber optics is unsatisfactory for HVDC system operation. Fiber connection can decrease the overall reliability of the protective plan in HVDC systems [45]. A delay or malfunction in the communication link can make the entire protective system inoperative, necessitating the presence of backup protection. Additionally, it imposes a limitation on the protection operation's speed, which is an essential attribute of any protection strategy. The research in [40] came to the conclusion that the protection mechanisms that are normally used in the AC grid cannot be immediately applied to the DC grid. When it comes to communication and protection decisions, DC grid protection requires faster speeds. Additionally, it requires greater bandwidth, advancements in relay coordination, and breaker technologies. Hence, it can be concluded that the HVDC system faces inherent challenges due to communication limitations.

2) COMMUNICATION STANDARDS

As previously mentioned, HVDC systems utilize various communication standards and protocols for operation and protection, i.e., IEC 60255, IEC 60834, IEC 61850, and IEC 61869, DNP3, IEC 60870-5-101/104, and IEC C37.118 [39],

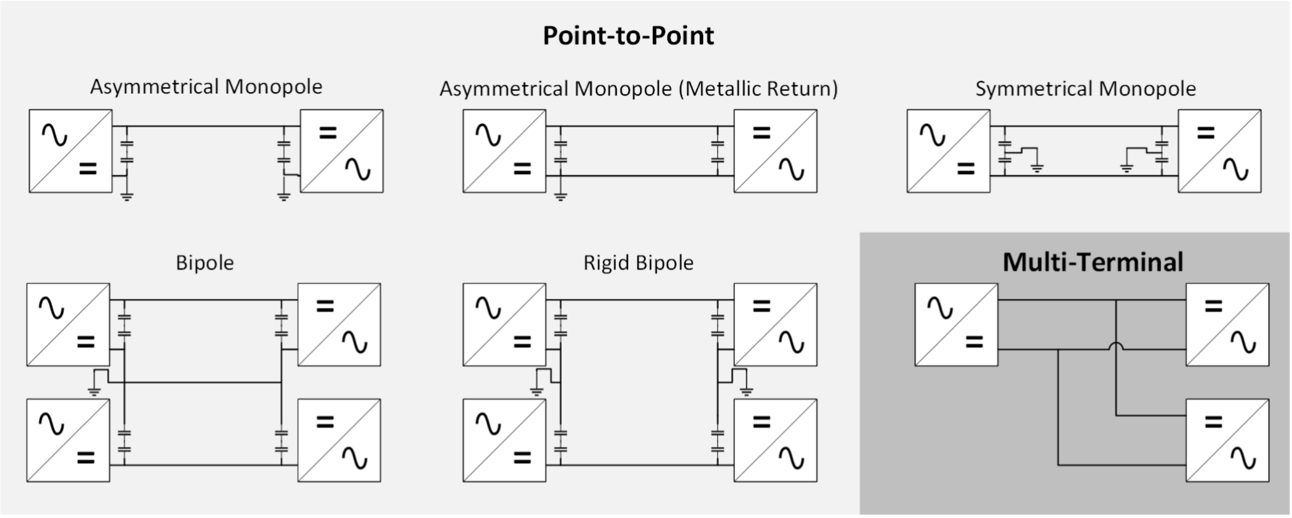

FIGURE 4. HVDC topologies.

[40]. They are not always secure and may be vulnerable to cyber attacks, i.e., DoS, FDIA, spoofing, etc. These kinds of cyber attacks can lead to disturbances in communications and as a result, to the physical HVDC system. For example, the authors in [45] demonstrated a spoofing attack on IEC 61850 to maliciously open a breaker in a power system. Security measures can be implemented to improve the security of the HVDC communication, i.e., using encryption. However, this increased cyber security also brings challenges by increasing communication latency.

3) REMOTE COMMUNICATIONS FOR CONTROL APPLICATIONS

Typical HVDC systems employ control functionalities to regulate various grid variables such as active or reactive power flows, voltage magnitudes, frequency, etc. Proper protection strategies are also vital to ensure the safe and secure operation of HVDC systems [47]. Furthermore, HVDC systems can provide some containment and mitigation mechanisms to protect the power grid against severe disturbances [48].

HVDC systems make use of digital technologies such as software algorithms, communication networks, and data processing mechanisms to deliver the aforementioned control and protection functionalities [49]. There are typically dedicated communication channels between HVDC stations, control centers, and other control facilities [50]. The HVDC controller can also potentially be accessed by multiple application entities linked to the HVDC stations through communication channels. Thereby, the number of remote and local access points to HVDC is high, thus expanding the potential cyber attack surface [51].

D. CONTROLLERS

Several technologies are adapted to achieve the desired control of the HVDC terminals. The main considerations regarding the implemented control system are the technologies used and the condition of the connected AC grids. Regarding the technologies considered in this work, the controllers for LCC, VSC, and MMC are covered. Controllers for HVDC terminals generally consist of multiple layers [52]. The outer layer is responsible for generating reference values for the inner layers. This can take one or several targets/reference parameters into account, such as active and reactive power control, AC and DC voltage control, etc. The inner controller is responsible for controlling the current flowing through the phase reactor. This is usually accomplished using the decoupled *dq*-current control framework. Finally, the firing controller generates the firing logic for the converter switches using techniques such as Pulse Width Modulation (PWM). A two-way communication between the HVDC stations and terminal controllers usually exists to enhance system control performance.

1) LCC CONTROLLERS

For LCC-HVDC systems, each converter station has different controlling tasks, while their control architecture depends mainly on the type of the connected AC grid (weak or strong). Both stations control the thyristor firing angle to control the DC power and voltage. One station acts as a rectifier regulating the DC link current, while the other acts as an inverter by regulating the DC voltage. The voltage control can be performed through the thyristor's extinction angle. Such configuration is mainly applied when the AC grid is considered weak. The reference set points of the controlled variables are achieved by a combination of Proportional Integral (PI) controllers and Phase Locked-Loops (PLLs). Additionally, voltage control is achieved through the converter station's On Load Tap Changer (OLTC) transformer [53].

2) VSC CONTROLLERS

As mentioned above, VSC-HVDC systems provide improved control of active and reactive powers. Thus, they are more

TABLE 2. Cyber attacks targeting HVDC systems components.

Targeted System	Attack Types	References
Voltage Source Converter (VSC)	FDIA	[61]-[64], [66],[69]
	DoS	[64]
Line Commutated Converter (LCC)	FDIA	[68], [72],[75],[76]
	Dos, Replay Attack	[72]
Modular Multilevel Converter (MMC)	FDIA	[65]-[67]
	DoS	[73],[74]
Load Frequency Control (LFC)	FDIA	[57],[58],[69]
	DoS	[57]
HVDC Ancillary Control and Services	FDIA	[56] , [59], [60], [70], [71]
	Dos, Replay Attack	[56],[60], [71]

VSC = Voltage Source Converters, LFC = Load Frequency Control, MMC = Modular Multilevel Converter, LCC = Line Commutated Converter, PLL = Phase-Locked Loop, AGC = Automatic Generation Control, PMC = Power Modulation Control

suitable for the connection of weak AC grids. The control variables can be set via vector control at the AC terminals by controlling the signals to the Insulated Gate Bipolar Transistor (IGBT) gates [54]. On the one hand, the operating mode of a VSC converter is not dictated by the power flow direction, meaning that the terms rectifier and inverter are used mainly for notation. On the other hand, the controllers must be consistent, considering the power balance. This means that both stations have additional control degrees of freedom utilized for controlling the reactive power and AC voltage, in addition to the DC current and active power. Additional methods for controlling the VSC-HVDC systems can be through the usage of techniques such as PWM. As such, the system can act as a current-controlled voltage source. Additional controllers are needed to enable the stable operation of VSCs in weak AC grids, such as advanced PLLs [55].

3) MMC CONTROLLERS

The MMC circuit has a similar structure to the VSC, with the main difference being that the energy storage elements on the DC side of the converter, e.g. capacitors, are distributed in the converter arms. The controller blocks can be divided into inner and outer loop controllers. The outer loop controller governs the active and reactive power exchange between the interconnected AC grids. Control strategies that are utilized in the outer loop controller are voltage and power controls. The inner loop controller is utilized for maintaining the DC voltage by employing PWM techniques. Such techniques could involve carrier-based or space-vector PWMs for optimizing harmonic distortion, switching losses, and voltage balancing.

4) WIDE AREA DAMPING CONTROLLERS

An additional controller that is utilized for HVDC control is the damping controller, used for addressing the issue of low-frequency oscillations. Wide-area monitoring systems can be utilized for WAMS-based oscillation control. Utilizing the presence of PMU measurements, the controller can be used to inject active power in the AC side of the system at the two ends of an HVDC line, which is proportional to the frequency difference obtained through the measurements. The effectiveness of such a controller was showcased in a practical implementation, as reported in [56].

III. CYBER SECURITY OF HVDC SYSTEMS

Following the overview of HVDC systems provided in Section II, Section III explores the cyber security aspect of the HVDC systems. This section presents a comprehensive state-of-the-art survey of the cyber security of HVDC systems. The survey covers the potential cyber threats, defense mechanisms, and co-simulation testbeds for HVDC systems. Each subsection aims to address the research questions presented in Section I.

A. CYBER THREATS

According to the literature review, we identified three categories of cyber threats targeting various components of HVDC systems. Table 2 summarizes the various cyber threats on HVDC systems and components. The targeted components include Voltage Source Converters (VSCs), Line Commutated Converters (LCCs), Modular Multilevel Converters (MMCs), Load Frequency Control (LFC), and HVDC ancillary control and services. From the attack categories, we identified three types of attacks, including FDIA, DoS, and replay attacks. These attacks aim at driving AC/HVDC systems in unstable conditions, causing large frequency deviations and oscillations that could possibly lead to widespread blackouts, reducing power quality, and drastically affecting overall system performances and efficiency. To cause this impact on the grid, the attacks specifically target different types of converters, i.e., LCC, VSC, and specifically MMC-VSC, and control mechanisms, including LFC, damping control, and other ancillary control services used in HVDC systems. In the following, each cyber attack type is briefly introduced, attack points are described, and the impact on HVDC systems is discussed.

1) FALSE DATA INJECTION ATTACKS

The most common approach to maliciously manipulate HVDC systems' behavior consists of FDIAs, which involve the injection of malicious or manipulated measurement data regarding the state of the electrical power grid. These measurements are possibly acquired by Remote Terminal Units (RTUs), collected and aggregated by Phasor Data Concentrator (PDC), and delivered to Supervisory Control and Data Acquisition (SCADA) systems, to be used by state estimation and control algorithms. If these communications between the components are not properly secured for instance, by using secure authentication and encryption techniques, attacks can be executed by undermining the integrity of the messages exchanged between PMUs and PDCs or between PDCs and HVDC systems [57]. Further, these kinds of attacks can remain stealthy and circumvent the regular bad data detector systems if the attacker has enough resources or knowledge of the system under attack [58], [59].

As discussed in [57] and [60], different attack approaches can be adopted to tamper with the reported measurements, including (1) false oscillation attack, (2) ramp attack, (3) scale attack, (4) data interchange attack, and (5) playback attack. Moreover, FDIA attacks can also be characterized in terms of magnitude, duration, and template of the injected false data. Examples of attack templates are provided in [61] where the data modification takes the form of an added bias, gradient, pulse, noise, or the scaling and sign inversion of the measurements. These different attack approaches have the objective of maximizing the attack impact while minimizing the probability of being detected by data detectors and other defense mechanisms. These latter mechanisms will be further discussed in Section III-B. Depending on the targeted system and on the intruder's desired outcome, the choice of the manipulated quantities can vary, including voltage, frequency, and power measurements.

When FDIAs are performed on VSCs, the voltage measurements of one or multiple grid buses can be tampered with to deteriorate the stability of the system, increase switching losses, and consequently decrease the efficiency of the targeted HVDC system [62]. In [63], a cyber attack tampering the reported active power to VSC is analyzed, and it is shown how the attack can lead to manipulated transmission power and result in a frequency deviation on the AC side and a voltage deviation on the DC side., Consequently, such an attack threatens the secure operation of the hybrid AC/DC grid. Various combinations of FDIA tampering with AC and DC voltage and power measurements can be used to attack VSC Multiterminal HVDC systems as presented in [64]. Moreover, as shown in [65], attacks can aim at manipulating the various reference values incorporated in VSC control strategies in order to alter the controller behavior.

In [66], an MMC controlled by a consensus-based distributed control scheme is considered, and the authors show how, by targeting the submodules' capacitor voltage balancing control mechanism, it is possible to cause an increase in the capacitor voltages and the tripping of the submodules for overvoltage protection. Subsequently, in [67], the authors focused on attacking MMC controller parameters and demonstrated how attacks on PI controller parameters in the voltage controller, current controller, and PLL can cause a significant increase in controller overshoot, steady-state error, and high oscillatory behaviors. Also, the authors in [68] concluded that an attacker could move the system closer to instability margins by tampering with either the measurements or reference values used by the MMC controller. Attacks on LCC systems have been studied in [69], and it has been shown that FDIA on the rectifier or inverter sides of HVDC systems operated in DC control mode can limit the power transmission or cause instability in the system. Further, it is also shown that FDIA on the inverter side of the HVDC system can result in communication failures, which can lead to a decrease in the inverter efficiency or device damage.

Regarding the control part of the HDVC system, damping control and load frequency control have been proven to be vulnerable to FDIA attacks [70]. Indeed, as analyzed in [71], manipulation of frequency measurements can cause low-frequency inter-area oscillations, by forcing the controller to increase the output power to damp the falsely reported frequency oscillations. In [72], it is shown that voltage magnitude and angle manipulation can affect the system stability. The impact of tampering with power and frequency measurements reported to LFC is further explored in [58]. These works show that LFC systems with AC/HVDC interconnection and emulated inertia can be more vulnerable to FDIA compared to the ones without inertia emulation and normal AC systems.

2) REPLAY ATTACKS

Similarly to FDIA, replay attacks aim at deceiving state estimation and control algorithms. Instead of injecting malicious or manipulated measurements, they rely on the retransmission of valid signals that have been previously intercepted by monitoring the communication channel. Given that the replayed signals contain invalid messages, if proper prevention and detection mechanisms are not implemented, the repeated messages are accepted by the receiving system [61]. This type of attack has been studied in [73] adopting two different approaches. In the first approach, the frequency measurements are intercepted during a severe transient event and then replayed during normal operations to the damping controller. In the second one, measurements are recorded while no system disturbances are present and then re-transmitted when a large system transient event occurs. With these approaches, it has been shown how the replay attack can trigger inter-area oscillations in the system and/or disturb, or even disable normal operations of the HVDC damping controller. Replay attacks can also be performed in combination with other types of malicious behavior to cover up the ongoing disturbances, and thus avoid the monitoring and control systems response [57]. As reported in [57], replay attacks are performed in combination with FDIA and DoS attacks to deceive HVDC Ancillary Service Control (HASC) and cause false control actions.

3) DENIAL OF SERVICE

DoS attacks aim at limiting or blocking the communications between data sender and receiver, thereby forcing control algorithms to operate on outdated data. Multiple studies analyzed the impact of DoS attacks on HVDC systems, targeting VSC [65], LCC [73], MMC [74], [75], LFC [58], and AGC and PMC [61]. Further, in [74] the authors analyzed three different types of delays in MMC-HVDC that, if caused by a cyber attack, can lead to a DoS. The considered attack points were sampling and data processing, signal modulation, and signal transmission. As for the previously discussed attacks, DoS attacks on HVDC systems can also create stability issues, outages, and appliance damage. It is particularly difficult to design and deploy effective countermeasures given the intrinsic nature of the attack.

4) CYBER THREAT SUMMARY AND KEY TAKEAWAYS

Even though the literature shows how FDIA attacks can be performed and the huge impact they can have on HVDC systems, such attacks are based on a number of assumptions on the attacker's ability. These assumptions include: (1) information access (i.e., full or local access, or blind), (2) spatial-temporal coordination ability, and (3) injection ability (i.e., unlimited or limited disturbance magnitude) [76]. Compared to FDIA, replay attacks are more realistic because they rely on the re-transmission of valid signals intercepted beforehand, thus, they do not require a complete knowledge of the targeted system. Still, they require the attacker to be able to monitor the data traffic and inject the replayed data, thus requiring access to and compromising other systems in the SCADA infrastructure. As discussed in [61], the crucial weakness enabling the successful injection of tampered data is the inherent lack of security in the IEEE C37.118 and IEC 61850 communication protocols. For this reason, it is crucial for the industry to upgrade its systems, adopt secure protocols, and adhere to standards like IEC 62351 which mandates the use of authenticated and encrypted communication.

According to the best of the authors' knowledge of the actual cyber attack on power grids, i.e., in the Ukrainian power grid cyber attacks in 2015 and 2016, the adversaries did not have comprehensive knowledge of power system operations. Therefore, the attack patterns are relatively random and do not target the most critical components, which potentially yield more severe impacts. In other studies [100], we have presented a cyber attack impact from a power system stability perspective. In [101], the authors presented that cyber attacks in power grids can accelerate cascading failure. The findings of these studies point out that cyber attacks involving power system knowledge can result in more severe impacts. Knowledge about cyber threats and power system operations is also crucial for formulating defense strategies against cyber attack. The effective mitigation of cyber threats necessitates a comprehensive understanding of the operational complexities of the power system, given the interdependent structure of these systems causes them fundamentally vulnerable to various disruptions. Furthermore, the integration of cybersecurity knowledge with a deep understanding of power system operations enables the development of more robust defense mechanisms. The robust defense mechanism should be able to reduce the likelihood of subsequent consequences, such as system-wide instability [100] and the acceleration of cascading failures [101].

B. CYBER DEFENSE

Most of the research on defense against cyber threats can be broadly classified into three groups: 1. Detection, 2. Mitigation and 3. Resiliency, as seen in Table 3. We define the individual defense mechanisms groups as follows:

1) **Detection**: Identify the attack by differentiating it from the normal behavior of the network e.g., intrusion detection system, anomaly detection.
2) **Mitigation**: In case of a successful attack, taking actions or responding to minimize the effect of the attack on the system and operation, e.g., incident response, backup and recovery, and security controls.
3) **Resiliency**: Taking suitable measures before an attack in order to cause minimum disruption and damage to the system, e.g., system hardening, zero trust, and awareness training.

In the following subsections, a literature survey of these defense strategies in the HVDC system are discussed.

1) DETECTION

Majority of the literature considers the detection of cyber attacks in an HVDC system using 3 techniques, i.e., threshold-based detection, data-driven detection, and model/rule-based detection as summarized in Table 3.

Hatton et al. [64] present two detection approaches to defend against spoofing attacks. The first method calculates the expected AC side current of the HVDC system by using its AC side voltage and the AC voltage just outside the terminals. If the difference between the predicted and measured AC side currents is above a predefined threshold, it is flagged as an attack. This method is shown to be capable of detecting the FDIA and replay attacks. The combined DC voltage & power measurement attack can also be easily detected by calculating the DC current using the voltage difference across the DC terminal. A mechanism for maintaining HVDC systems' power order commands security is proposed by Nuqui et. al [78]. The proposed method can detect inadvertent/insecure power order commands sent to the HVDC system at the right time

TABLE 3. Defense methods for cyber threats in HVDC system.

References	Detection	Mitigation	Resiliency
Hatton et. al [64]	Threshold based	-	-
Nuqui et. al [78]	Threshold based	-	-
Pan et. al [59]	Threshold based	-	-
Page et. al [79]	Threshold based	-	-
Hemmati et. al [80]	Threshold-based	-	-
Gholami et. al [62]	Threshold based	Injecting control for firewall	-
Burgos-Mellado et. al [66]	Threshold based	Inject estimated measurement	-
Hou et. al [76]	Threshold based	Inject control to adjust power	-
Sun et. al [57]	Data Driven	Inject control to adjust power	-
Qiu et. al [60]	Data Driven	Inject control to adjust power	-
Sun et. al [51]	Data driven	Inject control to adjust power	-
Roy et. al [61]	Data-driven	Inject estimated measurement	-
Chen et. al [71]	Data-driven, Model/Rule based	-	-
Yao et. al [81]	Model/Rule based	Inject control to adjust power	Model communication with physical layer
Hou et. al [82]	-	Inject estimated measurement	-
Cao et. al [74]	-	-	Model communication with physical layer
Cao et. al [75]	-	-	Model communication with physical layer.
Shen et. al [83]	-	-	Model communication with physical layer

and stop them from being executed while issuing an alarm. This method involves three stages as follows:

- The transmission lines' power flows resulting from a requested change in the power order command sent to the HVDC station are continuously estimated by using the concept of Power Transfer Distribution Factors (PTDF) [84].
- The possible effects of the received power order command are predicted based on the estimated transmission lines flow from the previous stage. The assessment considers threshold violations, voltage stability issues, harmonics, etc.
- If the requested change in the power order command is predicted to result in any unwanted security issues, its execution is stopped. Furthermore alarm is issued to inform the HVDC station and the grid control center operators.

Pan et al. [59] developed a residual generator with linear transfer operations capable of achieving a fast and accurate detection and isolation of such attacks. Page et. al [79] identify the potential cyber attacks on the measurements used by the HVDC control system. The proposed method uses the average model representation of HVDC systems [85] to calculate error vectors for DC current and voltage measurements. The measured values from the DC current and voltage at the rectifier and inverter sides are then compared with calculated error vectors. If the difference is above a certain threshold, the existence of a cyber attack can be detected. The simulation results presented in [79] show the effectiveness of the proposed approach in detecting the spoofing attacks on the HVDC system rectifier DC current and inverter DC voltage measurements.

Hemmati et. al [80] propose a multifunctional control mechanism for HVDC systems. This proposed control mechanism enables the HVDC system to provide ancillary services such as frequency and voltage regulation and Fault Ride Through (FRT) capability. A framework that enables this control mechanism to distinguish between fault and cyber attack conditions is also proposed in this paper. When a short circuit fault appears in the system, different system variables (e.g., AC and DC side powers, voltages, and currents) change according to Kirchhoff's Voltage Law (KVL) and Kirchhoff's Current Law (KCL) rules. On the contrary, when an attacker tries to modify one of these parameter values maliciously while neglecting its relations with other system parameters, the cyber attack can be easily detected by using control approaches such as the ones proposed in [80].

Gholami et. al [62] present a detection strategy using a predictive control-based approach. If the difference between predicted and measured active and reactive powers exceeds a pre-set threshold, the attack can be detected. Burgos-Mellado et. al [66] detect FDIA attacks by estimating the capacitor voltage magnitude using the previous timestamp values. This is achieved by a Kalman filter-based voltage estimation. This estimated value can then be compared with the measured voltage. If the difference between two values exceeds a certain threshold, then the attack can be detected. Hou et. al [76] detect the attack by checking the rate of frequency deviation and DC current value and comparing it with a threshold.

Sun et al. [57] propose a Squeeze- Excitation based double Convolution Neural Network (SE-DCNN) to defend against FDIA attacks on the grid frequency of HVDC systems. The proposed method is tested on different frequency FDIAs, including false oscillation attacks, scaling attacks, ramping attacks, playback attacks, and data interchange attacks. By running the simulations on a reduced model of the HVDC links between Spain and France considered in the INTerconexion ELectrica Francia-Espana (INELFE) project, it is shown that the developed method performs well in identifying different frequency attack types and time durations. The authors of [57] continued their work on developing defensive mechanisms against frequency FDIAs on the HVDC systems in [60] by proposing a novel method that utilizes the Hilbert Huang Transform (HHT) to decompose the system measurements into the Band-limited Mode Functions (BMFs) with Variational Mode Decomposition (VMD) algorithm. To automatically classify different types of frequency FDIAs on the HVDC systems (e.g., ramping attacks, scaling attacks, etc.), a Multi-kernel Support Vector Machine (MSVM) is also proposed. The K-means approach, which is a fast, unsupervised machine learning technique, is also used in the proposed defensive approach to calculate the attack duration time.

Sun et al. [51] propose a cyber attack detection framework using a special kind of artificial intelligence algorithm called Attack Shuffle convolutional neural Network (ASNet), which learns the intrinsic characteristics of cyber attacks on HVDC systems. First, a Continuous Wavelet Transform (CWT) method is used to extract the time-frequency features of the input measurements. The results obtained from the CWT are then used as inputs to the ASNet to identify the type of cyber attack. Continuous wavelet transforms, and ASNet is used to detect the attacks quickly. Roy et. al [61] proposed a Multi-Agent System to detect and neutralize cyber attacks targeting the Automatic Generation Control (AGC) and HVDC systems. The attack detection is performed centrally by a supervisory control agent, while the attack mitigation is decentralized by remote field agents installed at local HVDC stations and generating units. To detect the occurrence of a cyber attack at the supervisory control agent, the Support Vector Data Description classifier is utilized for anomaly detection, as it can detect unseen events while being trained just using the secure normal data.

In [71], Chen et. al state that HVDC applications typically rely on one or two-way communication links between the HVDC station and control center, nearby substations, and other control facilities. HVDC station configurations, including HVDC controller settings and parameters, are also usually transmitted to relevant control center applications for stability assessment purposes. These access points to HVDC stations increase the risk of potential cyber attacks targeting their performance.

HVDC systems can be used for different applications in power grids (such as Wide Area Damping Control (WADC), which is designed to reduce low-frequency interarea oscillations) by relying on the collected PMUs data through the Wide Area Measurement, Protection, and Control (WAMPAC) platform. Two different approaches are proposed in [71] to detect the occurrence of FDIAs targeting WAMPAC-based HVDC applications. In the first approach, a learning-based model capable of classifying between normal and attacked grid conditions is built using Extreme Learning Machine (ELM) theory. The collected PMU measurements (including voltage, current, and power phasors) are used as inputs to this model. The second detection approach proposed in [71] is actually a model-based method that considers the correlations between physical measurements obtained from PMU data. PMU data in a power grid are linked together and follow physical laws and circuit equations, such as Ohm's law and Kirchhoff's laws (KVL and KCL). Therefore, each measurement value can be predicted using others in the grid. This predicted value can then be compared with the actual measured one. If there is a considerable difference between these two quantities, the existence of an attack can be detected. The performance of the proposed detection methods by [71] is tested on a two-area system designed for analyzing HVDC systems WADC application. Yao et. al [81] detect the attack based on the timestamp and message hash code.

2) MITIGATION

In the case of mitigation, the literature focuses on injection control or estimated for detection. Gholami et. al [62] mitigate the attack by enabling or disabling the firewall gate. Burgos-Mellado et. al [66] mitigate the attack by compensating the untrustworthy voltage with voltage estimated by the Kalman Filter estimate. Hou et al. [82] propose an optimal cyber defense strategy for HVDC systems to reduce the grid frequency deviations resulting from manipulated measurements. It is assumed that an attacker is trying to increase the frequency deviations in the grid by attacking an HVDC station controller. The attacker does so by injecting a positive (if the pre-attack frequency deviation of the grid is positive) or negative (if the pre-attack frequency deviation of the grid is negative) value to the station controller. After the defender (e.g., the grid operator) detects the occurrence of the attack, they try to find an optimal sequence of corrective injections into the HVDC station controller to oppose the attacker and restore the grid frequency to normal, acceptable ranges.

This sequence of both cyber attacks and defense strategies is viewed as a multi-stage decision-making problem in [82], which is then transformed into a single-level Mixed Integer Quadratic Programming (MIQP) problem. The simulation results presented in [82] show that the proposed defense strategy can effectively restrict the frequency deviations (by preventing the frequency deviations from going beyond the ±0.5 Hz range) in the face of cyber attacks on a two-terminal point-to-point LCC HVDC system. Sun et al. [57] developed an SE-DCNN framework for defending against frequency FDIAs is also used to propose an HVDC control approach that is capable of suppressing the frequency attack impacts on the integrated AC/DC power grid. In case a cyber attack is detected, the mitigation algorithm sends control commands to adjust the current power flow back to the scheduled power flow. In [60] a Hybrid Data Driven (HDD)-based control framework for the HVDC system is proposed to defend against the attack and reduce the impact of the attack on the performance of the ancillary services provided by the HVDC systems. Sun et al. [51] developed a Wide area power oscillation and damping control (WH-PODC) framework to mitigate the effects of cyber attacks. Based on a type of attack identified by the detection algorithm, a suitable control strategy is activated, which modifies the power output of integrated cyber attack defense control and reanalyzes the Low-frequency oscillation model. Yao et. al [81] mitigate the attack by injecting control sequences when an attack is detected. The papers use Single input single output controlled autoregressive and moving average models for predictive control.

Roy et. al [61] the mitigation strategy developed uses the MAS remote field agents to generate alternative control signals when notified by the supervisory control agent in case of an attack. The remote field agents predict control signals using a data-driven Support vector regression model. Hou et. al [76] further propose an event-triggered cyber defense strategy to mitigate the effects of rapid frequency deviations caused by non-simultaneous cyber attacks on the MIDC system. The strategy involves coordinating compromised LCC HVDC systems and AC systems using a mixed-integer quadratic programming framework, which is solved online and updated when new cyber attacks occur.

3) RESILIENCY

Finally, a few other papers talk about the cyber resiliency strengthening of attacks by modeling communication layers and their effects on the physical system. Yao et al. [81] proposed a resilient wide-area damping control scheme for HVDC systems based on a Secure Networked Predictive Control (SNPC) mechanism. The paper models the cyber layer along with the physical layer to show the effects of deception attacks on the network. Along with deception attacks the paper also considers data modification, time delay, packet dropout, data replay, and data breach. The mechanism aims to ensure data confidentiality, integrity, and authenticity. Cao et. al in [74] and [75] investigated the importance of modeling the cyber-related components involved in the control system of MMC-HVDC systems for analyzing their stability margins. Specifically, the effects of measurement sampling and data processing delays, signal transmission delays, and PWM modulation procedure delays are incorporated into the state space model of the MMC- HVDC system. Then, two approaches based on Pade approximation in [74] and Rekasius substitution in [75] are proposed to derive the stability margins of the system. Through conducting simulation studies on a multi-terminal VSC-HVDC system in MATLAB/Simulink in these two papers, it is proved that the mentioned cyber delays can result in system instabilities and induce sub-synchronous oscillations (around 35 Hz) in the system variables. The findings of [74] and [75] are also interesting from the cyber security point of view, as the attackers can create stability issues in the system by conducting time delay attacks on the measurements used by the HVDC control system. Shen et. al [83] consider the communication failures in the wide-area control for inter-area oscillations. They propose a dynamic heuristic-based wide-area damping control mechanism to dampen inter-area oscillation in a Voltage source converter-based HVDC system. The model is able to perform damping control under one and two-channel communication failure without needing an accurate model of the physical layer.

4) CYBER DEFENSE SUMMARY AND KEY TAKEAWAYS

The current literature on cyber defense for HVDC systems highlights the importance of detection, mitigation, and resiliency strategies against cyber threats. Common detection methods, including threshold-based, data-driven, and model-based techniques, each have limitations. Threshold-based methods may miss subtle attacks, while data-driven approaches can struggle with novel threats. Model-based methods, though promising, require deep system knowledge. Mitigation strategies, often reactive, focus on corrective actions like adjusting system parameters, but there is a need for more proactive prevention measures.

Resiliency efforts, such as modeling cyber-physical interactions, aim to strengthen HVDC systems against attacks, but these models are often too complex and lack integration into system design. Embedding resiliency from the outset could help ensure both recovery and resistance to cyber threats. A holistic approach to cyber defense should bridge cybersecurity with system design to create a more robust defense framework.

Advances in AI and data-driven techniques offer new opportunities for cyber security but also present challenges, such as model poisoning and adversarial attacks. Future research should focus on developing AI systems that are transparent, explainable, and resilient while emphasizing proactive defense measures. The integration of adaptive, self-learning models into HVDC systems could significantly enhance their security against evolving threats.

C. HVDC CO-SIMULATION TESTBEDS

Power grids are a critical infrastructure that must meet stringent requirements for availability. Therefore, conducting tests and experiments on actual power grids is unfeasible. Therefore, CPS modelling and simulation are required to assess the system vulnerability and cyber attack impacts on the power system. Power system simulation can be integrated with IT/OT system simulation to create co-simulation. The co-simulation provides a more realistic result by considering both aspects of cyber and physical systems. The state-of-the-art power system modeling and co-simulation are presented in a number of survey papers that can be found in [1], [92], [93], [94], [95]. However, all of them are focused on general power systems rather than HVDC systems. Therefore, in this study, we specifically identify the state-of-the-art CPS co-simulation models for HVDC systems.

The state-of-the-art HVDC co-simulations are summarized in Table 4. The table summarizes the power system models used to simulate the HVDC system, tools for the power system simulator, and the IT/OT simulator. There are baseline power system models that have been modified by incorporating HVDC elements from 4 bus up to 118 bus models. The models are in line with current real-world power systems, which are primarily based on HVAC but are gradually incorporating HVDC technology. To simulate the power grids under the cyber attack scenarios, the state-of-the-art research uses various power system simulators. Some of these tools include MATLAB Simulink, Power Systems Computer Aided Design (PSCAD), Real-Time Digital Simulator (RTDS), and Piecewise Linear Electrical Circuit Simulation (PLECS). Among those power system simulators, MATLAB Simulink is the most popular power system simulator because of its versatility in model implementation.

TABLE 4. HVDC co-simulation testbed.

Ref.	Year	Power System Model	Power System Simulator	IT/OT Simulator
[67]	2023	Two-terminal MMC–HVDC system	MATLAB Simulink	-
[86]	2022	16-machines 68-bus with VSC based HVDC	MATLAB Simulink	-
[87]	2022	10-machine 39-bus onshore AC system	MATLAB Simulink	-
[88]	2022	two-area power grid with HVDC, HVAC, and energy storage	MATLAB Simulink	-
[81]	2021	16-machines 68-bus AC/DC hybrid power system	MATLAB Simulink	-
[75]	2021	-	MATLAB Simulink	Communication model
[77]	2021	IEEE 12-bus AC/DC test system	MATLAB Simulink	-
[74]	2021	-	MATLAB Simulink	-
[68]	2021	-	MATLAB Simulink	-
[80]	2021	Two-bus HVDC system	MATLAB Simulink	-
[89]	2020	16-machines 68-bus with VSC-based HVDC	MATLAB Simulink	-
[58]	2020	10-bus model with HVDC	MATLAB Simulink	-
[59]	2020	10-bus model with HVDC	MATLAB Simulink	-
[83]	2019	IEEE 39-bus system with HVDC	MATLAB Simulink	-
[90]	2014	IEEE 118-bus system	MATLAB Simulink	-
[62]	2019	IEEE 9-bus equipped with HVDC	MATLAB Simulink	-
[91]	2018	three-area IEEE 39-bus test system	MATLAB Simulink	-
[69]	2023	10-bus model with HVDC	PSCAD	-
[57]	2021	INELFE project model	PSCAD	-
[60]	2021	WECC and EI	PSCAD	-
[78]	2020	BPA Micro WECC	RTDS	-
[72]	2021	Kundur's two-area system	RTDS	Virtual PMU server and PDC
[51]	2023	-	RTDS	-
[66]	2022	-	PLECS	-
[64]	2019	4-bus test system	-	-
[71]	2020	Kundur's two-area system	-	-
[79]	2020	Bipole series multiterminal HVDC	-	-
[76]	2022	multi-infeed HVDC	-	-
[61]	2022	IEEE 39-bus system with HVDC	-	-
[63]	2023	IEEE 14 bus DC grid	-	-
[73]	2018	Modified IEEE 39-Bus AC-HVDC	-	-

However, from a fidelity standpoint, PSCAD and RTDS offer superior performance due to their electromagnetic transient capability. According to the literature review, the majority of research for HVDC systems omits cyber system simulations. Therefore, the cyber attack scenarios on HVDC systems are only based on the prior assumption when the adversaries successfully compromise the IT/OT system. Amongst them, some research has already integrated IT/OT systems into cyber attack scenarios in HVDC. In [75], the authors incorporate a communication model to assess the stability of the HVDC system. However, this work did not perform actual simulations of the HVDC CPS. Wide-area monitoring, protection, and control for HVDC cyber security were investigated in [72]. The OT simulation incorporates PMUs, PDCs, Intelligent Electronic Devices (IEDs), SCADA systems, and communication links. The OT devices are simulated using Raspberry Pi and virtual servers. Using the co-simulation, this research primarily focused on FDIA scenarios. The FDIA detection primarily focused on the analysis of simulated data samples and PMU measurements. Therefore, this implementation is not applicable for more advanced cyber attacks, i.e., Advanced Persistent Threat (APT). Based on our review of HVDC co-simulation for cyber security, we have derived the following summary and key points:

- The state-of-the-art cyber attack simulations on HVDC systems are based on the premise that the IT/OT system has been compromised, allowing the attackers to execute FDIA, Replay, or DoS attacks. The attack scenarios do not resemble the actual real-world cyber attack on power grids, i.e., Ukrainian power grids in 2015 [96], and 2016 [97]. Furthermore, the simulated cyber attacks do not comprehensively represent the stages of the cyber kill chain [98]. Therefore, the future co-simulation of cyber attack on HVDC systems should consider this constraint accordingly to improve the fidelity of the cyber attack scenarios.
- We identified there is very limited research on HVDC cyber security that implements the comprehensive co-simulation models. Despite the fact that the majority of the research presents a narrative about a cyber attack on an HVDC system, the studies are primarily concentrated on power systems simulation only. It is crucial to include IT/OT elements in order to create a more thorough simulation of cyber attacks. Therefore, future research should implement both cyber and physical HVDC systems to present more comprehensive cyber attack scenarios.

IV. CONCLUSION AND RECOMMENDATIONS

Section IV provides synthesizes the key findings from the analysis of HVDC systems and their associated cyber security challenges, as discussed in Sections II and III. It highlights the requirements for more robust security measures tailored to the unique vulnerabilities of HVDC systems. Building on the insights gained, we offer specific recommendations for future research and practical implementations, emphasizing the importance of early-stage threat detection, comprehensive defense mechanisms, and the integration of advanced co-simulation platforms to ensure the resilient operation of the HVDC system.

A. CONCLUSION

In this survey, cyber security for HVDC systems was investigated in three parts, including the cyber threats, defense, and testbeds. In the first part of the paper, we introduced HVDC cyber-physical systems and their components. Subsequently, the second part identified potential cyber threats on the HVDC system, i.e., FDIA, replay attack, and DoS attacks. In the third part, the state-of-the-art defenses for cyber attack on HVDC system were summarized into three categories, i.e., detection, mitigation, and resiliency. In the last part of the survey, the co-simulation testbeds for HVDC cyber security research were investigated.

According to the systematic literature review, the state-of-the-art cyber security research on HVDC systems can be summarized as follows:

1. The current cyber security research on HVDC systems only considers the later stage of the cyber kill chain after the adversaries successfully compromise the system, i.e., FDIA, replay attack, and DoS. The early phases of cyber kill chain have not been included in the state-of- the-art studies. Therefore, most of the research is only based on the prior assumption that the HVDC cyber attacks have already compromised the Operational Technology (OT) system. Rather than focusing on the latter phase of the cyber kill chain, the mitigation strategies should implement a defense-in-depth strategy. The defense-in-depth aims to investigate the attack processes represented in all stages of the cyber kill chain. Before the attack reaches an adverse level in the later phase of the cyber kill chain, i.e., commutation failure or possibly HVDC system disruption. Therefore, it would be preferable if the attack could be prevented at an early stage before resulting in adverse impacts. For example, the detection can be performed using an IDS. In our previous research [99], we proposed a communication-based IDS for detecting anomalies in the early stage of the cyber kill chain. This solution is potentially applicable for detecting anomalies in the HVDC cyber-physical system.
   Beyond conventional cyber attacks, the adversaries may have specialized domains of knowledge pertaining to the operation of the power system. With this information, adversaries can target inner layers of the grid control system using insider threats, weaponized malware, and exploiting access control and authentication mechanisms. In this case, the cyber attack may lead to a more severe impact from disturbing system stability and accelerating cascading failures. Consequently, it is imperative to not only detect the attack but also proactively prevent this form of attack. Beyond the detection, prevention mechanisms are also possible to be implemented. However, the implementation of prevention mechanisms is quite challenging as it has the potential to obstruct legitimate operations caused by false positives. Therefore, future research aims to minimize and mitigate false positive results to ensure that HVDC and HVAC systems are resilient.
2. The state-of-the-art cyber defense for HVDC system primarily focuses on the detection using data-driven and rule-based thresholds. For the mitigation, the research uses control injection for power adjustment. Meanwhile, some research proposes resiliency improvement through HVDC modelling and simulation. Based on the current trends, the mitigation only focuses on power system aspects and omits the cyber mitigation.
3. The current research is heavily focused on the modelling of the HVDC physical systems and does not incorporate the cyber element. Although existing research aims to provide a solution for cyber attacks on the HVDC, they actually only consider the physical element and consider cyber attacks based on assumptions.

B. RECOMMENDATIONS

Based on the aforementioned conclusions, recommendations and future research directions are outlined as follows:

1) INCORPORATE MORE REALISTIC AND ADVANCED CYBER ATTACKS ON HVDC SYSTEM

According to the literature, real cyber attacks are more complex and consist of seven stages which are called the cyber kill chain [98], [99]. These stages include reconnaissance, weaponization, delivery, exploitation, installation, command, and control. The current research does not consider the early stages and mainly focuses on the later stages of the cyber chain. Therefore, future research should pay more attention to the early stages of the cyber kill chain to stop the attack at the early stages and prevent more adverse impact on the HVDC system. In summary, the potential future research directions include 1) the implementation of comprehensive cyber threat intelligence and 2) the implementation of full-spectrum cyber kill chain attack scenarios using cyber range. A comprehensive cyber threat intelligence enables power system operators to anticipate potential attacks with a proactive defense posture, where vulnerabilities can be addressed before they are exploited. Meanwhile, the use of full-spectrum cyber kill chain attack scenarios through cyber ranges presents a critical opportunity for research and training. Cyber ranges simulate realistic attack environments, enabling researchers and security teams to test and refine their defense strategies across the entire stages of an attack. This comprehensive approach ensures that defenses are not only reactive but also robust across various stages of a cyber attack, providing a more resilient power system.

2) DEVELOP MORE EFFICIENT DEFENSIVE MECHANISMS

Although some of the researchers have already tried to propose cyber defense mechanisms for the HVDC systems in their works, more effort is still needed to develop better algorithms. That is because the performance of the current defensive approaches proposed in the literature are not validated for different operating conditions and configurations of the HVDC systems. Some of the proposed approaches are also not fast enough to be applicable for attack defense purposes in real-world HVDC systems applications. Furthermore, the currently proposed attack detection approaches generally cannot distinguish between cyber attacks and fault conditions in the system.

Furthermore, in order to develop an effective defensive mechanism, it is imperative to possess a comprehensive understanding of power system operations and cyber threats. A comprehensive understanding of cyber threats enables the implementation of defense measures at the first phase of the cyber kill chain, so effectively countering sophisticated attacks such as advanced persistent threats and zero-day attacks. Meanwhile, power system knowledge helps to avoid adverse impacts on the power system operation, including cascading failures and blackouts. Power system knowledge is also critical to formulating effective power system restoration strategies. These constraints are crucial for future research on the defense mechanism of cyber attacks on power grids.

3) INVESTIGATION ON PROTECTION SYSTEM VULNERABILITIES

While the majority of research has concentrated on the cyber security of HVDC control systems, there is a lack of exploration on the protection systems, especially the AC and potentially DC circuit breakers with their fault detection mechanisms. Although DC circuit breakers have not been implemented yet, it could be an important consideration for HVDC cyber security. These breakers rely on input measurements and trip signals to ensure safe operation. An attacker who gains access to these elements could manipulate or disable the system's fault protection, causing an adverse impact. Therefore, future research should prioritize investigating the vulnerabilities within these protection mechanisms to strengthen HVDC system security. In summary, the potential future research directions include 1) vulnerability assessment of fault detection mechanisms, 2) securing trip signals against spoofing attacks, 3) simulation and testing of cyber-physical attacks on protection systems, and 4) development of advanced intrusion detection systems to discriminate traffic anomalies caused by protection and anomalies cause by spoofing attacks.

4) IMPLEMENT MORE COMPREHENSIVE CO-SIMULATION FOR HVDC SYSTEMS

From the literature review, it can be seen that nearly all of the researchers validated their proposed cyber attack and defense mechanisms on small-scale or IEEE standard test systems. The main problem with this approach is that we cannot be sure about the applicability of the proposed method to real- world systems. One possible solution to overcome this limitation is to build digital twins of the hybrid AC/DC systems. Digital twins can be considered as one of the emergent concepts that provide a virtual clone of the power system which can be used to replicate its behavior, performance, and reaction to various operating conditions. One of the potential applications that can be expected from power system digital twins is to provide a safe and accurate representation of the system under study for conducting credible cyber attack and defense investigations. In summary, the potential future research directions include 1) the development of high-fidelity and comprehensive cyber-physical model for HVDC systems, 2) the integration of cyber-physical co-simulation with cyber range to validate cyber security mitigation mechanisms under realistic operating conditions, and 3) implementation of digital twin for enabling accurate modeling and analysis of system behavior and allowing for enhanced predictive maintenance, improved system optimization, and more effective risk mitigation against potential disturbances.

REFERENCES

[1] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.

[2] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electr. Power Syst. Res.*, vol. 215, Feb. 2023, Art. no. 108975.

[3] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6816–6827, Nov. 2018.

[4] A. S. L. V. Tummala and R. K. Inapakurthi, "A two-stage Kalman filter for cyber-attack detection in automatic generation control system," *J. Modern Power Syst. Clean Energy*, vol. 10, no. 1, pp. 50–59, Jan. 2022.

[5] M. Zhou, C. Liu, A. A. Jahromi, D. Kundur, J. Wu, and C. Long, "Revealing vulnerability of N-1 secure power systems to coordinated cyber-physical attacks," *IEEE Trans. Power Syst.*, vol. 38, no. 2, pp. 1044–1057, Mar. 2023.

[6] Y. Yang, G. Raman, J. C. Peng, and Z.-S. Ye, "Resilient consensus-based AC optimal power flow against data integrity attacks using PLC," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3786–3797, Sep. 2022.

[7] C. Tu, X. He, X. Liu, and P. Li, "Cyber-attacks in PMU-based power network and countermeasures," *IEEE Access*, vol. 6, pp. 65594–65603, 2018.

[8] F. Almutairy, L. Scekic, M. Matar, R. Elmoudi, and S. Wshah, "Detection and mitigation of GPS spoofing attacks on phasor measurement units using deep learning," *Int. J. Electr. Power Energy Syst.*, vol. 151, Sep. 2023, Art. no. 109160.

[9] S. De Silva, J. Kim, E. Cotilla-Sanchez, and T. Hagan, "On PMU data integrity under GPS spoofing attacks: A sparse error correction framework," *IEEE Trans. Power Syst.*, vol. 36, no. 6, pp. 5317–5332, Nov. 2021.

[10] V. S. Rajkumar, M. Tealane, A. Stefanov, and P. Palensky, "Cyber attacks on protective relays in digital substations and impact analysis," in *Proc. 8th Workshop Modeling Simulation Cyber-Phys. Energy Syst.*, Apr. 2020, pp. 1–6.

[11] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A unified deep learning anomaly detection and classification approach for smart grid environments," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1137–1151, Jun. 2021.

[12] X. Liang and M. Abbasipour, "HVDC transmission and its potential application in remote communities: Current practice and future trend," *IEEE Trans. Ind. Appl.*, vol. 58, no. 2, pp. 1706–1719, Mar. 2022.

[13] Z. Zhuo, N. Zhang, Q. Hou, E. Du, and C. Kang, "Backcasting technical and policy targets for constructing low-carbon power systems," *IEEE Trans. Power Syst.*, vol. 37, no. 6, pp. 4896–4911, Nov. 2022.

[14] M. Moradi-Sepahvand and T. Amraee, "Hybrid AC/DC transmission expansion planning considering HVAC to HVDC conversion under renewable penetration," *IEEE Trans. Power Syst.*, vol. 36, no. 1, pp. 579–591, Jan. 2021.

[15] K. Sun, H. Xiao, J. Pan, and Y. Liu, "VSC-HVDC interties for urban power grid enhancement," *IEEE Trans. Power Syst.*, vol. 36, no. 5, pp. 4745–4753, Sep. 2021.

[16] Y. Zhang, A. M. Shotorbani, L. Wang, and W. Li, "Distributed voltage regulation and automatic power sharing in multi-terminal HVDC grids," *IEEE Trans. Power Syst.*, vol. 35, no. 5, pp. 3739–3752, Sep. 2020.

[17] J.-S. Kim, J.-Y. Park, Y.-J. Kim, and O. Gomis-Bellmunt, "Decentralized robust frequency regulation of multi-terminal HVDC-linked grids," *IEEE Trans. Power Syst.*, vol. 38, no. 4, pp. 3279–3292, Jul. 2023.

[18] M. Langwasser, G. De Carne, M. Liserre, and M. Biskoping, "Primary frequency regulation using HVDC terminals controlling voltage dependent loads," *IEEE Trans. Power Del.*, vol. 36, no. 2, pp. 710–720, Apr. 2021.

[19] L. Peng, Y. Xu, A. Abolmasoumi, L. Mili, Z. Zheng, S. Xu, B. Zhao, Y. Tang, and W. Zhong, "AC/DC hybrid power system damping control based on estimated model predictive control considering the real-time LCC-HVDC stability," *IEEE Trans. Power Syst.*, vol. 39, no. 1, pp. 506–516, Feb. 2023.

[20] C. Guo, L. Xu, S. Yang, and W. Jiang, "A supplementary damping control for MMC-HVDC system to mitigate the low-frequency oscillation under low inertia condition," *IEEE Trans. Power Del.*, vol. 38, no. 1, pp. 287–298, Feb. 2023.

[21] Y. Li, H. Wang, and H. Yang, "A predictive control method for LCC HVDC participated black start with commutation failure prevention," *IEEE Trans. Power Del.*, vol. 38, no. 4, pp. 2348–2359, Jan. 2023.

[22] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering—A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, Jan. 2009.

[23] A. Pragati, M. Mishra, P. K. Rout, D. A. Gadanayak, S. Hasan, and B. R. Prusty, "A comprehensive survey of HVDC protection system: Fault analysis, methodology, issues, challenges, and future perspective," *Energies*, vol. 16, no. 11, p. 4413, May 2023.

[24] E. Taherzadeh, H. Radmanesh, S. Javadi, and G. B. Gharehpetian, "Circuit breakers in HVDC systems: State-of-the-art review and future trends," *Protection Control Modern Power Syst.*, vol. 8, no. 1, pp. 1–16, Dec. 2023.

[25] M. Radwan and S. Azad, "Protection of multi-terminal HVDC grids: A comprehensive review," *Energies*, vol. 15, no. 24, p. 9552, Dec. 2022.

[26] M. Muniappan, "A comprehensive review of DC fault protection methods in HVDC transmission systems," *Protection Control Modern Power Syst.*, vol. 6, no. 1, p. 1, Dec. 2021.

[27] U. Javed, N. Mughees, M. Jawad, O. Azeem, G. Abbas, N. Ullah, M. S. Chowdhury, K. Techato, K. S. Zaidi, and U. Tahir, "A systematic review of key challenges in hybrid HVAC–HVDC grids," *Energies*, vol. 14, no. 17, p. 5451, Sep. 2021.

[28] T. Abedin, M. S. H. Lipu, M. A. Hannan, P. J. Ker, S. A. Rahman, C. T. Yaw, S. K. Tiong, and K. M. Muttaqi, "Dynamic modeling of HVDC for power system stability assessment: A review, issues, and recommendations," *Energies*, vol. 14, no. 16, p. 4829, 2021.

[29] R. P. P. Smeets and N. A. Belda, "High-voltage direct current fault current interruption: A technology review," *High Voltage*, vol. 6, no. 2, pp. 171–192, Apr. 2021.

[30] M. Perez-Molina, D. Larruskain, P. E. Lopez, G. Buigues, and V. Valverde, "Review of protection systems for multi-terminal high voltage direct current grids," *Renew. Sustain. Energy Rev.*, vol. 144, Jul. 2021, Art. no. 111037.

[31] H. Zhou, J. Yuan, F. Chen, and B. Chen, "Inductive fault current limiters in VSC-HVDC systems: A review," *IEEE Access*, vol. 8, pp. 38185–38197, 2020.

[32] J. V. M. Farias, A. F. Cupertino, H. A. Pereira, S. I. Seleme, and R. Teodorescu, "On converter fault tolerance in MMC-HVDC systems: A comprehensive survey," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 6, pp. 7459–7470, Dec. 2021.

[33] A. Alassi, S. Bañales, O. Ellabban, G. Adam, and C. MacIver, "HVDC transmission: Technology review, market trends and future outlook," *Renew. Sustain. Energy Rev.*, vol. 112, pp. 530–554, Sep. 2019.

[34] M. A. Elizondo, R. Fan, H. Kirkham, M. Ghosal, F. Wilches-Bernal, D. Schoenwald, and J. Lian, "Interarea oscillation damping control using high-voltage DC transmission: A survey," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6915–6923, Nov. 2018.

[35] L. Zhang, Y. Zou, J. Yu, J. Qin, V. Vittal, G. G. Karady, D. Shi, and Z. Wang, "Modeling, control, and protection of modular multilevel converter-based multi-terminal HVDC systems: A review," *CSEE J. Power Energy Syst.*, vol. 3, no. 4, pp. 340–352, Dec. 2017.

[36] R. Fu, M. E. Lichtenwalner, and T. J. Johnson, "A review of cybersecurity in grid-connected power electronics converters: Vulnerabilities, countermeasures, and testbeds," *IEEE Access*, vol. 11, pp. 113543–113559, 2023.

[37] J. Hou, C. Hu, S. Lei, and Y. Hou, "Cyber resilience of power electronics-enabled power systems: A review," *Renew. Sustain. Energy Rev.*, vol. 189, Jan. 2024, Art. no. 114036.

[38] R. Nuqui, "Cyber attack resilient hvdc system (cards)(final scientific/technical report)," ABB Inc., Raleigh, NC, USA, Tech. Rep. DOE-ABB-000824, 2019.

[39] M. Jiang and H. Yu, "Alberta's experience of coordinating HVDC operation with under-voltage remedial action scheme," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–4.

[40] M. Wang, M. Abedrabbo, W. Leterme, D. V. Hertem, C. Spallarossa, and S. Oukaili, "A review on ac and DC protection equipment and technologies: Towards multivendor solution," in *Proc. CIGRE Winnipeg Colloq. Study Committees*, vol. 3, 2017, pp. 1–11.

[41] Y. Xu, Y. Yang, T. Li, J. Ju, and Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control systems," in *Proc. IEEE Conf. Energy Internet Energy Syst. Integr. (EI)*, Nov. 2017, pp. 1–6.

[42] W. Wen, R. Lyu, B. Li, H. Cao, J. Yu, B. Li, and M. Popov, "A soft start-up method for DC micro-grid based on improved two-level VSC with DC fault ride-through capability," *Frontiers Energy Res.*, vol. 11, Mar. 2023, Art. no. 1079099.

[43] G. P. Agrawal, *Fiber-Optic Communication Systems*. Hoboken, NJ, USA: Wiley, 2012.

[44] N. Singh, "Application of fiber optics for the protection and control of power systems," in *Optical To Terahertz Engineering*, vol. 1, no. 1. U.K.: Springer, Apr. 2023, pp. 101–120.

[45] S. Sarangi, B. K. Sahu, and P. K. Rout, "A comprehensive review of distribution generation integratedDCmicrogrid protection: Issues, strategies, and future direction," *Int. J. Energy Res.*, vol. 45, no. 4, pp. 5006–5031, Mar. 2021.

[46] V. S. Rajkumar, M. Tealane, A. Stefanov, A. Presekal, and P. Palensky, "Cyber attacks on power system automation and protection and impact analysis," in *Proc. IEEE PES Innov. Smart Grid Technol. Eur. (ISGT-Eur.)*, Oct. 2020, pp. 247–254.

[47] L. Liu, A. Lekic, and M. Popov, "Robust traveling wave-based protection scheme for multiterminal DC grids," *IEEE Trans. Power Del.*, vol. 38, no. 5, pp. 3117–3129, Apr. 2023.

[48] B. Luscan, S. Bacha, A. Benchaib, A. Bertinato, L. Chédot, J. C. Gonzalez-Torres, S. Poullain, M. Romero-Rodríguez, and K. Shinoda, "A vision of HVDC key role toward fault-tolerant and stable AC/DC grids," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 6, pp. 7471–7485, Dec. 2021.

[49] D. Roberson, H. C. Kim, B. Chen, C. Page, R. Nuqui, A. Valdes, R. Macwan, and B. K. Johnson, "Improving grid resilience using high-voltage DC: Strengthening the security of power system stability," *IEEE Power Energy Mag.*, vol. 17, no. 3, pp. 38–47, May 2019.

[50] S. Yang, H. Chen, P. Sun, H. Wang, F. Blaabjerg, and P. Wang, "Resilient operation of an MMC with communication interruption in a distributed control architecture," *IEEE Trans. Power Electron.*, vol. 36, no. 10, pp. 12057–12069, Oct. 2021.

[51] K. Sun, W. Qiu, Y. Dong, C. Zhang, H. Yin, W. Yao, and Y. Liu, "WAMS-based HVDC damping control for cyber attack defense," *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 702–713, Jan. 2023.

[52] F. M. Gonzalez-Longatt, J. M. Roldan, J. L. Rueda, C. A. Charalambous, and B. S. Rajpurohit, *Implementation of Simplified Models of Local Controller for Multi-terminal HVDC Systems in DIgSILENT PowerFactory*. Cham, Switzerland: Springer, 2014, pp. 447–472.

[53] L. M. Castro, J. H. Tovar-Hernández, N. González-Cabrera, and J. R. Rodríguez-Rodríguez, "Real-power economic dispatch of AC/DC power transmission systems comprising multiple VSC-HVDC equipment," *Int. J. Electr. Power Energy Syst.*, vol. 107, pp. 140–148, May 2019.

[54] J. Khazaei, P. Idowu, A. Asrari, A. Shafaye, and L. Piyasinghe, "Review of HVDC control in weak AC grids," *Electr. Power Syst. Res.*, vol. 162, pp. 194–206, Sep. 2018.

[55] M. F. M. Arani and Y. A. I. Mohamed, "Analysis and performance enhancement of vector-controlled VSC in HVDC links connected to very weak grids," *IEEE Trans. Power Syst.*, vol. 32, no. 1, pp. 684–693, Jan. 2017.

[56] B. J. Pierre, F. Wilches-Bernal, D. A. Schoenwald, R. T. Elliott, D. J. Trudnowski, R. H. Byrne, and J. C. Neely, "Design of the Pacific DC intertie wide area damping controller," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 3594–3604, Sep. 2019.

[57] K. Sun, W. Qiu, W. Yao, S. You, H. Yin, and Y. Liu, "Frequency injection based HVDC attack-defense control via squeeze-excitation double CNN," *IEEE Trans. Power Syst.*, vol. 36, no. 6, pp. 5305–5316, Nov. 2021.

[58] K. Pan, J. Dong, E. Rakhshani, and P. Palensky, "Effects of cyber attacks on AC and high-voltage DC interconnected power systems with emulated inertia," *Energies*, vol. 13, no. 21, p. 5583, Oct. 2020.

[59] K. Pan, E. Rakhshani, and P. Palensky, "False data injection attacks on hybrid AC/HVDC interconnected systems with virtual inertia—Vulnerability, impact and detection," *IEEE Access*, vol. 8, pp. 141932–141945, 2020.

[60] W. Qiu, K. Sun, W. Yao, W. Wang, Q. Tang, and Y. Liu, "Hybrid data-driven based HVdc ancillary control for multiple frequency data attacks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8035–8045, Dec. 2021.

[61] S. D. Roy, S. Debbarma, and J. M. Guerrero, "Machine learning based multi-agent system for detecting and neutralizing unseen cyber-attacks in AGC and HVDC systems," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 12, no. 1, pp. 182–193, Mar. 2022.

[62] A. Gholami, M. Mousavi, A. K. Srivastava, and A. Mehrizi-Sani, "Cyber-physical vulnerability and security analysis of power grid with HVDC line," in *Proc. North Amer. Power Symp. (NAPS)*, Oct. 2019, pp. 1–6.

[63] J. Hou, S. Lei, Y. Song, L. Zhu, W. Sun, and Y. Hou, "The cost and benefit of enhancing cybersecurity for hybrid AC/DC grids," *IEEE Trans. Smart Grid*, vol. 14, no. 6, pp. 4758–4771, Nov. 2023.

[64] J. Hatton, B. K. Johnson, D. Roberson, and R. Nuqui, "Increased grid resilience via cyber-secure VSC multiterminal HVDC systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2019, pp. 1–5.

[65] S. Sahoo, T. Dragicevic, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—Challenges and vulnerabilities," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5326–5340, Oct. 2021.

[66] C. Burgos-Mellado, F. Donoso, T. Dragicevic, R. Cárdenas-Dobson, P. Wheeler, J. Clare, and A. Watson, "Cyber-attacks in modular multilevel converters," *IEEE Trans. Power Electron.*, vol. 37, no. 7, pp. 8488–8501, Jul. 2022.

[67] A. Devnath, M. Rahman, and M. Rana, "Impact analysis of cyber-attack on MMC-HVDC control system with countermeasures," *Int. J. Dyn. Control*, vol. 12, no. 6, pp. 1952–1962, 2023.

[68] T. Ding, Z. Zeng, B. Qin, J. Zhao, Y. Yang, F. Blaabjerg, and Z. Dong, "Quantifying cyber attacks on industrial MMC-HVDC control system using structured pseudospectrum," *IEEE Trans. Power Electron.*, vol. 36, no. 5, pp. 4915–4920, May 2021.

[69] Q. Jiang, B. Li, T. Liu, F. Blaabjerg, and P. Wang, "Study of cyber attack's impact on LCC-HVDC system with false data injection," *IEEE Trans. Smart Grid*, vol. 14, no. 4, pp. 3220–3231, Jul. 2023.

[70] G. Zhang, J. Li, Y. Xing, O. Bamisile, and Q. Huang, "Data-driven load frequency cooperative control for multi-area power system integrated with VSCs and EV aggregators under cyber-attacks," *ISA Trans.*, vol. 143, pp. 440–457, Dec. 2023.

[71] B. Chen, S.-i. Yim, H. C. Kim, and R. Nuqui, "Cyber attack detection for WAMPAC-based HVDC applications," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo. (T&D)*, Oct. 2020, pp. 1–5.

[72] B. Chen, S.-i. Yim, H. Kim, A. Kondabathini, and R. Nuqui, "Cybersecurity of wide area monitoring, protection, and control systems for HVDC applications," *IEEE Trans. Power Syst.*, vol. 36, no. 1, pp. 592–602, Jan. 2021.

[73] R. Fan, J. Lian, K. Kalsi, and M. A. Elizondo, "Impact of cyber attacks on high voltage DC transmission damping control," *Energies*, vol. 11, no. 5, p. 1046, Apr. 2018.

[74] J. Cao, C. Dong, X. Yu, R. Wang, Q. Xiao, and H. Jia, "Modelling and stability assessment of the MMC-HVDC energy interconnected system with the cyber delay of communication network," *IET Energy Syst. Integr.*, vol. 3, no. 1, pp. 86–98, Mar. 2021.

[75] J. Cao, C. Dong, X. Yu, Y. Mu, Q. Xiao, and H. Jia, "Modeling and Rekasius substitution stability analysis of the multi-terminal MMC-HVDC cyber-physical system," in *Proc. IEEE Energy Convers. Congr. Expo. (ECCE)*, Oct. 2021, pp. 3388–3394.

[76] J. Hou, S. Lei, W. Yin, W. Sun, and Y. Hou, "Cybersecurity enhancement for multi-infeed high-voltage DC systems," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 3227–3240, Jul. 2022.

[77] A. A. Aljabrine, A. A. Smadi, Y. Chakhchoukh, B. K. Johnson, and H. Lei, "Resiliency improvement of an AC/DC power grid with embedded LCC-HVDC using robust power system state estimation," *Energies*, vol. 14, no. 23, p. 7847, Nov. 2021.

[78] R. Nuqui, H. Lee, A. Kondabathini, M. Overeem, and J. Barton, "Cyber secured power orders for resilient HVDC systems," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo. (T&D)*, Oct. 2020, pp. 1–5.

[79] C. L. Page, B. K. Johnson, D. Roberson, and R. Nuqui, "Increasing grid resilience via cyber-secure series multiterminal LCC HVDC transmission systems," in *Proc. 52nd North Amer. Power Symp. (NAPS)*, Apr. 2021, pp. 1–6.

[80] R. Hemmati and H. Faraji, "Multifunctional scheme for frequency/voltage/stability control in HVDC line under concurrent cyber-attacks and faults," *IET Gener., Transmiss. Distrib.*, vol. 16, no. 7, pp. 1334–1348, Apr. 2022.

[81] W. Yao, J. Nan, Y. Zhao, J. Fang, X. Ai, W. Zuo, J. Wen, and S. Cheng, "Resilient wide-area damping control for inter-area oscillations to tolerate deception attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4238–4249, Sep. 2021.

[82] J. Hou, S. Lei, W. Yin, C. Peng, and Y. Hou, "Optimal cyber defense strategy of high-voltage DC systems for frequency deviation mitigation," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Nov. 2020, pp. 1–5.

[83] Y. Shen, W. Yao, J. Wen, H. He, and L. Jiang, "Resilient wide-area damping control using GrHDP to tolerate communication failures," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2547–2557, May 2019.

[84] H. Ronellenfitsch, M. Timme, and D. Witthaut, "A dual method for computing power transfer distribution factors," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 1007–1015, Mar. 2017.

[85] J. Arrillaga, *High Voltage Direct Current Transmission* (IEE Power Engineering Series). no. 29. U.K.: The Institution of Electrical Engineers (IEE), 1998.

[86] Y. Zhao, W. Yao, C.-K. Zhang, X.-C. Shangguan, L. Jiang, and J. Wen, "Quantifying resilience of wide-area damping control against cyber attack based on switching system theory," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2331–2343, May 2022.

[87] Y. Zhao, W. Yao, C.-K. Zhang, X. Ai, and J. Wen, "Resilient wide-area damping control to mitigate strong cyber attack: A multiple-controller switching approach," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2326–2337, May 2023.

[88] Y. Jiang, S. Wu, H. Yang, H. Luo, Z. Chen, S. Yin, and O. Kaynak, "Secure data transmission and trustworthiness judgement approaches against cyber-physical attacks in an integrated data-driven framework," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 52, no. 12, pp. 7799–7809, Dec. 2022.

[89] Y. Zhao, W. Yao, J. Nan, J. Fang, X. Ai, J. Wen, and S. Cheng, "Resilient adaptive wide-area damping control to mitigate false data injection attacks," *IEEE Syst. J.*, vol. 15, no. 4, pp. 4831–4842, Dec. 2021.

[90] J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, and K. C. Sou, "Efficient computations of a security index for false data attacks in power networks," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3194–3208, Dec. 2014.

[91] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, "Attack detection and identification for automatic generation control systems," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4760–4774, Sep. 2018.

[92] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 446–464, 1st Quart., 2017.

[93] B. B. Gupta and T. Akhtar, "A survey on smart power grid: Frameworks, tools, security issues, and solutions," *Ann. Telecommun.*, vol. 72, nos. 9–10, pp. 517–549, Oct. 2017.

[94] M. Vogt, F. Marten, and M. Braun, "A survey and statistical analysis of smart grid co-simulations," *Appl. Energy*, vol. 222, pp. 67–78, Jul. 2018.

[95] J. Montoya, "Advanced laboratory testing methods using real-time simulation and hardware-in-the-loop techniques: A survey of smart grid international research facility network activities," *Energies*, vol. 13, no. 12, p. 3267, Jun. 2020.

[96] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *Proc. 70th Annu. Conf. Protective Relay Engineers (CPRE)*, Apr. 2017, pp. 1–8.

[97] M. J. Assante, R. M. Lee, and T. Conway, "ICS defense use case, no. 6: Modular ICS malware," SANS, USA, Tech. Rep., Aug. 2017, vol. 2, no. 1.

[98] E. M. Hutchins, M. J. Cloppert, and R. M. Amin. (Jul. 2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. [Online]. Available: https://www. lockheedmartin.com/content/dam/lockheed-Martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[99] A. Presekal, A. Stefanov, V. S. Rajkumar, and P. Palensky, "Attack graph model for cyber-physical power systems using hybrid deep learning," *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 4007–4020, Jun. 2023.

[100] I. Semertzis, A. Ştefanov, A. Presekal, B. Kruimer, J. L. R. Torres, and P. Palensky, "Power system stability analysis from cyber attacks perspective," *IEEE Access*, vol. 12, pp. 113008–113035, 2024.

[101] V. S. Rajkumar, A. Ştefanov, A. Presekal, P. Palensky, and J. L. R. Torres, "Cyber attacks on power grids: Causes and propagation of cascading failures," *IEEE Access*, vol. 11, pp. 103154–103176, 2023.

ALFAN PRESEKAL (Member, IEEE) received the bachelor's degree in computer engineering from Universitas Indonesia, in 2014, and the master's degree in secure software systems from the Department of Computing, Imperial College London, U.K., in 2016. He was an Assistant Professor of computer engineering with the Department of Electrical Engineering, Universitas Indonesia. He is currently a Researcher in cyber resilient power grids within the Intelligent Electrical Power Grids, Department of Electrical Sustainable Energy, Delft University of Technology. His main research interests include cyber security, cyber-physical systems, and artificial intelligence.

MOHSEN JORJANI (Member, IEEE) was born in Sari, Iran, in 1992. He received the Ph.D. degree in electrical power systems engineering from Tarbiat Modares University (TMU), Tehran, Iran, in 2022. Then, he joined Delft University of Technology, Delft, The Netherlands, as a Postdoctoral Researcher. His research interests include power system cyber security, operation, and control.

VETRIVEL SUBRAMANIAM RAJKUMAR (Graduate Student Member, IEEE) received the B.Eng. degree in electrical engineering from Anna University, India, in 2013, and the M.Sc. degree in electrical power engineering from Delft University of Technology, The Netherlands, in 2019. He is currently a Ph.D. Researcher with the Intelligent Electrical Power Grids Group, Department of Electrical Sustainable Technology, Delft University of Technology. His research interests include cyber security and resilience for power grids.

HIMANSHU GOYEL (Graduate Student Member, IEEE) received the bachelor's degree in electrical engineering from the University of Mumbai, and the Master of Science degree in electrical engineering from Indian Institute of Technology Madras, Chennai, India. He is currently pursuing the Ph.D. degree in cybersecurity for power systems with Delft University of Technology, Delft, The Netherlands. He has professional experience, including his work as an Engineer with Grid-Sentry and Rakuten Mobile Inc., Tokyo. His research interests include power systems optimization, cybersecurity, digital substation, machine learning, and smart power grids.

NICOLA CIBIN (Graduate Student Member, IEEE) received the B.Sc. degree in information engineering and the M.Sc. degree in telecommunications engineering from the University of Padua, Italy, in 2019 and 2021, respectively. After he was a Research Assistant with Aalborg University, Denmark, from 2021 to 2023. He joined as a Ph.D. Student the Cyber Resilient Power Grids (CRPG) Research Group, Delft University of Technology, The Netherlands. His research interests include telecommunication networks, cyber security, smart grids, and blockchain.

IOANNIS SEMERTZIS (Graduate Student Member, IEEE) received the Diploma degree in electrical and computer engineering from the Democritus University of Thrace, Greece, in 2019, and the M.Sc. degree in electrical power engineering from Delft University of Technology, Delft, The Netherlands, in 2021, where he is currently pursuing the Ph.D. degree with the Department of Electrical Sustainable Energy. His main research interests include cyber security, cyber-physical power systems, power system stability, and artificial intelligence for power system applications.

ALEXANDRU ŞTEFANOV (Member, IEEE) received the M.Sc. degree from the University Politehnica of Bucharest, Romania, in 2011, and the Ph.D. degree from University College Dublin, Ireland, in 2015. He is currently an Associate Professor of intelligent electrical power grids with the Department of Electrical Sustainable Energy, Delft University of Technology, The Netherlands. He is the Director of the Control Room of the Future (CRoF) Technology Centre. He is leading the Cyber Resilient Power Grids (CRPG) Research Group. He holds the professional title of Chartered Engineer from Engineers Ireland. His research interests include cyber security of power grids, resilience of cyber-physical systems, and next generation grid operation.

PETER PALENSKY (Senior Member, IEEE) received the M.Sc. degree in electrical engineering and the Ph.D. and Habilitation degrees from Vienna University of Technology, Austria, in 1997, 2001, and 2015, respectively. He co-founded an Envidatec, a German startup on energy management and analytics, and joined the Lawrence Berkeley National Laboratory, Berkeley, CA, USA, as a Researcher, and the University of Pretoria, South Africa, in 2008. In 2009, he was appointed as the Head of the Business Unit on Sustainable Building Technologies, Austrian Institute of Technology (AIT), and later the first Principal Scientist of complex energy systems with AIT. In 2014, he was appointed as a Full Professor of intelligent electric power grids with Delft University of Technology. He is active in international committees, such as ISO and CEN. His research interests include energy automation networks, smart grids, and modeling intelligent energy systems. He also serves as an IEEE IES AdCom Member-at-Large in various functions for IEEE. He is also the Editor-in-Chief of *IEEE Industrial Electronics Magazine* and an associate editor of several other IEEE publications and regularly organizes IEEE conferences.