Power System Stability Analysis from Cyber Attacks Perspective

Semertzis, Ioannis; Ștefanov, Alexandru; Presekal, Alfan; Kruimer, Bas; Torres, José Rueda; Palensky, Peter

DOI
10.1109/ACCESS.2024.3443061

Publication date
2024

Document Version
Final published version

Published in
IEEE Access

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

IEEE POWER & ENERGY SOCIETY SECTION

Received 10 July 2024, accepted 5 August 2024, date of publication 13 August 2024, date of current version 23 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3443061

SURVEY

Power System Stability Analysis From Cyber Attacks Perspective

IOANNIS SEMERTZIS[1], (Graduate Student Member, IEEE), ALEXANDRU ȘTEFANOV[1], (Member, IEEE), ALFAN PRESEKAL[1], (Member, IEEE), BAS KRUIMER[2], (Member, IEEE), JOSÉ LUIS RUEDA TORRES[1], (Senior Member, IEEE), AND PETER PALENSKY[1], (Senior Member, IEEE)

[1]Department of Electrical Sustainable Energy, Delft University of Technology, 2628 CD Delft, The Netherlands
[2]Digital Grid Operations, DNV Energy Systems, 6812 AR Arnhem, The Netherlands

Corresponding author: Ioannis Semertzis (i.semertzis@tudelft.nl)

This work was supported by the RESCUE Project funded by the Dutch Research Council under Grant NWO ESI.2019.006.

ABSTRACT Power grid digitalization introduces new vulnerabilities and cyber security threats. The impact of cyber attacks on power system stability is a topic of growing concern, which is yet to be comprehensively analyzed. Traditional power system stability analysis is based on the impact of non-malicious small, and large physical disturbances. However, cyber attacks introduce a new dimension to power system stability, in which malicious cyber actors can selectively target critical systems and applications and cause severe stability issues. Hence, in this work, the traditional disturbances considered in power system stability classification are expanded from physical to cyber-physical disturbances caused by cyber attacks. Based on a thorough state-of-the-art, an analysis of how cyber attacks can translate into physical disturbances affecting the traditional power system stability categories is performed. The system stability analysis is expanded by mapping the power system stability categories with the defined cyber-physical attack types. The findings of this work showcase the importance of cyber security for power system stability.

INDEX TERMS Cyber-attacks, cyber security, cyber-physical power systems, power system stability, resilience, smart grid.

ACRONYMS

AGC	Automatic Generation Control.
AI	Artificial Intelligence
AVR	Automatic Voltage Regulator
CPPS	Cyber-Physical Power System
CVE	Common Vulnerability Exposure
DNP3	Distributed Network Protocol 3
DoS	Denial of Service
EMS	Energy Management System
FACTS	Flexible Alternating Current Transmission System
FDI	False Data Injection
GOOSE	Generic Object-Oriented Substation Event
GPS	Global Positioning System
HMI	Human-Machine Interface
HVDC	High Voltage Direct Current
ICCP	Inter-Control Communications Protocol
ICS	Industrial Control System
IDS	Intrusion Detection System
IEDs	Intelligence Electronic Devices
IPS	Intrusion Prevention System
IT	Information Technology
MAC	Message Authentication Code
MitM	Man-in-the-Middle
ML	Machine Learning
MMS	Manufacturing Messaging Service
OSI	Open Systems Interconnection
OT	Operational Technology
PDC	Phasor Data Concentrator
PMU	Phasor Measurement Unit
RES	Renewable Energy Source

The associate editor coordinating the review of this manuscript and approving it for publication was Elizete Maria Lourenco.

RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SQL	Structured Query Language
SV	Sampled Values
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WAMPAC	Wide Area Monitoring Protection and Control

I. INTRODUCTION

Electrical power systems are experiencing an unprecedented evolution in terms of achieving the energy transition. Digitalization aims to transform the traditional power grids into advanced Cyber-Physical Power Systems (CPPS), providing new communication and computational capabilities to address the growing complexity of future power systems operation. Consequently, Operational Technology (OT) communication networks are deployed for real-time monitoring and control of the physical power system in substations and control centers, ensuring the stability of the physical power system. In the OT domain, Information Technology (IT) solutions are being integrated to enhance the operational capabilities of the local control and monitoring units. The overall OT communication network is connected with the conventional IT business network, although segregated by utilizing firewalls and demilitarized zones.

Power grid digitalization introduces new vulnerabilities and cyber security threats. The lack of security measures like encryption and authentication in the Industrial Control System (ICS) standard protocols, e.g., IEC 61850 and Modbus, makes the OT communication networks vulnerable to cyber attacks originating from the IT network [1]. Today's OT protocols often lack cyber security mechanisms, which cannot be easily implemented due to operational latency constraints and legacy hardware. Due to their sheer size and complexity, the CPPSs are more vulnerable to cyber actors, as the attack surface is vast. Cyber attacks targeting critical ICS infrastructure have significantly increased during the past decade. This trend can be seen in Fig. 1, showing reported attacks on ICSs, ranging from individual industrial complexes to power systems [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13]. The cyber-physical interdependency of CPPS, i.e., centralized and decentralized monitoring and control applications for grid operations, enables malicious actors to target power system operation.

Cyber attacks on power system control and protection are of significant interest. Power system stability is achieved through multiple control and protection systems, which need to operate in a coordinated manner. These cyber attacks can vary in magnitude and can be local or distributed. Additionally, the impact of such attacks on CPPS depends on the vulnerabilities and resilience of the physical power system. Attacks on an already stressed power grid could easily result in an unstable operation, leading parts of the grid to collapse. Thus, the impact of cyber attacks on power system stability is a topic of growing concern for system operators, which is yet to be comprehensively analyzed.

Power system stability is classified into rotor angle, voltage, frequency, resonance, and converter-driven on short and long-term, subject to small and large-signal physical disturbances [14]. However, cyber security introduces a new dimension to power system stability disturbances, as attackers can target the physical power grid through the communication layers of the CPPS. Given the rising threat of cyber attacks on critical ICS infrastructures, including electrical power grids, there is a pressing need to understand the impact of these attacks on power system stability. Furthermore, it is necessary to expand the current scope of system stability studies by analyzing how cyber-physical interactions affect the physical mechanisms of each stability category. Thus, this work provides an extended power system stability analysis, assessed from cyber attacks perspective.

A. RELATED WORK

Cyber security of power grids has been an important research topic in the past decade. Additionally, power system stability is a topic of advanced research effort, as energy transition challenges the current practices and requires a complete transformation of the existing power grids. New technologies like Renewable Energy Sources (RES), power electronics, and advanced control algorithms introduce new challenges and solutions to the traditional power system stability analysis problem. As stated in [15], the rise of CPPS introduces the challenge of how such systems can be modeled and how the traditional analysis, which focuses solely on the physical power system, can be enhanced by the presence of the cyber layer. Still, research on the impact of cyber attacks on power system stability has attracted attention quite recently.

Table 1 shows a summary of previous survey papers on the topics of power system stability, CPPS modeling, and cyber security studies in the context of electrical power systems. There are many surveys regarding power system stability, ranging from applications of Machine Learning (ML), modeling approaches, and metrics [16], [17], [18], [19]. The majority of existing work focuses on enhancing the stability assessment methods and researching their applicability to the concept of dynamic security assessment. In all related work, the importance of real-time stability and security assessment is pivotal, as the current and future challenges of power system operation cannot be addressed with existing methods. The reviewed studies are not focused on the cyber security of power systems.

In [20], the authors identified that the existing CPPS testbeds are mostly simulation-based due to their ability to expand economically. In [21], researchers conducted a survey on the cyber security of inverter-based power systems. As stated before, the integration of inverter-based RES has reduced the overall system inertia, affecting system stability and power quality. The study covers a range of topics, from the structure of the future smart grids to detection and

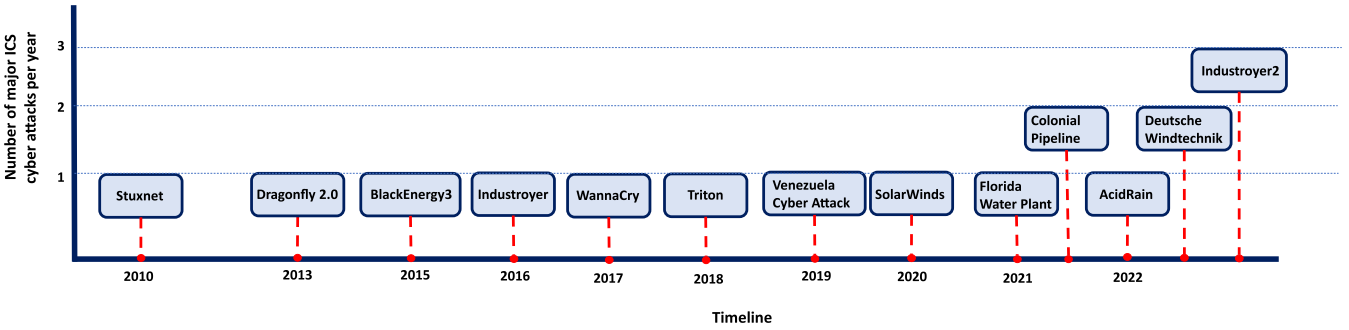

FIGURE 1. Timeline of major cyber attacks targeting critical industrial infrastructures [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13].

mitigation strategies for cyber attack types, but not power system stability. In [22], the authors conducted a survey to assess the validity of CPPS models for cyber security applications. The focus was on CPPS modeling, and although power system stability was highlighted as an issue, the survey focused on other research directions.

In [23] and [24], the authors reviewed the features and tools for co-simulation methods in the context of smart grids. In both reviews, the criteria for the co-simulating models were assessed, along with the research areas. In [23], the focus was on co-simulation approaches for cyber security studies, while [24] covered many research directions in the context of smart grids. Studies [25] and [26] focused on Supervisory Control and Data Acquisition (SCADA) systems in the context of future power grids. The cyber-physical system testbeds were reviewed and investigated by the tools and techniques to uncover vulnerabilities. Additionally, the requirements, constraints, and applications of these testbeds were analyzed. In [26], intrusion detection methods for SCADA systems utilizing Artificial Intelligence (AI) methods are analyzed, focusing on the methodologies, datasets, and testbeds that are used. In this study, different cyber-physical models for ICSs were reviewed aside from power systems.

As renewable energy sources are a vital part of future power systems, researchers focused on CPPS models with high penetration of wind and solar. Surveys investigated cyber security on wind and photovoltaic systems, as well as microgrids [27], [28], [29]. In [27], a review of the integration of power electronics-interfaced renewable energy sources and the emergence of CPPSs is conducted. Regarding cyber security, the paper presented the emerging research objectives and techniques for integrating communication networks with power system simulations to create CPPS testbeds. In [28] security of photovoltaic systems is discussed, while the research on microgrid cyber security is presented in [29].

In [30], the authors focused on the cyber security of Intelligent Electronic Devices (IEDs) of power substations. The possible cyber attacks are reviewed, along with countermeasures. As in the case of the studies described above, the impact of cyber attacks on power system stability is mentioned, mainly in the cases of measurement manipulation attacks and time-delay attacks. Finally, in [31], a review of the smart grid security, emphasizing the aspects of situational awareness, is conducted. A threat modeling framework is proposed, and the cyber attacks on CPPS are reviewed based on their impact. The paper focuses on threat detection and defense capabilities, such as intrusion detection systems, moving target defense, co-simulation techniques, and impact assessment of cyber attacks through situational awareness and power system metrics. Overall, to the best of the authors' knowledge, there are no similar review papers covering the impact of cyber attacks on power system stability. Furthermore, the implications of cyber security on power system stability are not covered in the existing stability definitions.

B. CONTRIBUTIONS

In this work, based on a thorough state-of-the-art, the impact of cyber attacks on each category of power system stability is assessed. An analysis of how cyber attacks can translate into physical disturbances affecting the traditional power system stability categories is performed. It is important to note that the aim of this work is not to modify the power system stability classification proposed in [14]. In this paper, the traditional disturbances considered in power system stability classification are expanded from physical to cyber-physical disturbances caused by cyber attacks.

The differences between this work and previous studies are summarized in Table 1. The presented research papers are selected considering the following research questions:

1) How to model cyber attacks for power system stability studies?
2) What are the critical OT systems for each stability category, and how can they be exploited by cyber actors?
3) How can cyber attacks cause physical disturbances that lead to system instability?

To address these questions, an advanced literature survey is conducted. The search terms used were "cyber attacks," "power system stability," and "impact assessment," among others. The reviewed studies are categorized based on the type of system stability and cyber attacks considered. The key contributions of this paper are summarized below:

- A comprehensive state-of-the-art review on cyber security for cyber-physical power systems is conducted. The current modeling approaches and limitations for

TABLE 1. Summary and comparison with relevant surveys.

Ref.	Stability studies	CPPS modelling	Target identification	Cyber attack types	Cyber attack impact on stability	Mapping of cyber attacks to stability categories	Remarks
[16]	✓	✗	✗	✗	✗	✗	Review of ML applications for stability studies in power systems.
[20]	✗	✓	✗	✗	✗	✗	Review on CPPS testbed architectures.
[21]	✗	✓	✓	✗	✗	✗	Review focusing on cyber security challenges of inverter-based power systems.
[22]	✗	✓	✓	✓	✗	✗	Review on CPPS modelling, focusing on cyber security.
[23]	✗	✓	✓	✓	✗	✗	Systematic review of features and tools for co-simulation on SG.
[27]	✗	✓	✗	✓	✗	✗	Review on modeling and cyber security challenges of power electronics-interfaced CPPS.
[30]	✗	✗	✓	✓	✓	✗	Review on cyber attacks on IEDs.
[31]	✗	✗	✓	✓	✗	✗	Review situational awareness of SG.
Current paper	✓	✓	✓	✓	✓	✓	Review and mapping of cyber attacks on each power system stability category.

considering the whole CPPS for stability studies are presented. Furthermore, the CPPS cyber vulnerabilities, which can be exploited by cyber actors, are identified.

- A state-of-the-art review on the impact analysis of cyber attacks on power system stability is performed. For each category of the existing classification of power system stability, e.g., rotor angle, voltage, frequency, resonance, and converter-driven, the effects of various cyber attacks are assessed. Furthermore, the most critical components and systems of the CPPS are identified.
- Each physical power system stability category is mapped with defined cyber-physical attack types. Based on a thorough impact analysis study, the cyber attacks that physically impact each stability category are classified into measurement manipulation, induced communication delays, and malicious command injection attacks. Thus, power system stability analysis is expanded by considering cyber-physical disturbances caused by cyber attacks.

C. PAPER STRUCTURE

The paper is organized as follows. Section II gives an overview of the structure of CPPS, the types of power system

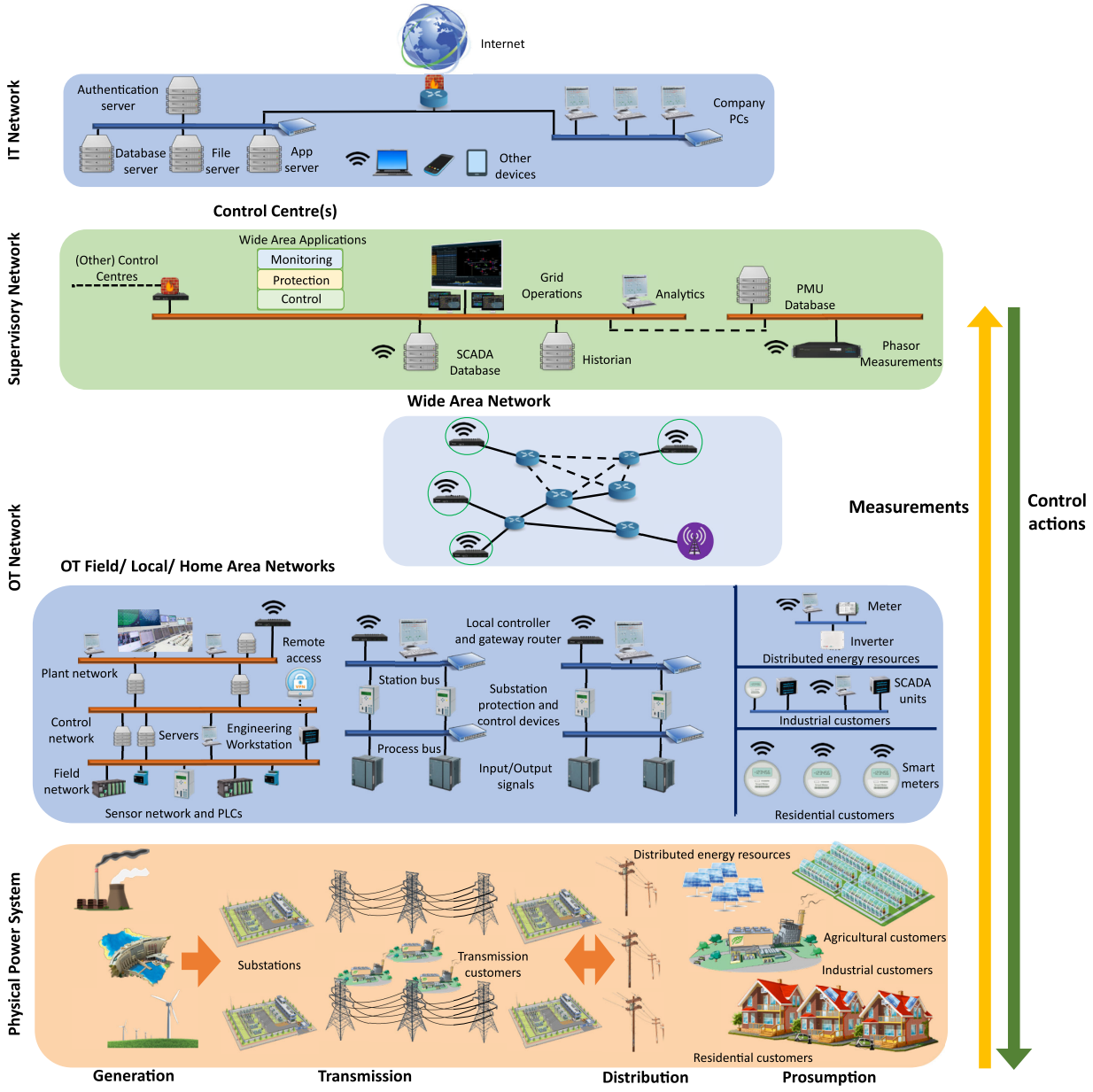

FIGURE 2. Cyber-physical power system representation.

stability mechanisms, and the modeling considerations for power system stability analysis considering the CPPS. In Section III, the cyber security vulnerabilities of the CPPS are presented, as well as the most prominent cyber attacks for cyber-physical impact. Section IV presents the findings and the analysis of the thorough state-of-the-art impact assessment of cyber attacks on power system stability. A discussion of the findings, along with research recommendations, is given in Section V, while the conclusion of this work is given in Section VI.

II. CYBER-PHYSICAL POWER SYSTEM AND STABILITY

CPPSs are complex systems that result from the integration of the cyber layer with the physical power grid. The term is used to describe the transformation of traditional power systems due to the integration of sensors, measurement units, communication networks, smart automation systems, and computational units. The high heterogeneity of devices and elements characterizes these interconnected networks. On the one hand, the advanced monitoring, communication, and control capabilities of CPPSs enable the optimization of future power grids, making them efficient, flexible, and reliable. On the other hand, the physical power system operation relies on the proper operation of its communication network. Communication failures or cyber attacks could physically impact the power grid's operation, especially with communication network-based Wide-Area Monitoring Protection and Control (WAMPAC) applications. The CPPS modeling

approaches, analysis, and classification of the models are covered extensively in [15], [16], [27]. This work focuses mainly on CPPS modeling approaches utilized for stability assessment, the differences between physical power system stability and CPPS stability, and the necessary interdependencies between the cyber and physical systems that need to be considered.

A. CYBER-PHYSICAL POWER SYSTEM OVERVIEW

Researchers usually consider two layers of the CPPS: the physical layer and the cyber layer. The physical layer is comprised of the physical assets of the power system, e.g., power and metering transformers, power lines, generating units, loads, and power electronic interfaces. It encapsulates all or selected aspects of power systems: *generation*, *transmission*, *distribution*, and *prosumption*. In this work, the term prosumption is used to describe grid connections with electrical power production and consumption capabilities, considering the presence of distributed energy sources on medium- and low-voltage networks. Given the scope of studies and considering the complexity, CPPS grid sizes can vary significantly, from smart homes to a national or regional transmission system.

The term cyber layer is either assessed as a single layer comprising the monitoring, control, communication, and application layers or divided into domain-specific layers. For instance, in [32], the authors defined three layers: the physical, cyber, and connection layers. The latter comprised the wide-area monitoring, protection, and control system. In [33], the layers that are described are the decision layer, communication and coupling layers, and the physical layer. The modeling and analysis of the communication layer of the CPPS requires a proper understanding of the different characteristics of the OT and IT layers, as well as the cyber security design paradigms and requirements for each.

A generic representation of the CPPS and its relations is given in Fig. 2. Considering the whole power system infrastructure, ranging from power plants to residential customers as the physical system, the network of sensors and actuators present in the field, local and home area networks are the first level of the Purdue model [34]. Depending on the facility, the level of automation and control capabilities may vary, but overall, the local control and monitoring capabilities fall in the second and third layers. On top of these localized networks, a complex and non-secure Wide Area Network is used for data transmission between geographically distributed networks, relaying measurements to the regional control centers. Wide area applications for monitoring, protection, and control are implemented, while historian servers and databases are used for data handling. A variety of Energy Management System (EMS) applications are used, like state estimation, remedial action schemes, optimal power flow, etc., based on wide-area measurements. Finally, separated from the OT supervisory and control networks through the utilization of firewalls and demilitarized zones stands the business IT networks. IT networks are the top levels of the Purdue model and, in the past, were completely segregated from the OT networks. However, considering the new requirements for interconnectivity, these environments have connections that need to be considered, especially for cyber security studies.

B. POWER SYSTEM STABILITY CATEGORIES

Based on the definitions provided in [14] and [35], the stability of the physical power system can be categorized into certain classes. These are rotor angle stability, voltage stability, frequency stability, converter-driven stability, and resonance stability.

1) ROTOR ANGLE STABILITY

Rotor angle stability describes the ability of a power system to maintain the balance of synchronous generators' mechanical and electrical torques after they are subjected to a disturbance [35], [36]. If the difference between the torques is nonzero, generators can experience angular swings, leading to loss of synchronism. This stability phenomenon is system-wide, and a potential loss of synchronism usually occurs within seconds after the initial disturbance. Stability is influenced by the nonlinear characteristics of the power system, namely the power-angle relationship. Typically in literature, rotor-angle instability is characterized as either small-disturbance or large-disturbance.

Small-disturbance rotor angle stability is concerned with the power system's ability to maintain synchronism under small disturbances. This kind of stability depends on the initial operating state of the system. For power systems with high penetration of RES, instability issues will be encountered due to the lack of damping torque [14]. Following a small disturbance or a change in topology, an unstable system is characterized by a complex conjugate pair of poorly damped eigenvalues of the linearized system state matrix. This stability issue can be either local or global in nature. Local stability problems, or local plant mode oscillations, are usually associated with the rotor angle oscillations of a single power plant against the rest of the system, while global problems are caused by the interactions between large groups of generators with each other. Such oscillations between different groups of generators are called interarea mode oscillations.

Large disturbance rotor angle stability is concerned with the ability of the power system to maintain synchronism when subjected to a severe disturbance, e.g. short-circuit on a transmission line. The system response is influenced by the nonlinear power-angle relationship and, in the case of severe disturbances, results in large rotor angle excursions. Large disturbance stability depends on the pre-disturbance state of the system and the magnitude of the disturbance. For small, simplified power system models, instability is usually related to the first swing instability due to insufficient synchronizing torque. On the other hand, in larger power systems, instability may be a result of the superposition of slow interarea swing modes and local-plant swing modes, causing a large excursion of rotor angle beyond the first swing.

2) VOLTAGE STABILITY

Voltage stability describes the ability of a power system to maintain voltages close to nominal value at all buses in the system after being subjected to a disturbance from a given initial operating point. This stability category mainly depends on the ability of the combined generation and transmission systems to provide the power requested by loads. Voltage instability occurs in the form of progressive fluctuation of voltages of some buses. This could result in local or regional loss of load, tripping of transmission lines, or other elements by their protection schemes, which may lead to cascading failures. It is important to mention that voltage stability issues could result in additional instability issues, such as rotor angle instabilities and loss of synchronism of generators. Historical outages and blackouts were influenced heavily by voltage instability [37]. Voltage collapse is an important consideration for voltage stability studies, as it describes the process by which a sequence of events can lead to blackout or extremely low voltages in a large part of the power system.

Voltage instability is mainly caused by the loads' reaction to a disturbance. It can occur when the capability of the transmission network and connected generation is not sufficient to restore the loads. Reactive power demand is the main consideration for voltage stability, which can cause both undervoltage and overvoltage issues. An additional consideration, especially in the case of interconnected transmission systems, is that voltage stability problems may also be experienced at the terminals of High Voltage Direct Current (HVDC) links. Such issues can arise due to the reactive power ''load'' characteristics of the converters when HVDC links are used to connect weak AC transmission systems. Such phenomena are fast, with a timeframe of up to one second. Voltage stability is usually characterized as small-disturbance and large disturbance, as in the case of rotor angle stability.

Small disturbances are usually considered to be small perturbations, such as incremental changes in system load. Voltage stability studies, as such, are influenced by the characteristics of loads, continuous controls, and discrete controls at a given instant of time. Large disturbance voltage stability refers to the system's ability to maintain steady voltages following large disturbances such as system faults, loss of generation, or circuit contingencies. This ability is determined by the system and load characteristics and the interactions of both continuous and discrete controls and protections. The study period of interest may extend from a few seconds to tens of minutes. Therefore, voltage stability may be either a short-term or a long-term phenomenon.

Short-term voltage stability involves dynamics of fast-acting load components such as induction motors, electronically controlled loads, HVDC links, and inverter-based generators. The study period of interest is in the order of several seconds, and analysis requires a solution of appropriate system differential equations, as in the case of rotor angle stability. In addition, for short-term voltage stability, the dynamic modeling of loads is essential. On the other hand, long-term voltage stability is influenced by slower-acting equipment, such as tap-changing transformers, thermostatically controlled load, and generator current limiters. This analysis is conducted in a study period of several minutes, and long-term simulations are required for the analysis of system dynamic performance. Instability can occur due to the loss of long-term equilibrium of consumption and power generation, the post-disturbance steady-state operating point being small-disturbance unstable, or when remedial actions are applied too late, leading to instability and possibly cascading failures.

3) FREQUENCY STABILITY

Frequency stability refers to the ability of the power system to maintain the frequency margins within acceptable limits following a severe disturbance. Such disturbances could result in a significant imbalance between generation and consumption. Severe contingencies can result in significant effects on system variables, which in turn invoke the actions of controllers and protection schemes. As the power system is controlled and protected by a plethora of various devices and schemes, evaluating the frequency stability of the system requires the integration of many control and protection models that are usually not considered in the conventional rotor angle stability and voltage stability studies. The responses of these systems can cover an expanded timeframe. The characteristic times of the processes utilized for control and protection range from seconds, such as under-frequency load shedding and interface protection of generating units, to several minutes, corresponding to the response of devices such as governor systems and load voltage regulators. Power system splitting is also an important aspect considered in this stability category. Frequency stability problems are associated with inadequacies in equipment responses, poor coordination of control and protection equipment, or insufficient generation reserve. Additionally, they can be decisively influenced by power electronics-interfaced generating units, given their frequency control schemes and the reduced inertia of the whole system.

Frequency stability studies are classified as short-term or long-term. For the former, a severe contingency could cause the disconnection of a part of the system from the rest of the grid. Regarding long-term studies, steam turbine speed control, and slower control and protection schemes, e.g., boiler operation, could cause instability in the long term, with the timeframe being from many seconds to several minutes. As in the case of rotor angle and voltage stability, frequency instability can lead to cascading failures and potential blackouts.

Both in the current and the future power grids, the control and protection schemes design, operation, and coordination play an important role in frequency stability. As these control schemes operate based on complex communication and control frameworks, both in a centralized and decentralized manner, the proper operation of the communication networks is essential.

4) CONVERTER-DRIVEN STABILITY

The controls of the converter-interfaced generators can result in couplings between the electromechanical dynamics of machines with electromagnetic transients in the network, leading to unstable oscillations in a wide frequency range. This is due to the voltage-source converter interface that is used for connection with the grid. This category of stability is further categorized based on the frequencies of the stability phenomena. Slow interaction phenomena occur for frequencies below 10 Hz, while fast interaction phenomena can occur with a frequency of many Hz or kHz.

Instability phenomena with low frequencies are classified as slow-interaction converter-driven stability. Although they can be similar to the ones caused by voltage instability, the mechanisms behind the instability are not the loads but the power electronic converter controls. This type of instability is driven by the dynamic interactions of the control systems of the power electronics-based devices with slower response components, such as the conventional control systems of synchronous generators, which result in low-frequency oscillations. An additional consideration is about the strength of the grid, as weak systems are more prone to this kind of instability. On the other hand, fast interaction instabilities can arise from the interactions between the fast inner loops of converter-interfaced systems controls such as generating units, HVDC, and Flexible Alternating Current Transmission Systems (FACTS) with fast-response components such as the transmission network, stator dynamics of synchronous machines, or other power electronic-based devices. The oscillations between the inner loops and the passive components can cause oscillations with frequencies up to many kHz. The placement of the power electronics-connected systems can influence such oscillations, as the high-frequency switching actions can lead to high-frequency oscillations. Additionally, these interactions can be facilitated by the connection with the main grid. These oscillations require active damping strategies in order to be mitigated. It is noted in [38] that synthetic inertia controllers are a key piece for such problems, as it is found that either they will trigger super-synchronous stability problems or can mitigate them.

5) RESONANCE STABILITY

Resonance occurs when energy exchange takes place periodically in an oscillatory manner. These oscillations are apparent in voltage, current, and torque magnitudes and grow when there is insufficient dissipation of energy. If these magnitudes exceed certain thresholds, resonance stability occurs. Sub-synchronous resonance can be associated with electromechanical resonance or electrical resonance. The term can be divided into two categories: i) torsional resonance, which occurs due to the resonance between series compensation and the mechanical torsional frequencies of the turbine-generator shaft, and ii) electrical resonance, which is purely electrical. Compared with the other system stability categories introduced in [35], resonance stability focuses on sub-synchronous oscillations, thus differentiating it from rotor-angle stability. Compared with converter-driven stability, resonance stability focuses on the interaction of fast-acting power electronics-based control devices with slower mechanical phenomena, such as torsional mechanical modes.

Torsional resonance is a well-studied electric power system condition where the network exchanges significant energy with a turbine generator at one or more of the natural sub-synchronous torsional modes of oscillation of the combined turbine-generator mechanical shaft. The oscillations can be poorly damped, undamped, or even negatively damped and growing, thus threatening the mechanical integrity of the turbine generator shaft. Torsional resonance can also occur due to the interaction of fast-acting control devices, such as HVDC lines, static var compensators, and power system stabilizers, with the torsional mechanical modes of nearby turbine generators.

Electrical resonance phenomena, although never observed in power systems with conventional generating units, can occur in systems with variable-speed induction generators due to the presence of converter controls [14]. Such stability issues can occur due to the fact that variable-speed doubly-fed induction generators are directly connected to the grid, which makes the electrical resonance between the generator and series compensation possible. Purely electrical resonance can occur between the series capacitor and the effective resistance of the induction generator when the system's resistance exceeds a certain threshold due to the effect of converter controls. These stability phenomena are electromagnetic in nature.

C. CYBER-PHYSICAL POWER SYSTEM MODELING

Modeling the CPPS is necessary for operational studies on power systems' cyber-physical resiliency and stability. Power system events, such as the 2003 blackouts in Italy and in the Northeast United States, are historical paradigms of how interrelated cyber-physical failures led to cascading failures and a blackout. In existing work, researchers categorized the models presented in literature according to various criteria. What is found is that parameters, such as time characteristics and component characteristics, scope of study, and system size, are the main considerations in designing a CPPS model. Developing the correct model to capture the cyber-physical interactions and interdependencies of the power systems is a challenging task due to the system's complexity.

The physical power system operates in a continuous time and is non-linear in nature. The mathematical approach for modeling it is based on a set of differential-algebraic equations. On the other hand, the cyber layer on top of it can be modeled in discrete time, governed by difference equations. As a result, CPPS is an integrated, multidimensional, heterogeneous system with complex intra-dependencies and interdependencies. Intra-dependencies of the CPPS model can be examined in each individual layer, and they refer to the interactions between components and systems within a layer. Concerning the physical power system, an example

of intra-dependencies can be seen in the form of the dynamic response of certain modeled components, such as synchronous generators and power transformers, to a disturbance, e.g., changing of speed, increased currents and heating, etc. In the case of the cyber layer, bandwidth and latency effects on the communication networks need to be modeled and captured [39]. Communication network channels have a finite limit of information that can be carried per unit of time. These limitations do not only affect the design of controllers and their normal operation but can also be prone to failures or targeted by cyber attacks. Other essential aspects for modeling the cyber layer are the sampling mechanisms and the delays present between the receiving and transmitting ends.

The interdependencies of the CPPS are examined with the modeled interaction between the cyber and physical layers. Such studies focus on how cascading failures in the physical or the cyber layer can affect the connecting components on the other or how a communication failure in the wide area network can result in physical impact due to the induced latencies and lost data packets in wide area control applications. Especially for applications such as coordinated and communication-assisted protection schemes, failures and delays in the cyber layer could lead to maloperation of the devices. Communication network packet drops due to failures or cyber attacks could severely affect the operation of real-time applications. Although network protocols are equipped with mechanisms that could prevent the loss of packages via re-transmission, additional delays will be added.

System-wide modeling and applications need to consider modeling limitations, such as computational burden for simulators and emulators, limited or extensive presence of cyber and physical uncertainties, convergence issues of the iterative solutions, data exchange between models, etc. Simulation solutions are the most efficient way to model such systems, achieving interaction between the various layers by means of co-simulation, etc. In the cases of modeling smaller systems, such as microgrids or the cyber-physical model of a digital substation, testbeds can be built containing both hardware-in-the-loop and software solutions. The aforementioned difficulties constitute the overall problem of scalability.

Defining and achieving the required fidelity of the CPPS model is pivotal for every application. The fidelity of the CPPS model is assessed based on how close its results are to its real-world counterpart. Traditional power system stability studies heavily rely on accurate physical models. The requirements for the physical model were mainly having the accuracy, fidelity, and necessary coverage to be suited for the stability study of interest. CPPS stability studies, on the other hand, require the modeling of the interactions between the cyber and physical layers. CPPS can be modeled as a closed-loop dynamic system by modeling network-connected control and protection components for the power system, enabling the application of WAMPAC. In these studies, power system measurements, either from SCADA or Phasor Measurement Units (PMU), are utilized to enable real-time monitoring and control capabilities for local and central controllers. Additionally, communication links are modeled for data exchange, considering the presence of induced delays resulting either from a communication failure or a cyber attacks. Such delays could cause instability in the physical power system due to improper operation of the wide-area controllers. Any cyber-physical model for stability analysis should be able to capture the state transition in response to internal changes or external inputs and disturbances. The differences between traditional power systems and CPPS stability analyses are summarized in Table 2.

TABLE 2. Power system and CPPS stability analysis comparison.

Category	Power system stability	CPPS stability
Assessed disturbances	1. Physical contingencies • Electrical faults • Loss of power lines • Loss of generators • Load variations • Equipment failure	1. Physical contingencies 2. Communication failures • Measurement noise • Equipment failure • Communication delay • Loss of data/packets 3. Cyber attacks • Modification of measurements • Denial-of-Service • Delay-induced attacks • Command injection • Replay attacks • Coordinated attacks 4. Human errors
Modeling considerations	1. Equipment models • Generators • Transformers • Loads • Power lines 2. Control functions • Voltage Regulator • Governor • Power System Stabilizer • Flexible AC Transmission Systems • HVDC Controls 3. Protection functions • Generator interface • Power lines • Transformers	1. Dynamic equipment models 2. Dynamic control functions 3. Protection functions 4. Wide-Area Monitoring and Control • Monitoring applications • Protection applications • Control applications 5. Communication network • Routers • Controllers • Gateways • Network switches • Firewall • Intrusion detection/prevention 6. Packet encapsulation mechanism • IEC 61850 • TCP/IP • IEC 60870-104 • DNP3 7. Communication links bandwidth • Telemetry • Fiber optics • Wireless communication

The timescale of the CPPS stability analysis is a major concern for the model design. As the physical system's dynamic response ranges from sub-seconds for converter-driven stability to minutes for long-term frequency stability, it is impractical to use a common model for every stability analysis. For instance, the study of fast oscillations and stability issues involving power electronics-connected generating units is assessed to be more accurate by utilizing electromagnetics transient simulations [40]. On the other hand, electromechanical simulations or quasi-dynamic simulations can be used for stability analysis in longer timeframes. Similarly, the cyber layer needs to be modeled to correspond to the physical system's operation.

CPPS testbeds are developed in various labs, which utilize specialized hardware, e.g., Real-Time Digital Simulator, together with network interfaces to create more realistic

TABLE 3. Cyber security differences between IT and OT systems.

Category	Information Technology	Operational Technology
Priorities	- Confidentiality - Integrity - Availability	- Security / Availability - Integrity - Confidentiality
Operational focus	- Communication	- Physical procedures - Safety
Cyber security consequences	- Data loss - Network operation disruption - Loss of trust - Monetary loss	- High revenue loss - Disruption of physical operation - Supply chain disruption - Risk to national security - Risk to human life
Standards	- Open: Ethernet, TCP/IP	- Serial and legacy standards - Industry-specific standards
Processing capacity	- Highly scalable processing	- Outdated systems/processors - Limited scalability
Life cycle	- 3-5 years	- Up to 20-30 years
Desired availability	- Low / Medium	- High
Security patching	- Always	- Where/when applicable
Encryption	- Always	- Where/when applicable
Operational requirement	- Speed	- Low latency
Network traffic	- Probabilistic	- Deterministic

models. Additional software tools for power system simulations are DIgSILENT PowerFactory, MATPOWER, PSS/E, etc. To simulate or emulate the communication network on top of these applications, solutions such as OMNeT++, OPNET, etc. can be utilized. A prominent method of coupling cyber-physical models is co-simulation. Co-simulation is a simulation technique to combine different types of models and simulate them in a unified fashion [41].

Overall, cyber security considerations regarding future power grid stability need to assess the interrelationship between the cyber and the physical layer. The impact of malicious actions targeting power system operation by injecting malicious commands, inducing time delays, or manipulating measurements can have significant cyber-physical effects, leading to system instabilities. Cyber security is one of the domains in which CPPS models could be utilized.

III. CYBER VULNERABILITIES AND ATTACKS

This Section presents the current identified cyber security landscape for electrical power systems. As shown in Fig. 1, cyber attacks targeting ICS are increasing in frequency. Cyber intrusion is a multistage process where the attackers utilize and exploit vulnerabilities, deploy worms and malware, perform credential theft, etc., to infiltrate the overall IT/OT network and place themselves inside the critical systems. For the cyber attackers to be able to target the power system operation, they need to utilize the IT/OT interconnections and vulnerabilities. In this analysis, the cyber kill chain framework is utilized to explain how attackers can systematically target the power system by navigating through IT and OT networks. Then, the identified vulnerabilities that can be utilized to affect the power system operation are discussed. Finally, the possible cyber attacks that malicious actors can launch to target the physical power system operations are presented.

A. CYBER SECURITY CONSIDERATIONS

Researchers in the field of cyber security employ frameworks that can describe the cyber attackers' tactics, objectives, and the stages in their operation. Such frameworks can be utilized to map specific actions to certain classes, enabling the development of detection, containment, and mitigation strategies. Assante and Lee [42] introduced the framework of the cyber kill chain for ICS in 2015. The goal was to highlight the critical differences between the cyber kill chain for IT and ICS. The kill chain for ICS has two stages e.g., cyber intrusion preparation and execution, and ICS attack development and execution. The first stage follows the approach of the general kill chain for IT systems. The main goal of the attacker is to establish a foothold and successfully navigate through the IT/OT systems to reach the targeted environment. The whole cyber intrusion operation can take months to achieve its goals, as is shown in the example of the Ukraine cyber attacks [4]. In this stage, IT cyber security practices can be

applied as usual, and the intruders need to move through business networks. Conventional vulnerabilities present in IT systems can be exploited, and the potential malware or viruses utilized do not necessarily need to be domain-specific.

On the contrary, in the second stage of the ICS cyber kill chain, the intruders utilize the IT/OT convergence to gain access to the more secluded OT infrastructure. These environments have specific characteristics that distinguish them from typical IT ones. The differences between IT and OT are summarized in Table 3. The operational differences between these two systems need to be considered. Otherwise, the attacker's actions could cause alarms and maloperation of the more sensitive OT systems. Such an incident occurred in the Triton cyber attack [8], where the remote access trojan that the attackers installed for code execution on the industrial computers had caused the safety instrumented system to shut down the industrial processes, resulting in alerting the security personnel.

In the context of CPPS, the cyber attack in Ukraine in 2015 is an example of the applicability of the cyber kill chain for ICS in mapping the actions of the cyber actors. Researchers attempted to cover the physical layer of a cyber-physical system through the form of a kill chain for cyber-physical systems [43]. The framework was proposed as an extension of its predecessor by introducing the perturbation of control and physical objectives following the ''Execution'' phase. Overall, the kill chain framework can assist researchers and security experts in mapping the attack stages and designing security measures and strategies. It is worth noting that the advanced IT/OT convergence that is expected in the future CPPS will lead to significant challenges regarding the applicability of cyber security measures. Cyber security methods such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), honeypots, etc., must be tailored to the specified environment.

B. CYBER VULNERABILITIES

OT systems have a longer lifecycle than traditional IT systems. IT cyber security is not covered in this study, as successful cyber attacks aim to gain access and extract digital information, meaning confidentiality is a major concern. On the other hand, by compromising and manipulating measurements or control commands, the attackers can cause physical damage, endangering both the operational and human safety of an ICS. In a recent report by Dragos Inc. published in 2022, the number of critical vulnerabilities on the whole spectrum of industrial systems has exploded [44]. Focusing on CPPS, the standards based on which the OT architecture of these systems are designed often lack cyber security considerations [45], [46]. Additionally, as the life cycle of the power system OT equipment is long, newly developed hardware will be implemented partially on substations, while vulnerable devices will still be present. Two classes of vulnerabilities are identified: the communication protocols used in CPPS and the software vulnerabilities.

1) COMMUNICATION PROTOCOLS

The standard communication protocols in power systems aim to connect the various industrial equipment and metering infrastructure to the local control systems and the control center. These industrial protocols are utilized to define the communication between the devices in the CPPS. Field devices such as Remote Terminal Units (RTU), IEDs, and Merging Units (MU) are connected through communication nodes and links to the local SCADA applications for local monitoring and control. Currently, most protocols are IP-based, using Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets for flexibility of implementation.

The communication between sensors, meters, IEDs, and the SCADA or Human Machine Interface (HMI) of a substation is realized with protocols such as Modbus, Distributed Network Protocol 3 (DNP3), and IEC 61850. Modbus is a well-known example of a standard communications protocol that was adopted across a wide area of industries, including power systems. It is implemented between programmable logic controllers and HMIs, utilizing the master-slave configuration [47]. The devices can also be configured to run these roles in parallel. The Modbus protocol works on two types of communications, serial line and TCP over Ethernet. Notable cyber security vulnerabilities of this protocol are derived from the lack of security applications, authentication mechanisms, encryption, and integrity validation [48]. Adversaries can intercept existing Modbus sessions and replicate the session by analyzing the traffic, making it susceptible to Man-in-the-Middle (MitM) attacks. Additionally, Modbus can be made more scalable by embedding its frame in a TCP packet. As a result, Modbus over TCP inherits cyber security issues of TCP [49]. Moreover, the application of Modbus over TCP does not properly implement the TCP message checksum. Hence, it can be easily intercepted and compromised by a spoofing attack.

DNP3 is a popular communications protocol used in power systems for SCADA operations. It was introduced to support communications between the control center and substations. The original objective of DNP3 was to transmit small-sized data packets using serial RS232 for relatively short-distance point-to-point communications. The protocol implements four layers from the Open Systems Interconnection (OSI) model, i.e., physical, data link, transport, and application. The latter variants of DNP3 were extended to work using TCP and UDP packets over Ethernet. While DNP3 is more reliable than Modbus, it also consists of vulnerabilities, making it prone to spoofing and distributed Denial of Service (DoS) attacks. In [50], 28 possible attack vectors that could target the DNP3 protocol were identified. Attacks targeting DNP3 can be categorized into the process of interception, interruption, modification, and fabrication. The protocol is also vulnerable to MitM attacks like packet sniffing and spoofing attacks. These attacks can result in three types of impact: 1) loss of confidentiality, 2) loss of awareness, or 3) loss of control.

Loss of confidentiality happens when the attacker successfully intercepts the communication. Loss of awareness occurs when the control center does not obtain precise and trustful information. The most critical type of attack is the loss of control, wherein attackers can take unauthorized control of the system.

IEC 61850 is a modern power system communications standard for substation automation and protection, which allows information exchange through several communication protocols, including Generic Object-Oriented Substation Event (GOOSE), Sampled Values (SV), and Manufacturing Messaging Service (MMS) [45]. Compared to Modbus and DNP3, IEC 61850 Ethernet-based communications provide larger bandwidth. In this standard, power system communication is mapped into TCP/IP packets sent over Ethernet and can be applied for local and wide-area communication [51]. For example, Routable IEC 61850 was implemented through data encapsulation into TCP packets [52]. This mechanism facilitates the expansion of IEC 61850 communication beyond the boundaries of a single substation, enabling its routing across more extensive areas of the OT networks. IEC 61850 is used to exchange control and measurement packets for local communication within a substation, between substations, as well as between substations and the control center. Although IEC 61850 is defined by its high scalability and increased functionalities, cyber security vulnerabilities are identified. IEC 61850 GOOSE and SV protocols are identified as vulnerable to spoofing attacks [53], [54], [55]. Additionally, a critical issue is derived from the problem that encryption measures are difficult to apply due to the low latency requirements (3-4 milliseconds) for power system protection applications.

The most commonly used standard for establishing communication between the substations and the control center is IEC 60780-5, as well as IEC 61850. From this category, IEC 60870-5-101 and IEC 60870-5-104 are the most widely used protocols. IEC 101 is a protocol for basic supervisory control and data acquisition, while IEC 104 has increased performance due to its network and transport layers, in addition to the application layer protocol [46]. IEC 104 can provide network access to IEC 101 using TCP/IP. Due to the vulnerabilities in the TCP/IP stack, common vulnerabilities are: i) messages are transmitted in plain text [56], and ii) lack of authentication mechanism. Thus, cyber actors can perform MitM attacks by sending malicious control commands or connecting to the network.

To address cyber security issues of the aforementioned standards, IEC 62351 is proposed, with a goal to enhance confidentiality, integrity, and authenticity. As such, many of the parts of this new standard are based on IEC 61850 and 60870. IEC 62351 is still in the process of development. It provides new definitions related to cyber security, like role-based access control, key management, and security architecture [57]. Some identified vulnerabilities, described in [58], enable cyber actors to perform replay attacks using GOOSE and SV. One vulnerability is related to time exchange based on the simple network time protocol. Security enhancements proposed in IEC 62351 rely on the implementation of cryptographic measures, such as RSA cryptography. However, entire packets are not encrypted using RSA, and only the protocol data unit is encrypted. This situation allows attackers to modify the unencrypted parts. Despite the implementation of IEC 62351, modification of packet counters and time stamps allows attackers to launch GOOSE and SV-based attacks. IEC 62351 prevents the manipulation of traffic by implementing a Message Authentication Code (MAC), which is a hash-based authentication to validate the integrity of data. Still, the attackers can modify time-related information using the vulnerabilities of the data encryption standard that MAC relies on. Consequently, this can violate the rules of packet processing, thereby triggering DoS conditions. Besides the possible theoretical exploits of IEC 62351, there is also an example of a real attack demonstration. Carcano et al. demonstrated cyber attacks targeting SCADA networks running IEC 62351 [59].

Additional protocols that are employed for measurement and communication in the power system are IEEE C37.118, IEEE C37.247, and Inter-Control Communications Protocol (ICCP). IEEE C37.118 defines a mechanism for real-time exchange of synchrophasor data and messaging formats, message types, and content [60]. The messaging format, as well as the requirements for data transfer, are defined by the standard. It uses a universal time source as a reference and time stamps based on the Global Positioning System (GPS) to provide time-synchronized measurements of power system parameters from different locations. This feature is crucial for implementing WAMPAC applications [61]. Cyber security considerations are mainly due to the lack of security mechanisms like authentication and encryption [62]. The lack of the aforementioned security mechanisms enables cyber attackers to manipulate the data packets for MitM attacks or to inject forged ones. These vulnerabilities can be utilized to target wide-area applications, enabling cyber actors to indirectly target the physical power system.

The C.37.247 defines the Phasor Data Concentrator (PDC) operation, which is used to synchronize, process, and transmit the data collected from individual PMUs [63]. Synchrophasor measurements from the distributed PMUs are received in real-time by the PDCs, which are used to shape the data in a single data stream and transmit it to higher levels. PDCs are used for timestamp alignment, filtering corrupted or false data, and maintaining a record of data. Regarding cyber security, the communication links used for data transmission to/from PDCs are not encrypted. Malicious actors can utilize the lack of encryption, vulnerabilities that enable access to the configuration and programming software of the devices, and lack of traffic control to launch DoS, MitM, and time delay attacks [64], [65].

Finally, ICCP, also known as IEC 60870-6/TASE.2, is a data exchange protocol commonly used for communication

between independent system operators, regional transmission operators, generators, control centers, and utilities over the wide-area network [66]. It facilitates communication between two control centers based on a client-server model. The vulnerabilities of this protocol are identified in [67] and enable cyber actors to attack the process control data, the ICCP servers, and server operating systems. These vulnerabilities mainly exploit the lack of security mechanisms like encryption and authentication. Without those two security properties, many possible exploitations can be performed over ICCP. Studies showed that security mechanisms can be applied to ICCP [68]. It can be encrypted and authenticated as secure ICCP. Implementation of secure ICCP relies on public-key cryptography.

In summary, the protocols employed by CPPS exhibit vulnerabilities to cyber attacks as a result of inadequate implementation of cyber security measures. The security measures employed in the field of IT communication protocols primarily rely on the implementation of cryptographic techniques. Nevertheless, the implementation of cryptography in CPPS is challenging due to the stringent demands for high availability and low latency. In [69], the author provided evidence that CPPS face difficulties when attempting to integrate cryptography into their systems. This is primarily attributed to the substantial amount of computational time that cryptographic processes demand. Although cryptographic algorithms like 2048-bit RSA and 1024-bit DSA are considered robust, the processing time of cryptographic operations respectively entailed a total of 61.04 milliseconds and 14.90 milliseconds. Due to limited time availability, this situation led to the utilization of cryptographic techniques that offer reduced security and computational requirements or, in many instances, the complete absence of cryptographic measures.

2) SOFTWARE VULNERABILITIES

In existing electrical power systems, software technologies for OT are mainly related to SCADA systems. In the future, this will be integrated with various software functionalities, i.e., energy management systems and advanced distribution management systems. SCADA is a control system architecture that consists of interconnected devices controlled by OT software. The main challenge for a SCADA software system is the regular software updates. Most of the existing software was created before cyber security issues became a major concern [70]. In [71], three groups of SCADA software vulnerabilities are identified: 1) improper input validation, 2) resource control, and 3) software code. SCADA software is susceptible to input value modification attacks such as buffer overflow and data injection. With regard to the code itself, OT systems tend to be less secure. This is because OT software is designed for high availability requirements, with less consideration of regular updates and security mechanisms.

Resource control vulnerabilities are mainly related to software updates and patch control mechanisms. Vulnerable

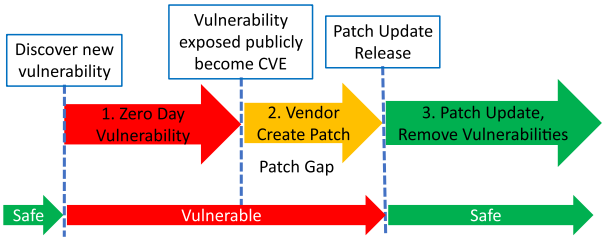

FIGURE 3. Lifecycle of a software vulnerability.

software that may have been deployed in the field must be updated and patched to eliminate vulnerabilities. However, software updates and patches in OT are challenging and can potentially disturb system operations. Fig. 3 shows the lifecycle of a software vulnerability that is applicable to SCADA software. In principle, software vulnerabilities will always exist. When limited parties identify these vulnerabilities, it becomes stage one, i.e., a zero-day vulnerability. The zero-day vulnerability is dangerous when exposed by adversaries. In the second stage, information is exposed publicly, and software vendors create software updates and patches to address the vulnerability. After this, it is no longer considered a zero-day vulnerability. For example, MITRE's Common Vulnerability Exposure (CVE) lists all the vulnerabilities in SCADA-related applications [72]. A patch update is released by the vendor to address specific vulnerabilities. However, as previously mentioned, patch updates in the SCADA system are quite challenging, and they may be deployed in remote locations [73], [74]. Hence, vulnerabilities in SCADA software are likely to stay present and unaddressed during the software lifecycle.

An example of the potential impact of the software code vulnerabilities is the Ripple20. In June 2020, nineteen software vulnerabilities were discovered by JSOF, an Israeli cyber security firm. These vulnerabilities affect devices using the Treck Inc. TCP/IP stack software library. The vulnerabilities are based on the exploitation of TCP packet fragmentation, tunneling mechanism [75], and DNS decompression mechanism [76]. Many networked devices widely use this software library for the TCP/IP stack across a plethora of industries, including SCADA, offices, healthcare, etc. By exploiting the vulnerabilities, adversaries can disrupt the functioning of the devices. An investigation in [76] shows an example of a malicious payload that can successfully switch off a UPS device remotely. These vulnerabilities are a significant problem since it is difficult to update software or firmware in embedded devices. Ripple20 is a real-world example of difficulties performing software updates for SCADA devices and systems. Legacy SCADA systems can also be integrated with energy management systems in the future power grid for various advantages.

Future power grid software like energy management systems and advanced distribution management systems can help achieve more intelligent grid operations. The operation of the power grid is not only dependent on human operators

but also on smart and intelligent systems. The software can be in the form of AI applications. The implementation of smart software or AI will advance the digitalization of the overall grid. However, the cyber security aspects cannot be overlooked. Adversarial machine learning is one such major potential threat that can fool the AI-based system. In [77] and [78], the authors show how adversarial machine learning can have adverse effects on the operation of smart software systems. Such adversarial machine learning may become a new type of threat to power system software systems in the near future.

C. CYBER ATTACKS

Despite the extensive presence of legacy systems and the many vulnerabilities present both in communication protocols and software applications, targeting the physical power system operation is challenging for cyber actors. The attackers need to establish footholds deep in the IT systems to access the OT domain, and navigating through these communication networks is a prolonged operation. However, due to the increasing IT/OT integration and the fast-paced digitalization of power systems, malicious actors can exploit new attack paths and vulnerabilities to jeopardize their operations. Such attack paths could be established by identifying access points deep in the OT networks, e.g., remote access mechanisms and infiltration via supply-chain attacks. In every phase of this intrusion, the cyber actors can perform different cyber attacks to discover, gain access, and compromise new assets or to erase any signs of their activity. Cyber attacks are defined as offensive, malicious attempts to steal, expose, alter, disable, or destroy information through unauthorized access to computer systems. As explained in Section III-A, a cyber intrusion in these systems is performed in different stages, each with a unique set of tools and targets. Cyber attacks can be categorized based on which aspect of the cyber security principle they target. For example, eavesdropping attacks target confidentiality, while cyber attacks on measurements or controls target availability. However, in this work, the main focus is on the cyber attacks targeting the operation of the electrical power system. The main cyber attacks that were assessed for causing disruptions or resulting in a physical impact are DoS attacks, MitM attacks, False Data Injection (FDI) attacks, and host-based attacks.

1) DENIAL OF SERVICE

DoS is a cyber attack with the objective of preventing legitimate access for users to specific system resources such as networks and hardware. This can be accomplished by flooding the target with packets or triggering a crash on the targeted system. For instance, a DoS attack on a network router, through packet flooding, could result in the drop of legitimate packets. Popular flood attacks include buffer overflow, SYN flood, and ICMP flood attacks. In [79], researchers studied the impact of a distributed DoS attack on advanced metering infrastructure. It is seen that communication performance is severely affected due to the attack. Furthermore, research also shows that DoS attacks can exploit power system communication protocols and standards, such as IEC 104 [80], C37.118 [81], and IEC 62351 [59]. Overall, DoS attacks are recognized as a severe potential cyber threat to the power system operation. DoS attacks can target systems with very strict timing requirements, inducing delays that could jeopardize the operation of controllers or protection schemes. Furthermore, DoS could be utilized in coordinated attacks to magnify the impact of other cyber-physical attacks.

2) MAN-IN-THE-MIDDLE

The concept of these attacks for the CPPS operation is that the cyber actors place themselves in the network and then intercept or spoof packets into the network traffic. As a result, the receiving device or software is tricked into executing erroneous commands. Due to the lack of encryption and authentication mechanisms in the OT environments, such attacks can be used for cyber-physical attacks. One of the variants of this attack is packet spoofing. Spoofing involves the modification of legitimate communication traffic with malicious attack traffic. As a result, malicious and erroneous packets can be induced in the network traffic, issuing control commands or misleading the human operators or automated controllers. Researchers in [82] demonstrated how spoofing and jamming attacks could target the communication network of power systems, while the work in [83] showcased a GPS spoofing attack targeting PMUs. These examples of spoofing attacks can be used to target the CPPS operation.

3) FALSE DATA INJECTION

Another category of MitM attack in the CPPS cyber security literature is the FDI attack. FDI attacks were initially proposed in [84] as a form of a MitM attack that can target the state estimation application in the power system control center. The cyber attack commences through multiple compromised metering devices, in which the attackers alter the measurements in a way that bad data detectors will not detect arbitrary errors. The erroneous measurements will then jeopardize the controlling applications of the control center, such as the Automatic Generation Control (AGC), optimal power flow, etc. As a result, the system operators will be misled. To launch a successful FDI, several assets must be compromised. Even in studies that examined the feasibility of FDI attacks, such as the ones presented in [85] and [86], considering limited information by the cyber attackers, a significant portion of the metering infrastructure of a power system needs to be compromised. On the other hand, FDI could enable cyber actors to achieve the most difficult task according to the cyber kill chain, the ability to re-launch a cyber attack [14]. Utilizing FDI attacks to mask another MitM attack, such as opening a circuit breaker or for more prolonged cyber attacks aiming to gradually destabilize the power grid, could be a terrifying perspective for system operators.

Gradually, the term involved to encompass many different forms of cyber attacks. In a survey presented in [87], the overall spectrum of FDI attacks was divided into certain types, such as *communication-based, network-based, physical-based,* and *cyber-based*. On the one hand, the significance of FDI attacks targeting electrical power systems is highlighted. On the other hand, on the overall spectrum of cyber security for CPPS, the feasibility of FDI attacks is still debatable. In a recent survey, which utilized questionnaires distributed to grid security experts, it is highlighted that the feasibility and the impact of FDI attacks can be reduced when considering realistic attack capabilities [88].

4) HOST-BASED ATTACK

A host-based attack, as its name implies, refers to an offensive action that specifically targets multiple hosts within IT-OT systems. These systems encompass a range of components, including SCADA servers, HMIs, databases, application servers, station control systems, RTUs, protection relays, and merging units. Host-based attacks can be categorized into three different classifications: software-based attacks, database attacks, and unauthorized access and control attacks.

Software-based attacks targeting power grids leverage vulnerabilities inherent in the software utilized in IT-OT systems, including SCADA and energy management systems. Typically, the software applications and security controls implemented in OT systems exhibit similar vulnerabilities as those found in conventional IT systems. The primary concern lies in the fact that the software and security controls implemented in IT systems have more frequent patching and updates compared to OT systems. Additional cyber attack types could target the security of sensitive databases utilized by the SCADA system. They are of paramount importance, as they serve as a storage for real-time data obtained from substations and store user access credentials. Zhu et al. categorize a database attack as an important cyber attack targeting SCADA systems [89]. The majority of databases operate using Structured Query Language (SQL). One of the prevalent forms of attacks directed towards databases is SQL injection. This attack highlights the manipulation of input handling within the database system.

Unauthorized access refers to the act in which an adversary successfully gains entry into a computer system without possessing valid credentials or authorization. Therefore, the attainment of unauthorized access and control can occur when attackers successfully bypass the authentication mechanisms. There exist various methodologies to accomplish this goal, including the utilization of keyloggers for credential theft, exploiting database vulnerabilities, employing brute force attacks, and exploiting buffer overflow vulnerabilities. This technique leverages weaknesses in a system to introduce harmful payloads into the targeted system. In order to enhance the severity of an attack, malicious actors may engage in privilege escalation techniques, thereby attaining administrative privileges that grant them unrestricted authority over the compromised system. SCADA systems commonly utilize common operating systems, such as Microsoft Windows. As these operating systems can be susceptible to unauthorized access attacks, it is imperative to ensure that operating systems utilized in IT-OT systems undergo regular updates and are protected with firewalls and antivirus software for enhanced security measures.

IV. CYBER ATTACKS IMPACT ON SYSTEM STABILITY

As described in the previous Section, vulnerabilities present in communication protocols and industrial software applications could be utilized by cyber actors to perform cyber attacks targeting the power system operation. The current study aims to investigate how cyber attacks originating from the cyber layer of the CPPS can cause a physical impact on the power system by initiating different stability phenomena. The mapping of cyber attacks with each stability category is performed based on a thorough state-of-the-art analysis of the impact of cyber attacks on each category of power system stability.

A. CYBER-PHYSICAL ATTACKS DEFINITIONS

Fig. 4 presents the connections between the identified cyber-physical attack types and power system stability categories. The traditional power system stability analysis is based on the impact of non-malicious small, and large physical disturbances. Each stability category, as specified in [14], is mapped with specific types of cyber-physical attacks. Three cyber attack types are identified, e.g., measurement manipulation, induced communication delays, and malicious command injection attacks. The definitions are provided below.

1) Measurement manipulation attacks encapsulate cyber attacks targeting the metering infrastructure of the CPPS and, through alterations of valid measurements, can result in erroneous actions either of the control and protection systems or of system operators. The control and protection systems are considered uncompromised. An example is FDI attacks launched from compromised PMUs, resulting in misleading system operators or the automated control systems.

2) Induced communication delay attacks encapsulate cyber attacks aiming to congest or disable either the communication network links of the CPPS or control and protection applications and devices, resulting in delayed or unperformed actions by either the control and protection systems or system operators. Examples of this cyber attack type are DoS and time-delay attacks. In such cases, the increased latency could severely affect the operation of coordinated protection schemes, controllers, and EMS applications.

3) Malicious command injection attacks encapsulate cyber attacks targeting the control and protection systems of the CPPS and, through the tampering of their internal settings or their received control commands, result in unauthorized actions. Examples of this category are spoofing attacks on circuit breakers or tampering with the settings of protection relays and control setpoints.

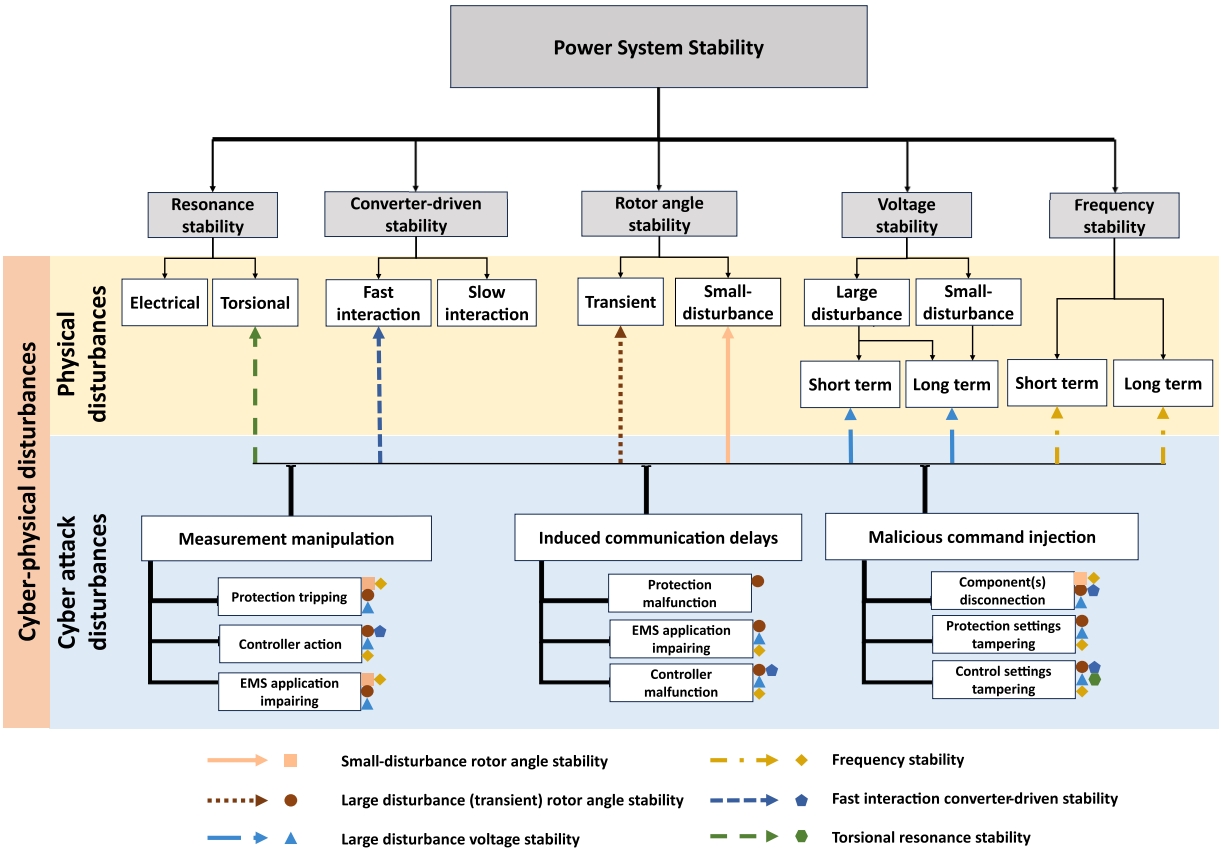

FIGURE 4. Power system stability classification, considering cyber-physical disturbances caused by cyber attacks.

The resulting cyber-physical disturbances caused by the defined cyber attack types are shown in Fig. 4. The cyber-physical disturbances are mapped with the power system stability categories they affect. The findings are derived from the analysis presented in the following sub-sections. Attackers can also launch coordinated cyber attacks, in which one or more of the aforementioned attack types are utilized to increase the impact.

B. ROTOR ANGLE STABILITY

It must be noted that most of the research on the impact of cyber attacks on rotor angle stability focused on the category of large disturbances (transient). Studies on the category of small-disturbance stability are still limited. Researchers examined how cyber attacks on measurements could lead to small-disturbance stability issues [90], [91], [92]. In [90], attackers implemented dynamic load-altering attacks on power system loads, which resulted in instability. As loads are protected by under/over frequency relays, an attack that alters the active power through control signals can cause an imbalance between generation and consumption, leading to small-disturbance instability. In particular, a successfully executed attack can cause frequency oscillations, affecting the rotor angle of generators, which may trip due to their interface protection. In [91], load measurements are altered by cyber actors to perform an FDI attack. The researchers assessed how the knowledge level of cyber attackers could affect how successful the attack is and the amount of measurements that need to be tampered with. The authors of [92] propose an FDI cyber attack with two purposes: 1) to destabilize the system through induced small-disturbance instabilities and 2) to affect the operation cost of the power system through falsified measurements that mislead the system operators. Both local and interarea modes are being targeted by manipulating the active power measurements of load buses. From the aforementioned studies, it is shown that cyber attackers can affect the small-disturbance stability of a power system by targeting the power system loads either directly through load-altering attacks or by manipulating the measurements sent to the control center operators. The identified studies for small-disturbance stability are summarized in Table 4, while the connection of small-disturbance stability with the defined cyber-physical attack types is shown in Fig. 4.

The impact of cyber attacks on large disturbance rotor angle stability is addressed in many more studies. Table 5 provides a summary of the reviewed studies for large disturbance rotor angle stability. Regarding cyber attacks, researchers focused on how malicious commands and data injections could lead to physical disturbances that could cause transient instability. The majority of the studies focused on FDI

TABLE 4. Impact of cyber attacks on small-disturbance stability studies.

Stability category	Targets	Cyber attack types	Power system simulation type	Mitigation strategy	Year	Refs.
Small-disturbance	Power loads	FDI	RMS	Protection scheme against dynamic load-altering attacks	2018	[90]
	Power measurements		Power flow	-	2021	[91]
	Economic operation			Moving target hierarchical solution algorithm	2023	[92]

attacks [93], [94], [95], [96], [97], [98], [99], [100], [101]. In [93], FDI attacks are performed on storage-based transient stability control schemes. A parametric feedback linearization control is utilized to detect and mitigate the impact on power system dynamics when FDI attacks target different measurements. The targeted measurements are the rotor angles from generators. The malicious measurements lead to erroneous operation of the controllers, causing interarea oscillations and local instabilities, leading to system-wide instability. The proposed algorithm is utilized to detect and mitigate the impact of the attacks. In [94], a dynamic state estimation method is proposed for generators under cyber attacks, based on a robust cubature Kalman filter. The main targets for the speculated cyber attacks are the control systems of generators or to mislead the human operators in the control room.

Regarding FDI attacks on the controllers, many studies examined how new controllers could be cyber resilient to such cyber attacks. The proposed controllers were designed with considerations derived from the mathematical model of FDI attacks. In this category of studies, artificial neural networks are utilized to mitigate these measurements. In [101], an auto-encoder model is proposed to reconstruct corrupted measurements after they are detected. The goal is to estimate the valid inputs the operators could utilize for transient stability assessment. The proposed controllers were assessed for normal contingencies and faults in the power system, with FDI attacks being a complementary case study. In these studies, the focus was not on cyber security, but the cyber attack scenarios were utilized to further assess the controller's performance. Additionally, in particular studies, the effect of FDI attacks on system stability is assessed based on a contingency that is caused by a physical fault, e.g., short-circuit. These scenarios examine how the falsified measurements could lead to instabilities, as the controllers, such as Automatic Voltage Regulators (AVR), governors, and power system stabilizers, are receiving wrong setpoints.

Another category of scenarios involved cyber-physical contingencies, mainly malicious breaker opening. Such scenarios are based on the real-world cyber attacks in Ukraine in 2015 and 2016, with the research focus being on the ability of cyber actors to initiate cascading failures in a power system [32], [102], [103], [104]. Such cyber attacks, although simple in conception, are quite challenging as they can introduce unforeseen contingencies in power system operation. These contingencies can be regarded as $N - k$, meaning that operational planning cannot capture all possible combinations that a potential cyber attack will target. In [102], a method of estimating the impact of feasible attacks from malicious opening of circuit breakers is proposed based on transient energy. Such screening approaches can significantly limit the scope of time-domain simulations, enabling faster response and categorization of the cyber-induced contingency. The scenarios resulted in both single-mode swings and interarea oscillations, which were assessed using the total transient energy index. An additional research direction regarding such scenarios utilizes game-theoretic analysis. In [103], Markovian strategies were utilized for designing a game between an electric utility and cyber attackers who employ switching attacks to destabilize the grid. Control actions are taken to mitigate the effects of the cyber attack based on the sign of the normalized rotor speed, thus utilizing a dynamic model of the power system.

The effects of DoS attacks on the control systems of power grids are examined in [36], [105], [106], [107], and [108]. In [36], the authors proposed an adaptive control scheme depending on the latency between sensors and controllers. DoS cyber attacks are modeled to test the resilience of the control scheme when subjected to induced latencies. Another study presented in [107] identified distributed control strategies for enhancing the CPPS stability using flocking mechanisms. Many of the applied algorithms assess the impact of latencies in the control mechanisms and how these can lead to stability issues. In many of these studies, although DoS attacks are mentioned, they are mostly represented by induced delays, which can be both non-malicious communication failures or cyber attacks.

Including PMUs in the power system metering infrastructure is the cornerstone for WAMC applications. As a result, spoofing attacks on PMU are a potential attack scenario that could severely affect rotor angle stability. In [109], GPS spoofing attacks were employed to assess the impact on a wide area damping controller. Spoofing attacks such as these violate the operational constraints of PMUs, as the measurements are not synchronized. The study showed that this category of cyber attacks could severely affect the

TABLE 5. Impact of cyber attacks on transient rotor-angle stability studies.

Stability category	Targets	Cyber attack types	Power system simulation type	Mitigation strategy	Year	Refs.
Transient rotor angle	Parametric feedback linearization controller	FDI	RMS	Adaptive control strategies	2017	[93]
	Measurement nodes		EMT	Dynamic state estimation algorithms	2019	[94]
			RMS	L1 Networked Adaptive Load Frequency Power Controller	2022	[108]
	Communication channels between relays, through IEC 61850 GOOSE		EMT	-	2020	[95]
	PMUs		RMS	Multiflock-based technique for generator coherence	2015	[96]
				Deep learning-based protocol	2016	[99]
				Unsupervised algorithms to detect and denoise signals	2023	[101]
	Voltage support devices		EMT	-	2013	[97]
	ML-based stability assessment		Monte Carlo simulations	-	2023	[98]
	State estimator		EMT	Non-linear controller for state estimator	2017	[100]
	Measurement nodes	DoS	EMT	Dynamic state estimation algorithms	2019	[94]
			RMS	L1 Networked Adaptive Load Frequency Power Controller	2022	[108]
	Protection relays		EMT	Communication-assisted protection scheme	2020	[95]
	SCADA		EMT + RMS	-	2013	[32]
	Remedial action schemes					
	Synchronous generator measurements		EMT	Distributed frequency control framework	2020	[105]
	PMUs				2017	[106]
				Hierarchical multi-agent model based on flocking theory	2014	[107]
	Circuit breakers	Switching	EMT	Transient energy-based screening of contingencies	2016	[102]
				Controller for cyber attack mitigation based on game theory	2016	[103]
			EMT + RMS	-	2013	[32]
			RMS	Cascading outage analysis model	2018	[104]
	PMUs	GPS spoofing	EMT	Proposes wide-area damping controller	2018	[109]
	IED	Falsifying relay settings	-	-	2018	[110]
	Multiple targets	Coordinated	RMS / EMT	-	2013, 2016, 2020	[32], [95], [102]

operation of the WAMC controller, although the physical impact is caused by a short-circuit event. Apart from cyber attacks targeting centralized and distributed control schemes in CPPS, malicious jeopardize of protection schemes are also assessed in the literature [95], [110]. In [95], the impact of cyber-physical attacks on communication-assisted protection schemes is assessed using a co-simulated CPPS testbed. DoS and FDI attacks were implemented to destabilize the power system, which led to rotor-angle instability. Overall, the reviewed studies on the impact of cyber attacks on transient rotor angle stability can be divided into two groups. One group focuses on the cyber-induced impact on the stability of the power system. This means that large disturbances are caused purely by cyber attacks. Cyber-physical attacks such as switching, spoofing, or falsifying relay settings attacks can cause large disturbances on the physical grid, leading to

instability. On the contrary, in the second group of studies, which mainly focused on FDI and DoS cyber attacks, non-malicious physical disturbances are considered to cause large disturbances. The considered cyber attacks target the operation of control and protection applications, thus enhancing the impact of the physical disturbance.

C. VOLTAGE STABILITY

In the reviewed literature regarding cyber attack scenarios, the differentiation between short-term and long-term voltage stability is not present. The studies are conducted on the microgrid level, the distribution level, and the transmission level. As the cyber security mechanisms and cyber attacks presented in the sections above are focused on the transmission system, studies regarding cyber security and stability on microgrids and distribution networks will not be covered in this work. Table 6 provides a summary of the reviewed studies for voltage stability.

Mainly FDI attacks are considered in voltage stability studies [111], [112], [113], [114], [115], [116], [117], [118]. The research problem is how malicious modifications targeting control systems can be detected and mitigated. In [111], a detection and mitigation framework is built to deal with FDI attacks on the state estimator of the control center. The cyber-physical attacks examined affected the long-term voltage stability, as the attackers manipulated the load measurements to mislead the operators. In [114], researchers highlighted how reinforcement learning methods could be utilized for creating adaptive FDI attacks, enabling the grid operation to be targeted by compromising limited areas of the system. The attacker's targets in this study are the substations of a transmission network. The loading conditions are extremely important, as stressed systems are more prone to such attacks. Researchers studied the stability impact by targeting different control and monitoring systems and launching FDI attacks, such as PMUs, automatic voltage controllers, and HVDC line commutated converters, as well as the state estimation algorithm in the control centers. As in the case of transient instability, researchers investigated the impact of cyber attacks on wide-area controllers. Again, it is highlighted that WAMPAC systems are critical targets for cyber attackers. AI methods are also utilized to detect corrupted measurements and to reconstruct valid ones, defending against data manipulation attacks [119].

DoS attacks on communication channels are also examined regarding their impact on voltage stability [112], [121]. It is shown that a DoS attack on the communication links cannot create instability except when a cyber-physical or physical event takes place. The voltage stability of the power system is assessed to be prone to cyber attacks targeting mainly the WAMPAC applications. Potential targets for DoS attacks are the communication nodes and links, such as the gateway routers and communication links transmitting PMU measurements, as shown in [112] and [121], respectively. The induced delays caused by packet floods can lead to packet losses and delayed response by voltage controllers. As a result, if DoS attacks are coordinated with other types of attacks that impact the power system operation, it could jeopardize any remedial actions taken by the aforementioned controllers.

Finally, in [120], a particular case showed how a targeted cyber attack targeting physical equipment could be used to cause voltage collapse. In the attack scenario, cyber actors maliciously open the circuit breaker connecting a generator in the power system. The voltage is restored, but the stressed conditions of the grid, e.g., overloading of transmission lines, cause a line to disconnect due to protection. On the one hand, malicious openings of critical circuit breakers require a proper understanding of the attacked power system. On the other hand, it is a very effective attack scenario that can cause instability and lead to cascading failures.

D. FREQUENCY STABILITY

Studies regarding the impact on frequency stability of cyber attack scenarios have been conducted considering both traditional synchronous generator-dominated power grids as well as penetration of converter-interfaced generating units. FDI attacks are the main cyber attack category considered [122], [123], [124], [125], [126], [127]. In [125], FDI attacks targeting virtual inertia-dominated systems are examined, examining their effects on frequency stability. It was identified that AC/DC systems with synthetic inertia are more vulnerable to cyber attacks. In [124], load-altering attacks, which are a subcategory of FDI attacks, on secondary frequency controllers are assessed. The findings showed that the system could be stable as long as the attacker did not launch an aggressive attack with abnormal control signals. A prominent target for FDI attacks is the AGC in the control center [125]. The goal of the adversary is to provide falsified measurements, leading to erroneous operation of the AGC and instability. The authors proposed a reconfigured AGC controller, which is able to mitigate the impact of FDI attacks. Additional WAMPAC applications can be targeted, such as wide-area under-frequency load-shedding schemes [128], [129], [130]. The effectiveness of FDI attacks is assessed on how the cyber actors can confuse system operators and the load-shedding mechanisms, causing frequency instability. In [129], the HVDC oscillation damping control is targeted. The induced oscillations, by means of FDI attacks, cause oscillations in the interconnected AC systems, due to the active power fluctuations.

DoS attacks targeting the load frequency control of power systems are examined in [131], [132], [133], and [134]. In [131], the authors showed that DoS attacks could have an impact when the attackers target the tie-lines measurements of frequency and powers. This is mainly due to the fact, that tie-line power flows need to be properly telemetered, and as a result DoS attacks could cause issues in the power exchange, leading to instabilities in the connected systems. The impact of time-delay attacks on load frequency control is assessed [133]. A cyber resilient controller is proposed, able to mitigate the effects of such attacks on frequency stability. It must be noted, that simplifications are made for the system

TABLE 6. Impact of cyber attacks on voltage stability studies.

Stability category	Targets	Cyber attack types	Power system simulation type	Mitigation strategy	Year	Refs.
Voltage	PMUs	FDI	RMS	Detection algorithm	2020	[111]
			Power flow	Generative adversarial networks capturing deviations	2020	[113]
			RMS	A deep learning-based approach to reconstruct manipulated signals for the wide-area monitoring system	2023	[119]
	Automatic voltage control		QD	Reinforcement learning application for mitigating FDI using bad data detection	2019	[114]
	HVDC line-commutated converters		EMT	-	2023	[115]
	State estimator		Power flow	Moving target defence framework	2022	[116], [118]
	AVR		RMS	-	2017	[117]
	Gateway between substation and control center	MitM	Power flow + EMT	-	2015	[112]
	Communication node connecting PMUs	DoS	Power flow + EMT	-	2015	[113]
	Router of automatic voltage control		EMT	-	2018	[121]
	Communication line	Induced outage	Power flow + EMT	-	2015	[112]
	Critical circuit breakers	Aurora attack / Switching	EMT	Proposal of an event and intrusion detection system	2017	[120]

to be linear and time-invariant. As a result, the impact of time delay attacks could be more severe, especially for such a centralized system. The reviewed studies for frequency stability, considering cyber attacks, are given in Table 7.

E. CONVERTER-DRIVEN AND RESONANCE STABILITY

The two types of converter-driven and resonance stability were recently introduced. As such, research work on cyber attacks did not specifically focus on these two types of stability. As the converter-connected generating units, mainly in the form of RES, are expected to dominate future power systems, the exploitation of such weaknesses can lead to the violation of the strict power system operating criteria. Studies that explored this issue are limited but are expected to rise as these kinds of instabilities occur more often [135], [136], [137], [138]. In [135], the authors designed a damping fuzzy controller resilient to DoS and FDI attacks. On the one hand, both attacks did not result in extensive instability phenomena, as the proposed controller was able to dampen them. On the other hand, oscillations are still present in the system, and an additional coordinated attack could lead to more severe damage. This case was not assessed. In [136], a strength evaluation method for power systems with high penetration of RES is proposed, considering cases of cyber attacks. MitM attacks are considered in the form of malicious command injection, targeting transmission line breakers. For the worst contingencies, it is found that the system becomes unstable due to the presence of oscillations of the converter-driven RES. Finally, in [138], due to the advanced communication network between transmission system operators and wind farm operators, the attackers can infiltrate the communication network and launch MitM and DoS attacks. The attackers are assumed to be able to cause physical impact by either issuing malicious dispatch commands to the wind farm operators or by causing a cyber-physical impact through line disconnection. The physical impact, especially in the case of the cyber-physical attack, could lead to oscillations between the converter-connected

TABLE 7. Impact of cyber attacks on frequency stability studies.

Stability category	Targets	Cyber attack types	Power system simulation type	Mitigation strategy	Year	Refs.
Frequency	Measurement devices	FDI	RMS	Frequency control scheme	2021	[122]
	AGC			-	2023	[123]
				AGC signal reconstruction	2021	[127]
	Secondary frequency control			-	2022	[124]
	Load frequency control			FDI detection, isolation, and recovery mechanism	2020	[125]
			EMT + Modal	H_∞ controller	2023	[126]
			RMS	Distributed event-triggered communication strategy	2022	[134]
	HVDC oscillation damping control		EMT	(i) Neural network to learn characteristics of cyber attacks, (ii) model-free defense framework, (iii) cyber attack-resilient damping control	2023	[129]
	Wide area load-shedding control		RMS	Data-classification method for reliable states	2023	[128]
	Wide area damping controllers	Unspecified cyber attacks	RMS + Monte Carlo simulations	-	2022	[130]
	Communication links	DoS	RMS	-	2021	[122]
	Load frequency control		EMT + Modal	H_∞ controller	2023	[126]
			RMS	Dynamic bandwidth allocation	2022	[134]
				-	2013	[131]
		Time-delay-switch attack	RMS	-	2014	[132]
				Resilient control strategy	2020	[133]
	Secondary frequency control	Load altering	RMS	-	2022	[124]

generating systems and the weakened grid, resulting in instability.

Regarding resonance stability, there is limited research on the subject of the impact of cyber attacks. Additionally, by utilizing the classification of stability as it was presented in [14], resonance stability studies had to be separated into those that are related to converter-driven stability and those that are more about synchronous machines [139], [140]. Overall, it is found that well-informed attackers can target specific areas of the power system, e.g., through generation dispatch commands that result in loading changes or by injecting small amounts of power at frequencies corresponding to the torsional sub-synchronous resonance frequencies that would result in resonance instabilities. The reviewed papers for converter-driven and resonance stability, considering cyber attacks, are given in Table 8.

V. DISCUSSION AND RECOMMENDATIONS

A. MODELING CHALLENGES

Modeling the CPPS is pivotal for addressing current and future challenges regarding power system operation, including cyber security. The consideration of the power system communication network is important for cyber security studies, as it enables the study of several cyber attacks, as well as shows through simulations how cyber-physical attacks can occur. A significant challenge is that the communication network exact topology and characteristics are usually not known. Thus, modeling approaches are usually rough approximations of the actual communication infrastructure. This is more evident in models that seek to capture multiple domains of the CPPS.

Starting from the physical layer, an important gap in current research is that power system models that are currently used for stability studies are based on old testbeds. For instance, IEEE 9-bus, 39-bus, 118-bus, and Kundur's two-area system are the most common models used for studies considering transmission grids. New validated models are needed that capture the current and future states of the power systems, e.g., integration of RES, HVDC interconnections, etc. Furthermore, coordinated control and protection schemes need to be modeled and incorporated into these models, providing more realistic results regarding power system operation. Including the aforementioned schemes adds computational burden and increases the costs for implementation

TABLE 8. Impact of cyber attacks on converter-driven and resonance stability studies.

Stability category	Targets	Cyber attack types	Power system simulation type	Mitigation strategy	Year	Refs.
Converter-driven	Wind farm controller	MitM	EMT	Cyber-resilient control mechanisms	2021	[138]
		FDI			2021, 2022	[135], [136]
		DoS			2021, 2022	[135], [138]
	Circuit breakers	Malicious command injection			2021, 2022	[136], [137]
Resonance	Load frequency control	Malicious command injection	RMS	Countermeasures discussion	2018	[139]
	Battery storage system	Induced active power oscillations through control actions			2022	[140]

if hardware-in-the-loop is considered. But overall, as the power system operation is kept in safe margins due to the coordinated operation of such schemes, their consideration is necessary, especially for impact analysis.

To model the cyber layer, the work so far utilized various methods, but they can be summarized as i) using hardware-in-the-loop solutions, such as network switches, IEDs, routers, and gateways, ii) using simulation environments which are coupled with the power system usually with a co-simulation, and iii) using graph theoretic and mathematical formulations to formulate the behavior through simulations. Such approaches are utilized to study specific aspects of the interaction between the cyber and the physical power system. The main challenge that is identified is the lack of a standardized approach and the absence of benchmark cyber-physical models that can be used for comparative studies. Additionally, each cyber infrastructure suffers from the limitation of accuracy and modularity. Highly accurate testbeds, which usually contain hardware solutions, are not easy to expand.

Additionally, cyber-originated contingencies and events differ from purely physical events for CPPS. For instance, non-malicious failures in communication networks, i.e., delays or packet losses, could impact the physical system, as the operation of critical applications may be hindered. On top of that, malicious actions could result in a much bigger impact, as large areas could be affected. Finally, the IT and OT interactions are not adequately captured through simulations. Usually, research regarding CPPS stability focuses on the interaction of OT and power system operation. But to create more realistic scenarios, understand the cyber actor capabilities, and form appropriate mitigation strategies, the overall IT/OT infrastructure needs to be addressed.

B. CYBER SECURITY CONSIDERATIONS

A major concern is that existing power grid communication protocols may not be cyber-secure. Proposed cyber security improvements are based on a combination of secure IT protocols as carriers and power grid protocols as payloads. Newer secure protocol standards for power grids, such as IEC 62351, have also been proposed, but with limited adoption. Therefore, the development and widespread adoption of cyber-secure power grid communication protocols remains challenging.

Present-day power systems contain insufficient security control mechanisms. Most of the existing security controls are adopted from typical IT systems. With increased power grid digitalization, the adoption of cutting-edge IT systems brings cyber security challenges. This may involve the inheritance of advanced cyber threats from the IT domain into the power system OT domain. Hence, the adoption of advanced security controls and applications in power grids is crucial and must be accelerated. What is expected is that AI will pave a new reality, both for cyber attackers and defenders. Utilizing attack models based on AI, such as generative adversarial networks, as well as deep learning-based security controls and applications, could address the ongoing challenges in cyber security forensics. With the ever-increasing threat of cyber attacks targeting power grids, advanced artificial intelligence applications for power grid cyber security will be needed in the near future.

A research direction could be on how cyber actors can access and target the power system OT environment. So far, the research on cyber attacks targeting power systems focuses on the later stages of the kill chain, namely the impact on the operation. Although this assumption is valid for stability studies, the overall goal of increasing the cyber resilience of the CPPS cannot be achieved by focusing only on impact mitigation. It is important for researchers to focus on the interdisciplinarity of the CPPS. Such an approach could enhance the overall system resilience, help researchers investigate the feasibility and applicability of cyber attack types, and develop comprehensive security measures.

Regarding the cyber attack types studied, especially in the context of cyber attacks on power system operations, researchers focused on FDI attacks. While FDI attacks have a solid mathematical formulation, their feasibility in the context of a real-world power system is yet to be tested. Additionally, an alarming trend in the literature is that the

term is being used for different attack scenarios. In some papers, the definition of FDI is different than the one presented in the original study. As a result, the FDI term is used to describe many different attack types, from spoofing to tampering and generally MitM attacks. The term needs to have a clear definition. Otherwise, it could encapsulate many different attack types, which could cause confusion to the research community.

Furthermore, it is important to consider coordinated cyber attacks with serial or parallel phases. A typical example found in the literature is the DoS attacks on measurement nodes. By itself, the attack could result in limited impact on the power system operation, but in combination with an additional cyber attack like switching or tampering, it could magnify the impact. Finally, the consideration of cyber vulnerabilities for power system stability studies, considering the CPPS interconnections, is of paramount importance as they could define the targets of the attackers.

C. POWER SYSTEM STABILITY TO CYBER ATTACKS

Regarding the impact of cyber attacks on power system stability, it was found that most of the existing research focused on rotor angle, voltage, and frequency stability. This was an expected outcome, as these definitions are better understood [35]. Converter-driven stability is expected to become a more emerging topic. Thus, as mentioned in Section V-A, it is important to have new testbeds that can capture the current and future states of the grid. Such models could be utilized to investigate the converter-driven stability more in-depth.

From the state-of-the-art analysis, it is found that researchers investigated mainly cyber attacks on control systems. Misleading or jeopardizing WAMPAC applications and local voltage and frequency controllers were the most common targets. The cyber attack scenarios involved tampering with the control setpoints or critical measurements, as well as induced delay attacks on the communication channels. Such cyber attacks require a deep understanding of the targeted control system by the attackers, and the effects are shown to be quite significant. A well-executed attack could severely affect the stability of the system. On the other hand, switching attacks targeting circuit breakers of important substations or power plants are also shown to be capable of resulting in significant impact. In both attack scenarios, the cyber actors were considered knowledgeable about the grid topology, systems, and operational characteristics. Two equally important future research directions are identified. The first is considering how cyber actors can obtain such information through insiders or extended reconnaissance. The other is to investigate more realistic attack scenarios, assessing not only the impact but the feasibility of such scenarios. In both cases, important conclusions could be drawn, improving the overall understanding of the vulnerabilities of both the cyber and the physical systems of a CPPS.

In the reviewed research, FDI attacks were the main cyber attack type utilized. An interesting fact is that these cyber attacks were used to test the effectiveness of proposed controllers by examining cases of cyber attacks occurring in parallel with physical contingencies. The latter was mainly a physical fault, such as a three-phase short-circuit, which brought the system to an unstable equilibrium, with the aim of the FDI attacks being to hinder the controller response. As a result, these scenarios do not fully address the cyber resilience of the CPPS, and more realistic ones are needed. Coordinated attacks could utilize FDI attacks as a way of masking the impact of other cyber attacks. However, current research still lacks such approaches. Furthermore, it must be noted that current research is mainly focusing on the physical aspect of CPPS operational stability. Studies investigating both the cyber and physical stability of CPPS are limited due to the modeling challenges of the cyber layer. Although the stability of the communication network could be evaluated, especially in the case of DoS and time delay attacks, the interactions between the cyber and physical systems need to be assessed further.

Finally, AI methods are expected to revolutionize the monitoring and control applications that are present in today's power systems. The availability of phasor measurements and the advanced computational infrastructure could significantly enhance the capabilities of automatic controllers, improve the situational awareness of grid operators, and be used for tasks such as anomaly detection, mitigation strategies, and faster grid restoration. Additionally, as the research on explainable AI is advancing, such models would not only be optimized but also gain the trust of the stakeholders and the community.

VI. CONCLUSION

This work presents a comprehensive assessment of the impact of cyber attacks on power system stability. The traditional disturbances considered in power system stability classification are expanded from physical to cyber-physical disturbances caused by cyber attacks. Each power system stability category is mapped with cyber-physical attack types based on a thorough state-of-the-art analysis. It has been found that knowledgeable cyber actors could severely impact all categories of power system stability by targeting the measurement infrastructure, critical control and protection applications, communication channels, or a combination of them. The interdependency of the physical power system with the complex communication and computational infrastructure can be exploited by cyber actors, enabling them to cause small or large disturbances to the physical power grid via the cyber layer. The aforementioned findings showcase the importance of considering cyber security for physical power system stability, which could lead to a further extension of the classification of power system stability.

Based on this study, key future research directions are identified. Comprehensive benchmark cyber-physical power system models need to be developed to analyze the cyber-physical interactions. Additionally, future algorithms and methods for the detection and mitigation of cyber attacks on power systems need to consider the timeframe of the affected stability phenomena and be implemented in the most

critical systems. As a result, computationally fast solutions for online stability assessment, intrusion detection systems, and mitigation algorithms need to be developed.

REFERENCES

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

[2] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, Apr. 2011.

[3] S. Bitchkei. (2023). *Dragonfly 2.0 Targets Energy Sector Gaining Access to SCADA Systems*. Accessed: Jan. 06, 2023. [Online]. Available: https://hitachi-systems-security.com/dragonfly-2-0-targets-energy-sector-gaining-access-to-scada-systems/

[4] 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.

[5] M. J. Assante, R. M. Lee, and T. Conway, "ICS defense use case no. 6: Modular ICS malware," Electr. Inf. Sharing Center (E-ISAC), Tech. Rep., Aug. 2017, vol. 2, pp. 1–27.

[6] N. Stoler. (2023). *Anatomy of the Triton Malware Attack*. Accessed: Jan. 06, 2023. [Online]. Available: https://www.cyberark.com/resources/threat-research-blog/anatomy-of-the-triton-malware-attack/

[7] K. Leetaru. (2019). *Could Venezuela's Power Outage Really be a Cyber Attack?*. Accessed: Jan. 06, 2023. [Online]. Available: https://www.forbes.com/sites/kalevleetaru/2019/03/09/could-venezuelas-power-outage-really-be-a-cyber

[8] (2023). *The SolarWinds Cyber Attack: What You Need to Know*. Accessed: Jan. 06, 2023. [Online]. Available: https://www.cisecurity.org/solarwinds

[9] L. Mathews. (2021). *Florida Water Plant Hackers Exploited Old Software and Poor Password Habits*. Accessed: Jan. 06, 2023. [Online]. Available: https://www.forbes.com/sites/leemathews/2021/02/15/florida-water-plant-hackers-exploited-old-software-and-poor-password-habits/

[10] J. Robertson, and W. Turton. (2023). *Colonial Hackers Stole Data Thursday Ahead of Shutdown*. Accessed: Jan. 06, 2023. [Online]. Available: https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown

[11] J. A. Guerrero-Saade, and M. van Amerongen. (2023). *AcidRain A Modem Wiper Rains Down on Europe*. Accessed: Jan. 06, 2023. [Online]. Available: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

[12] (2023). *Cyber Attack on Deutsche Windtechnik*. Accessed: Jan. 06, 2023. [Online]. Available: https://www.deutsche-windtechnik.com/en/news/details/cyber

[13] D. K. Zafra. (2023). *INDUSTROYER.V2: Old Malware Learns New Tricks*. Accessed: Jan. 06, 2023. [Online]. Available: https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks

[14] N. Hatziargyriou, J. Milanovic, C. Rahmann, V. Ajjarapu, C. Canizares, I. Erlich, D. Hill, I. Hiskens, I. Kamwa, B. Pal, P. Pourbeik, J. Sanchez-Gasca, A. Stankovic, T. Van Cutsem, V. Vittal, and C. Vournas, "Definition and classification of power system stability—Revisited & extended," *IEEE Trans. Power Syst.*, vol. 36, no. 4, pp. 3271–3281, Jul. 2021.

[15] M. Abdelmalak, V. Venkataramanan, and R. Macwan, "A survey of cyber-physical power system modeling methods for future energy systems," *IEEE Access*, vol. 10, pp. 99875–99896, 2022.

[16] O. A. Alimi, K. Ouahada, and A. M. Abu-Mahfouz, "A review of machine learning approaches to power system security and stability," *IEEE Access*, vol. 8, pp. 113512–113531, 2020.

[17] A. Mehrzad, M. Darmiani, Y. Mousavi, M. Shafie-Khah, and M. Aghamohammadi, "A review on data-driven security assessment of power systems: Trends and applications of artificial intelligence," *IEEE Access*, vol. 11, pp. 78671–78685, 2023.

[18] M. Amroune, "Machine learning techniques applied to on-line voltage stability assessment: A review," *Arch. Comput. Methods Eng.*, vol. 28, no. 2, pp. 273–287, Mar. 2021.

[19] L. Xiong, X. Liu, Y. Liu, and F. Zhuo, "Modeling and stability issues of voltage-source converter-dominated power systems: A review," *CSEE J. Power Energy Syst.*, vol. 8, no. 6, pp. 1530–1549, Nov. 2022.

[20] A. A. Smadi, B. T. Ajao, B. K. Johnson, H. Lei, Y. Chakhchoukh, and Q. Abu Al-Haija, "A comprehensive survey on cyber-physical smart grid testbed architectures: Requirements and challenges," *Electronics*, vol. 10, no. 9, p. 1043, Apr. 2021.

[21] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy," *IEEE Access*, vol. 10, pp. 35846–35875, 2022.

[22] 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.

[23] R. M. Czekster, C. Morisset, J. A. Clark, S. Soudjani, C. Patsios, and P. Davison, "Systematic review of features for co-simulating security incidents in cyber-physical systems," *Secur. Privacy*, vol. 4, no. 3, pp. 1–20, May 2021.

[24] P. Mihal, M. Schvarcbacher, B. Rossi, and T. Pitner, "Smart grids co-simulations: Survey & research directions," *Sustain. Comput. Informat. Syst.*, vol. 35, Sep. 2022, Art. no. 100726.

[25] S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," *Comput. Secur.*, vol. 70, pp. 436–454, Sep. 2017.

[26] O. A. Alimi, K. Ouahada, A. M. Abu-Mahfouz, S. Rimer, and K. O. A. Alimi, "A review of research works on supervised learning algorithms for SCADA intrusion detection and classification," *Sustainability*, vol. 13, no. 17, p. 9597, Aug. 2021.

[27] H. Cui, Y. Zhang, K. L. Tomsovic, and F. Li, "Power electronics-interfaced cyber-physical power systems: A review on modeling, simulation, and cybersecurity," *WIREs Energy Environ.*, vol. 11, no. 6, pp. 1–24, Nov. 2022.

[28] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G.-S. Seo, W. Song, M. D. R. Greidanus, S. Sahoo, F. Blaabjerg, J. Zhang, L. Guo, B. Ahn, M. B. Shadmand, N. R. Gajanur, and M. A. Abbaszada, "A review of cyber–physical security for photovoltaic systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 4, pp. 4879–4901, Aug. 2022.

[29] B. Canaan, B. Colicchio, and D. Ould Abdeslam, "Microgrid cybersecurity: Review and challenges toward resilience," *Appl. Sci.*, vol. 10, no. 16, p. 5649, Aug. 2020.

[30] J. Wang and D. Shi, "Cyber-attacks related to intelligent electronic devices and their countermeasures: A review," in *Proc. 53rd Int. Universities Power Eng. Conf. (UPEC)*, Sep. 2018, pp. 1–6.

[31] M. N. Nafees, N. Saxena, A. Cardenas, S. Grijalva, and P. Burnap, "Smart grid cyber-physical situational awareness of complex operational technology attacks: A review," *ACM Comput. Surveys*, vol. 55, no. 10, pp. 1–36, Oct. 2023.

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

[33] V. Aravinthan, T. Balachandran, M. Ben-Idris, W. Fei, M. Heidari-Kapourchali, A. Hettiarachchige-Don, J. N. Jiang, H. Lei, C.-C. Liu, J. Mitra, M. Ni, M. Papic, M. Parvania, M. Sephary, C. Singh, A. Srivastava, A. Stefanov, H. Sun, and S. Tindemans, "Reliability modeling considerations for emerging cyber-physical power systems," in *Proc. IEEE Int. Conf. Probabilistic Methods Appl. Power Syst. (PMAPS)*, Jun. 2018, pp. 1–7.

[34] P. Bernus and L. Nemes, "A framework to define a generic enterprise reference architecture and methodology," *Comput. Integr. Manuf. Syst.*, vol. 9, no. 3, pp. 179–191, Jul. 1996.

[35] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, and V. Vittal, "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions," *IEEE Trans. Power Syst.*, vol. 19, no. 3, pp. 1387–1401, Aug. 2004.

[36] A. Farraj, E. Hammad, and D. Kundur, "A cyber-physical control framework for transient stability in smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1205–1215, Mar. 2018.

[37] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized phasor measurement applications in power systems," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 20–27, Jun. 2010.

[38] M. Yu, A. J. Roscoe, C. D. Booth, A. Dysko, R. Ierna, J. Zhu, N. Grid, and H. Urdal, "Use of an inertia-less virtual synchronous machine within future power networks with high penetrations of converters," in *Proc. Power Syst. Comput. Conf. (PSCC)*, Genoa, Italy, Jun. 2016, pp. 1–7.

[39] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proc. IEEE*, vol. 95, no. 1, pp. 138–162, Jan. 2007.

[40] S. Dennetiere, H. Saad, Y. Vernay, P. Rault, C. Martin, and B. Clerc, "Supporting energy transition in transmission systems: An operator's experience using electromagnetic transient simulation," *IEEE Power Energy Mag.*, vol. 17, no. 3, pp. 48–60, May 2019.

[41] C. Gomes, "Co-simulation: A survey," in *ACM Comput. Surv.*, vol. 51, no. 3, pp. 1–33, 2018.

[42] M. Assante and R. Lee, "The industrial control system cyber kill chain," *SANS Institute InfoSec Reading Room*, vol. 1, no. 1, pp. 1–2, Oct. 2015.

[43] A. Hahn, R. K. Thomas, I. Lozano, and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," *Int. J. Crit. Infrastruct. Protection*, vol. 11, pp. 39–50, Dec. 2015.

[44] *Cybersecurity Year in Review*, document 2022 ICS/OT, DRAGOS Inc., 2023.

[45] *Communication Networks and Systems for Power Utility Automation*, Standard IEC 61850, 2013.

[46] *Telecontrol Equipment and Systems—Part 5-104: Transmission Protocols—Network Access for IEC 60870-5-101 Using Standard Transport Profiles*, Standard IEC Standard 60870, 2006.

[47] B. G. Thomas and C. Controls, "Introduction to the modbus protocol," *Tech. supp. to control Netw.*, vol. 9, no. 4, pp. 4–7, Jul. 2008.

[48] R. Nardone, R. J. Rodríguez, and S. Marrone, "Formal security assessment of modbus protocol," in *Proc. 11th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2016, pp. 142–147.

[49] M. de Vivo, G. O. de Vivo, R. Koeneke, and G. Isern, "Internet vulnerabilities related to TCP/IP and T/TCP," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 29, no. 1, pp. 81–85, Jan. 1999.

[50] E. Samuel, "A taxonomy of attacks on the DNP3 protocol," in *Proc. Int. Conf. Crit. Infrastruct. Protection*, 2009, pp. 67–81.

[51] C. Brunner, "IEC 61850 for power system communication," in *Proc. IEEE/PES Transmiss. Distribution Conf. Expo.*, Apr. 2008, pp. 1–6.

[52] S. S. M. Hussain, C. Yaohao, M. M. Roomi, D. Mashima, and E.-C. Chang, "An open-source framework for publishing/subscribing IEC 61850 R-GOOSE and R-SV," *SoftwareX*, vol. 23, Jul. 2023, Art. no. 101415.

[53] 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-Europe)*, The Hague, Netherlands, Oct. 2020, pp. 247–254.

[54] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5643–5654, Sep. 2020.

[55] 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 Model. Simul. Cyber-Physical Energy Syst.*, Apr. 2020, pp. 1–6.

[56] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, "Intrusion detection system for IEC 60870-5-104 based SCADA networks," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2013, pp. 1–5.

[57] C. R. and M. Uslar, "Smart grid security: IEC 62351 and other relevant standards," in *Standardization Smart Grids*. Berlin, Germany: Springer, 2013, pp. 129–146.

[58] M. Strobel, N. Wiedermann, and C. Eckert, "Novel weaknesses in IEC 62351 protected smart grid control systems," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Nov. 2016, pp. 266–270.

[59] A. Carcano, A. Di Pinto, Y. Dragoni, and A. Carcano, *The Future of Securing Intelligent Electronic Devices Using the IEC 62351-7 Standard for Monitoring*, Standard 62351-7, 2019.

[60] *IEEE Standard for Synchrophasor Data Transfer for Power Systems*, Standard Std C37.118.2-2011, 2011, pp. 1–53.

[61] S. Vahidi, M. Ghafouri, M. Au, M. Kassouf, A. Mohammadi, and M. Debbabi, "Security of wide-area monitoring, protection, and control (WAMPAC) systems of the smart grid: A survey on challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1294–1335, 2nd Quart., 2023.

[62] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.

[63] *IEEE Standard for Phasor Data Concentrators for Power Systems*, IEEE Standard C37.247, 2019, pp. 1–44.

[64] K. P. Swain, A. Tiwari, A. Sharma, S. Chakrabarti, and A. Karkare, "Comprehensive demonstration of man-in-the-middle attack in PDC and PMU network," in *Proc. 22nd Nat. Power Syst. Conf. (NPSC)*, Dec. 2022, pp. 213–217.

[65] A. Chawla, A. Singh, P. Agrawal, B. K. Panigrahi, B. R. Bhalja, and K. Paul, "Denial-of-service attacks pre-emptive and detection framework for synchrophasor based wide area protection applications," *IEEE Syst. J.*, vol. 16, no. 1, pp. 1570–1581, Mar. 2022.

[66] J. T. Robinson, T. Saxton, A. Vojdani, D. Ambrose, G. Schimmel, R. R. Blaesing, and R. Larson, "Development of the intercontrol center communications protocol (ICCP) [power system control]," in *Proc. Power Ind. Comput. Appl. Conf.*, 1995, pp. 449–455.

[67] M. Franz, "ICCP exposed: Assessing the attack surface of the utility stack," in *Proc. SCADA Secur. Sci. Symp.*, 2007, pp. 1–14.

[68] J. T. Michalski, A. Lanzone, J. Trent, and S. Smith. (2007). *Secure ICCP Integration Considerations and Recommendations*. Accessed: Aug. 28, 2023. [Online]. Available: https://energy.sandia.gov/wp-content/gallery/uploads/Michalski-2007-3345.pdf

[69] A. Hahn, "Operational technology and information technology in industrial control systems," in *Advances in Information Security*. Berlin, Germany: Springer, 2016, pp. 51–68.

[70] D. Ranathunga, M. Roughan, H. Nguyen, P. Kernick, and N. Falkner, "Case studies of SCADA firewall configurations and the implications for best practices," *IEEE Trans. Netw. Service Manage.*, vol. 13, no. 4, pp. 871–884, Dec. 2016.

[71] D. Upadhyay and S. Sampalli, "SCADA (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101666.

[72] *Common Vulnerabilities and Exposures (CVE) of SCADA*. Accessed: Sep. 20, 2023. [Online]. Available: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SCADA

[73] D. Gonzalez, F. Alhenaki, and M. Mirakhorli, "Architectural security weaknesses in industrial control systems (ICS) an empirical study based on disclosed software vulnerabilities," in *Proc. IEEE Int. Conf. Softw. Archit. (ICSA)*, Hamburg, Germany, Mar. 2019, pp. 31–40.

[74] G. Yadav and K. Paul, "PatchRank: Ordering updates for SCADA systems," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Zaragosa, Spain, Sep. 2019, pp. 110–117.

[75] M. Kol and S. Oberman. (2020). *CVE-2020-11896 RCE and CVE-2020-11898 Info Leak*. Accessed: Aug. 25, 2023. [Online]. Available: https://www.jsof-tech.com/wp-content/uploads/2020/06/JSOF_Ripple20_Technical_Whitepaper_June20.pdf

[76] M. Kol, A. Schon, and S. Oberman. (2020). *CVE-2020-11901*. Accessed: Nov. 25, 2023. [Online]. Available: https://www.jsof-tech.com/wp-content/uploads/2020/08/Ripple20_CVE-2020-11901-August20.pdf

[77] J. D. Tygar, "Adversarial machine learning," *IEEE Internet Comput.*, vol. 15, no. 5, pp. 4–6, Sep. 2011.

[78] H. Ying, X. Ouyang, S. Miao, and Y. Cheng, "Power message generation in smart grid via generative adversarial network," in *Proc. IEEE 3rd Inf. Technol., Netw., Electron. Autom. Control Conf. (ITNEC)*, Chengdu, China, Mar. 2019, pp. 790–793.

[79] S. Asri and B. Pranggono, "Impact of distributed denial-of-service attack on advanced metering infrastructure," *Wireless Pers. Commun.*, vol. 83, no. 3, pp. 2211–2223, Aug. 2015.

[80] R. Kalluri, L. Mahendra, R. K. S. Kumar, and G. L. G. Prasad, "Simulation and impact analysis of denial-of-service attacks on power SCADA," in *Proc. Nat. Power Syst. Conf. (NPSC)*, Bhubaneswar, India, Dec. 2016, pp. 1–5.

[81] S. M. Farooq, S. Nabirasool, S. Kiran, S. M. Suhail Hussain, and T. S. Ustun, "MPTCP based mitigation of denial of service (DoS) attack in PMU communication networks," in *Proc. IEEE Int. Conf. Power Electron., Drives Energy Syst. (PEDES)*, Chennai, India, Dec. 2018, pp. 1–5.

[82] K. Gai, M. Qiu, Z. Ming, H. Zhao, and L. Qiu, "Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2431–2439, Sep. 2017.

[83] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to GPS spoofing," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3535–3548, Jul. 2019.

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

[85] Y. Song, X. Liu, Z. Li, M. Shahidehpour, and Z. Li, "Intelligent data attacks against power systems using incomplete network information: A review," *J. Modern Power Syst. Clean Energy*, vol. 6, no. 4, pp. 630–641, Jul. 2018.

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

[87] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[88] B. Singer, A. Pandey, S. Li, L. Bauer, C. Miller, L. Pileggi, and V. Sekar, "Shedding light on inconsistencies in grid cybersecurity: Disconnects and recommendations," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2023, pp. 38–55.

[89] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proc. Int. Conf. Internet Things 4th Int. Conf. Cyber, Phys. Social Comput.*, Oct. 2011, pp. 380–388.

[90] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2862–2872, Jul. 2018.

[91] M. Jafari, M. A. Rahman, and S. Paudyal, "False data injection attack against power system small-signal stability," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2021, pp. 1–5.

[92] J. Hou, J. Wang, Y. Song, W. Sun, and Y. Hou, "Small-signal angle stability-oriented false data injection cyber-attacks on power systems," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 635–648, Jan. 2023.

[93] A. Farraj, E. Hammad, and D. Kundur, "On the impact of cyber attacks on data integrity in storage-based transient stability control," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3322–3333, Dec. 2017.

[94] Y. Li, Z. Li, and L. Chen, "Dynamic state estimation of generators under cyber attacks," *IEEE Access*, vol. 7, pp. 125253–125267, 2019.

[95] A. A. Jahromi, A. Kemmeugne, D. Kundur, and A. Haddadi, "Cyber-physical attacks targeting communication-assisted protection schemes," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 440–450, Jan. 2020.

[96] J. Wei, D. Kundur, and K. L. Butler-Purry, "A novel bio-inspired technique for rapid real-time generator coherency identification," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 178–188, Jan. 2015.

[97] B. Chen, S. Mashayekh, K. L. Butler-Purry, and D. Kundur, "Impact of cyber attacks on transient stability of smart grids with voltage support devices," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2013, pp. 1–5.

[98] Z. Zhang, K. Zuo, R. Deng, F. Teng, and M. Sun, "Cybersecurity analysis of data-driven power system stability assessment," *IEEE Internet Things J.*, vol. 10, no. 17, pp. 15723–15735, Sep. 2023.

[99] J. Wei and G. J. Mendis, "A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids," in *Proc. Joint Workshop Cyber-Phys. Secur. Resilience Smart Grids (CPSR-SG)*, Apr. 2016, pp. 1–6.

[100] M. Ayar, R. D. Trevizan, S. Obuz, A. S. Bretas, H. A. Latchman, and N. G. Bretas, "Cyber-physical robust control framework for enhancing transient stability of smart grids," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 2, no. 4, pp. 198–206, Dec. 2017.

[101] M. Kesici, M. Mohammadpourfard, K. Aygul, and I. Genc, "Deep learning-based framework for real-time transient stability prediction under stealthy data integrity attacks," *Electric Power Syst. Res.*, vol. 221, Aug. 2023, Art. no. 109424.

[102] D. Wu, F. Ma, M. Javadi, and J. N. Jiang, "Fast screening severe cyber attacks via transient energy-based impact analysis," *CSEE J. Power Energy Syst.*, vol. 2, no. 3, pp. 28–34, Sep. 2016.

[103] A. Farraj, E. Hammad, A. A. Daoud, and D. Kundur, "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1846–1855, Jul. 2016.

[104] B. Huang, M. Majidi, and R. Baldick, "Case study of power system cyber attack using cascading outage analysis model," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Portland, OR, USA, Aug. 2018, pp. 1–5.

[105] Z. Wang and J. Wang, "A practical distributed finite-time control scheme for power system transient stability," *IEEE Trans. Power Syst.*, vol. 35, no. 5, pp. 3320–3331, Sep. 2020.

[106] M. Ayar, S. Obuz, R. D. Trevizan, A. S. Bretas, and H. A. Latchman, "A distributed control approach for enhancing smart grid transient stability and resilience," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 3035–3044, Nov. 2017.

[107] J. Wei, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2687–2700, Nov. 2014.

[108] N. M. Alyazidi, "Improve$_1$ networked adaptive approach to load frequency power control under cyber attacks," *IEEE Access*, vol. 10, pp. 131680–131690, 2022.

[109] D. Roberson and J. F. O'Brien, "Variable loop gain using excessive regeneration detection for a delayed wide-area control system," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6623–6632, Nov. 2018.

[110] H. Huang and K. Davis, "Power system equipment cyber-physical risk assessment based on architecture and critical clearing time," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids*, Oct. 2018, pp. 1–6.

[111] M. Ghafouri, M. Au, M. Kassouf, M. Debbabi, C. Assi, and J. Yan, "Detection and mitigation of cyber attacks on voltage stability monitoring of smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5227–5238, Nov. 2020.

[112] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015.

[113] Y. Li, Y. Wang, and S. Hu, "Online generative adversary network based measurement recovery in false data injection attacks: A cyber-physical approach," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2031–2043, Mar. 2020.

[114] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2158–2169, Mar. 2019.

[115] 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.

[116] H. Zhang, B. Liu, X. Liu, A. Pahwa, and H. Wu, "Voltage stability constrained moving target defense against net load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3748–3759, Sep. 2022.

[117] D. I. Dogaru and I. Dumitrache, "Robustness of power systems in the context of cyber attacks," in *Proc. 21st Int. Conf. Control Syst. Comput. Sci. (CSCS)*, Bucharest, Romania, May 2017, pp. 506–512.

[118] H. Zhang, N. Fulk, B. Liu, L. Edmonds, X. Liu, and H. Wu, "Load margin constrained moving target defense against false data injection attacks," in *Proc. IEEE Green Technol. Conf. (GreenTech)*, Houston, TX, USA, Mar. 2022, pp. 51–56.

[119] M. Elimam, Y. J. Isbeih, S. K. Azman, M. S. E. Moursi, and K. A. Hosani, "Deep learning-based PMU cyber security scheme against data manipulation attacks with WADC application," *IEEE Trans. Power Syst.*, vol. 38, no. 3, pp. 2148–2161, May 2023.

[120] U. Adhikari, T. Morris, and S. Pan, "WAMS cyber-physical test bed for power system, cybersecurity study, and data mining," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2744–2753, Nov. 2017.

[121] M. Ni, Y. Xue, H. Tong, and M. Li, "A cyber physical power system co-simulation platform," in *Proc. Workshop Model. Simul. Cyber-Phys. Energy Syst. (MSCPES)*, Porto, Portugal, Apr. 2018, pp. 1–5.

[122] C. Chen, K. Zhang, M. Ni, and Y. Wang, "Cyber-attack-tolerant frequency control of power systems," *J. Modern Power Syst. Clean Energy*, vol. 9, no. 2, pp. 307–315, Mar. 2021.

[123] M. Jafari, M. Ashiqur Rahman, and S. Paudyal, "Optimal false data injection attacks against power system frequency stability," *IEEE Trans. Smart Grid*, vol. 14, no. 2, pp. 1276–1288, Mar. 2023.

[124] C. Chen, X. Zhang, M. Cui, K. Zhang, J. Zhao, and F. Li, "Stability assessment of secondary frequency control system with dynamic false data injection attacks," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3224–3234, May 2022.

[125] 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.
[126] G. Zhang, J. Li, O. Bamisile, Y. Xing, D. Cai, and Q. Huang, "An H_∞ load frequency control scheme for multi-area power system under cyber-attacks and time-varying delays," *IEEE Trans. Power Syst.*, vol. 38, no. 2, pp. 1336–1349, Mar. 2023.
[127] C. Chen, Y. Chen, J. Zhao, K. Zhang, M. Ni, and B. Ren, "Data-driven resilient automatic generation control against false data injection attacks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8092–8101, Dec. 2021.
[128] M. Khalaf, A. Ayad, M. M. A. Salama, D. Kundur, and E. F. El-Saadany, "Mitigation of cyber-attacks on wide-area under-frequency load-shedding schemes," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2377–2389, May 2023.
[129] 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.
[130] 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.
[131] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-service (dos) attacks on load frequency control in smart grids," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2013, pp. 1–6.
[132] A. Sargolzaei, K. Yen, and M. N. Abdelghani, "Delayed inputs attack on load frequency control in smart grid," in *Proc. ISGT*, Feb. 2014, pp. 1–5.
[133] S. Shahkar and K. Khorasani, "A resilient control against time-delay switch and denial of service cyber attacks on load frequency control of distributed power systems," in *Proc. IEEE Conf. Control Technol. Appl. (CCTA)*, Aug. 2020, pp. 718–725.
[134] M. M. Hossain, C. Peng, H.-T. Sun, and S. Xie, "Bandwidth allocation-based distributed event-triggered LFC for smart grids under hybrid attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 820–830, Jan. 2022.
[135] A. Amini, M. Ghafouri, A. Mohammadi, M. Hou, A. Asif, and K. Plataniotis, "Secure sampled-data observer-based control for wind turbine oscillation under cyber attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 3188–3202, Jul. 2022.
[136] M. Ghafouri, U. Karaagac, A. Ameli, J. Yan, and C. Assi, "A cyber attack mitigation scheme for series compensated DFIG-based wind parks," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5221–5232, Nov. 2021.
[137] H. Du, J. Yan, M. Ghafouri, R. Zgheib, and M. Debbabi, "Online attack-aware risk management for PMSG-based wind farm depending on system strength evaluation," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids*, Oct. 2022, pp. 218–223.
[138] H. Du, J. Yan, M. Ghafouri, R. Zgheib, M. Kassouf, and M. Debbabi, "Modeling of cyber attacks against converter-driven stability of PMSG-based wind farms with intentional subsynchronous resonance," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids*, Oct. 2021, pp. 391–397.
[139] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, "Resonance attacks on load frequency control of smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4490–4502, Sep. 2018.
[140] B. Li, B. Zhang, and D. S. Kirschen, "Cyber-physical attack leveraging subsynchronous resonance," 2022, *arXiv:2207.04149*.

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 B.Sc. and M.Sc. degrees (Hons.) in power systems engineering from the University Politehnica of Bucharest (UPB), Romania, in 2009 and 2011, respectively, and the Ph.D. degree (Hons.) from University College Dublin, Ireland, in 2014. From 2015 to 2018, he was a Professional Engineer with the Future Networks Section, Operations Department, ESB Networks, the distribution system operator in Ireland. From 2018 to 2019, he was a Senior Engineer with NovoGrid Ltd., Dublin, Ireland. Since 2019, he has been an Assistant Professor in intelligent electrical power grids with the Faculty of Electrical Engineering, Mathematics and Computer Science, TU Delft. He is currently the Technical Director of the Control Room of the Future (CRoF) Technology Centre, Department of Electrical Sustainable Energy. His research interests include cyber security for power grids, resilience of cyber-physical systems, and next generation grid operation. He holds the professional title of a Chartered Engineer from Engineers Ireland.

ALFAN PRESEKAL (Member, IEEE) received the B.Eng. degree in computer engineering from Universitas Indonesia, in 2014, and the M.Sc. degree in secure software system from the Imperial College, London, U.K., in 2016. He is currently pursuing the Ph.D. degree with the Department of Electrical Sustainable Energy, Delft University of Technology, The Netherlands. He was a Junior Lecturer with the Department of Electrical Engineering, Universitas Indonesia, from 2017 to 2019. He participated in an exchange research program with the Department Information and Communication Engineering, Tokyo Institute of Technology, from 2012 to 2013. He was also the Webmaster and on the communication activities committee, IEEE Indonesia Section, from 2017 to 2019. He holds various certifications from CISCO, EC Council, and CompTIA in the cyber security area. His main research interests include cyber security, cyber-physical systems, and artificial intelligence for power system applications.

BAS KRUIMER (Member, IEEE) was born in Curaçao, The Netherlands Antilles, in 1963. He received the degree in power engineering from Delft Technical University, Delft, The Netherlands, in 1988. He worked for ABB in substation automation, protection, and network control nationally and internationally. In 2002, he joined KEMA T&D Consulting leading the Design and Engineering Team. In 2006, he led the Quality Management Systems Business of KEMA Quality, and in early 2008, he joined Infra Company of Dutch Utility Eneco, today named Joulz. In August 2010, he joined Quanta Technology, Rotterdam, The Netherlands. During his professional years, he has contributed to Dutch Cigre and to IEEE and has been an active player in the IEC 61850 developments for many years.

JOSÉ LUIS RUEDA TORRES (Senior Member, IEEE) was born in 1980. He received the Diploma degree (cum laude) in electrical engineering from the Escuela Politécnica Nacional, Quito, Ecuador, in August 2004, and the Ph.D. degree (Hons.) in electrical engineering from the National University of San Juan, in November 2009. He is currently an Associate Professor leading the Research Team on Dynamic Stability of Sustainable Electrical Power Systems, Intelligent Electrical Power Grids Section, Electrical Sustainable Energy Department, Delft University of Technology, Delft, The Netherlands. From September 2003 to February 2005, he worked in Ecuador, in the fields of industrial control systems and electrical distribution networks operation and planning. Between August 2010 and February 2014, he was a Postdoctoral Research Associate with the Institute of Electrical Power Systems, University Duisburg-Essen, Duisburg, Germany. His research interests include physics-driven analysis of stability phenomena dynamic equivalencing of HVDC-HVAC systems, probabilistic multi-systemic reliability and stability management, and adaptive-optimal resilient multi-objective controller design. Currently, he is a member of the Technical Committee on Power and Energy Systems of International Federation of Automatic Control (IFAC), the Chairman of the IEEE PES Working Group on Modern Heuristic Optimization, the Secretary of CIGRE JWG C4/C2.58/IEEE ''Evaluation of Voltage Stability Assessment Methodologies in Transmission Systems,'' the Vice-Chair of the IEEE PES Intelligent Systems Subcommittee, and the Vice-Chair of the IFAC Technical Committee TC 6.3. Power and Energy Systems on Social Media.

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 became appointed as the Head of the Business Unit on Sustainable Building Technologies, Austrian Institute of Technology (AIT), where he was a first Principal Scientist in complex energy systems. In 2014, he was appointed as a Full Professor in intelligent electric power grids with TU Delft. He is active in international committees, such as ISO or 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.