Received: 5 April 2021 | Revised: 5 February 2022 | Accepted: 26 April 2022

DOI: 10.1002/wene.448

ADVANCED REVIEW

WIREs ENERGY AND ENVIRONMENT WILEY

Power electronics-interfaced cyber-physical power systems: A review on modeling, simulation, and cybersecurity

Hantao Cui[1] | Yichen Zhang[2] | Kevin L. Tomsovic[3] | Fangxing (Fran) Li[3]

[1]School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, Oklahoma, USA

[2]Energy Systems Division, Argonne National Laboratory, Lemont, Illinois, USA

[3]Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, Tennessee, USA

Correspondence
Kevin L. Tomsovic, Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, USA.
Email: tomsovic@utk.edu

Funding information
National Science Foundation, Grant/Award Number: EEC-1041877; CURENT Industry Partnership Program

Edited by: Damian Flynn, Associate Editor and Peter Lund, Editor-in-Chief

Abstract

We present the review of two interlinked challenges in modern electric power systems: the transformation to a cyber-physical system, and the integration of power electronics-interfaced renewables. Electric power systems are being modernized with the integration of power electronics-interfaced devices (PEID) and communication-enabled cyber-applications. This paper reviews the concepts, studies, and testbeds for cyber-physical power systems (CPPS), as well as the modeling of power electronics-based devices for physical power system stability simulations. The CPPS concept is introduced in the National Institute of Standard Technology framework for cyber-physical systems, with an emphasis on CPPS subsystems. For the physical subsystem, PEID components are generalized into the primary source and the grid interface, while controllers are generalized as a reference generator and a reference tracker. Next, the cybersecurity research objectives are summarized, followed by a categorization of CPPS studies. Further, testbed techniques for integrating communication networks with power system simulation are reviewed. Also, challenges and future directions in the area of CPPS are discussed.

This article is categorized under:

Energy Infrastructure > Systems and Infrastructure

KEYWORDS

converter modeling, cyber-physical system, renewable energy

1 | INTRODUCTION

Power systems are benefiting from the integration of wide-area monitoring and control systems, which stream data over communication networks. Such integration creates a cyber-physical power system (CPPS) with power flow in the grid and data flow in communication networks. Traditional methods and tools for the physical power system cannot take into account the dynamics in the cyber system. Therefore, the composition of CPPS needs to be clarified, and the research methods for CPPS modeling, optimization, control, and cybersecurity need to be reviewed toward fully understanding cyber-physical interactions.

In the physical system, power electronic technologies have been utilized for renewable integration, high-voltage direct current transmission (HVDC), flexible alternating current (AC) transmission system, and many other advanced fast grid supporting functionalities, such as power buffer and electric springs, due to their high controllability. It is projected that future resilient and low-carbon power grids will heavily rely on massive power electronics-interfaced devices (PEIDs), which will significantly reshape power system dynamics.

Large-scale integration of PEIDs can affect the traditional dynamic behaviors that have been well understood by the system operators, industry, and academia. Therefore, modeling and simulation of power electronic-enabled power systems are essential for transforming power grids from depending on fossil fuel to utilizing renewable energy. Fidelity and scalability are two main factors considered in simulation, and cannot be achieved at the same time under limited computation resources. Modeling techniques, particularly order reduction, model equivalencing, and parameter estimation, are major thrusts of scalable simulations as they can reduce the complexity by only slightly sacrificing the fidelity. On the other hand, power electronic devices are controlled using digital technology. Unlike traditional components, digitally controlled devices can switch between different designated functions such as grid-forming and grid-following modes, rendering future power systems discrete-event continuous-time systems, namely, hybrid systems.

This review is organized as follows: Section 2 reviews the overall cyber-physical power system framework, including the definition, subsystems, and realizations. Section 3 reviews the dynamic modeling of power electronic devices in the physical subsystem for large-scale simulation, covering the model structure, control modes, and practical simplifications. Section 4 reviews the cybersecurity challenges and the developed CPPS testbeds. Section 5 discusses the challenges and future directions for CPPS research. Section 6 concludes the review.

2 | CYBER-PHYSICAL FRAMEWORK, CYBERSECURITY, AND TESTBEDS

Modern electric power systems are the integration of physical systems and cyber-applications over communication networks. Such integrated systems are known as cyber-physical systems (CPS). Modeling and simulation of cyber-physical power systems (CPPS) are crucial for understanding cyber-physical interactions, which cannot be modeled in the traditional, physical system-centered frameworks. This section discusses the NIST framework for describing and analyzing CPS, followed by a review of the CPPS subsystem realizations.

The NIST framework for CPS (Griffor et al., 2017) defines that "CPS are smart systems that include engineered interacting networks of physical and computational components." The framework also defined three terminologies for CPS: *domains* which are the field of CPS applications; *facets*, which are the views of the CPS responsibilities in the system engineering process; and *aspects*, which are the grouping of concerns relevant to shareholders. This CPS framework is illustrated in Figure 1.

The CPPS falls within the energy domain, which includes the electric power system and energy supply systems. Various functional aspects have been studied in the literature, including system dynamics and control, market and economics, and cybersecurity. These aspects are commonly conceptualized as closed-loop decision-making between the physical and the cyber-systems through sensing and actuation, as illustrated in Figure 2. The closed-loop CPS concepts are realized using various software and hardware-in-the-loop implementations for assurance of efficacy in real systems. This section will focus on the functionality and realization of the CPPS.

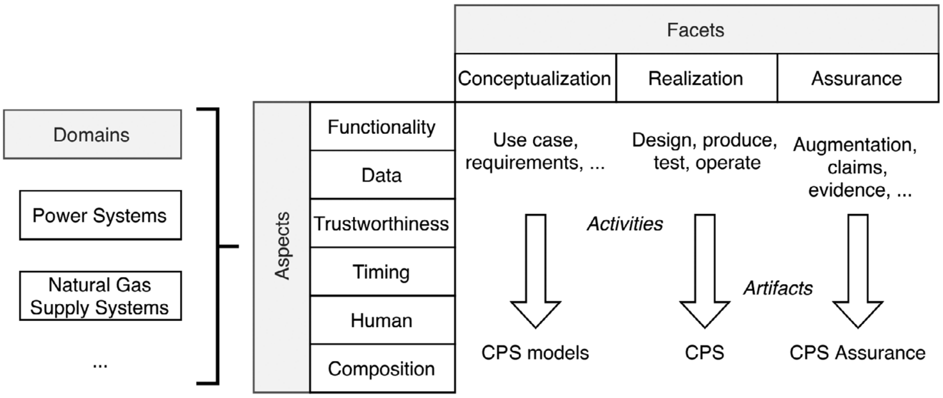

FIGURE 1 NIST framework for CPS: Domains, facets, and aspects

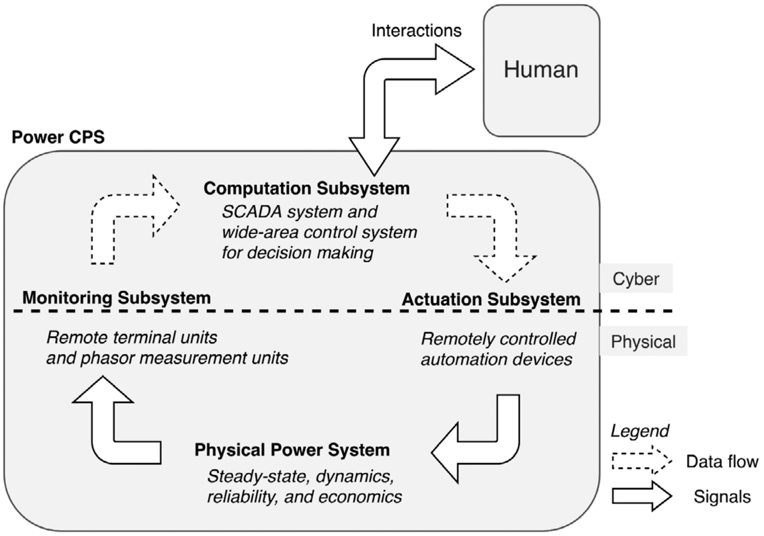
Interactions
Human
Power CPS
Computation Subsystem
SCADA system and wide-area control system for decision making
Monitoring Subsystem
Actuation Subsystem
Cyber
Physical
Remote terminal units and phasor measurement units
Remotely controlled automation devices
Physical Power System
Steady-state, dynamics, reliability, and economics
Legend
Data flow
Signals

FIGURE 2 Conceptualization for cyber-physical power system application

TABLE 1 Communication protocols for cyber-physical power systems (CPPS) components

CPPS components	Communication protocols
SCADA	Modbus (TCP/IP), DNP3, IEC 60870-5
PMU/wide-area control systems	IEEE/IEC 60255-118-1-2018 (preceded by IEEE C37.118)
Substation automation	IEC 61850
AMI	IEC 61968, ANSI C12.19, OSGP
Distributed energy resources	IEEE 2030.5 (SEP2), IEC 61850, OpenADR, DNP3

The CPPS is composed of four major subsystems: physical, monitoring and actuation, computation, and communication subsystems. The monitoring and actuation subsystems contain networked devices that are at the same time physical devices connected to the power grid and computational nodes with communication over networks. The computing subsystem makes decisions by processing measurement information and commands the actuation system. Human interfaces are also available for interacting with the computation and actuation subsystems. Next, the identified CPS aspects, the corresponding realization techniques, and the implemented testbed platforms will be discussed.

2.1 | Monitoring and actuation subsystems

The monitoring subsystem takes measurements from the physical system and streams data in predefined protocols. Actuation systems receive signals in predefined protocols and act on physical devices. Measurement and actuation subsystems exist in the power systems infrastructure, including the Supervisory Control and Data Acquisition (SCADA) system, PMU-based wide-area control systems, and substation automation system (SAS) in transmission grids, advanced metering infrastructure (AMI), and communication-enabled distributed energy resources (DER) in distribution systems. The definition and composition of these underlying infrastructures can be found in Sun et al. (2016). In all infrastructures, monitoring and actuation subsystems are interface through communication networks and utilize various communication protocols.

Communication protocols are defined by device vendors and standard organizations for monitoring and actuation. Table 1 summarizes the communication protocols for applications in CPPS. These protocols include unidirectional for sensor data streaming (such as the IEEE/IEC 60255-118-1-2018 for synchrophasor data streaming) and bidirectional for sensing and control (such as the Distributed Network Protocol 3 for distribution system automation). Note that all the protocols are in the application layer of the TCP/IP model, meaning that they can readily run over standard TCP/IP networks.

It is important to note that not all CPPS realizations explicitly implement industry-grade communication protocols. Some CPPS platforms implement ad hoc communication protocols using network sockets (Li et al., 2020), a publishsubscribe framework (Gjermundrod et al., 2009), or a peer-to-peer messaging framework (Palmintier et al., 2017), while others assume the content being sent or received but omit the protocol in which the messages are transmitted. Still, to realize interoperability with industry-level control room software and hardware from vendors, the support for standard communication is crucial.

2.2 | Communication subsystem

The communication subsystem provides the medium in which information can flow. As a cyber-physical system, the timing in communication networks can affect the physical system dynamics through communication-enabled applications. The communication subsystems are realized in two categories of simulation technologies: discrete-event-based simulation and process-based emulation. Both categories have been applied for CPPS simulations.

Discrete-event simulators often use small time steps on the order of nanoseconds for simulating predefined network scenarios. Network Simulator 3 (NS-3) is one such example that allows running software on simulated nodes. Process-based emulators use Linux networking stacks and virtualization techniques to create virtual nodes. Communication processes behave in the emulated network as if they would in a real network of the same configuration. Below are commonly used open-source tools for communication subsystem modeling.

- Discrete-event simulators: OMNet++ (Varga, 2010), NS-3 (Riley & Henderson, 2010), and OPNET (Chang, 1999).
- Process-based emulators: RINSE (Liljenstam et al., 2006) and Mininet (Lantz et al., 2010).

Power systems testbeds with integrated communication subsystems can be called communication-in-the-loop testbeds. To study the impact of communication latency, Zhong et al. (2019) propose a co-simulation framework by integrating the continuous-time *Dome* simulator with NS-3 to simulate point-to-point communication delays. To obtain data from physical simulation and stream it over communication networks, the cyber-physical co-simulation framework in Cui et al. (2019) integrates the Mininet emulator with C37.118-based PMU data streaming for wide-area controls. Such testbeds are capable of simulating bidirectional cyber-physical interactions that traditional physical-system-focused testbeds cannot capture.

2.3 | Computation subsystem

The computation subsystem is where measurement data are processed and control decisions are made. The computation subsystem covers algorithms ranging from established environments (such as commercial energy management system software) to research prototypes. Among data processing methods, state estimation is one approach commonly used in steady-state and dynamic analyses (Abur & Exposito, 2004). The state estimator determines the power network states by minimizing measurement errors from sensors and communication and computing best estimates of the system state. State estimation applies to topology errors (Ashok & Govindarasu, 2012), SCADA and PMU data (Yang et al., 2013), and DAE-based dynamic models (Zhao et al., 2019). State estimation serves as a preprocessor for other computing subsystems, including real-time wide-area control (Raoufat et al., 2017) and electricity markets (Zhang, Li, et al., 2020).

Various applications exist in the SCADA system and PMU networks based on computation. For example, the SCADA system for transmission systems enables operators to collect field data, regulate voltage, control tap changers, and configure protective relays from the supervisory control center (Enescu & Bizon, 2017; Thomas & McDonald, 2017). The PMU network and applications enable advanced monitoring and control, such as real-time oscillation monitoring, source locating, and event identification (Brahma et al., 2016; Nabavi et al., 2015; Vanfretti et al., 2011). Such applications can be integrated as algorithms and software packages in the computation subsystem.

2.4 | Physical subsystem

Depending on the time horizon of the functional aspect under study, the physical power system characteristics can be represented by snapshots, time-series calculations, or continuous-time simulations of transmission and distribution grids. Snapshot representations of power systems cover power flow and optimal power flow and can be applied to both transmission and distribution systems. Time-series calculations are snapshot calculations for different operating conditions. Time-domain simulations include positive-sequence phasor domain simulations and three-phase electromagnetic transient simulations in transmission systems, as well as the three-phase models in distribution simulators. Below is a nonexhaustive list of physical system analysis tools:

- *Steady-state and optimization*: PSAT (Milano, 2006), MATPOWER (Zimmerman et al., 2011), PyPSA (Brown et al., 2017), pandapower (Thurner et al., 2018). Steady-state and optimization tools are essential for calculating power flow and performing electricity market simulations.
- *Transient stability analysis (TSA)*: PSAT (Milano, 2006), InterPSS (Zhou & Zhou, 2007), MatDyn (Cole & Belmans, 2011), ANDES (Cui et al., 2020), Real-Time Digital Simulator (McLaren et al., 1992), OPAL-RT ePHASORsim (Jalili-Marandi et al., 2013), DPSim (Mirz et al., 2019). Transient stability analysis tools are crucial for understanding the dynamic performance and control of physical power systems. Power electronics interfaced devices are simulated as average models in stability analysis tools.
- *Electromagnetic transient (EMT) analysis*: ATP-EMTP (Haginomori et al., 2016), PSCAD (PSCAD, 2021), eMEGAsim (Paquin et al., 2009). Such tools allow high-granularity simulation of power electronics to include the topology and internal switching but are computationally demanding.
- *Distribution system analysis: GridLab-D* (Chassin et al., 2008), OpenDSS (Montenegro et al., 2017), DIgSILENT (DIgSILENT, 2021). Distribution system analysis tools perform snapshot calculations and numerical integration for three-phase unbalanced distribution systems.

One particular interest at the system level is the characterization of PEIDs, namely, modeling PEID for transient stability simulation. Such models need to convey sufficient PEID dynamics within reasonable computational demands. Multiple approaches can be taken to model PEID in physical subsystems with a trade-off between granularity and computational speed. Such approaches range from a full-scale EMT simulation in PSCAD (Kenyon et al., 2021) or RTDS (Guo et al., 2020), to the co-simulation of EMT and TSA (Biswas et al., 2019) that provide details for part of a medium-scale system, and to TSA that uses average models for large-scale systems (Ramasubramanian et al., 2017). The following section reviews the PEID modeling and control techniques used in transient stability simulation software for representing large-scale physical subsystem.

3 | MODELING OF PEID FOR SYSTEM SIMULATION

PEID can be modeled at multiple levels based on the need for granularity and computation speed. Although PEID with switching details is modeled using EMT programs, it can be unnecessarily complex for grid-level stability studies. Therefore, instead of focusing on power electronic topologies and switching, the major emphasis from the system's perspective is to model the conversion and synchronization of energy flow from the input to the output. Averaged converter models for transient stability simulation are considered and discussed in Section 3.1 together with the overall structure of a generic PEID. The corresponding control dynamics have dominant impacts on this procedure and will be the focus in Section 3.2.

3.1 | General model components

The models of a PEID mainly consist of two parts, the primary source, and the grid interface, as illustrated in Figure 3. Each of these parts contains both physical models and controls. The primary source is designed to absorb energy either from external sources like wind and solar or from the grid in the case of HVDC. The energy management function controls the electronic features to maximize energy extraction, typically, the maximum power point tracking (MPPT) approach. The primary sources usually admit standard modeling procedures. Interesting readers can refer to Villalva et al. (2009) for the models of photovoltaics, Hussein and Batarseh (2011) for battery energy storage, and Mullane and O'Malley (2005) and Zhang et al. (2018) for wind turbines.

The grid interface aims to convert the extracted energy into the synchronized AC power flow. This is done by two cascaded control modules, that is, the reference generator and the reference tracker. The reference generator will compute the internal references of active and reactive power (known as *PQ* control) or voltage and frequency (known as *V*

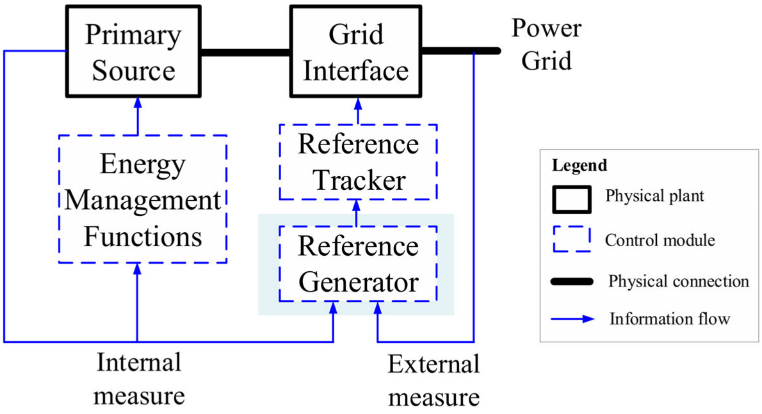

FIGURE 3 Components of a generic power electronic device from power system perspective

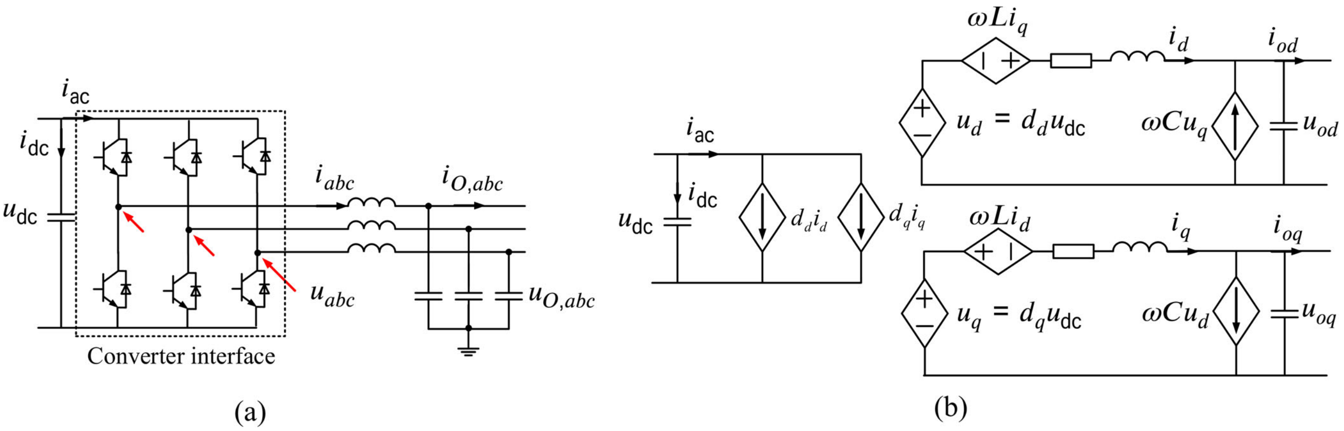

FIGURE 4 Voltage-source converter model. (a) Topology. (b) Averaged model

*f*control), while the reference tracker will ensure the converter outputs desired values using two-loop proportional-integral (PI) controllers. The *PQ* control is the basic form of grid-following controls, and the *Vf* control is the basic form of grid-forming controls. More advanced functionalities can be realized by customizing the reference generator module. It is the reference generator that mainly determines how PEIDs are modeled from the power grid viewpoint.

The PEIDs are physically connected to the grid through self-commutated converters (known as Voltage Source Converters, as opposed to Line-Commutated Converters), the topology of which is illustrated in Figure 4a. The aforementioned converter controls will open and close the switches to control the output voltage u_{abc} such that the terminal voltages $u_{O,abc}$ and currents $i_{O,abc}$ will track the reference signals from the reference generators. For simplicity, it is typical to average the switching behavior over a duty cycle, known as the averaged model. Since most converter controls are designed in the direct axis (d-axis) and quadrature axis (q-axis) framework, it is also convenient to converts the three-phase averaged model into the *dq* space (Sozer & Torrey, 2009). The averaged equivalent circuit of the converter interface is shown in Figure 4b. The terms d_d and d_q denote the duty ratios in *dq* spaces and are controlled by the reference tracker. The averaged models can be integrated with the standard control loops and retain most of the relevant dynamics from the system viewpoint. This approach has been widely employed for verifying converter controls and associated impact on the power grid (Liu et al., 2011).

As seen in Figure 4b, the converter essentially tracks the voltage commands in the dq space, that is, u_d and u_q. Given the high switching frequency, this tracking time is extremely fast and can be omitted in most power grid studies. In this case, the converter is considered as "ideal." Thus, the reference signals $u_d^{\cdot}$ and $u_q^{\cdot}$, which will be discussed in later sections, can "pass through" the converter to become the terminal conditions, that is, $u_d^{\cdot} = u_d$ and $u_q^{\cdot} = u_q$. If the grid is modeled in three-phase, then $\mathbf{u}_{dq}$ will be converted into three-phase signals. If the grid is modeled in positive sequence, then the variables in the *dq*-axis can be directly incorporated into the algebraic equations.

3.2 | Types of converter control methods

A PEID can be controlled as a current source (the grid-following mode) for feeding energy to a string grid, or as a voltage source (the grid-forming mode) to regulate terminal frequency and voltage for systems with weak frequency and voltage supports. As mentioned, the *PQ* control is the basic form of grid-following controls, where the reference tracker receives a pair of active and reactive power commands, as shown in Figure 5a. The *V f* control is the basic form of grid-forming controls as the commands for the reference tracker are the voltage and frequency, as shown in Figure 5c. In each mode, many auxiliary functions can be implemented through the reference generator. The reference generator will calculate the *PQ* or *V f* as a function of grid measurements so that the converter-interfaced sources will respond appropriately to grid events as shown in Figure 5b,d, respectively. A summary of existing modes with their advantages and disadvantages can be found in Shourangiz-Haghighi et al. (2020).

Grid-following converters have been widely used for utility-scale renewable energy integration due to the simplicity of converter control (Chow & Sanchez-Gasca, 2020). They utilize the voltage and frequency control capabilities of the existing transmission systems. However, one drawback of the grid-following converters is their reliance on phase lock loops (PLLs), which can introduce stability issues (Huang et al., 2019). On the other hand, grid-forming converters are more preferred when interfacing with weak systems that have limited capability in voltage or frequency control (Matevosyan et al., 2019). Therefore, recent work has studied the application of grid-forming converters for microgrids and black-starts (de Souza Ribeiro et al., 2018; Tayyebi et al., 2018). However, one issue with the grid-forming converter is overcurrent during severe AC faults. As remediation, a control switching is needed from grid-forming to grid-following in addition to current limiters when severe faults are detected (Zhang et al., 2009).

3.2.1 | Different converter control methods

To realize different functionalities in Figure 5, tracking controllers should be properly designed to regulate the outputs to desired values. These converter control methods can be categorized based on the reference frames that they are implemented, including the *dq* synchronous reference frame, the *αβ* stationary reference frame, and the *abc* frame (Blaabjerg et al., 2006). The *dq*-axis based on rely on the phase-locked loop technology to transform three-phase voltage and current into the *dq*-axis, where the variables become stationary instead of periodic. Hence, PI controllers can be designed based on linear time-invariant systems. Despite the satisfactory performance of *dq*-axis based PI control under balanced conditions, its performance deteriorates under unbalanced grid conditions. To improve the performance, two sets of *dq*-axis-based PI controllers are implemented to regulate independently both the positive- and the negative-sequence components (Liserre et al., 2006). If the control is designed under the *αβ* stationary reference frame, the PI control will be replaced by the proportional resonant (PR) controllers. Such structures can control both positive-

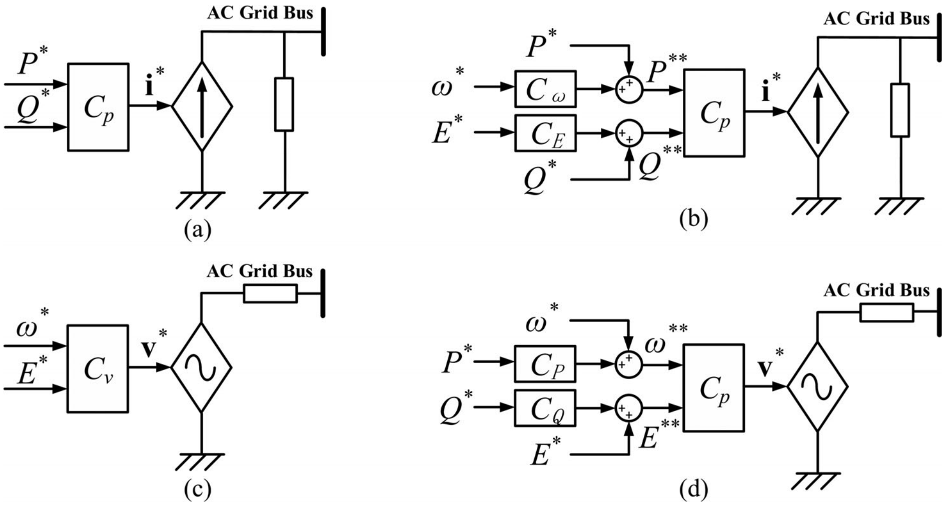

FIGURE 5 Simplified representations of converter-interfaced sources (Rocabert et al., 2012). (a) Grid-following mode. (b) Grid-following mode with auxiliary functions. (c) Grid-forming mode. (d) Grid-forming mode with auxiliary functions

and the negative-sequence components by a single block and thus is preferred under unbalanced grids. The $\alpha\beta$ stationary reference frame will rely on a frequency-locked loop, which can provide a fast response with low overshooting (Rocabert et al., 2012). Other methods that can provide similar tracking functions include predictive control (Kouro et al., 2009), flatness-based control (Variani & Tomsovic, 2016), back-stepping control (Martin et al., 2015), etc. It is also worth mentioning that PI, PR, and predictive control can also be implemented in the *abc* frame, which requires high sampling rate to obtain high performance (Timbus et al., 2009) but can be readily realized by modern microcontrollers and digital signal processors.

In the following, we will demonstrate the control diagrams of grid-forming and grid-following converters in the most commonly used synchronous reference frame.

3.2.2 | Converters controlled as a current source and auxiliary functions in the synchronous reference frame

A diagram of *PQ* control is depicted in Figure 6. The reference tracker contains two loops, that is, the power loop and the current loop. The control is constructed using the *dq*-axis. The entire control system uses the phase-lock loop to generate the angle for Park's transformation. Given the desired power output, the reference currents are calculated using the algebraic relations between power and *dq*-axis currents and voltages as

$$P = v_q i_q + v_d i_d \ , \ Q = v_d i_q - v_q i_d.$$

The diagram in Figure 6 simplifies the relations considering that $v_q = 0$. The current controller is a pair of PI controllers together with cross-axis decoupling terms and feed-forward terms for the connection voltage (Kroutikova et al., 2007). Finally, the internal *dq*-axis reference voltages are obtained to generate the pulse-width modulation for converter control. If averaged models are employed, the *dq*-axis reference voltages will be equivalent to the duty ratio in the *dq*-axis shown in Figure 4. Grid-following converters have high parallel output impedance and are suitable to operate in parallel with other grid-following converters.

The last important component in the modeling of the reference tracker is the current limiter. Since the active and reactive power can be operated under different modes, the total apparent power may exceed the converter rating. In this case, one of the current references should be limited. The power limiter can be operated under *P*-priority mode or *Q*-

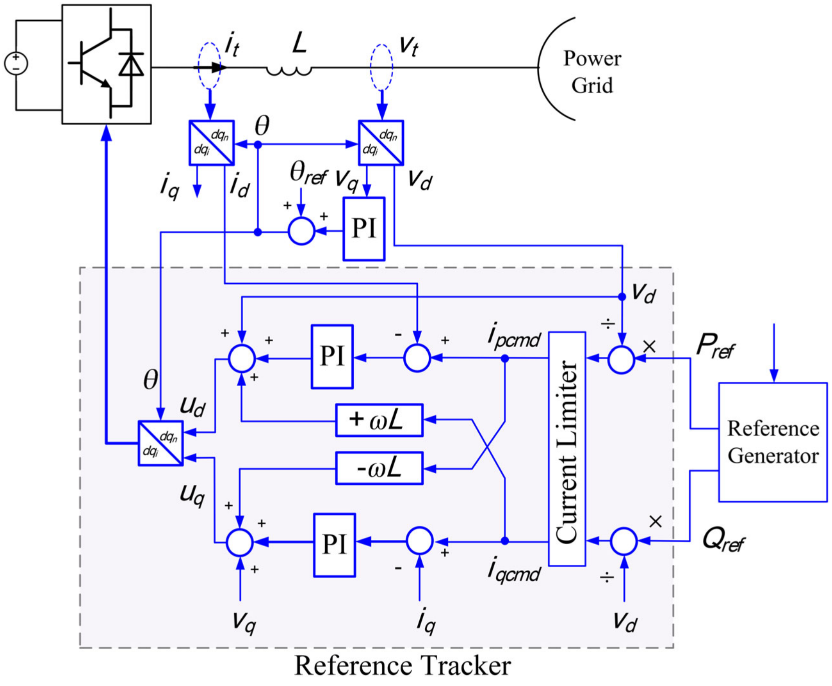

FIGURE 6 Fundamental grid-following control: PQ control diagram

priority mode (CIRED, 2018). The mode of the power limiter is controlled based on external grid conditions. Usually, the *P*-priority mode is activated if no fault or low voltage event is detected. A low-voltage event can trigger the *Q*-priority mode to have the converter feed reactive power for voltage support.

This basic version of grid-following control can be enhanced in many different ways through the reference generator. The most common form is to use the reference $P^{\cdot}$ to regulate the DC-link voltage. The difference between the desired and measured DC-link voltage is sent to a PI controller to obtain the active power reference. In these cases, the converter is usually powered by a renewable source, and another converter is connected at the other side of the DC-link to provide the MPPT function (Zhang et al., 2018). With the increasing penetration of grid-following converters, which do not respond to grid events in its original design, power system dynamic performance, particularly frequency response, can degrade and result in large frequency excursions even under small power disturbances (Zhang et al., 2017). This issue can be resolved by implementing various grid-supporting functions in the reference generators, linking the stored energy inside the converter-interfaced sources with grid measurements.

For active power control, one of the most common proposals is to add the rate-of-change-frequency (RoCoF) as a supplementary signal to the active power reference, known as inertia emulation (Wilches-Bernal et al., 2016). Also, grid frequency deviation can be used to provide primary frequency support (Gautam et al., 2011). Additionally, mixing both signals can enhance the support at both inertial and primary stages (Wang, Zhang, et al., 2018). However, grid frequency measurement usually contains noise, and filters will be needed before RoCoF or deviation signals can be computed, which limits the strength of the support. To address this issue, power surge control injects a predesigned control signal once the supportive function is activated (Wang & Tomsovic, 2018).

For voltage support, the reactive power support aims to regulate the voltage of either the terminal bus (Hansen et al., 2006) or a remote bus (Moursi et al., 2008). Since maintaining the voltage profile at the point of common coupling of a converter-interfaced source is essential for its stable, reliable, and efficient operation, these two modes are widely deployed. The power factor of a converter-interfaced source can be considered constant by properly controlling the reactive power loop. An overview of the commonly used reference signals is depicted in Figure 7.

For large-scale bulk power system simulation with massive numbers of PEIDs, detailed models of the two-loop PI control in the reference tracker and phase-lock loop may prohibit scalability. Thus, equivalent aggregate models that are appropriate particularly for positive sequence simulations have been developed (CIRED, 2018; Shao et al., 2013; Zhang et al., 2019), which has been widely used in commercial software in the industry. Thus, we term these as "industrial models." In these models, the phase-lock loop dynamics are omitted. The models of reference tracker and converter are simplified as the first-order inertia elements with proper time constants to represent the overall response time. Since the detailed reference tracker is omitted, the dynamic relations between the measurements and the final commands $u_d^{\cdot}$ and $u_q^{\cdot}$ cannot be established. To this end, the industrial models usually employ the current in the *dq*-axis as the command and interface variables.

3.2.3 | Converters controlled as a voltage source with auxiliary functions in the synchronous reference frame

The diagram of the $V f$ control is depicted in Figure 8. The reference tracker in the grid-forming mode employs two PI loops to control volwotage and current, respectively. In contrast to the grid-following case, the control system does not rely on the phase-lock loop to generate the angle for Park's transformation. Instead, the reference frequency is

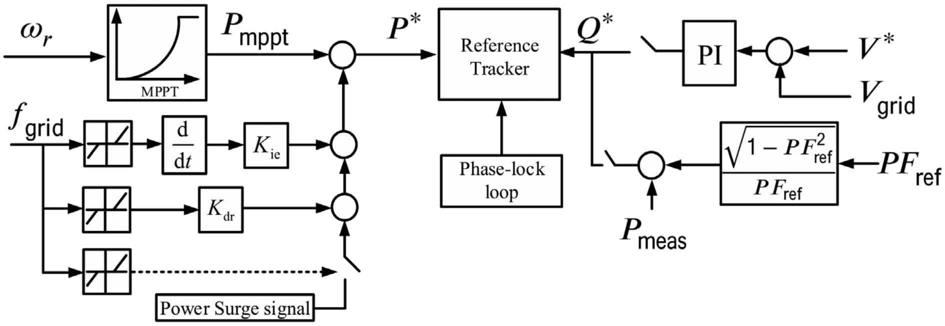

FIGURE 7 Various reference signals of active and reactive power in grid-following mode

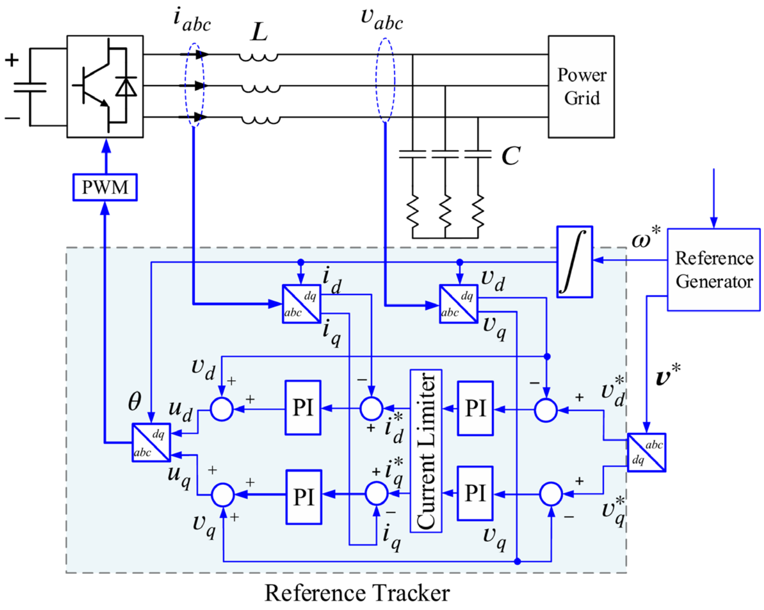

FIGURE 8 Fundamental grid-forming control: *V*/*f* control diagram

integrated to obtain the internal angle, which is analogous to the synchronous generator rotor angle. The existence of the phase-lock loop is the essential difference between the grid-forming and grid-following converters. Based on Figure 8, feed-forward loops can also be added for cross-axis decoupling (Pogaku et al., 2007).

The grid-forming converter presents a low-output impedance, so they need a load-sharing algorithm to operate in parallel with other grid-forming converters. Thus, the *V*/*f* control usually works with load sharing functions designed in the reference generators. The most common load-sharing algorithm is droop control (Guerrero et al., 2011). The advantage of droop control lies in its decentralized nature, which does not need expensive communication infrastructure and therefore no delay-induced stability issues. The fundamental form of the droop control reads as

$$\omega^{\cdot} = \omega_{\text{set}} - m(P_{\text{meas}} - P_{\text{set}}),\ V^{\cdot} = V_{\text{set}} - n(Q_{\text{meas}} - Q_{\text{set}}),$$

where $\omega^{\cdot}$ and $V^{\cdot}$ are the reference signal for tracking, ω_{set} and V_{set} are the nominal frequency and voltage given by the secondary controller, respectively, P_{set} and Q_{set} are the nominal active and reactive power, respectively, P_{meas} and Q_{meas} are the measured active and reactive power, respectively, m and n are the droop coefficients. The droop coefficients are chosen such that they share the load in proportion to their nominal outputs. For example, if K droop-controlled sources are in the grid, their coefficients can be given by Majumder et al. (2010).

$$m_1 P_{\text{rate},1} = \cdots = m_K P_{\text{rate},K},\quad n_1 Q_{\text{rate},1} = \cdots = n_K Q_{\text{rate},K}.$$

One disadvantage of the droop control, however, is that it does not improve the dynamic performance of the system. As shown in Equation (2), an abrupt change in P_{meas} and Q_{meas} due to disturbances will generate sharp reference signals, resulting in a high rate-of-change in frequency and voltage. The high rate-of-change in frequency and voltage may trigger relay actions and even power outages. To tackle this challenge, various modifications to the grid-forming control have been proposed.

The virtual synchronous generator (VSG) is one of the most widely studied approaches (Huang et al., 2017; Ma et al., 2017). VSG control will take full models of a synchronous generator to generate the voltage and frequency references. The reference generator of a VSG is shown in Figure 9. As shown, two fundamental components are the electric machine winding model to calculate the voltage reference and the mechanical model to obtain the speed reference. Other equipments, such as, the automatic voltage regulator and power system stabilizer, can be added to further improve the stability.

Similar to the model simplification strategy in the grid-following case, the grid-forming converter model can be simplified by replacing the reference trackers with the first-order inertia elements (Ramasubramanian et al., 2017). As seen, the reference trackers usually perform the standard tracking functions and contribute to major sources of the model

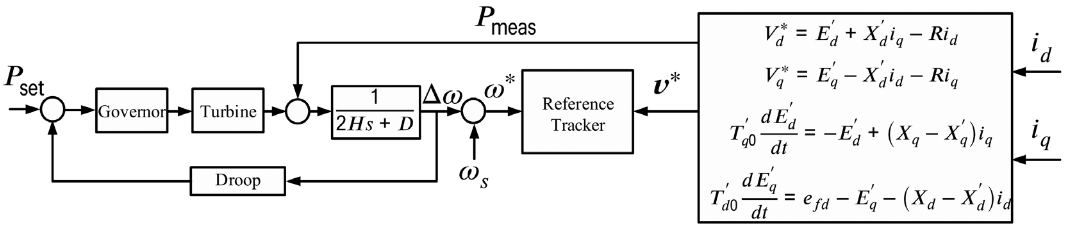
P_{meas}
P_{set}
Governor
Turbine
$\frac{1}{2Hs+D}$
$\Delta\omega$
ω^*
ω_s
Droop
Reference Tracker
v^*
$V_d^* = E_d' + X_d' i_q - R i_d$
$V_q^* = E_q' - X_d' i_d - R i_q$
$T_{q0}' \frac{dE_d'}{dt} = -E_d' + (X_q - X_q') i_q$
$T_{d0}' \frac{dE_q'}{dt} = e_{fd} - E_q' - (X_d - X_d') i_d$
i_d
i_q

FIGURE 9 Reference generator of the virtual synchronous generator (VSG) control (Ma et al., 2017)

simplification. The reference generators, on the other hand, determine the essential functions of the PEIDs and usually will be preserved in physical system simulations.

3.3 | Challenges for systems with high penetration of PEID

The increasing penetration level of PEID and the retirement of traditional synchronous generators are also posing challenges to the secure operation of large-scale power grids. Synchronous generators are electric machines that convert energy from mechanical to electrical with stored kinetic energy. Analogously, PEID is a purely electronic device that converts DC power to AC with optimal electric energy storage at the DC link. The most distinct characteristic between the two is the ability to instantaneously respond to grid disturbances. While synchronous generators will physically decelerate or accelerate by converting inertia to electric power, or vice versa, at the inception of events, PEID has to rely on measurements and control loops, which embed delays at the 10-ms level (Milano et al., 2018), to achieve an inertia-like response.

The stability challenges imposed by high penetration of PEID are classified into modeling, stability, and control challenges. The modeling challenges can limit the ability of simulations to capture the dynamics outside the modeled timescale. Stability challenges can impact the operation of the grid following disturbances, and the control challenges require more sophisticated schemes to deal with the fast dynamics in a low inertia system.

3.3.1 | Consensus on the models of PEID

The previous sections of this review presented the two types of PEIDs, that is, grid-following and grid-forming converters, for system-level transient stability simulation. Currently, the industry has reached a consensus on the grid-following converter models after two iterations, and the latest revision is known as the second-generation renewable models (Pourbeik, 2014). In this generation, grid-scale solar PV and wind systems share the generic converter model, electrical control model, and the plant-level control models (Weber, 2014), while wind systems can utilize additional models for aerodynamics, turbine, pitch angle control, and torque control (also known as Pref control). The models have been approved by interconnection-level coordinators such as the Western Electricity Coordinating Council (WREMT Force, 2016; WREMT Force, 2019). The models are designed to be generic for wind, solar, and battery storage and thus lack the specificity of the renewable power source. For example, variable solar irradiation and wind speed cannot be modeled with these models. Also, there are no DC-link details for any PEID or rotor-side converter details for the Doubly Fed Induction Generator.

For the grid-forming converters, the presented model in the previous section summarizes the consensus in the literature. That is, the inner-loop current control and the outer-loop voltage controllers are the de facto standard for grid-forming PEIDs, and different designs (Arani & El-Saadany, 2012; Ochoa & Martinez, 2016; Tayyebi et al., 2018; Zhong & Weiss, 2010) are at the Reference Generator for computing the high-level signals. From the converter point of view, these are auxiliary signals that can be synthesized based on local and remote measurements or received from supervisory controllers. For example Wang et al. (2015) utilize frequency and active power control for synchronization, but as we will discuss in the next subsection, a frequency signal at the electromechanical timescale will cease to exist when the system is fully electronic. Other studies utilize nonconventional signals for PEID (Hong & De León, 2016), but a communication link is required, which incurs additional communication delays at the level of 100 ms.

Another challenge in PEID modeling is the need to capture the fast dynamics in a high PEID penetration grid. There are views that the suitable modeling granularity of PEID will be between the full switching model and the average model (Misyris et al., 2021), but the specific models remain to be developed. The model development will also depend on the control capabilities provided by vendors and approved by system operators. For example, Scotland reported high-frequency oscillations (Leslie, n.d.) in a high PEID-penetration system. The exact causes remain to be investigated with new methodology and tools, but the controller settings and the interferences between PEIDs can be suspect. Further studies are required to identify the mechanism and suggest additions to existing models, such as saturation, limits, and conditional control loops, before such phenomena can be reproduced by numerical simulations.

3.3.2 | Stability issues internal to converters

Grid-following converters rely on PLLs to synchronize with the external grid and thus can suffer from issues due to PLL. A typical PLL (Ortega & Milano, 2015) includes a phase detector to determine the q-axis component of the voltage V_q, a Loop Filter (LF) to eliminate the error between the measured and the estimated voltages, and a Voltage-Controlled Oscillator (VCO), which takes the frequency deviation signal to reveal the estimated V_q. It is also common to filter the output of the PLL to reduce the high-frequency signals caused by the LF and VCO.

The outstanding issue with the PLL is the delay due to the multiple loops. In a grid disturbance where discontinuity of voltages are observed, the estimated phase angle will deviate from the angles, which are algebraic variables and can have instantaneous jumps in the timeframe of milliseconds. Studies have reported the impacts of PLL delays on the performance of grid-following inverters (Hu et al., 2016) and instability issues related to the converter control (Goksu et al., 2014; Hu et al., 2019; Wang, Huang, et al., 2018).

Remedies for the PLL-induced issues can be identified based on improved design of PLLs (Huang et al., 2021) or other synchronization techniques, such as Kalman Filter-based methods (Bagheri et al., 2015), which are linear and can be pretrained. However, disturbances and the subsequent discontinuities in PEID states also cause accuracy issues in such methods. This area remains an open topic needing further studies.

3.3.3 | Stability issues at the grid level

Large-scale integration of PEID and the reduction of synchronous generators also create system-level issues due to the reduction of inertia. Traditionally, the swing equation of machine dynamics determine the rate of change of frequency ($\dot{\omega}$) following power imbalances:

$$2H\dot{\omega} = P_m - P_e - D\Delta\omega,$$

where H is the aggregated machine inertia, ω is the machine angular frequency, and D is the aggregated damping coefficient. In a system with reduced H, the rate of change of frequency will increase for the same power mismatch and thus require more rapid control to maintain frequency stability. Moreover, in a fully renewable system, that is, $H = 0$, the balance of power generation and consumption will not be "buffered" physically by the kinetic energy previously stored in generators, requiring designed control systems to fully take charge of the power balancing.

The mechanism of frequency stability in a smaller time scale than the electromechanical one has not been fully understood. Recent studies start with the definition of frequency with attempts to derive alternative representations. In positive-sequence simulations, nongenerator bus frequency is traditionally obtained based on the rate-of-change of voltage angles. Recent studies derived a Frequency Divider Formula (FDF) (Milano & Ortega, 2017) which "distributes" the generator frequency to buses based on the B matrix. The FDF provides more accuracy compared with the rate-of-change method, but it remains undefined for a fully renewable system, and the formula cannot account for the controls of grid-forming inverters emulating generator inertia. In fact, the frequency of the power grid will continue to exist but become more dependent on the controllers of PEID as the integration level increase.

In addition, increasing PEID levels challenge the existing framework of power system stability. Transient stability is defined as the ability of a generator or group of generators to remain in synchronism immediately following a severe and sudden system disturbance. As mentioned, the retirement of synchronous generators and the increase of PEID will push transient dynamics to a smaller time scale. It requires new standards to account for the effects of PEID and relevant controls when evaluating system transient stability (Kundur et al., 2004). Recently, an IEEE PES Task Force in the Power System Dynamic Performance Committee published a report on revisited and extended stability definitions with the inclusion of new stability issues from converter-interfaced renewables and their controllers, and reduced grid inertia (Hatziargyriou et al., 2020).

Further, the reduced inertia brings a new challenge on estimating and distributing the system inertia and integrating distributed control for optimal response. Such inertia can come from the hybrid operation of the PEID system and conventional synchronous systems at reduced capacity. Studies have shown temporal variations of system inertia (Ulbig et al., 2014), and variations are expected to be severe due to intermittent resource availability without coordinated planning. Also, distributed controls that can achieve fast frequency stabilization at the inertia level or primary frequency response are open for future research. Such controls can be based on physical signals (such as DC voltages) without communications or based on consensus control through communication networks, which will be elaborated in the subsequent sections.

4 | CPPS CYBERSECURITY: OBJECTIVES, STUDIES, AND TESTBEDS

The objectives, research approaches, and testbeds for the cybersecurity of CPPS are reviewed in this subsection. CPPS security analysis includes four key objectives:

- **Confidentiality**: private or confidential information is not disclosed to unauthorized parties.
- **Integrity**: data, programs, and systems are only changed in a specific, authorized manner.
- **Availability**: systems respond promptly to authorized users.
- **Authenticity**: the state of information is genuine from the original sender and trusted.

The confidentiality requirement prevents unauthorized access to critical system information to reduce risks of system-dependent sophisticated attacks. The integrity requirement guards the CPS against unauthorized information alteration or destruction. The availability requirement ensures timely and reliable access to information. The authenticity requirement avoids falsified information and fake sources. CPPS vulnerabilities come from four major components:

- **Hardware**: equipment and devices may be purposefully disconnected (availability). Hardware includes pure power devices and network-enabled equipment.
- **Software**: firmware and computation software may be removed (availability) or altered in functionality (integrity and confidentiality).
- **Data**: stored program configurations and system descriptions may be removed, maliciously encrypted (availability), disclosed (confidentiality), falsified, or fabricated (integrity and authenticity).
- **Communication Infrastructure**: data streamed over communication networks can be deleted or withheld (availability), intercepted (confidentiality), modified, or fabricated (integrity and authenticity).

Cybersecurity studies in CPPS are approached from various perspectives. Yardley et al. (2013) investigate security testing from three aspects: the need for a methodology of defining tests, the need for a means of comparing and measuring the security of the system, and the current lack of tools and instrumentation for carrying out tests. Some concerns raised still exist today, such as the lack of standard tests, security measurements, and toolchains. Rasmussen et al. (2017) review the security assessment methods from three perspectives: monitoring, contingency analysis, and preventive control actions with an emphasis on the security of the physical system. Li et al. (2019) summarized cyberattack methods in CPPS into False Data Injection Attack (FDIA), Denial of Services (DoS), man-in-the-middle (ARP spoofing, DNS spoofing), replay, and others (GPS spoofing, load altering, delay attack). The paper also reviewed vulnerabilities in various parts of the CPPS, ranging from SCADA systems, WAMS, AMI, Substation. Wang, Tai, et al. (2018) review the characteristics, construction methods, consequences, prevention, and mitigation of cyberattacks in CPPS with a focus on FDIA.

Due to its complex nature, the classification of CPPS studies varies, depending on the perspective. Palensky et al. (2014) review two fundamentally different approaches for simulating CPS: discrete event-based and continuous-time simulations. Schmidt and Åhlund (2018) discuss building CPS and classified research as theoretical, data-driven, combinations of data-and theoretical, and mixed. Shi et al. (2018) analyze the challenges in modeling interactions in CPS and classifies existing studies into graph-based, dynamics-based mechanisms, probabilistic, and simulation studies.

This review classifies existing work into three categories, based on the level of abstraction: graph and network theory-based abstract studies, optimization, and control-based mechanism studies, and testbed-based simulation studies. The first category aims to describe and analyze CPPS using abstract models of graphs, complex networks, and state machines. The second category models part of the CPPS in detail using discrete-event models, DAE models, or optimization models for analyzing how certain cyber events can impact the physical system in principle. The third category simulates CPPS behaviors for specific computation subsystems by utilizing testbeds with power and cyber models that closely resemble their counterparts in the real world.

4.1 | Network theory-based studies and mechanism studies

Complex network theory-based studies aim to model the relationships between the vertices and edges that represent the corresponding elements in the power systems and cyber networks. These studies typically assume the mapping between the physical and the cyber layers (Falahati & Fu, 2014; Guo et al., 2017; Han et al., 2015; Lei et al., 2014) as well as the basic ways in which individual failures in one system will affect another. For example, (Buldyrev et al., 2010) studies the cascading failure in the Italian system by mapping the power grid to the cyber-layer and assuming the power dependency between the electric and cyber nodes. Although graph and network theory-based studies can provide high-level insights, they may not be useful in operational guidance due to the lack of details, especially when based on assumed topology mappings.

The CPPS mechanism studies take a further step into modeling the states in power networks. The physical system and controller dynamics are typically modeled by DAE. For the cyber-system, cybersecurity incidents are considered as alterations to signals for the computing subsystem, and communication networks are not explicitly modeled. For example, Xiang et al. (2017) model coordinated attacks between load redistribution and generators, and between load and lines. The impacts of the attacks are assumed and are formulated as bi-level optimization problems where the attacker at the upper level maximizes load curtailment while the defender at the lower level counters load reduction. Gunduz and Jayaweera (2018) propose a Markov-chain-based approach for quantifying the reliability of the physical and the cyber-systems. Ekomwenrenren et al. (2019) focus on routing in communication networks and uses MILP to minimize traffic routing delays for wide-area damping control. Wang et al. (2019) propose a dynamic data injection attack model for multiple operating conditions based on bi-level optimization with considerations for parameter and forecast uncertainty. Zhang, Krishnan, et al. (2020) study cyberattacks and detection in transactive energy systems through the co-simulation of power flow and market clearing programs.

Recent studies also employ machine learning methods for cybersecurity mechanism studies. Wickramasinghe et al. (2018) generalize recent deep learning-based approaches for the security of CPS in general. Ferrag et al. (2020) review the approaches for cybersecurity intrusion detection using deep learning methods. In Yan et al. (2017), a deep Q-learning-based method is proposed for analyzing sequential topology attacks. Wei and Mendis (2016) propose a deep-learning approach to identify and mitigate information corruption for maintaining transient stability. A detection algorithm for false data injection is proposed in Niu et al. (2019) using convolutional neural networks. A network attack detection approach using bi-directional Recurrent Neural Networks for IEEE 1815.1 standard compliant power systems is proposed in Kwon et al. (2020).

It is worth noting that the network theory-based methods and mechanism studies employ various abstractions and assumptions, and thus, have considerable practical limitations. For example, communication protocols and topology are typically omitted with no detail for the communication subsystem. Some studies also assume considerable knowledge or observability of the system, deviating from the situations in actual systems.

4.2 | CPPS testbed implementations and verifications

Testbed verification is one of the best ways to deal with the immense details in cyber-systems and observe the impacts on the physical power system (Shi et al., 2018). Compared with conventional numerical-based methods, testbed verification can reveal the cyber-physical interactions following cyberattacks and physical incidents. CPPS testbeds are emerging in recent decades with focuses on SCADA and substation automation, wide-area monitoring and control, and cybersecurity. Testbeds typically employ a physical subsystem simulator that progresses the simulation at the wall-clock speed (known as a "real-time simulator") to synchronize all components. There are exceptions, however, to simulate power systems in real-time using electronics-based reconfigurable emulators (Yang et al., 2014). Most CPPS testbeds employ a communication simulation or emulation program for communication system characterization.

Testbeds can be viewed as co-simulation environments that jointly simulate established power systems, communication simulators, and the computation algorithm or hardware device under study. In terms of the architecture, testbeds can be decomposed by the function (physical, communication, information/control) or the representation of components (simulation, emulation, and physical) (Ashok et al., 2011). In addition, testbeds are designed to include the level of details involved in the field of study. For example to study intrusion detection, Adhikari et al. (2014) describe a testbed suited for network intrusion and detection events in power systems based on RTDS, a data collection and processing engine, and a MATLAB/RSCAD parameter calculation engine. The platform is useful to represent real-world events and operator training in addition to research (Figure 10).

CPPS testbeds with various implementations have been reported. Chen et al. (2014) describe a communication-in-the-loop real-time testbed using RTDS and OPNET, linked through LabVIEW PXI with FPGA, for modeling intelligent electronic devices in SASs. The involvement of the commercial simulator and the data acquisition platform guarantees performance but limits scalability. Liu et al. (2015) present *Deterlab*, a cyber-physical testbed using RTDS, synchrophasors, and NS-3 for model real-life cyber events, including man-in-the-middle attacks, DoS, and communication failures. The advantage of including NS-3, a discrete-event network simulator, enables high-fidelity communication network modeling. Sun et al. (2016) review the cybersecurity vulnerabilities and cyber-protection systems, and the Smart City CPS testbed for cybersecurity studies covering control centers all the way down to customers.

For wide-area, large-scale systems, Leger et al. (2016) report a testbed for wide-area monitoring and control with two-way digital communication between intelligent electronic devices, control centers, and applications. The testbed employs industry-grade communications between PMU, PDC, and controllers. With the industry-grade protocols in place, the platform can replicate real-world transmission system monitoring, control, and actuation subsystems. Bassey et al. (2017) implement wide-area control in a testbed composed of RTDS and NS-3 for interarea oscillation damping control. Tong et al. (2019) present a CPS testbed design with HIL and non-real-time synchronization techniques as a workaround for subsystems running in non-real-time. In addition, Cui et al. (2019) propose a four-layer communication-in-the-loop Large-Scale Testbed with the emphasis on modeling the networked component layer that interacts with the physical and the network layers. One advantage of the Large-Scale Testbed is an implementation to eliminate the one-way delay between grid simulators and PMU simulators when acquiring data through rapid distributed messaging.

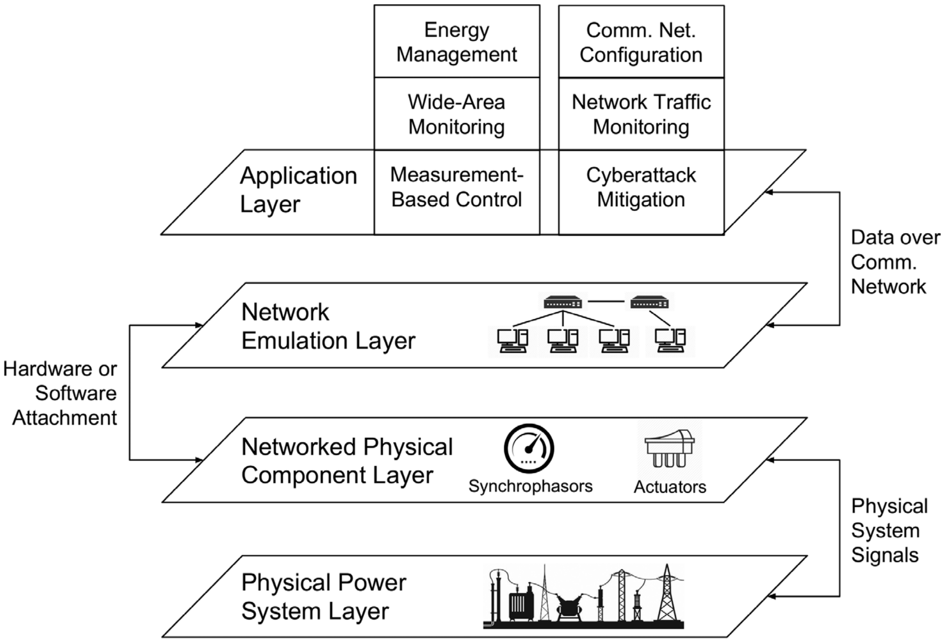

FIGURE 10 Software architecture of the four-layer large-scale testbed

To summarize, a number of CPPS testbeds have been developed for cyber-physical interaction studies with significant modeling details. It is worth noting the disconnection between the aforementioned mechanism studies and testbed validations due to abstractions and assumptions. This situation can improve if testbed projects provide standard tools and data exchange protocols for early stage mechanism studies.

5 | CHALLENGES AND RESEARCH DIRECTIONS

The CPPS is an active yet emerging research field that covers the physical, monitoring, and actuation, computation, and communication subsystems. A variety of challenges are open for research, ranging from modeling and tooling to control and security. Below summarizes the emerging options and research directions.

5.1 | Unified and standard models

As discussed in the classification, there lacks consensus in the cyber-physical models, especially in how the cyber components should be characterized. In terms of methodology, existing numerical models need to be unified with information flow-based cyber systems. To compare the effectiveness of cyber-physical studies and promote interoperability, standard CPS models involving continuous and discrete-event models need to be developed.

5.2 | Improved co-design and simulation tools

Computer-aided design and simulation can speed up the understanding and application of CPPS. The design and simulation tools of today are highly domain-specific and did not consider both cyber and physical components when originally invented, nor do they provide unified CPPS models. Future research and development can focus on CPPS co-design and simulation software that treats the CPPS as an integrated system to enable top-down design and component-based testing.

5.3 | Feedback and control systems

Control systems have been widely applied in the physical power grid at the local, regional, and interconnection levels. Existing controls need to be revisited and redesigned to consider the impacts of communication, cyber-physical interactions, and interactions between multiple CPS. Emerging work has applied formulation verification approaches to guarantee control performance and system safety using feedback loops. With human factors in the feedback loop, theoretical and application control studies are needed to ensure the safe operation of CPPS.

5.4 | Cloud infrastructure and computing

Cloud infrastructure is the cornerstone for computing. Existing work has explored cloud-based energy management systems and simulations for scaling up computing capability. However, the challenges and disadvantages of shared cloud infrastructure are not clearly understood by the power community, especially for applications that are time-critical. Future research and development can focus on the software and architecture for cloud-enabled computing subsystems to achieve high scalability and low latency.

5.5 | Cybersecurity defense-in-depth methods

Cyberattacks on critical infrastructure have alarmed experts following numerous incidents in industrial control systems and foreign power grids. Sophisticated attacks are of the worst consequence due to their knowledge of the system and precise targeting. Defending CPPS against sophisticated attacks remains a challenging research task given the complexity in the subsystems and the countless enumeration of attack vectors. Therefore, systematic approaches are required for prototyping, simulating, and testing defense-in-depth cybersecurity strategies.

6 | CONCLUSIONS

This review summarizes the CPPS framework and its realization with the physical, monitoring, actuation, and computation subsystems are summarized. In particular, recent work on the modeling of PEID in large-scale physical subsystems. From the perspective of power systems, the model structure of PEID is generalized into a reference generator, reference tracker, and network interface. The voltage-source and current-source types of controls are discussed, followed by model simplification for industry applications. Next, the cybersecurity objectives and vulnerabilities are discussed with a review of studies based on three categories. Further, the testbed approaches for CPPS studies are presented, including testbed implementation and studies. Finally, challenges and research directions are discussed in the area of CPPS.

AUTHOR CONTRIBUTIONS

Hantao Cui: Conceptualization (equal); investigation (equal); writing – original draft (equal); writing – review and editing (equal). **Yichen Zhang:** Conceptualization (equal); investigation (equal); methodology (equal); writing – original draft (equal); writing – review and editing (equal). **Kevin L. Tomsovic:** Conceptualization (equal); funding acquisition (lead); investigation (equal); methodology (equal); project administration (equal); resources (equal); supervision (lead); writing – review and editing (lead). **Fangxing (Fran) Li:** Conceptualization (equal); project administration (equal); writing – review and editing (equal).

FUNDING INFORMATION

This work was supported in part by the Engineering Research Center Program of the National Science Foundation and the Department of Energy under NSF Award Number EEC-1041877 and the CURENT Industry Partnership Program.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study

ORCID

Hantao Cui https://orcid.org/0000-0002-4259-5925
Yichen Zhang https://orcid.org/0000-0002-6925-0775
Kevin L. Tomsovic https://orcid.org/0000-0002-2867-8556
Fangxing (Fran) Li https://orcid.org/0000-0003-1060-7618

RELATED WIREs ARTICLES

Addressing technical challenges in 100% variable i

REFERENCES

Abur, A., & Exposito, A. G. (2004). *Power system state estimation: Theory and implementation*. CRC Press.

Adhikari, U., Morris, T. H., & Pan, S. (2014). *A cyber-physical power system test bed for intrusion detection systems*. IEEE Power and Energy Society General Meeting, Washington D.C., USA, vol. 2014.

Arani, M. F. M., & El-Saadany, E. F. (2012). Implementing virtual inertia in DFIG-based wind power generation. *IEEE Transactions on Power Systems*, *28*(2), 1373–1384.

Ashok, A. & Govindarasu, M. (2012). *Cyber attacks on power system state estimation through topology errors* [Conference presentation]. 2012 IEEE Power and Energy Society General Meeting, San Diego, CA, USA. IEEE, 1–8.

Ashok, A., Hahn, A., & Govindarasu, M. (2011). *A cyber-physical security testbed for smart grid: System architecture and studies* [Conference presentation]. Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, TN, USA. ACM, 20, 2011.

Bagheri, A., Mardaneh, M., Rajaei, A., & Rahideh, A. (2015). Detection of grid voltage fundamental and harmonic components using Kalman filter and generalized averaging method. *IEEE Transactions on Power Electronics*, *31*(2), 1064–1073.

Bassey, O., Chen, B., Butler-Purry, K. L., & Goulart, A. (2017). Implementation of wide area control in a real-time cyber-physical power system test bed [Conference presentation]. 2017 North American Power Symposium, NAPS 2017, Morgantown, WV, USA.

Biswas, R. S., Tan, J., Jain, H., Gevorgian, V., & Zhang, Y. (2019). Equivalent test bed in PSCAD and PSLF for studying advanced power systems controller performance [Conference presentation]. 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington D.C., USA. IEEE, 1–5.

Blaabjerg, F., Teodorescu, R., Liserre, M., & Timbus, A. (2006). Overview of control and grid synchronization for distributed power generation systems. *IEEE Transactions on Industrial Electronics*, *53*(5), 1398–1409. https://doi.org/10.1109/tie.2006.881997

Brahma, S., Kavasseri, R., Cao, H., Chaudhuri, N., Alexopoulos, T., & Cui, Y. (2016). Real-time identification of dynamic events in power systems using PMU data, and potential applications-models, promises, and challenges. *IEEE Transactions on Power Delivery*, *32*(1), 294–301.

Brown, T., Hörsch, J., & Schlachtberger, D. (2017). PyPSA: Python for power system analysis. *arXiv*. https://doi.org/10.5334/jors.188

Buldyrev, S., Parshani, R., Paul, G., Stanley, H., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature*, *464*, 1025–1028.

Chang, X. (1999). *Network simulations with OPNET* [Conference presentation]. Proceedings of the 31st Conference on Winter Simulation—A bridge to the future - WSC '99, Phoenix, AZ, USA. ACM Press. https://doi.org/10.1145/324138.324232

Chassin, D. P., Schneider, K., & Gerkensmeyer, C. (2008). *GridLAB-D: An open-source power systems modeling and simulation environment* [Conference presentation]. 2008 IEEE/PES Transmission and Distribution Conference and Exposition, Chicago, IL, USA. IEEE, 1–5.

Chen, B., Butler-Purry, K. L., Goulart, A., & Kundur, D. (2014). *Implementing a real-time cyber-physical system test bed in RTDS and OPNET* [Conference presentation]. 2014 North American Power Symposium, NAPS 2014, Pullman, WA, USA.

Chow, J. H., & Sanchez-Gasca, J. J. (2020). *Power system modeling, computation, and control*. John Wiley & Sons.

CIRED. (2018). *Modelling of inverter-based generation for power system dynamic studies* (CIRED Technical Report-727).

Cole, S., & Belmans, R. (2011). *MatDyn, a new Matlab based toolbox for power system dynamic simulation* [Conference presentation]. 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA. 1–1.

Cui, H., Li, F., & Tomsovic, K. (2019). Cyber-physical system testbed for power system monitoring and wide-area control verification. *IET Energy Systems Integration*, *2*(1), 32–39.

Cui, H., Li, F., & Tomsovic, K. (2020). Hybrid symbolic-numeric framework for power system modeling and analysis. *IEEE Transactions on Power Systems*, 36(2), 1373–1384.

de Souza Ribeiro, L. A., Freijedo, F. D., de Bosio, F., Lima, M. S., Guerrero, J. M., & Pastorelli, M. (2018). Full discrete modeling, controller design, and sensitivity analysis for high-performance grid-forming converters in islanded microgrids. *IEEE Transactions on Industry Applications*, *54*(6), 6267–6278.

DIgSILENT. (2021, March 29). *Home*. https://www.digsilent.de/en/

Ekomwenrenren, E., Alharbi, H., Elgorashi, T., Elmirghani, J., & Aristidou, P. (2019). Stabilising control strategy for cyber-physical power systems. *IET Cyber-Physical Systems: Theory and Applications*, *4*(3), 265–275.

Enescu, F. M., & Bizon, N. (2017). SCADA applications for electric power system. In *Reactive power control in AC power systems* (pp. 561–609). Springer.

Falahati, B., & Fu, Y. (2014). Reliability assessment of smart grids considering indirect cyber-power interdependencies. *IEEE Transactions on Smart Grid*, *5*(4), 1677–1685. https://doi.org/10.1109/tsg.2014.2310742

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419

Gautam, D., Goel, L., Ayyanar, R., Vittal, V., & Harbour, T. (2011). Control strategy to mitigate the impact of reduced inertia due to doubly fed induction generators on large power systems. *IEEE Transactions on Power Systems*, *26*(1), 214–224. https://doi.org/10.1109/tpwrs.2010.2051690

Gjermundrod, H., Gjermundrod, H., Bakken, D., Hauser, C., & Bose, A. (2009). GridStat: A flexible QoS-managed data dissemination framework for the power grid. *IEEE Transactions on Power Delivery*, *24*(1), 136–143. https://doi.org/10.1109/tpwrd.2008.917693

Goksu, O., Teodorescu, R., Bak, C. L., Iov, F., & Kjaer, P. C. (2014). Instability of wind turbine converters during current injection to low voltage grid faults and PLL frequency based stability solution. *IEEE Transactions on Power Systems*, *29*(4), 1683–1691.

Griffor, E. R., Greer, C., Wollman, D. A., & Burns, M. J. (2017). *Framework for cyber-physical systems: Volume 1 overview* (Technical Report-NIST Special Publication 1500-201). National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.1500-201

Guerrero, J. M., Vasquez, J. C., Matas, J., de Vicuna, L. G., & Castilla, M. (2011). Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization. *IEEE Transactions on Industrial Electronics*, *58*(1), 158–172. https://doi.org/10.1109/tie.2010.2066534

Gunduz, H., & Jayaweera, D. (2018). Reliability assessment of a power system with cyber-physical interactive operation of photovoltaic systems. *International Journal of Electrical Power and Energy Systems*, *101*(April), 371–384. https://doi.org/10.1016/j.ijepes.2018.04.001

Guo, J., Han, Y., Guo, C., Lou, F., & Wang, Y. (2017). Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties. *Energies*, *10*(1), 87. https://doi.org/10.3390/en10010087

Guo, M., Li, X., Gao, Z., & Su, G. (2020). *Simulation and analysis on stability improvement of Zhangbei renewable energy transmission via VSC-HVDC based on RTDS* [Conference presentation]. 2020 4th International Conference on HVDC (HVDC), Xi'an, China. IEEE, 299–303.

Haginomori, E., Koshiduka, T., Arai, J., & Ikeda, H. (2016). *Power system transient analysis: Theory and practice using simulation programs (ATP-EMTP)*. John Wiley & Sons.

cHan, Y., Wen, Y., Guo, C., & Huang, H. (2015). Incorporating cyber layer failures in composite power system reliability evaluations. *Energies*, *8*(9), 9064–9086. https://doi.org/10.3390/en8099064

Hansen, A. D., Sørensen, P., Iov, F., & Blaabjerg, F. (2006). Centralised power control of wind farm with doubly fed induction generators. *Renewable Energy*, *31*(7), 935–951. https://doi.org/10.1016/j.renene.2005.05.011

Hatziargyriou, N., Milanovic, J., Rahmann, C., Ajjarapu, V., Canizares, C., Erlich, I., Hill, D., Hiskens, I., Kamwa, I., & Pal, B. (2020). Definition and classification of power system stability-revisited & extended. *IEEE Transactions on Power Systems*, *36*(4), 3271–3281.

Hong, T., & De León, F. (2016). Controlling non-synchronous microgrids for load balancing of radial distribution systems. *IEEE Transactions on Smart Grid*, *8*(6), 2608–2616.

Hu, J., Wang, S., Tang, W., & Xiong, X. (2016). Full-capacity wind turbine with inertial support by adjusting phase-locked loop response. *IET Renewable Power Generation*, *11*(1), 44–53. https://doi.org/10.1049/iet-rpg.2016.0155

Hu, Q., Fu, L., Ma, F., & Ji, F. (2019). Large signal synchronizing instability of PLL-based VSC connected to weak AC grid. *IEEE Transactions on Power Systems*, *34*(4), 3220–3229.

Huang, L., Wu, C., Zhou, D., & Blaabjerg, F. (2021). A double-PLLs-based impedance reshaping method for extending stability range of grid-following inverter under weak grid. *IEEE Transactions on Power Electronics*, *37*(4), 4091–4104.

Huang, L., Xin, H., Li, Z., Ju, P., Yuan, H., Lan, Z., & Wang, Z. (2019). Grid-synchronization stability analysis and loop shaping for PLL-based power converters with different reactive power control. *IEEE Transactions on Smart Grid*, *11*(1), 501–516.

Huang, L., Xin, H., Wang, Z., Wu, K., Wang, H., Hu, J., & Lu, C. (2017). A virtual synchronous control for voltage-source converters utilizing dynamics of DC-link capacitor to realize self-synchronization. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, *5*(4), 1565–1577. https://doi.org/10.1109/jestpe.2017.2740424

Hussein, A. A.-H. & Batarseh, I. (2011). *An overview of generic battery models* [Conference presentation]. 2011 IEEE Power and Energy Society General Meeting. IEEE. doi: https://doi.org/10.1109/pes.2011.6039674

Jalili-Marandi, V., Ayres, F. J., Ghahremani, E., Belanger, J., & Lapointe, V. (2013). *A real-time dynamic simulation tool for transmission and distribution power systems* [Conference presentation]. 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, CA. IEEE. https://doi.org/10.1109/pesmg.2013.6672734

Kenyon, R. W., Sajadi, A., Hoke, A., & Hodge, B.-M. (2021). *Open-source PSCAD grid-following and grid-forming inverters and a benchmark for zero-inertia power system simulations* [Conference presentation]. 2021 IEEE Kansas Power and Energy Conference (KPEC), Manhattan, KS, USA. IEEE, 1–6.

Kouro, S., Cortes, P., Vargas, R., Ammann, U., & Rodriguez, J. (2009). Model predictive control—A simple and powerful method to control power converters. *IEEE Transactions on Industrial Electronics*, *56*(6), 1826–1838. https://doi.org/10.1109/tie.2008.2008349

Kroutikova, N., Hernandez-Aramburo, C., & Green, T. (2007). State-space model of grid-connected inverters under current control mode. *IET Electric Power Applications*, *1*(3), 329. https://doi.org/10.1049/iet-epa-20060276

Kundur, P., Paserba, J., Ajjarapu, V., Andersson, G., Bose, A., Canizares, C., Hatziargyriou, N., Hill, D., Stankovic, A., & Taylor, C. (2004). Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions. *IEEE Transactions on Power Systems*, *19*(3), 1387–1401.

Kwon, S., Yoo, H., & Shon, T. (2020). IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system. *IEEE Access*, *8*, 77572–77586. https://doi.org/10.1109/access.2020.2989770

Lantz, B., Heller, B., & McKeown, N. (2010). *A network in a laptop* [Conference presentation]. *Proceedings of the ninth ACM SIGCOMM workshop on hot topics in networks - Hotnets '10*, Cambridge, MA, USA. ACM Press. https://doi.org/10.1145/1868447.1868466

Leger, A. S., Spruce, J., Banwell, T., & Collins, M. (2016). *Smart grid testbed for wide-area monitoring and control systems* [Conference presentation]. 2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Dallas, TX, USA. IEEE, 1–5.

Lei, H., Singh, C., & Sprintson, A. (2014). Reliability modeling and analysis of IEC 61850 based substation protection systems. *IEEE Transactions on Smart Grid*, *5*(5), 2194–2202. https://doi.org/10.1109/tsg.2014.2314616

Leslie, J. *Managing declining inertia and short circuit levels*. https://www.esig.energy/download/managing-grid-stability-in-a-high-ibr-network-julian-leslie/?wpdmdl=8504&refresh=61f14353799ba1643201363.

Li, F., Tomsovic, K., & Cui, H. (2020). A large-scale testbed as a virtual power grid: For closed-loop controls in research and testing. *IEEE Power and Energy Magazine*, *18*(2), 60–68.

Li, F., Yan, X., Xie, Y., Sang, Z., & Yuan, X. (2019). *A review of cyber-attack methods in cyber-physical power system* [Conference presentation]. APAP 2019 - 8th IEEE International Conference on Advanced Power System Automation and Protection, New York, NY, US. 1335–1339.

Liljenstam, M., Liu, J., Nicol, D. M., Yuan, Y., Yan, G., & Grier, C. (2006). RINSE: The real-time immersive network simulation environment for network security exercises (extended version). *Simulation*, *82*(1), 43–59. https://doi.org/10.1177/0037549706065544

Liserre, M., Teodorescu, R., & Blaabjerg, F. (2006). Multiple harmonics control for three-phase grid converter systems with the use of PI-RES current controller in a rotating frame. *IEEE Transactions on Power Electronics*, *21*(3), 836–841. https://doi.org/10.1109/tpel.2006.875566

Liu, R., Vellaithurai, C., Biswas, S. S., Gamage, T. T., & Srivastava, A. K. (2015). Analyzing the cyber-physical impact of cyber events on the power grid. *IEEE Transactions on Smart Grid*, *6*(5), 2444–2453.

Liu, X., Wang, P., & Loh, P. C. (2011). A hybrid AC/DC microgrid and its coordination control. *IEEE Transactions on Smart Grid*, *2*(2), 278–286. https://doi.org/10.1109/tsg.2011.2116162

Ma, Y., Cao, W., Yang, L., Wang, F. F., & Tolbert, L. M. (2017). Virtual synchronous generator control of full converter wind turbines with short-term energy storage. *IEEE Transactions on Industrial Electronics*, *64*(11), 8821–8831. https://doi.org/10.1109/tie.2017.2694347

Majumder, R., Chaudhuri, B., Ghosh, A., Majumder, R., Ledwich, G., & Zare, F. (2010). Improvement of stability and load sharing in an autonomous microgrid using supplementary droop control loop. *IEEE Transactions on Power Systems*, *25*(2), 796–808. https://doi.org/10.1109/tpwrs.2009.2032049

Martin, A. D., Cano, J. M., Silva, J. F. A., & Vazquez, J. R. (2015). Backstepping control of smart grid-connected distributed photovoltaic power supplies for telecom equipment. *IEEE Transactions on Energy Conversion*, *30*(4), 1496–1504. https://doi.org/10.1109/tec.2015.2431613

Matevosyan, J., Badrzadeh, B., Prevost, T., Quitmann, E., Ramasubramanian, D., Urdal, H., Achilles, S., MacDowell, J., Huang, S. H., Vital, V., et al. (2019). Grid-forming inverters: Are they the key for high renewable penetration? *IEEE Power and Energy Magazine*, *17*(6), 89–98.

McLaren, P., Kuffel, R., Wierckx, R., Giesbrecht, J., & Arendt, L. (1992). A real time digital simulator for testing relays. *IEEE Transactions on Power Delivery*, *7*(1), 207–213. https://doi.org/10.1109/61.108909

Milano, F. (2006). An open source power system analysis toolbox [conference presentation]. *2006 IEEE Power Engineering Society General Meeting*, PES, Montreal, Quebec, CA. Vol. 20, No 3. 1199–1206.

Milano, F., Dörfler, F., Hug, G., Hill, D., & Verbic, G. (2018). *Foundations and challenges of low-inertia systems* [Conference presentation]. 2018 Power Systems Computation Conference (PSCC), Dublin, Ireland.

Milano, F., & Ortega, A. (2017). Frequency divider. *IEEE Transactions on Power Systems*, *32*(2), 1493–1501.

Mirz, M., Vogel, S., Reinke, G., & Monti, A. (2019). DPsim—A dynamic phasor real-time simulator for power systems. *SoftwareX*, *10*, 100253. https://doi.org/10.1016/j.softx.2019.100253

Misyris, G. S., Chatzivasileiadis, S., & Weckesser, T. (2021). Grid-forming converters: Sufficient conditions for RMS modeling. *Electric Power Systems Research*, *197*, 107324.

Montenegro, D., Dugan, R. C., & Reno, M. J. (2017). *Open source tools for high performance quasi-static-time-series simulation using parallel processing* [Conference presentation]. 2017 IEEE 44th Photovoltaic Specialist Conference (PVSC), Washington D.C., USA. IEEE, 3055–3060.

Moursi, M. E., Joos, G., & Abbey, C. (2008). A secondary voltage control strategy for transmission level interconnection of wind generation. *IEEE Transactions on Power Electronics*, *23*(3), 1178–1190. https://doi.org/10.1109/tpel.2008.921195

Mullane, A., & O'Malley, M. (2005). The inertial response of induction-machine-based wind turbines. *IEEE Transactions on Power Systems*, *20*(3), 1496–1503. https://doi.org/10.1109/tpwrs.2005.852081

Nabavi, S., Zhang, J., & Chakrabortty, A. (2015). Distributed optimization algorithms for wide-area oscillation monitoring in power systems using interregional PMU-PDC architectures. *IEEE Transactions on Smart Grid*, *6*(5), 2529–2538.

Niu, X., Li, J., Sun, J. & Tomsovic, K. (2019). *Dynamic detection of false data injection attack in smart grid using deep learning* [Conference presentation]. 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington D.C., USA. IEEE. https://doi.org/10.1109/isgt.2019.8791598

Ochoa, D., & Martinez, S. (2016). Fast-frequency response provided by DFIG-wind turbines and its impact on the grid. *IEEE transactions on power systems*, *32*(5), 4002–4011.

Ortega, A., & Milano, F. (2015). Generalized model of VSC-based energy storage systems for transient stability analysis. *IEEE Transactions on Power Systems*, *31*(5), 3369–3380.

Palensky, P., Widl, E., & Elsheikh, A. (2014). Simulating cyber-physical energy systems: Challenges, tools and methods. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *44*(3), 318–326.

Palmintier, B., Krishnamurthy, D., Top, P., Smith S., Daily, J., & Fuller, J. (2017). *Design of the HELICS high-performance transmission-distribution-communication-market co-simulation framework* [Conference presentation]. 2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Pittsburgh, PA, USA. IEEE. doi: https://doi.org/10.1109/mscpes.2017.8064542

Paquin, J.-N., Belanger, J., Snider, L., Pirolli, C., & Li, W. (2009). *Monte-carlo study on a large-scale power system model in real-time using eMEGAsim* [Conference presentation]. 2009 IEEE Energy Conversion Congress and Exposition, San Jose, CA, USA. IEEE. doi: https://doi.org/10.1109/ecce.2009.5316251

Pogaku, N., Prodanovic, M., & Green, T. C. (2007). Modeling analysis and testing of autonomous operation of an inverter-based microgrid. *IEEE Transactions on Power Electronics*, *22*(2), 613–625. https://doi.org/10.1109/tpel.2006.890003

Pourbeik, P. (2014). *Specification of the second generation generic models for wind turbine generators* (Electric Power Research Institute Report).

PSCAD. (2021). *Home*. https://www.pscad.com/

Ramasubramanian, D., Yu, Z., Ayyanar, R., Vittal, V., & Undrill, J. (2017). Converter model for representing converter interfaced generation in large scale grid simulations. *IEEE Transactions on Power Systems*, *32*(1), 765–773. https://doi.org/10.1109/tpwrs.2016.2551223

Raoufat, M. E., Tomsovic, K., & Djouadi, S. M. (2017). Dynamic control allocation for damping of inter-area oscillations. *IEEE Transactions on Power Systems*, *32*(6), 4894–4903.

Rasmussen, T. B., Yang, G., Nielsen, A. H., & Dong, Z. (2017). *A review of cyber-physical energy system security assessment* [Conference presentation]. 2017 IEEE Manchester PowerTech, Powertech 2017, Manchester, UK.

Riley, G. F., & Henderson, T. R. (2010). The ns-3 network simulator. In *Modeling and tools for network simulation* (pp. 15–34). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-12331-3_2

Rocabert, J., Luna, A., Blaabjerg, F., & Rodríguez, P. (2012). Control of power converters in AC microgrids. *IEEE Transactions on Power Electronics*, *27*(11), 4734–4749. https://doi.org/10.1109/tpel.2012.2199334

Schmidt, M., & Åhlund, C. (2018). Smart buildings as cyber-physical systems: Data-driven predictive control strategies for energy efficiency. *Renewable and Sustainable Energy Reviews*, *90*(2017), 742–756. https://doi.org/10.1016/j.rser.2018.04.013

Shao, M., Miller, N. W., Sanchez-Gasca, J. J., & MacDowell, J. (2013). *Modeling of GE wind turbine-generators for grid studies* (General Electric Technical Report-GE WTG Modeling-v4.5).

Shi, L., Dai, Q., & Ni, Y. (2018). Cyber-physical interactions in power systems: A review of models, methods, and applications. *Electric Power Systems Research*, *163*(June), 396–412. https://doi.org/10.1016/j.epsr.2018.07.015

Shourangiz-Haghighi, A., Diazd, M., Zhang, Y., Li, J., Yuan, Y., Faraji, R., Ding, L., & Guerrero, J. M. (2020). Developing more efficient wind turbines: A survey of control challenges and opportunities. *IEEE Industrial Electronics Magazine*, *14*(4), 53–64. https://doi.org/10.1109/mie.2020.2990353

Sozer, Y., & Torrey, D. (2009). Modeling and control of utility interactive inverters. *IEEE Transactions on Power Electronics*, *24*(11), 2475–2483. https://doi.org/10.1109/tpel.2009.2029576

Sun, C. C., Liu, C. C., & Xie, J. (2016). Cyber-physical system security of a power grid: State-of-the-art. *Electronics (Switzerland)*, *5*(3), 40.

Tayyebi, A., Dörfler, F., Kupzog, F., Miletic, Z., & Hribernik, W. (2018). *Grid-forming converters - Inevitability, control strategies and challenges in future grids application* [Conference representation]. CIRED 2018 Ljubljana Workshop, Ljubljana, Slovenia. https://www.cired-repository.org/handle/20.500.12455/1249

Thomas, M. S., & McDonald, J. D. (2017). *Power system SCADA and smart grids*. CRC Press.

Thurner, L., Scheidler, A., Schafer, F., Menke, J. H., Dollichon, J., Meier, F., Meinecke, S., & Braun, M. (2018). Pandapower - An open-source python tool for convenient modeling, analysis, and optimization of electric power systems. *IEEE Transactions on Power Systems*, *33*(6), 6510–6521.

Timbus, A., Liserre, M., Teodorescu, R., Rodriguez, P., & Blaabjerg, F. (2009). Evaluation of current controllers for distributed power generation systems. *IEEE Transactions on Power Electronics*, *24*(3), 654–664. https://doi.org/10.1109/tpel.2009.2012527

Tong, H., Ni, M., Zhao, L., & Li, M. (2019). Flexible hardware-in-the-loop testbed for cyber physical power system simulation. *IET Cyber-Physical Systems: Theory and Applications*, *4*(4), 374–381.

Ulbig, A., Borsche, T. S., & Andersson, G. (2014). Impact of low rotational inertia on power system stability and operation. *IFAC Proceedings Volumes*, *47*(3), 7290–7297.

Vanfretti, L., Dosiek, L., Pierre, J. W., Trudnowski, D., Chow, J. H., García-Valle, R., & Aliyu, U. (2011). Application of ambient analysis techniques for the estimation of electromechanical oscillations from measured PMU data in four different power systems. *European Transactions on Electrical Power*, *21*(4), 1640–1656.

Varga, A. (2010). OMNeT++. In W. Klaus, G. James, & G. Mesut (Eds.), *Modeling and tools for network simulation* (pp. 35–59). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-12331-3_3

Variani, M. H., & Tomsovic, K. (2016). Two-level control of doubly fed induction generator using flatness-based approach. *IEEE Transactions on Power Systems*, *31*(1), 518–525. https://doi.org/10.1109/tpwrs.2015.2404788

Villalva, M., Gazoli, J., & Filho, E. (2009). Comprehensive approach to modeling and simulation of photovoltaic arrays. *IEEE Transactions on Power Electronics*, *24*(5), 1198–1208. https://doi.org/10.1109/tpel.2009.2013862

Wang, B., Zhang, Y., Sun, K., & Tomsovic, K. (2018). *Quantifying the synthetic inertia and load-damping effect of a converter-interfaced power source* [Conference presentation]. 2018 IEEE International Energy Conference (ENERGYCON). IEEE. doi: https://doi.org/10.1109/energycon.2018.8398838

Wang, H., Ruan, J., Zhou, B., Li, C., Wu, Q., Raza, M. Q., & Cao, G. Z. (2019). Dynamic data injection attack detection of cyber physical power systems with uncertainties. *IEEE Transactions on Industrial Informatics*, *15*(10), 5505–5518.

Wang, Q., Tai, W., Tang, Y., & Ni, M. (2018). Review of the false data injection attack against the cyber-physical power system. *IET Cyber-Physical Systems: Theory & Applications*, *4*(2), 101–107. https://doi.org/10.1049/Fiet-cps.2018.5022

Wang, S., Hu, J., Yuan, X., & Sun, L. (2015). On inertial dynamics of virtual-synchronous-controlled DFIG-based wind turbines. *IEEE Transactions on Energy Conversion*, *30*(4), 1691–1702.

Wang, S., & Tomsovic, K. (2018). A novel active power control framework for wind turbine generators to improve frequency response. *IEEE Transactions on Power Systems*, *33*(6), 6579–6589. https://doi.org/10.1109/tpwrs.2018.2829748

Wang, W., Huang, G. M., Kansal, P., Anderson, L. E., O'Keefe, R. J., Ramasubramanian, D., Mitra, P., & Farantatos, E. (2018). *Instability of PLL-synchronized converter-based generators in low short-circuit systems and the limitations of positive sequence modeling* [Conference presentation]. 2018 North American Power Symposium (NAPS), 1–6.

Weber, J. (2014). *2nd generation wind turbine models in PowerWorld* [Conference presentation]. Online. PowerWorld Client Conference.

Wei, J. & Mendis, G. J. (2016). *A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids* [Conference presentation]. 2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG), Vienna, Austria. https://doi.org/10.1109/cpsrsg.2016.7684102

Wickramasinghe, C. S., Marino, D. L., Amarasinghe, K., & Manic, M. (2018). *Generalization of deep learning for cyber-physical system security: A survey* [Conference presentation]. *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*. IEEE. doi:https://doi.org/10.1109/iecon.2018.8591773

Wilches-Bernal, F., Chow, J. H., & Sanchez-Gasca, J. J. (2016). A fundamental study of applying wind turbines for power system frequency control. *IEEE Transactions on Power Systems*, *31*(2), 1496–1505. https://doi.org/10.1109/tpwrs.2015.2433932

WREMT Force. (2016). *WECC battery storage dynamic modeling guideline* (Western Electricity Coordinating Council Technical Report).

WREMT Force. (2019). *Solar photovoltaic power plant modeling and validation guideline* (Western Electricity Coordinating Council Technical Report).

Xiang, Y., Wang, L., & Liu, N. (2017). Coordinated attacks on electric power systems in a cyber-physical environment. *Electric Power Systems Research*, *149*, 156–168. https://doi.org/10.1016/j.epsr.2017.04.023

Yan, J., He, H., Zhong, X., & Tang, Y. (2017). Q-learning-based vulnerability analysis of smart grid against sequential topology attacks. *IEEE Transactions on Information Forensics and Security*, *12*(1), 200–210. https://doi.org/10.1109/tifs.2016.2607701

Yang, L., Ma, Y., Wang, J., Wang, J., Zhang, X., Tolbert, L. M., Wang, F., & Tomsovic, K. (2014). *Development of converter based reconfigurable power grid emulator* [Conference presentation]. Pittsburg, PA, USA. 2014 IEEE Energy Conversion Congress and Exposition (ECCE). IEEE. doi:https://doi.org/10.1109/ecce.2014.6953944

Yang, P., Tan, Z., Wiesel, A., & Nehorai, A. (2013). Power system state estimation using PMUs with imperfect synchronization. *IEEE Transactions on Power Systems*, *28*(4), 4162–4172.

Yardley, T., Berthier, R., Nicol, D., & Sanders, W. H. (2013). *Smart grid protocol testing through cyber-physical testbeds* [Conference presentation]. Washington D.C., USA. 2013 IEEE PES Innovative Smart Grid Technologies Conference, ISGT 2013.

Zhang, L., Harnefors, L., & Nee, H.-P. (2009). Power-synchronization control of grid-connected voltage-source converters. *IEEE Transactions on Power Systems*, *25*(2), 809–820.

Zhang, Q., Li, F., Shi, Q., Tomsovic, K., Sun, J., & Ren, L. (2020). Profit-oriented false data injection on energy market: Reviews, analyses and insights. *IEEE Transactions on Industrial Informatics*, *17*, 5876–5886.

Zhang, Y., Krishnan, V. V., Pi, J., Kaur, K., Srivastava, A., Hahn, A., & Suresh, S. (2020). Cyber physical security analytics for Transactive energy systems. *IEEE Transactions on Smart Grid*, *11*(2), 931–941.

Zhang, Y., Melin, A. M., Djouadi, S. M., Olama, M. M., & Tomsovic, K. (2018). Provision for guaranteed inertial response in diesel-wind systems via model reference control. *IEEE Transactions on Power Systems*, *33*(6), 6557–6568. https://doi.org/10.1109/tpwrs.2018.2827205

Zhang, Y., Raoufat, M. E., Tomsovic, K., & Djouadi, S. M. (2019). Set theory-based safety supervisory control for wind turbines to ensure adequate frequency response. *IEEE Transactions on Power Systems*, *34*(1), 680–692. https://doi.org/10.1109/tpwrs.2018.2867825

Zhang, Y., Tomsovic, K., Djouadi, S. M., & Pulgar-Painemal, H. (2017). Hybrid controller for wind turbine generators to ensure adequate frequency response in power networks. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, *7*(3), 359–370. https://doi.org/10.1109/jetcas.2017.2675879

Zhao, J., Gómez-Expósito, A., Netto, M., Mili, L., Abur, A., Terzija, V., Kamwa, I., Pal, B., Singh, A. K., Qi, J., et al. (2019). Power system dynamic state estimation: Motivations, definitions, methodologies, and future work. *IEEE Transactions on Power Systems*, *34*(4), 3188–3198.

Zhong, Q.-C., & Weiss, G. (2010). Synchronverters: Inverters that mimic synchronous generators. *IEEE Transactions on Industrial Electronics*, *58*(4), 1259–1267.

Zhong, W., Liu, M. & Milano, F. (2019). *A co-simulation framework for power systems and communication networks* [Conference presentation]. Milan, Italy. 2019 IEEE Milan PowerTech. IEEE, 1–6.

Zhou, M., & Zhou, S. (2007). *Internet, open-source and power system simulation* [Conference presentation]. Tampa, FL, USA. 2007 IEEE Power Engineering Society General Meeting, PES, 1–5.

Zimmerman, R. D., Murillo-Sanchez, C. E., Thomas, R. J., Murillo-Sánchez, C. E., & Thomas, R. J. (2011). MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education. *IEEE Transactions on Power Systems*, *26*(1), 12–19.

How to cite this article: Cui, H., Zhang, Y., Tomsovic, K. L., & Li, F. (F.) (2022). Power electronics-interfaced cyber-physical power systems: A review on modeling, simulation, and cybersecurity. *WIREs Energy and Environment*, *11*(6), e448. https://doi.org/10.1002/wene.448