IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received August 5, 2020, accepted August 12, 2020, date of publication August 14, 2020, date of current version August 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3016826

Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications

RAJAA VIKHRAM YOHANANDHAN[1], (Member, IEEE), RAJVIKRAM MADURAI ELAVARASAN[2], PREMKUMAR MANOHARAN[3], AND LUCIAN MIHET-POPA[4], (Senior Member, IEEE)

[1]Department of Electronics and Instrumentation Engineering, SRM Institute of Science and Technology at Kattankulathur Campus, Chennai 603203, India
[2]Electrical and Automotive Parts Manufacturing Unit, AA Industries, Chennai 600123, India
[3]Department of Electrical and Electronics Engineering, GMR Institute of Technology, Rajam Andhra Pradesh 532127, India
[4]Faculty of Engineering, Østfold University College, 1757 Halden, Norway

Corresponding authors: Rajvikram Madurai Elavarasan (rajvikram787@gmail.com) and Lucian Mihet-Popa (lucian.mihet@hiof.no)

ABSTRACT Cyber-Physical System (CPS) is a new kind of digital technology that increases its attention across academia, government, and industry sectors and covers a wide range of applications like agriculture, energy, medical, transportation, etc. The traditional power systems with physical equipment as a core element are more integrated with information and communication technology, which evolves into the Cyber-Physical Power System (CPPS). The CPPS consists of a physical system tightly integrated with cyber systems (control, computing, and communication functions) and allows the two-way flows of electricity and information for enabling smart grid technologies. Even though the digital technologies monitoring and controlling the electric power grid more efficiently and reliably, the power grid is vulnerable to cybersecurity risk and involves the complex interdependency between cyber and physical systems. Analyzing and resolving the problems in CPPS needs the modelling methods and systematic investigation of a complex interaction between cyber and physical systems. The conventional way of modelling, simulation, and analysis involves the separation of physical domain and cyber domain, which is not suitable for the modern CPPS. Therefore, an integrated framework needed to analyze the practical scenario of the unification of physical and cyber systems. A comprehensive review of different modelling, simulation, and analysis methods and different types of cyber-attacks, cybersecurity measures for modern CPPS is explored in this paper. A review of different types of cyber-attack detection and mitigation control schemes for the practical power system is presented in this paper. The status of the research in CPPS around the world and a new path for recommendations and research directions for the researchers working in the CPPS are finally presented.

INDEX TERMS Cyber-physical power system (CPPS), CPPS modelling, CPPS simulation, cyber-physical social system (CPSS), cyber attack, cyber security, smart grid.

ACRONYMS

ADC	Analog to Digital Converter
AGC	Automatic Generation Control
AMI	Advanced Metering Infrastructure
CPN	Coloured Petri Net
CPPS	Cyber-Physical Power System
CPS	Cyber-Physical System
CPSS	Cyber-Physical Social System
DAC	Digital to Analog Converter
DAI	Distributed Averaging based Integral
DER	Distributed Energy Resource
DFSM	Deterministic FSM
DG	Distributed Generator
DR	Demand Response
DSM	Demand Side Management
EV	Electric Vehicle
FACTS	Flexible AC Transmission System
FSM	Finite State Machine
GPS	Global Positioning System
HMAS	Holonic Multi-Agent System
ICT	Information and Communication Technology

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

HVDC	High-Voltage Direct Current
IED	Intelligent Electronic Device
MDP	Markov Decision Process
NDFSM	Non-Deterministic FSM
NIST	National Institute of Science and Technology
PDF	Probability Distribution Function
PMU	Phasor Measurement Unit
RBD	Reliability Block Diagram
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCD	State Chart Diagram
SMP	Semi Markov Process
SPN	Stochastic Petri Net
VPP	Virtual Power Plant
WAC	Wide-Area Control
WADC	Wide-Area Damping Controller
WAMS	Wide-Area Measurement System
WAMPAC	Wide-Area Monitoring Protection and Control
ZOH	Zero-Order Hold

I. INTRODUCTION

In the past years, the power and control system engineers are working very hard to develop the tools and techniques for improving the performance of monitoring and control of the physical power system. At the same time, computer science and electronics engineers are working on the cyber system to enhance the performance of the computing and communication systems. It leads to the development of computing ubiquitous. In our day to day life, every gadget and electronic devices are integrated with low-cost computing and communication networks. There is no doubt it will going to create a significant impact on the energy system [1]. The integration of physical and cyber system evolves into a new digital technology called Cyber-Physical System (CPS). Nowadays, CPS increases its attention in all sectors like agriculture, energy, medical, oil & gas industries, and transportation, etc. The CPS is defined as a heterogeneous multi-dimensional system with integrated cyber part (control, computing, communication) to attain the characteristics of stability, robustness, efficiency, and reliability in physical systems applications. In the CPS, the cyber system acquires the data from the physical system by the sensor and fed back the control signal to the physical system to attain the common goals, as shown in Fig. 1. To maintain the efficient and secure operation of the power systems, it is necessary to integrate the physical power system with a cyber system [2]. The integration of the physical power system with a cyber system [3], [4] evolves into a strongly coupled cyber-physical power system (CPPS). The CPPS covers all the domains of the electric power systems like Generation, Transmission, Distribution, and Utilization, as shown in Fig. 2. A Cyber Physical Power System (CPPS) is a system that combines and coordinates the internet and physical power system elements. These systems are distributed networks executing in unpredictable environments and built from control systems and embedded systems to monitor and regulate the physical power system in real time. CPPSs are designed as a structure of interacting elements with physical input and output. This is not about adding computing and communication techniques to conservative inventions where both sides maintain distinct individualities. This is about the integration of computing and networking with physical power systems to generate novel innovations in science, technical skills, and creations. *Cyber* is an integration of communication, computation, and control systems. *Physica*l means natural and human-made power systems that are governed and managed by the physics regulations and functioning in constant time. In CPPSs, the cyber and physical systems are those firmly incorporated at all stages and dimensions. CPPS uses embedded computers and networks to compute, communicate, and organize physical power system actions. Simultaneously, a CPPS receives feedback on how physical power system events impact computations and vice versa as shown in Fig. 1. Just as the Internet facilitates a way for the humans to interact with each other, CPPSs will transform in a way, how we interact with the physical power system world around us. To enable standard communication link between heterogeneous systems, CPPS-Interconnection Protocol is used. This protocol is mainly designed for special CPSs such as CPPSs, which require overall instruction and performance guarantee for cyber physical interaction. The main objective of this protocol is to offer CPPSs heterogeneity at three different levels: function interoperability, policy regulation, and performance assurance. Later, the transport protocol services used in the design of CPS-Interconnection Protocol. As an intellectual challenge, CPPS is about the intersection, not the union of the physical power system and the cyber. It is not adequate to individually understand the physical power system components and the computational components. We must instead understand their interaction as shown in Fig. 2. The design of such systems, therefore, requires understanding the joint dynamics of computers, software, networks, and physical power systems.

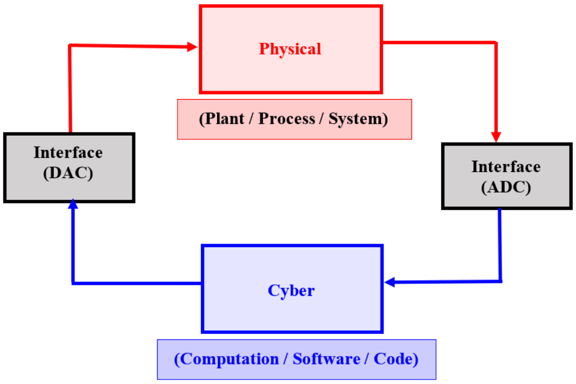

FIGURE 1. Structure of the cyber-physical system.

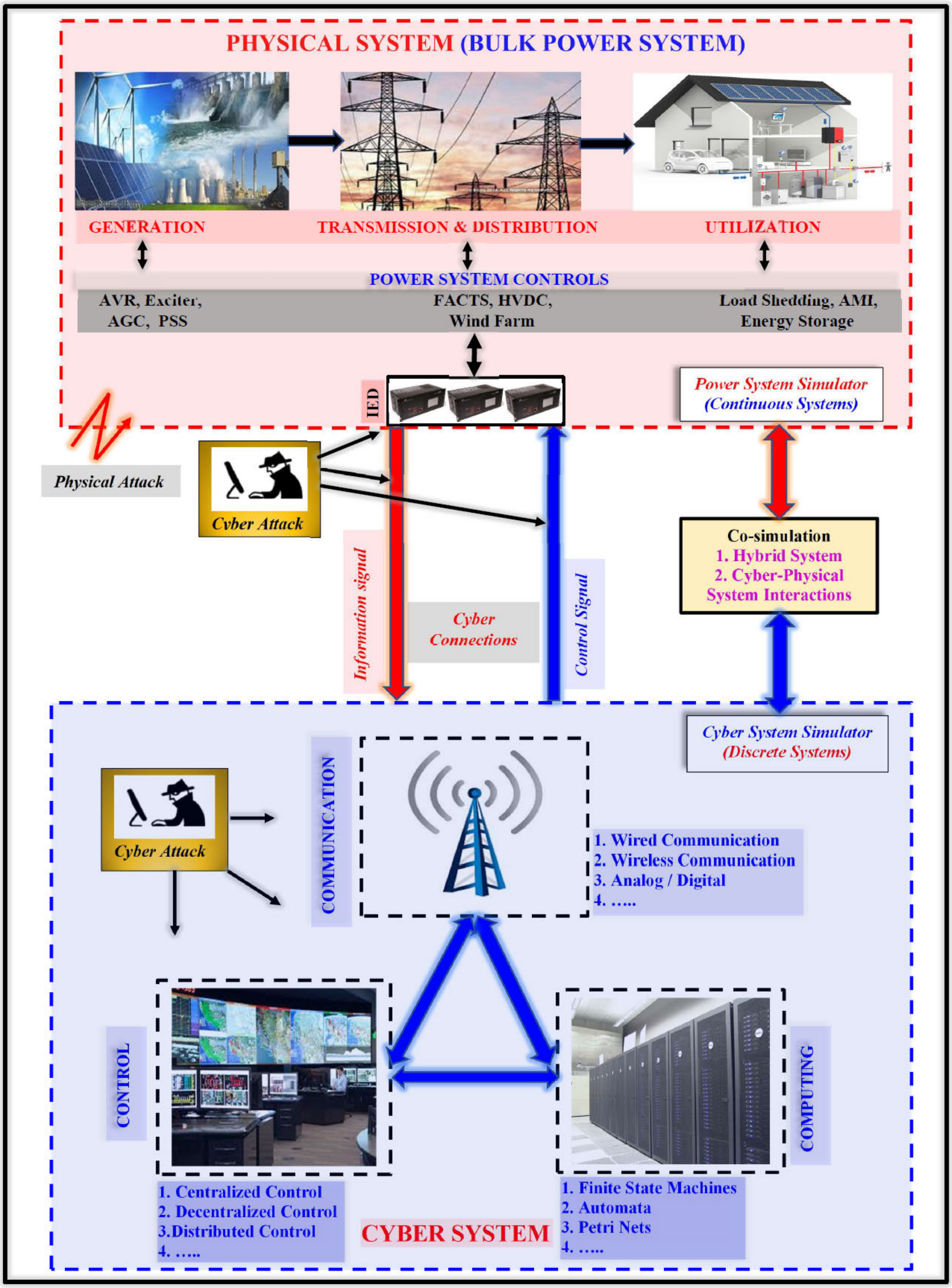

FIGURE 2. Structure of the cyber-physical power system (CPPS).

There are three levels of interactions in the CPPS. The first level of interaction occurs between the generator, transformer, transmission line, and dynamic load, etc. with the power system controller. The power system controller senses the information from the power system core components and calculates the control signal, then fed back to the power system core components for the optimized operations of the power grid.

The effect of delay in transmitting the generator status information to the power system control center on power system stability is investigated in [5], [6]. The evaluation of the impact of the delay on the power system stability by eigenvalue sensitivity and eigenvalue tracing method is presented in [7]. The calculation of the time-delay margin to determine the maximum delay time that the system can sustain without losing its stability is presented in [5], [8].

The compensation of time delay using fuzzy logic based wide-area damping controller method [9], linear matrix inequalities & Lyapunov stability method [10], and Lyapunov based time-varying multiple delayed systems methods are presented in [11]. The modelling of different types of time delays in a wide-area closed-loop control system is presented in [12]. The time-delayed power system stability analysis by integral quadratic constraints method [13], multiple time-delayed signals methods [14], and realistic delay modelling method [15] are investigated.

The second level of interaction occurs between the power system control and the communication infrastructure. The communication infrastructure acts as a backbone that coordinates all the functions of the subsystems (sensor, actuators, interfaces, control, computing, and communication units) in CPPS. The communication effects like data loss, bad data, time-delay, etc., severely impacts the performance of the CPPS. The authors in [16], [17] demonstrated the impact of time-varying communication delay on the stability of the practical large-scale CPPS in the transmission domain. The impact of asynchronous communication delays between the distributed phasor data concentrators for oscillation monitoring application of a wide-area power system is investigated in [18]. The impact of coordinated physical and cyber uncertainties (communication delay and packet dropout) on closed-loop control of a wide-area power system application is presented in [19]. The modelling of different types of delayed CPS for stability analysis and control using Delayed Differential Equation (DDE) method [20], Solution Operator Discretization with Linear Multistep and Implicit Runge-Kutta (SOD-LMS/IRK) method [21], Partial and Explicit Infinitesimal Generator Discretization (PEIGD) method [22], Pseudo-Spectral Discretization of Solution Operator method [23], Time integration-based Discretization of Infinitesimal Generator (IGD) method [24], and the comparison of different types of stability analysis method for the delayed cyber-physical system is investigated in [25].

The third level of interaction occurs between the communication infrastructure and the cyber system. The components of cyber systems are master and slave system, master server, communication server, bidirectional communication structure, high-performance computing stations, intelligent control application software, cyber-attack security and defence mechanisms, etc. The primary function of the cyber system is to perform the advanced operations in the power grid like load forecasting, state estimation, var optimization, voltage control, oscillation monitoring, wide-area monitoring & control, operations planning, model validation, stability analysis, etc. As the size of the power grid networks is growing day by day to meet the load demand, the size of the cyber system also growing in the same manner, and no longer will it be a conventional electric power system. Due to this, CPPS is becoming a complex system with strong interactions between physical and cyber systems with the deployment of a huge number of Intelligent Electronic Devices (IEDs) in the electric power grid. The secure operation of the power grid does not only depend on power flow in the physical system but also depends on information flow in the cyber system, i.e., Information and Communication Technology (ICT). Even though the cyber system ensures efficient, safe, and secure operation for the power grid, the power blackouts occurred in the power grid history is mainly due to the failure of the cyber system.

The main drawback of CPPS is the cyber-attack and cybersecurity problem. The CPPS is a big heterogeneous networked transmission and distribution system with a huge load that has a chance of entering of a cyber-attack. The components of the cyber systems are severely vulnerable to external cyber threats and cyber-attacks through cyber connections due to the flaw in cybersecurity features. Since the cyber-attack does not damage the physical power system directly, but once coordinated with a physical attack, it creates the same impact as physical damage and leads to system instability. Therefore, it is necessary to review the various cyber-attacks and cybersecurity measures in CPPS.

Researchers around the world have conducted various research on CPPS from different perspectives [26]–[28]. The main characteristic of CPPS are the strong interdependency between the cyber and physical systems. The authors have investigated the impacts of various cyber contingency on a physical system using the model-based method [29]–[31]. With the development of synchrophasor technology for wide-area monitoring and control of CPPS, the cyberattacks are increasing nowadays [32]–[34]. The authors did extensive research on the analysis of different types of cyber-attacks like denial-of-service attack, false data injection attack, and man-in-the-middle attack in CPPS and shown the jeopardize of stability [35]–[37]. To protect the complex power grid control networks of CPPS, it is necessary to perform the risk and vulnerability assessment under cyber-attacks [38]–[40]. The various methods of risk [41]–[44] and vulnerability assessment [45]–[48] from the component level to system-wide impacts, with cyber model assessment and physical model assessment, are performed. Substantial work on cyber-attack detection and mitigation for CPPS by monitoring the network traffic of the Supervisory Control and Data Acquisition (SCADA)/Phasor Measurement Unit (PMU) system in the power system control centre was performed in [49]–[52].

It forms the overall cybersecurity feature for the CPPS, which is entirely different from the traditional information security with advanced data analytics and machine learning algorithms. It can able to distinguish the normal and attack activities in the cyber systems. The research interest of designing Wide-Area Damping Controller (WADC) for damping inter-area oscillations in the large-scale CPPS considering the cyber-attack on the physical power system is increased nowadays [53]–[55]. The cyber-physical attack resilient Wide-Area Control (WAC) technique aims to enhance the stability of CPPS at an earlier stage before the system reaches the blackout condition [56], [57]. It is designed to be adaptive to the continuous expansion of the modern CPPS considering the cyber contingencies on the physical power system with its high dimensionality and complex interconnection structure.

Nowadays, more researchers working in the field of CPPS, especially to analyze the stability of CPPS in the control system point of view. It is necessary to analyze the electric power grid as a whole cyber-physical social system, i.e., integrated physical and cyber (control, communication, and computing) part with cybersecurity features. The traditional method of modelling, simulation, and analysis of electric power system operation is entirely based on the physical part of the power grid. This no longer supports the future CPPS research and development. Also, it is difficult to assess the impact of cyber contingency on physical power systems for the safe operation of CPPS. The integration and the unification of cyber and physical systems are needed to optimize the configuration of the cyber side for ensuring the safe and secure operation of the electric power grid. In recent years it is difficult to see the literature survey on different types of modelling, simulation, and analysis methods with cybersecurity applications for CPPS. Therefore, it is necessary to review the different types of modelling, simulation, and analysis methods available for reflecting the characteristics of cyber and physical systems in CPPS. In this review paper, different types of cyber and physical system integrated modelling methods, and simulation software packages are presented. The different types of cyber-attacks and cybersecurity measures for CPPS also reviewed. The status of CPPS in the developed countries and research directions & recommendations in CPPS are finally presented. Fig. 3 shows the structure of this survey.

The remainder of this paper is organized as follows: The different types of modelling methods that cover the physical and cyber part of CPPS are presented in Section II. Section III presents the different types of software used for the modelling and simulation of CPPS. Section IV discusses the different types of cyber-attacks and cybersecurity measures for CPPS. The status of the CPPS in the developed countries is presented in Section V. Section VI gives the outlook of future CPPS. Section VII discusses the current issues and research directions. Finally, the conclusion is given in Section VIII.

II. MODELLING OF CPPS

The main characteristics of CPPS modelling are the tight interaction between the physical and cyber systems at different time, space, and scales. The physical system is dynamic that consists of a generator, transformer, transmission line, load, etc. are physically connected with energy flow. In contrast, the cyber system is a static system that consists of cyber components connected through a communication network with information flow. The complex interaction between the physical and cyber system in CPPS act as a critical point of failure with both the systems are in different topologies. In the large-scale CPPS, the failure of one system leads to catastrophic cascading failure in the overall system. The performance of the one system heavily depends upon another system, i.e., interdependent nature of cyber and physical systems. The comparison between the characteristics of the cyber system and the physical system is shown in Table 1.

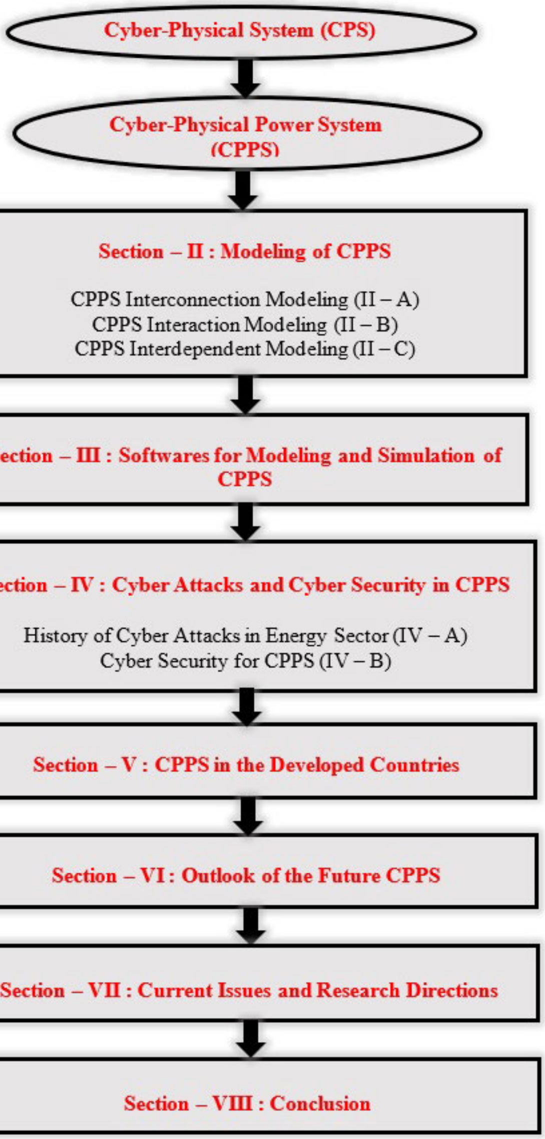
Cyber-Physical System (CPS)
Cyber-Physical Power System (CPPS)
Section – II : Modeling of CPPS
CPPS Interconnection Modeling (II – A)
CPPS Interaction Modeling (II – B)
CPPS Interdependent Modeling (II – C)
Section – III : Softwares for Modeling and Simulation of CPPS
Section – IV : Cyber Attacks and Cyber Security in CPPS
History of Cyber Attacks in Energy Sector (IV – A)
Cyber Security for CPPS (IV – B)
Section – V : CPPS in the Developed Countries
Section – VI : Outlook of the Future CPPS
Section – VII : Current Issues and Research Directions
Section – VIII : Conclusion

FIGURE 3. **Structure of the survey in CPPS.**

Both physical and cyber system has its uncertainties independently. The integration of renewable energy into the physical system, which is stochastic in nature, affects the steady-state operating condition of the power flow in the system. In cyber systems, the cyber-attacks on control, computing, and communication functions alter the information flow. These uncertainties are unpredictable, which increases the risk of safe and secure operation of the power system. The interaction characteristics of the physical and cyber systems complicate the modelling of CPPS. Therefore, it is necessary to develop the modelling framework for a critical understanding of complexity and interdependency in CPPS and analyze in terms of both qualitative and quantitative

TABLE 1. Characteristics of physical and cyber system in CPPS.

S. No	Characteristics	Physical System	Cyber System
1.	Components	Generator, Transformer, Transmission Line, Circuit Breaker, Protective Relay, Load, etc.	Control Systems, Computing Devices, Communication Networks
2.	Nature of System	Continuous, Dynamic behaviour	Discrete, Static behaviour
3.	Modelling	Differential-Algebraic Equations	Difference Equations
4.	System State	Energy Flow	Information Flow
5.	Branch Model	Power Grid Model – Energy Generation, Energy Transmission and Energy Distribution	Information Flow Oriented Model – Data Transmission, Data Processing, and Data Pool
6.	Condition	Generation and Load Balance, Power Transmission Limits	Interdependent operation balance among Control, Computing, and Communication functions
7.	Contingency	Physical Contingency.	Cyber Contingency
8.	Types of Contingency	Line Fault, Generator Outage, Load Outage, Environmental effects, etc.	Cyber Attacks, Communication Latency, Malicious Control effects, etc.
9.	Stability & Security	Power System Stability & Power System Security	Networked Control System Stability & Cyber Security
10.	Event Synchronization	Asynchronous	Synchronous

approaches between physical and cyber systems. This will help to prevent the spreading of catastrophic cascading failure events in a networked CPPS.

The modelling of CPPS is broadly classified into three categories.

(A) CPPS Interconnection Modelling (the act of physical and cyber system in a distinct manner)

(B) CPPS Interaction Modelling (effect of physical and cyber systems has on each other)

(C) CPPS Interdependent Modelling (degree of physical and cyber systems depends on each other)

A. CPPS INTERCONNECTION MODELLING (THE ACT OF PHYSICAL AND CYBER SYSTEM IN A DISTINCT MANNER)

In this modelling, the CPPS is modelled by the interconnection of a physical system, cyber system, and the system need to interconnect them. The physical system consists of physical components of the power system needs to be monitored and controlled. The cyber system consists of a computational algorithm that involves a control or communication algorithm. The systems need to interconnect the physical and cyber systems are Analog to Digital Converter (ADC), Digital to Analog Converter (DAC), and Digital Networks. The hybrid dynamical system theory is used to model the CPPS, which consists of differential equations to represent the continuous-time behaviour of the physical system and difference equations to represent the discrete behaviour of cyber systems, converters, and digital networks [58]. It captures the mixed behaviour of continuous, discrete systems & their interconnections in CPPS.

1) PHYSICAL COMPONENTS MODELLING

The physical system is a continuous-time system modelled by a differential equation with a time parameter t that parameterizes the variables of the system, i.e., the state of the system [58]–[60]. The mathematical equation of the physical system is given in equation (1) and (2). Let z represents the state of the physical system with $\mathbb{R}^{n_P}$ as the Euclidean space for state space, $u \in \mathbb{R}^{m_P}$ represents the input signal for the physical system, $y \in \mathbb{R}^{r_P}$ represents the output of the physical system defined by the output function h.

$$y = h\,(z, u)\,, \quad \dot{z} \in F_P\,(z, u) \tag{1}$$

$$(z, u) \in C_P \subset \mathbb{R}^{n_P} \times \mathbb{R}^{m_P} \tag{2}$$

In specific applications, it is necessary to limit the values of state and input to the physical system. In that case, the values are constrained to the set C_P.

2) CYBER COMPONENTS MODELLING

The function of cyber components is to executing the algorithms, perform the computations, and transmitting the data over the digital networks. The state variables of the cyber components are discrete values that are updated at the discrete events taken from the discrete sets rather than from a continuum [58], [61], [62]. The mathematical equation of the cyber system is given in equation (3) and (4). Let $\eta \in \Upsilon$ represents the state of the cyber system with $\mathbb{R}^{n_C}$ as the Euclidean space for the state space, $\nu \in V \subset \mathbb{R}^{m_C}$ represents the input signal for the cyber system, $\zeta \in \mathbb{R}^{r_C}$ represents the output of the cyber system defined by the output function K, which is the function of the input and the state (ν, η).

$$\eta^{+} \in G_C\,(\eta, \nu)\,, \quad \zeta = K(\eta, \nu) \tag{3}$$

$$(\eta, \nu) \in D_C \subset \Upsilon \times \nu \tag{4}$$

In specific applications, it is necessary to limit the values of state and input to the cyber system. In that case, the values are constrained to the set D_C. The mathematical modelling of the cyber components in the cyber system is as follows.

a: PURE FINITE STATE MACHINES

The Finite State Machine (FSM) is a computational model that expresses the relationship between input and state of the system. It is used to represent the control execution flow (or) simulation of a sequential logic in many applications. At every value of the input, the state and output of the FSM are updated. The states, inputs, and outputs of the FSM taking the values from the discrete sets and updated at discrete transitions when triggered by its inputs. Let ν denotes the inputs take the value from the set Σ, q denotes the states take the value from the set Q, r denotes the outputs takes the value from the set Δ, and q_0 denotes the initial value of the state of FSM. The output function is given by $K : Q \to \Delta$ and the transition function is given by $\delta : Q \times \Sigma \to Q$.

When the input $\nu \in \Sigma$ is applied to the FSM, a transition occurs from the initial state $q_0 \in Q$ of the FSM to a new state by $q_1 = \delta(q_0, \nu)$. The FSM output is updated to $k\,(q_1)$ after the transition and this transition mechanism in FSM is represented mathematically by the difference equation in equation (5).

$$q^{+} = \delta\,(q, \nu) \quad \zeta = K\,(q)\,(q, \nu) \in Q \times \Sigma \tag{5}$$

This model is similar to the cyber components model given in equation (3) and (4) with $\Upsilon = Q, G_C = \delta, \eta = q, \nu = \Sigma, D_C = \Upsilon \times \nu$.

b: FSM WITH CONDITIONAL STRUCTURES AS GUARDS

In certain applications, the transition occurs in FSM based on the conditional structure, for instance, the transition is triggered in the FSM when the input $\nu < 0$. The conditional structure is a Boolean expression; if its evaluation gives *true* condition, the transition is enabled, and if it was *false* it would be aborted. The mathematical modelling of FSM with transition according to the conditional structure is defined by, let the function $\ell Q \times \Sigma \times \Delta \to R$ be the testing function for the transition condition for each state $q \in Q$. Assume that the conditional structure $\ell\,(q, \nu, \zeta)$ designed to satisfy for the value of less than or equal to zero as given in equation (6) otherwise not satisfied. The transition triggered in FSM based on the conditional structure (ℓ) model is given by

$$q^{+} = \delta\,(q, \nu)\,,\ \zeta = K\,(q)\,,\ \ell\,(q, \nu, \zeta) \leq 0,\ \ (q, \nu) \in Q \times \Sigma \tag{6}$$

This model is similar to the cyber components model in equation (3) and (4) with $\Upsilon = Q, G_C = \delta, \eta = q, \nu = \Sigma, D_C = \{(q, \nu) \in Q \times \nu : l\,(q, \nu, K\,(q)) \leq 0\}$.

c: MODELLING OF COMPUTER COMPUTATIONS AND DISCRETE-TIME ALGORITHMS

There are two types of computations, one-shot computation, and iterative computation. The computation model is represented in a discrete-time system with ν as the input of the model, and the output of the computation model is ζ. The mathematical model of the one-shot computation is given by

$$\zeta = \tilde{K}\,(\nu) \tag{7}$$

where the function $\tilde{K}$ represents the modelling of the computation being performed. This model is similar to the cyber components model in equation (3) and (4), with $\eta = \emptyset, \Upsilon = \emptyset, \nu = \Sigma, D_C = \nu, G_C = \emptyset, K = \tilde{K}$. The iterative computation technique requires a number of steps to perform the computation. It is defined as a discrete-time system with additional variables as $m \in \mathbb{R}^{n_c-1}$ and the counter as $k \in \{0, 1, 2, \ldots k^*\}, k^* \in \{0, 1, 2, \ldots\} =: \mathbb{N}$ that performs k^* iterations to produce the final outcome of the computations. Denoting $\eta = [m^T K]^T$ as the state of the computation model, ν as the input signal and $\tilde{K}$ as the function performing the iterative computation, the computational model is given by

$$\eta^{+} = \begin{bmatrix} \tilde{K}(m, k, \nu) \\ k+1 \end{bmatrix}, \quad \zeta = m,\ m \in \mathbb{R}^{n_C-1}, \\ k \in \left\{0, 1, 2, \ldots, k^* - 1\right\}, \nu \in V \tag{8}$$

The model represented in the eqn (8) is similar to the cyber components model in equation (3) and (4) with $\eta = \begin{bmatrix} m \\ k \end{bmatrix}, \Upsilon = \mathbb{R}^{n_C-1} \times \{0, 1, 2, \ldots, K^*\}, \nu = \Sigma, G_C = \begin{bmatrix} \tilde{K}(m, k, \nu) \\ k+1 \end{bmatrix}$ and $K\,(\eta) = m \forall \eta \in \Upsilon, D_C = \mathbb{R}^{n_C-1} \times \{0, 1, 2, \ldots, K^* - 1\}$. The difference equations are used to model the discrete-time algorithms. The discrete-time feedback controller can be designed by discretizing the continuous-time controller designed by the continuous-time system design tools or designing the discrete-time feedback controller directly. The discrete-time algorithm can be written as

$$\eta^{+} = G_C\,(\eta, \nu)\,\zeta = K\,(\eta) \tag{9}$$

where G_C is obtained by discretizing the continuous-time control algorithm.

3) MODELLING OF THE INTERFACE SYSTEM BETWEEN CYBER AND PHYSICAL COMPONENTS

The model represents the behaviour of the cyber and physical system has different dynamics: the cyber system has discrete dynamics while the physical system has a continuous dynamic. The interfaces are used to interconnect the cyber and physical systems and convert the signals appropriately [58], [63], [64]. The mathematical model of the interfaces used to interconnect the cyber and physical system, and finally, the cyber system, physical system, and interfaces are interconnected to define the complete model of CPS.

a: ANALOG TO DIGITAL CONVERTER (ADC)

ADC is a sampling device or sensor which provides the information measured from the physical system to the cyber system. The main function of ADC is to sample the output (y) of the physical system at a sampling rate of T_s^* then the samples are sent to the embedded computer in the cyber system. The model of ADC has two states, sample state and timer state. If the timer attains the sampling time of T_s^* the timer is reset to zero, and the sampler state is updated with the recent output from the physical system. The mathematical model of the sampling device is given in equation (10) and (11)

$$\dot{\tau}_s = 1,\ \dot{m}_s = 0 \quad when\ \tau_s \in [0, T_s^*] \tag{10}$$

$$\tau_s^+ = 0,\ m_s^+ = v_s \quad when\ \tau_s \geq T_s^* \tag{11}$$

where $\tau_s \in \mathbb{R}_{\geq 0}$ denotes the timer state, $m_s \in \mathbb{R}^{rp}$ denotes the sample state, and $v_s \in \mathbb{R}^{rp}$ denotes the input of the sampling device. In the practical ADC, a time delay exists between the triggering of ADC to sample its input and update its output called ADC acquisition time. This time delay reduces the number of samples per second to be sampled by the ADC. In addition to this, the digital output value of ADC is stored in a sample state finite length digital words, which causes the quantization effect. This model omits the quantization effects and ADC acquisition time, but these can be included in the model if needed.

b: DIGITAL TO ANALOG CONVERTER (DAC)

The DAC converts the digital signal into an analog signal for their use in the physical system. The Zero-Order Hold (ZOH) model is a commonly used model for the DAC, which updates its output at discrete instants of time periodically and held constant in between the updates until the new information is available at the next sampling time. The mathematical modelling of the DAC as ZOH is given in the equation (12) and (13), which is similar to the equation (10) and (11).

$$\dot{\tau}_h = 1,\ \dot{m}_h = 0 \quad when\ \tau_h \in [0, T_h^*] \tag{12}$$

$$\tau_h^+ = 0,\ m_h^+ = v_h \quad when\ \tau_h \geq T_h^* \tag{13}$$

Let $\tau_h \in \mathbb{R}_{\geq 0}$ be the timer state, $m_h \in \mathbb{R}^{rc}$ be the sample state, and $v_h \in \mathbb{R}^{rc}$ be the inputs of the DAC. The operation of DAC is as follows: if $\tau_h \geq T_h^*$, the state of the timer is reset to zero, and the sample state is updated with the new input v_h(output of the embedded computer in the cyber system).

c: DIGITAL NETWORKS

The transfer of information between the cyber and physical systems (or) between the subsystems of a cyber system occurs over a digital network. It bridges all the subsystems and components and transmits the sampled information at discrete-time instants. If the triggering condition is satisfied, the information provided at its input is transmitted over the digital network and stores that information until the new information arrives. Let assume the information was transformed over the digital communication network at the time instants $\{t_i\}_{i=1}^{i^*}, i^* \in \mathbb{N} \cup \{\infty\}$, satisfying $T_N^{*min} \leq t_{i+1} - t_i \leq T_N^{*max} \forall i \in \{1, 2, \ldots .i^* - 1\}$, where T_N^{*min} and T_N^{*max} are constants satisfying $T_N^{*min}, T_N^{*max} \in [0, \infty]$ and $T_N^{*min} \leq T_N^{*max}$, i^* denotes the number of transmission events, T_N^{*min} denotes the minimum possible time in between the transmission events, T_N^{*max} denotes the maximum amount of time elapsed between the transmission events. If the digital network transmits the data at a high rate, then T_N^{*min} is small, otherwise T_N^{*min} is large for a slow data rate transmission network. The T_N^{*max} denotes the maximum delay time in transmitting the data in a digital network.

The mathematical model of the digital network is given in equation (14) and (15).

$$\dot{\tau_N} = 1,\ \dot{m_N} = 0 \ when\ \ \tau_N \in [0, T_N^{*max}] \tag{14}$$

$$\tau_N^+ \in \left[T_N^{*min}, T_N^{*max}\right], \quad m_N^+ = v_N \ when\ \ \tau_N \leq 0 \tag{15}$$

At every t_i, the information v_N available at the input side of the communication link is transferred over the digital network. The internal variable m_N is updated for each transmission event and keeps the information at the output of the network and remains constant between the communication events. The internal variable m_N not only maintains the recently transmitted information but also previously transmitted information. This digital network is an interface between a cyber and physical system that interconnects the continuous and discrete dynamics. The model of the digital network is represented by the combination of both difference and differential equations by hybrid inclusions method. This is usually employed in CPS for modelling the digital network as given in equation (16)-(18)

$$\dot{\lambda} \in F_I(\lambda, w) \quad when \quad (\lambda, w) \in C_I \tag{16}$$

$$\lambda^+ \in G_I(\lambda, w) \quad when \quad (\lambda, w) \in D_I \tag{17}$$

$$\psi = \varphi(\lambda) \tag{18}$$

where λ denotes the state, w denotes the input signal, ψ denotes the output, F_I denotes the continuous dynamics on C_I, and G_I denotes the discrete dynamics on D_I of the digital interface.

4) COMBINING MODELS OF CYBER AND PHYSICAL COMPONENTS

The complete mathematical modelling of the CPS is obtained by the interconnection of the models of individual cyber and physical components with interfaces [58], [65], [66]. Fig. 4 shows the feedback interconnection modelling of CPS.

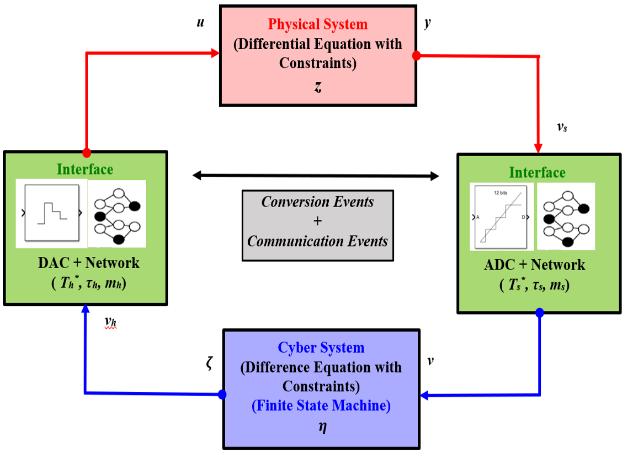

FIGURE 4. CPPS interconnection modelling.

The individual models of the CPS are interconnected to obtain the complete mathematical model of CPS, which combines the continuous and discrete dynamics through combinations of differential and difference equation form or hybrid inclusion form.

B. CPPS INTERACTION MODELLING (EFFECT OF PHYSICAL AND CYBER SYSTEMS HAS ON EACH OTHER)

The interaction between cyber and physical systems plays a significant role in the efficient control of CPPS. In the past research works, the assumptions about the interactions phenomena in CPPS are left implicitly or unspecified in the system design. This leads to catastrophic failure in the safety-critical systems like CPPS. It is necessary to explicitly specify the assumptions of interactions and integrate the interaction model with the design of CPPS to ensure the safety of the system. In this section, the different types of CPPS interaction model are presented. From the literature review, the CPPS interaction model is broadly classified into four types, as shown in Fig. 6. They are i) Graphical Model ii) Mechanism Model iii) Probabilistic model and iv) Simulation Model.

1) GRAPHICAL MODEL

The graphical model gives the visualization-based relationship between the physical and cyber systems. It helps to construct the structure of the electric power grid and supports to analyze the operation of the power grid from the various attacks. The following section gives the different types of graphical modelling methods, quantitative analysis of variables involved in each model, and theories of individual models with graphical illustration are presented as follows.

a: GRAPH THEORY-BASED MODEL

In CPPS, the electrical power system components like generator, circuit breaker, protective relay, and loads are connected through transmission lines, whereas the cyber system consists of cyber components are connected through the communication networks. In order to monitor and control CPPS, it is assumed that each component in the physical system is integrated with the cyber node. It transmits the component state information to the remote-control centre through routers and switches, as shown in Fig. 5. Once the information is received in the control centre, the information is processed, and the control signal is generated then sent through the routers to the control devices like Flexible AC Transmission System (FACTS) devices, etc.

Given that the one-on-one relationship between the physical system and the cyber system, the failure of the physical or cyber systems affects other systems or vice versa. The graph theory-based method would be the best method to study the internal relations between the physical and cyber systems in CPPS. A graph consists of a set of vertices (V) and edges (E). Based on the principle of graph theory technique the physical components are considered as vertices V_p and the transmission line connecting the physical components are considered as an edges E_p which form the directed sparsely connected graph, $G_p = (V_p, E_p)$ [67]–[69]. Similarly, the cyber components like routers, servers, computing clusters in cyber systems are considered as vertices V_c and the wireless/wired communication between the cyber components is considered as an edges E_c which form the directed sparsely connected graph $G_c = (V_c, E_c)$ [70], [71]. Fig. 7 represents the example of graph theory-based modelling of CPPS. The vertices are energy storage devices, while the edges represent the energy flow (power flow) between the two vertices.

The edges are represented as a directional arrow to indicate the positive power flow as P_i^{in} for $i \in \{1, 2\}$ from the head vertex V_j^{head} to the tail vertex V_j^{tail}. The $V^s \in R^{N_s}$ and $V^t \in R^{N_t}$ denotes the source and sink vertices, respectively [72]. In the cyber system, the vertices are data nodes, while the edges represent the information flow between the two vertices [26]. The edges are represented as a directional arrow to indicate the information flow as I_i^{in} for $i \in \{1, 2\}$, as shown in Fig. 7. The power system contingency like transmission line outage is represented by the removal of edges in the graph G_p whereas the removal of the vertex V_c represents the failure of the cyber node from the graph G_c. The graphical model of a CPPS is represented as a directed topology graph. The physical and cyber system state variables are considered as a "data node," and the information flow between the physical and cyber system is considered as an "information edge." The graph theory model is integrated with the dynamic system theory model to analyse the effect of cyber disturbances on the power system components [73].

b: FINITE STATE MACHINE (FSM) MODEL

FSM or Finite State Automata, or simply called as a State Machine, is a mathematical model of the computation. The FSM found in many applications that perform the predetermined sequence of actions based on the sequence of the events presented to the FSM. It is at any one of the states from the list of a finite number of states at any given time. It changes from one state to another state when triggered by the inputs: the change of one state to another state is called state transition. There are two types of FSM: Deterministic FSM (DFSM) and Non-Deterministic FSM (NDFSM) [74]. A five-element tuple represents a deterministic FSM:

$$(Q, \Sigma, \delta, q_0, F) \tag{19}$$

where Q represents the finite set of states, Σ is a finite non-empty input, δ is a series of transition functions, q_0 represents the initial state, and F is the set of accepting (final) states. There must be one transition for each state when the input is given from the set Σ. The DFSM is represented in Fig. 8.

Similar to DFSM, the NDFSM is represented by an above five-element tuple. Unlike DFSM, NDFSM has multiple transitions for each state for input from the set Σ. Additionally, NDFSM has a null transition represented by ε, which allows the machine to transition from one state to another state without reading the input from the set Σ. The NDFSM is shown in Fig. 9.

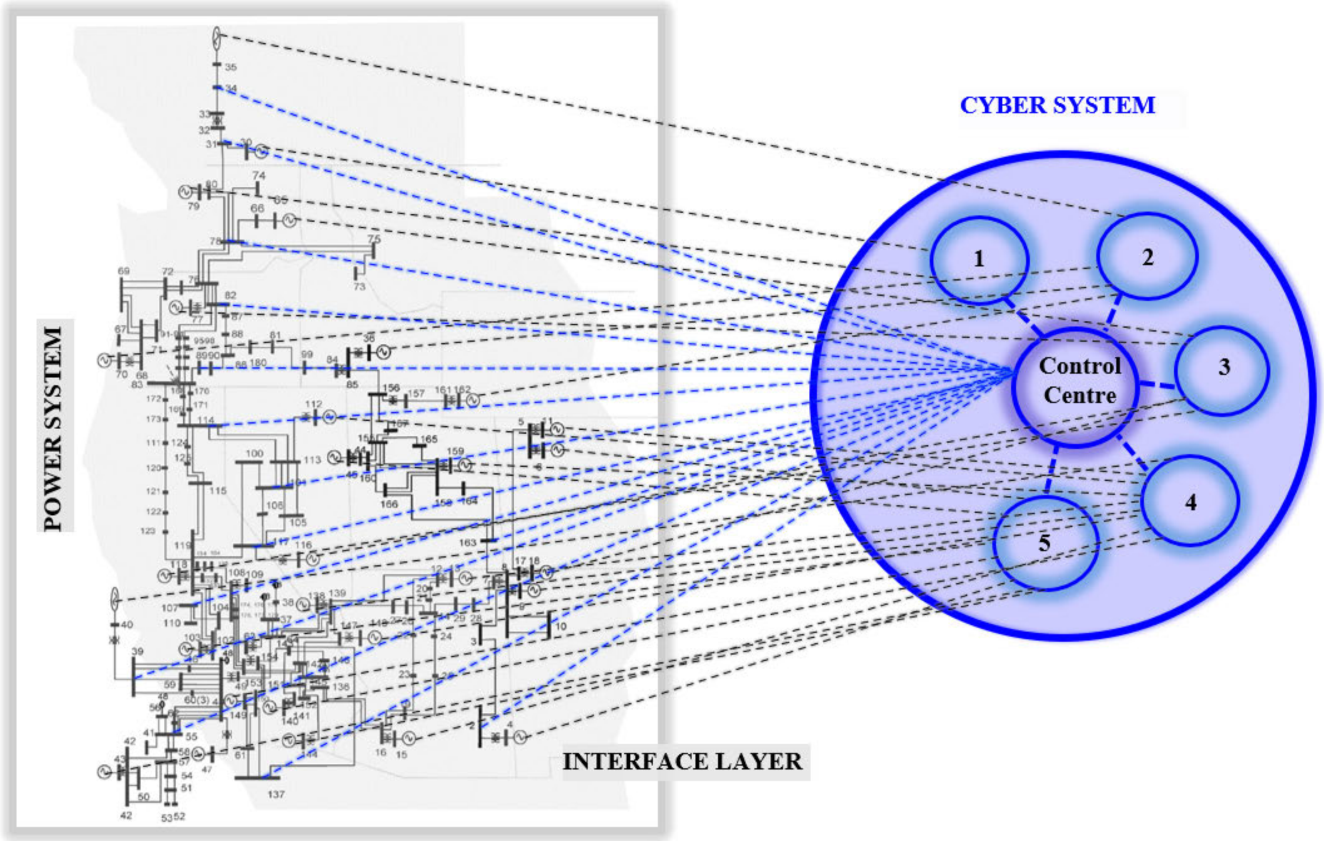

FIGURE 5. Interaction mechanism in CPPS.

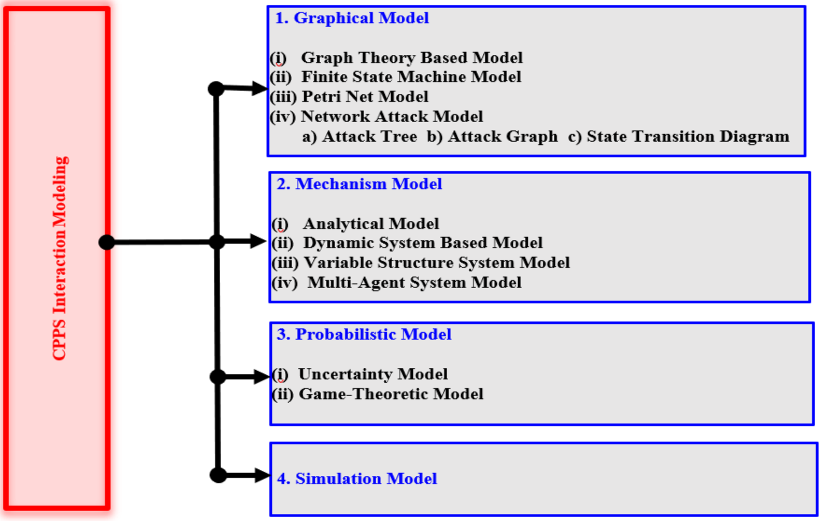
CPPS Interaction Modeling
1. Graphical Model
(i) Graph Theory Based Model
(ii) Finite State Machine Model
(iii) Petri Net Model
(iv) Network Attack Model
a) Attack Tree b) Attack Graph c) State Transition Diagram
2. Mechanism Model
(i) Analytical Model
(ii) Dynamic System Based Model
(iii) Variable Structure System Model
(iv) Multi-Agent System Model
3. Probabilistic Model
(i) Uncertainty Model
(ii) Game-Theoretic Model
4. Simulation Model

FIGURE 6. Classification of CPPS interaction modelling.

In the CPPS, the state transition occurs in both physical and cyber systems for different events under different conditions [75], [76]. The FSM generates the State Chart Diagram (SCD) for cyber and physical systems, which represents the dynamic behaviour of the system through state transitions throughout its life cycle. SCD is used to make the power system operation process clear and visible and analyze the critical interactions in CPPS qualitatively. In [49], the usual sequential order of the control commands is modelled as $\{t_i, t_{i+1}\}$ where $\{t_1, t_2, \ldots t_n\}$ are the defined set of transitions.

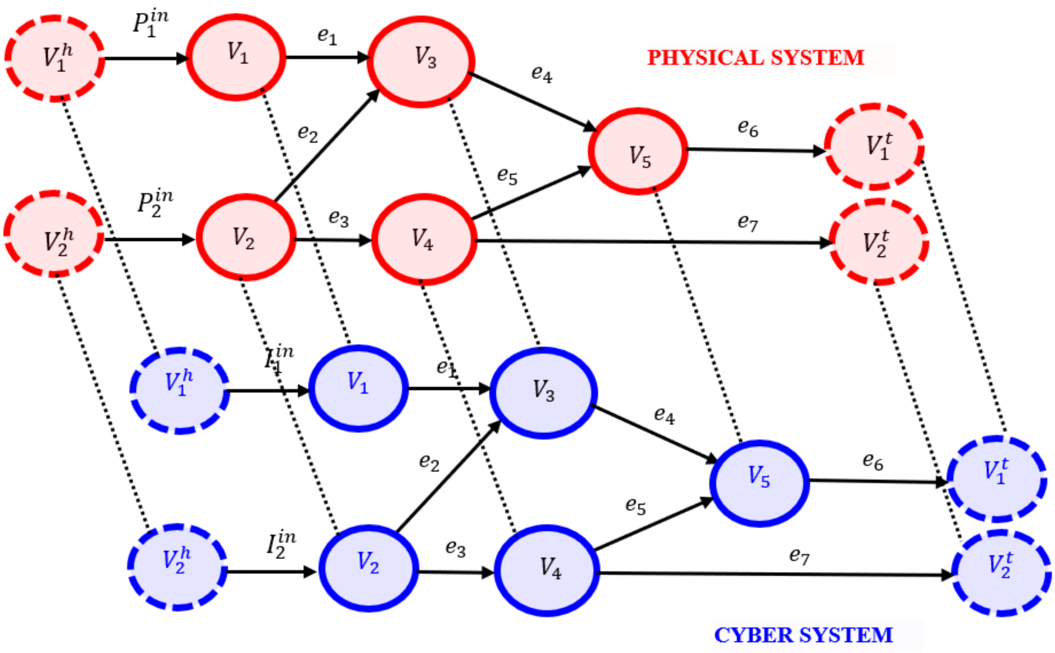

FIGURE 7. Graph theory-based modelling of CPPS.

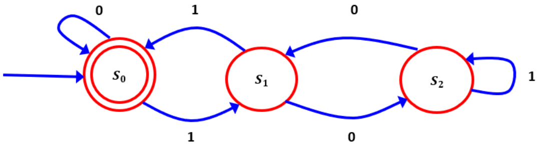

FIGURE 8. Deterministic FSM.

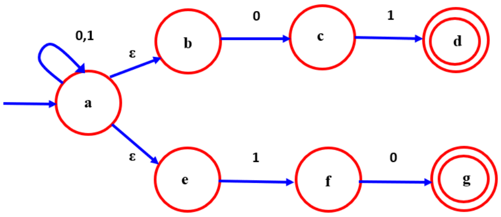

FIGURE 9. Non-deterministic FSM.

The false sequential logic attack on the SCADA system changes the control commands as $\{t_{i+1}, t_i\}$. The detailed analysis of how this attack perturbs the behaviour of the physical system can be obtained by SCD. In [39], the FSM is used to enhance the performance of the aircraft electrical distribution system by reconfiguring the control strategy under different operating conditions and fault scenarios [77]. The advanced features of FSM modelling of CPPS are flexible to model the interactions, easy to move from abstract to code execution, low processor overhead, and easy determination of reachability of a state.

c: PETRI NET MODEL

The Petri net is a mathematical modelling language for the distributed and parallel system to describe the state changes and transitions that occur in the system. It is a class of discrete-event dynamic system which represents the relationship between events, conditions, and its control behaviour in a large-scale system. The Petri net model is the best suitable language tool to study the interaction phenomena between the continuous nature of the physical system and the discrete nature of the cyber system in CPPS [78], [79]. Petri net is a graph-based model to illustrate the control behaviour of CPPS exhibiting the asynchronous, concurrency, and distributed event characteristics in their operation. The FSM can be converted into the Petri net model and vice versa to investigate the cascading failure in the system [80]. The Petri net model consists of four fundamental components, such as place, transition, arc, and token, as shown in Fig. 10.

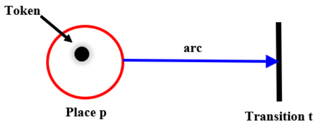

FIGURE 10. Basic petri net components.

The place is represented graphically as a circle, transitions as a bar, arcs are directed line segments, and tokens as dots. The places (P) are used to represent the components and their state in CPPS. The transitions (T) consisting of input functions (I) and Output functions (O) are used to describe the discrete events in CPPS that may result in different states. The arcs denote the relationship that exists between the places and transitions. Finally, the tokens are used to define the active state of the Petri net, which forms the marking of the net (MP).

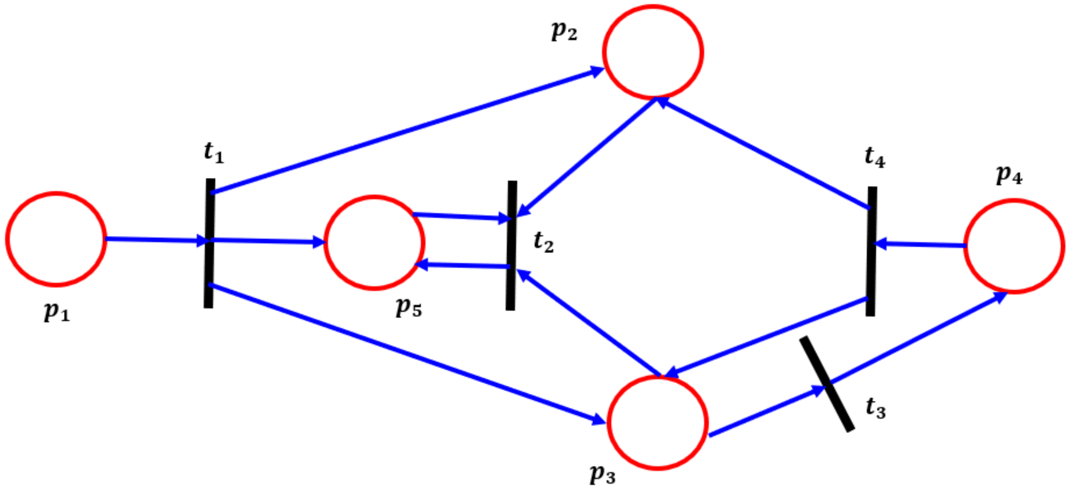

FIGURE 11. Petri net example.

The model of the Petri net can be described by both graphically and using set notations. Using the above notations the Petri net is described as a five-tuple, $M = (P, T, I, O, MP)$, where P represents the set of places, $P = \{p_1, p_2, \ldots p_n\}$, T represents the set of transitions, $T = \{t_1, t_2, \ldots t_m\}$, I represents the input function for all the transitions, $I = \{I_{t1}, I_{t2}, \ldots I_{tm}\}$, O represents the output function for all the transitions, $O = \{O_{t1}, O_{t2}, \ldots O_{tm}\}$, and MP represents the marking of places with tokens. The initial marking of places is referred to as MP_0. Each place has either zero tokens (or) some integer number of tokens. An example Petri net graph is shown in Fig. 11 can be described by the mathematical model using the previous notation as [81]:

$$\left.\begin{aligned}
&M = \{P, T, I, O, MP\}\\
&P = \{p_1, p_2, p_3, p_4, p_5\}\\
&T = \{t_1, t_2, t_3, t_4\}\\
&I(t_1) = \{p_1\}\\
&I(t_2) = \{p_2, p_3, p_5\}\\
&I(t_3) = \{p_3\}\\
&I(t_4) = \{p_4\}\\
&O(t_1) = \{p_2, p_3, p_5\}\\
&O(t_2) = \{p_5\}\\
&O(t_3) = \{p_4\}\\
&O(t_4) = \{p_2, p_3\}\\
&MP = (0, 0, 0, 0, 0)
\end{aligned}\right\} \tag{20}$$

The cyberattack or cyber intrusion in CPPS is a stochastic event rather than a deterministic event. The stochastic event can be modelled by the stochastic Petri net model by introducing the stochastic time-varying delay parameter between enabling and firing conditions of the state transition mechanism [82]. The analysis of the impacts of cyberattacks on CPPS is based on the tokens in the Petri net model, which are indistinguishable. Therefore, coloured Petri net (CPN) model is used to analyse and identify the type of cyberattack on CPPS. In CPN, each token is appended with a data value called a token colour, which describes the data type and its complex operations so that the cyberattacks can be detected by a unique identity in the model [83]. A stochastic CPN model is proposed to analyze the cyberattacks on large-scale CPPS and described the threat propagation process in CPPS quantitatively [84]. In [85], a hierarchical method-based construction of the Petri net model for a large-scale power system is proposed. Many smaller Petri nets are constructed separately for each subsystem through different domain experts.

The Petri net model describing the phenomena of blackout occurred in the U.S. and Canada on August 14, 2003, is shown in Fig. 12. It represents a coordinated cyber-attack occurred initially on units control system (P_1) and finally, the propagation of failure causes the Sammis-star line outage and other transmission line outages in northern Ohio (P_6). The main drawback of the Petri net model is modelling of the large-scale CPPS is very difficult due to an increase in the size of the state-space, and also the computation time increases exponentially with the increase of the system size.

d: NETWORK ATTACK MODEL

In the last decade, the CPPS adopting more advanced ICTs to improve the operating efficiency and reliability of the system. The ICTs are more vulnerable to cyber-attacks launched by malicious insiders or national cyber attackers and therefore cause serious cybersecurity problems in the CPPS. The cyber-attack on CPPS refers to the attack behaviours performing an organized action of tracking the communication network or control commands without permission and exploiting the vulnerability of the system to destroy or limit its function. These cyber-attacks degrade the smart grid performance and leads to system blackouts. Due to the complex interaction characteristics between the physical and cyber systems, the failure of the cyber network creates serious consequences in the physical system. The behaviour of the CPPS may be

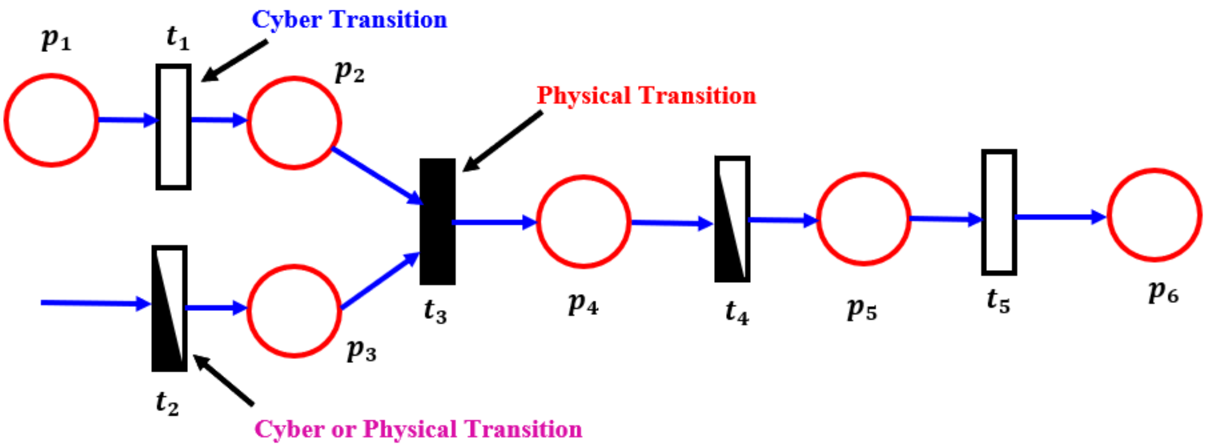

FIGURE 12. Petri net model for hypothetical attacks in blackout example.

changed due to the network attacks and make the system in an unsafe condition that damages the system. Therefore, it is necessary to review the different types of cyber-attack model for CPPS to analyze the impacts of cyber-attacks and its consequences on weakening the CPPS functions such as safety, stability, and economy of the system through modelling and simulation approaches. The cyber-attack model helps to understand and evaluate the resilience of CPPS against cyber-attack. The power system engineers use this model: i) To identify the problem from the level of component and subsystem and respond to the cyber-attack on CPPS in advance ii) To improve the situation awareness and protect the CPPS from the future cyber-attacks iii) To evaluate the security status of a cyber domain of the power grid and iv) To design and develop more resilient CPPS. The following section presents the different types of network attack modelling in CPPS.

2) ATTACK TREE

The attack tree shows all the possible paths for cyberattacks in the power system in a graphical manner. It helps to provide a different way of cyber network intrusion and describes the process of cyber-attack structurally and intuitively [86], [87]. The vulnerability and risk assessment of critical parts of the CPPS can be done by the attack tree method [88], [89]. In [86], the attack tree model was deployed to construct the cyber-physical threat model with respect to the power system contingencies. However, the attack tree method is suitable only for modelling a restricted type of attack and not suitable for modelling simultaneous attacks or coordinated attack scenarios on multiple components. In [90], the attack tree is transformed into the Stochastic Petri Net (SPN) model for the effective capturing of the network attack.

Fig. 13 represents the attack tree for smart grid applications [91]. Level 1 represents the constant power delivery to the customer without any disturbance. Level 2 represents the physical system consequences that lead to the power grid blackout; for instance, changes in reference value of exciter and prime mover into abnormal values. Level 3 represents the cyberattacks on CPPS that lead to physical consequences. By compromising the SCADA and Remote Terminal Unit (RTU), the attacker controls the exciter and prime mover, affecting the power generating system. Finally, level 4 represents the attack technique to perform the attack.

3) ATTACK GRAPH

The attack graph represents the behaviour of an attacker and explores the different ways that the attacker can exploit the system vulnerabilities to attain the desired state. An attack graph consists of a collection of attack scenarios in the computer networks, whereas each scenario represents the sequence of actions performed by an attacker to intrude into the system with a particular goal of service interruption, access to the confidential database, access to the main host, etc. This model utilizes the information of the network topology and calculates the probability of flaw that can be identified by an attacker to implement the intrusion and penetration. The system operator uses the attack graphs to identify the suitable security measures to defend their systems. If the size of the network is increasing, an automatic generation method is applied by the attack graph model to identify the network flaws for modelling of large-scale complex network attack behaviour. The attack graph model is used to perform the security assessment for the power systems control unit [92]. The automatic generation method is combined with an attack graph model to quantitatively evaluate the impact of cascading failures in the CPPS [93]. The Bayesian attack graph model is used to assess the attack procedure and the likelihood of compromise of the cyber components in smart grid systems with the consideration of uncertainty in cyber-attacks [94]. The attack graph model is useful for the operators to analyze the patterns of sequential cyber topological attacks in identifying the critical cyber-attacks thereby cascading outages can be avoided in the CPPS [267].

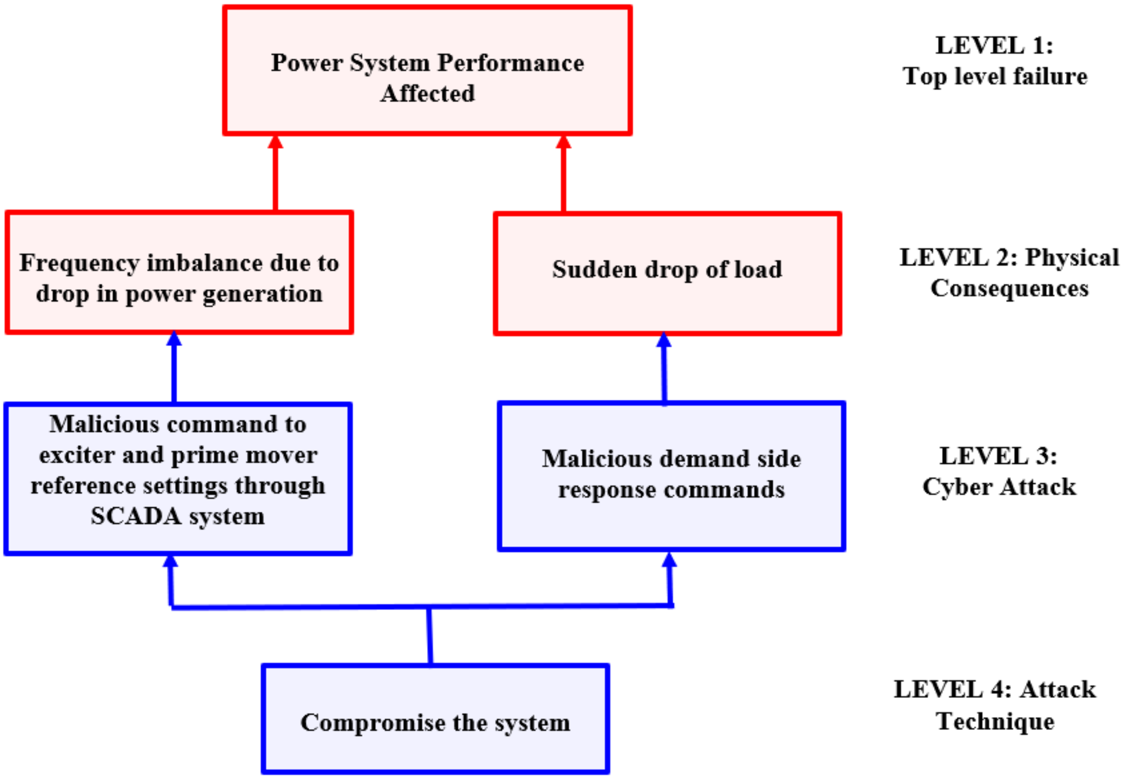
Power System Performance Affected
LEVEL 1: Top level failure
Frequency imbalance due to drop in power generation
Sudden drop of load
LEVEL 2: Physical Consequences
Malicious command to exciter and prime mover reference settings through SCADA system
Malicious demand side response commands
LEVEL 3: Cyber Attack
Compromise the system
LEVEL 4: Attack Technique

FIGURE 13. Attack tree.

The attack graph serves various applications like intrusion detection, security defence, network security, and forensic analysis, etc. Overall, it gives a bird's eye view of every attack scenario in CPPS that can lead to a critical security breach. The advantage of the attack graph is taking into account of local vulnerabilities through the interaction effects and global vulnerabilities through interconnection effects and very much useful for security analysis of power control systems. The calculation of system vulnerabilities based on the connection model of the attack graph is shown in Fig. 14. The connection model of the attack graph includes serial, parallel, and series-parallel complex. Table 2 highlights the main characteristics of different schemes in attack graph modelling for cyber-physical systems, and Table 3 presents the detailed taxonomy of network attack models [98], [114].

The vulnerability function of the state (S) transfer is defined as;

$$P_v(c) = P(C \leq c) = 1 - e^{-\lambda c} \tag{21}$$

where c represents the equivalent cost of attacks, C represents the equivalent cost of attacks after achieving the objective, λ represents the vulnerability factor which expresses the difficult level of a successful attack [92]. The state transfer (cyber-attack) becomes more complicated when λ becomes smaller. If the value of the function $P_v(c)$ becomes bigger, the vulnerability of the target system becomes bigger; therefore, the probability of successful cyber-attacks on CPPS becomes higher. The mathematical model of vulnerabilities is defined as follows:

a) Serial Model

$$\begin{aligned} P_s(c) &= P(C_1 + C_2 + \ldots + C_n \leq c) \\ &= 1 - \sum_{i=1}^{n} \frac{\prod_{\substack{j=1 \\ j\neq i}}^{n} \lambda_j e^{-\lambda_j c}}{\prod_{\substack{j=1 \\ j\neq i}}^{n} (\lambda_j - \lambda_i)} \end{aligned} \tag{22}$$

where $\forall i \neq j \rightarrow \lambda_i \neq \lambda_j, n \geq 2$.

b) Parallel Model

$$\begin{aligned} P_s(c) &= P(min(C_1, C_2, \ldots C_n) \leq c) \\ &= 1 - e^{-\sum_{i=1}^{n} \lambda_i c} \end{aligned} \tag{23}$$

c) Series-Parallel complex model:

Traversing through all the paths from the initial state to the target state, each and every feasible path is a serial model, and the calculation between each feasible path from the initial state to the final state is treated as a parallel model.

4) STATE TRANSITION DIAGRAM

In this model, the behaviour of an attack is modelled as a Markov decision process (model checking prediction method) similar to the methods based on attack graphs. In the Markov process, the states are unobservable (hidden); hence we cannot observe the state of the model directly, but the output of the model depends on the current state.

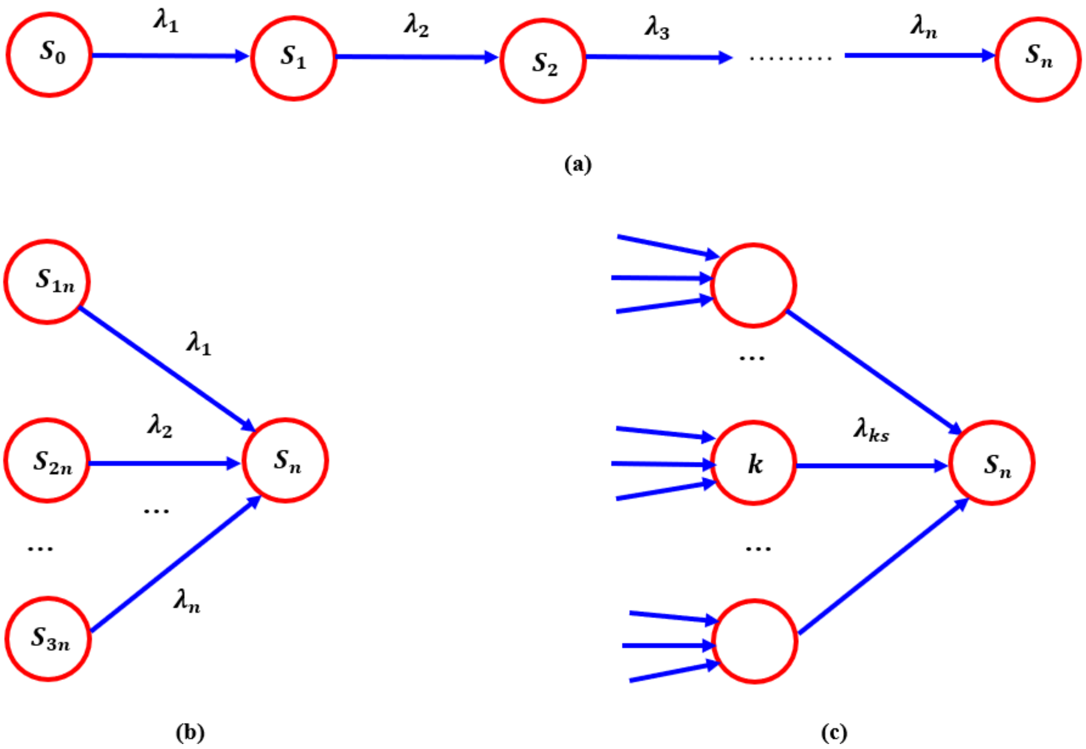

FIGURE 14. Connection model of the attack graph. (a) Serial model. (b) Parallel model. (c) Series-parallel complex model.

The Markov model predicts the attack behaviour considering the probability of the state transition of the system under different attack behaviours for evaluating the system vulnerabilities [30], [117]. This model describes all the types of attacks and meet the detection requirements of CPPS. Also, the multiple system states, the attack behaviour that leads to change in the system state, and the changing trend in the system states can be captured clearly and exactly by using this model. Markov models are well suited for intrusion detection and attack prediction even in the case of unobservable states & transitions and do not require the complete state information of the system.

Fig. 15 shows an example of a Markov model for attack prediction, which is visualized as a graph [118]. It represents four states of attack progress from a normal state to a successful compromise (cyber-attack). The attack sequence consists of different classes such as enumeration, host & service probing, exploitation, etc. Based on the attack sequences, we can predict the next state of an attacker and can find the most likely path from the present state mode. From the most likely path, the actions of the attacker can be predicted, and a probability threshold is assigned for each attack path to avoid the false positive so that the lowest probability is discarded and such paths are not evaluated for further actions.

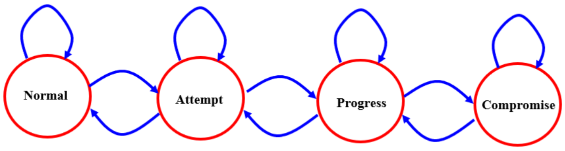

FIGURE 15. Hidden Markov model states for predicting cyber attacks.

5) MECHANISM MODEL

The combination of continuous event dynamic behaviour system and discrete event static behaviour system, the mixture of energy flow and information flow, and the interactions between the cyber and physical systems in CPPS can be analysed by using the mechanism models.

a: ANALYTICAL MODEL

In the CPPS, both power devices and cyber devices are energized by independent power supplies for reliability considerations. The interaction characteristics between the cyber and physical system in CPPS is influenced by the impacts of the cyber network reliability (i.e.) influencing the power measurement signals and control signal information. If an attacker initiates an attack, for example, false data injection attacks the attacker can control the IEDs, RTU, SCADA, etc. and tamper the critical information about the status of the power grid through synchronized measurement data, oscillatory monitoring results, electricity regulation pricing, and state estimation reports, etc. In the analytical model framework, the cyber network failure is generally considered as a data fluctuation (bad data, outlier, missing data, etc.) relevant to some function of the power system and implement a specific power system

TABLE 2. Characteristics of different schemes in attack graph modelling for cyber-physical systems.

Method	Aim	Proposed Solution	Merits	Demerits
Attack graph modelling [267]	To protect the CPPS from critical topological attacks	Pattern of attack sequences and novel attack search strategy is introduced considering cascading outages.	Reduces the storage for risky attack sequences while keeping the key information, and enhances the system performance and accuracy.	Testing on large-scale CPPS is needed.
Attack graph modelling [95]	To provide the minimum security for organization assets with various requirements.	A vertex cover algorithm and graph isomorphism for minimum security requirements.	Effective organization control.	Manual actions.
Distributed attack graph generation [96]	To construct the vulnerability-based attack graph for a distributed system.	Parallel and distributed computation-based attack graph for a distributed system.	Overcome the state explosion problem and suitable for real-time attack detection and prediction.	Needs assessment of the advantages gained by allowing duplicate privilege expansion.
pwnPr3d [97]	To perform automatic attack graph generation based on network modelling.	Probabilistic threat modelling approach.	Built-in security capabilities & independent of manual work and security expertise.	Testing on a real-life system is needed to validate the approach.
Attack graph modelling [98]	To analyse the basic problems of attack graph usage in network security.	Attack graph modelling and reachability analysis with core building phases of attack graph generation process being developed.	Classification of attack graph modelling with network security applications.	Real-time attack graph modelling with network security applications to be considered.
Attack graph modelling & Attack tree [99]	To compare the attack graph and fault tree method for cyber-attack perception.	Empirical evaluation between attack graph and fault tree method.	Both computer science and non-computer science background experts are considered for the evaluation.	Requires a further larger study to identify whether the method can indeed aid cyber-attack perception among non-experts.
Attack graph modelling [100]	To analyze the security threats for interoperable medical devices.	Design of secure interoperability architectures.	A detailed attack graph-based analysis of threats on PCA under various levels of interoperability is presented.	Multiple and coordinated attacks on medical devices to be considered.
Attack tree [101]	To construct the attack tree for risk assessment of connected vehicles.	Graph transformation-based modelling of car architecture and determining the state evolution for analysing the cyber-attack.	Designed to support the conceptual phase of the autonomous vehicle's cyber-physical system.	Requires input data about the structural and behavioural model of the service nodes, hardware components, and the attacker model.
Attack graph modelling [102]	To develop the realistic graph-based alert correlation system.	Attack scenario detection method that detects multistep attacks and extracts different types of alerts.	Global alert correlation system with robust attack analysis framework.	Need to compare with other existing methods using a unique data set and unique set of benchmark criteria.
Attack graph modelling [103]	To model the attack graph for ambulatory medical devices.	Vulnerability identification, risk assessment, and mitigation strategies for ambulatory medical devices.	The number of steps required to identify the attack is minimum.	Need to consider the architecture and style of the attack graph.
Attack graph modelling [104]	To extend the network security model for Multi-host, Multi-stage Vulnerability Analysis (MulVAL) framework.	Modelling of multiple attack techniques on advanced types of communication.	Models various types of cyber-attacks and supports short-range communication protocol.	Need to consider the characteristics of wireless devices.
Hercule [105]	To develop the multi-stage log-based intrusion analysis system.	HERCULE – An automatic multi-stage log-based intrusion analysis system.	Panoramic view of the logs generated by different system components.	Need to consider the computation time.
Safelite [106]	To develop a security modelling and analysis framework for large-scale network systems.	Automatically converts an attack graph into Hierarchical Attack Representation Models (HARMs) and visualizes the HARMs with relevant security information.	Avoids state-space explosion problem.	Computational time for calculating the probability of attack success is more.

TABLE 2. ***(Continued.)*** **Characteristics of different schemes in attack graph modelling for cyber-physical systems.**

Bayesian Attack Graph (BAG)[94]	To evaluate the reliability of the SCADA system with cybersecurity considerations.	Two Bayesian attack graph models are built to illustrate the attack procedures and to evaluate the probabilities of successful cyber-attacks.	The frequency of intrusions through various paths and the loss of load probabilities are estimated.	A more realistic probabilistic model for large-scale CPPS is needed.
Metamodel [107]	To develop the cybersecurity risk management approach for a cyber-physical system.	Integrated cybersecurity risk management framework for assessing and managing the risks in a proactive manner.	Cascading vulnerabilities and threats can be analysed	Manual calculation of KPI for CPS.
Attack graph modelling [108]	To quantify the level of network security for IoT devices.	Depth-first branch and bound (DFBnB) heuristic optimization algorithm-based quantification of network security level.	Physical location of the devices and different communication protocols are considered.	Need to consider the cost of different exploits along an attack path.
Graphical security model [109]	To propose a framework for security modelling and assessment of the IoT.	Graphical security model for the IoT.	Mitigates the impact of network attacks in the large-scale IoT networks.	Multiple and coordinated attacks to be considered.
Attack graph modelling [110]	To assess the security of enterprise systems.	Probabilistic attack graphs.	Composition of vulnerabilities is modelled, which shows all the paths of attacks that allow network penetration.	Limited to small scale enterprise networks.
Attack graph modelling [111]	To propose metrics for measuring the enterprise-wide cybersecurity risk.	Victimization metrics to measure the overall network vulnerabilities.	Interactive visualization showing multiple metrics trends over time with a - friendly user approach.	Need to consider the computation time.
Attack graph modelling [112]	To develop a security analysis tool considering heterogeneity & dynamic interactions of attacks.	Simulation-based tool for security analysis with the heterogeneity of attackers.	Dynamic generation of attack paths for large-scale networks.	Need to consider additional types of attack patterns.
Attack graph modelling [113]	To model the interaction between the network administrator and multi-path attacker for hardening the network security.	Game-theoretic model for network hardening.	Robust solutions.	Need to consider the multiple types of attacks.
GrSMs [114]	To survey the different security models and their applications.	Listed the different graphical security models in terms of security metrics, availability of tools, and their applications.	Users can select a suitable graphical security model based on their security concerns.	Need to consider the comparison of adaptability and scalability feature for each graphical method.
Temporal logic [115]	To compare the different types of temporal logics for model checking.	Comparison between interval temporal logic model checking point-based temporal logic model checking.	Three semantic variants of the interval temporal logic are considered.	Need to study the complexity issues.
Attack graph modelling [116]	To model and visualize an attack graph for different cyber-physical systems.	The CPSs are modelled by Architecture Analysis, and Design Language and security analysis are performed by JKind model checker embedded software.	The generated attack graph can benefit system administrators to select the best arrangement of countermeasures automatically.	Need a complete and accurate model of the system.

application analysis corresponding to the changes in measurement information of CPPS. Table 4 lists some analytical models of power system applications under cyber-attacks.

The PMU is a device used to estimate the real-time voltage and current phasor values of CPPS using a common time source through a Global Positioning System (GPS) for synchronization. The PMU is an essential element in the Wide-Area Measurement System (WAMS) of CPPS for monitoring, protection, and control applications. Using the phasor values (magnitude and angle of voltage and current),

TABLE 3. Detailed taxonomy of network attack model.

Network Attack Model	
Attack Tree	1. Attack Tree
	2. Defense Tree
	3. Ordered Weighted Averaging (OWA) Tree
	4. Protection Tree
	5.Attack Response Tree
	6. Attack Countermeasure Tree
	7. Attack Défense Tree
	8. Attack Fault Tree
Attack Graph	1. Attack Graph
	2. Exploit Dependency Graph
	3. Bayesian Attack graph
	4. Topological Vulnerability Analysis
	5. Logical Attack Graph
	6. Multiple Prerequisite Attack Graph
	7. Compromise Graph
	8. Hierarchical Attack Graph
	9. Countermeasure Graph
	10. Attack Scenario Graph
	11. Attack Execution Graph
	12. Conservative Attack graph
	13. Security argument Graph
	14. Incremental Flow Graph
Tools	1. SeaMonster
	2. AttackTree+
	3. SecuITree
	4. NuSMV
	5. RedSeal
	6. Skybox
	7. TVA
	8. MulVAL
	9. Cauldron
	10. NetSPA
	11. GARNET
	12. NAVIGATOR
	13. ADVISE
	14. CyberSAGE
	15. Sphinx
	16. Safelite
	17. Firemon
	18. CyGraph
	19. ADTool 2.0
	20. ATSyRa
	21. Attack Navigator
Applications	1. Networks Security Metrics Calculation
	2. Network Hardening
	3. Real-Time Security Monitoring & Analysis

we can capture the wide-area snapshot of the CPPS and real-time behavior of the power system. The applications of PMU in power systems are voltage stability monitoring, oscillation stability analysis, state estimation, wide-area monitoring & control, var optimization, blackout analysis, real-time electricity pricing, and transmission line fault detection, etc. Using the time-synchronized data from PMU, we can build the analytical model and analyze the impact of cyber network attacks on the function module [119]. The analytical model can also be built to analyze the tampered data on power system measurements on voltage stability, Automatic Generation Control (AGC), and power system frequency control [120], [121]. Besides, the analytical model can also be used to assess the loss of revenue quantitatively when the confidential data is tampered from the power system measurements by setting the analytical model to parameters such as the electricity price information and revenue of the power system operator [122].

In CPPS, the actual data is first gathered in the WAC centre. After performing the data cleansing operation and removing the ambient disturbances by state estimator, the corresponding data is used by the other advanced power system applications. The advanced cyber-attacks performed by the attacker easily bypasses the bad data detection and identification module from the state estimator, which can eliminate only ambient disturbances. The false data injection attack effectively bypasses the intrusion monitoring and detection system and tamper the confidential data coming from the state estimator. This impacts the performance of the power system application module, which is solely based on these data sources. By developing the analytical model for CPPS state estimation, the impacts of cyber-attacks on state estimation results can be assessed quantitatively [123], [124], and the performance of the function module can be evaluated quantitatively based on these changes in the state estimation results. Regarding cyber-attacks, the state estimation model can use both AC power flow and the DC power flow. In the case of the AC power flow model, the process takes more time and does not converge to the optimal global solution [69], [125], [126]. On comparing the results of ac power flow with dc power flow in state estimation model for cyber-attack analysis, it indicates that the attacker using the dc model for a specific type of false data injection attack at the RTU level introduces more errors in the measurements which triggers the bad data monitoring and detection mechanism. But in the case of the AC power flow model, the non-linear equations of the state estimation model are robust to this type of attack, which is advantageous to the system operator only if the attacker does not know system data, which would allow the attacker to perform the attack analysis. If an attacker is well aware of the system data, then he could be able to execute an attack that is unnoticed through AC state estimation [127].

b: DYNAMIC SYSTEM BASED MODELS

In the CPPS stability analysis, the physical system is modelled by differential equations with energy flow, and the difference equations model the cyber system with information flow. The perturbation effect on the physical system from the cyber system is modelled by the stimulant of the generator states (frequency and angle) in the rotor swing equation of the generator. In [126], an attacker constructed the attack vector for stealth cyber-attack to control the synchronous generator in the cyber controlled Distributed Energy Resources (DERs) to continuously maintain the physical instability of the smart grid. The CPPS can be modelled as a closed-loop dynamic system through constructing the dynamic models of the power system components such as exciter, power system stabilizer, prime mover, synchronous generator, High Voltage Direct Current (HVDC) and FACTS devices, with an interaction between information flow and energy flow. The closed-loop system analysis is performed for WADC of CPPS.

TABLE 4. Common analytical models of power system applications under cyber attacks.

Objectives	Equations	Details
Effect of Time Synchronization Attack (TSA) in Transmission Line Fault Detection [119]	$\Delta D = \left(\frac{1}{2\gamma L}\right) ln \left(\frac{(A+B)(C+D.exp(j\Delta\theta))}{(C+D)(A+B.exp(j\Delta\theta))}\right)$	Where $\Delta\theta$represents the fault location error caused by TSA, $\Delta\theta$ represents asynchronism of phase angle measurements between receiving end and the sending end caused by TSA, L represents the length of the transmission line, γ represents the attenuation constant, and *A, B, C, D* represents the formulas of sending end and receiving end voltage and current respectively.
Effect of Time Synchronization Attack in Voltage Stability Monitoring [119]	$\bar{Z}'_T = 2\frac{V_S exp(j\Delta\theta_s) - V_R exp(j\Delta\theta_R)}{I_S exp(j\Delta\theta_s) - I_R exp(j\Delta\theta_R)}$ $\bar{Z}'_{sh} = -\frac{V_S I_R + V_R I_S}{{I_R}^2 exp(j2\Delta\theta_R) - {I_S}^2 exp(j2\Delta\theta_S)} \times$ $(exp\, j(\Delta\theta_S + \Delta\theta_R))$ $\bar{Z}'_L = \frac{V_R exp(j\Delta\theta_R)}{I_R exp(j\Delta\theta_R)}$	$\bar{Z}'_T, \bar{Z}'_{sh}, \bar{Z}'_L$ are the T-equivalent parameters for calculating voltage stability monitoring affected by TSA.
Effect of Time Synchronization Attack in Event Locating [119]	$(x_i - x_e)^2 + (y_i - y_e)^2 - V_e^2(t_i - t_e)^2 = 0$	when $t_i, i = 1,2,3,4$ is the disturbing event arrival time to the i^{th} PMU, (x_i, y_i) and (x_e, y_e) are the coordinates of the i^{th} PMU and the disturbance event location, V_e is the event propagation speed in the electric power grid network.
Advanced Metering Infrastructure (AMI) under False Data Injection Attack in Smart Grid [120]	$VSI(N_r) = V_S^4 - 4(P_r X - Q_r R)^2$ $- 4(P_r R + Q_r X)V_S^2$	where $VSI(N_r)$ represents the voltage stability index at the receiving end of (N_r) a branch, V_S is the magnitude of the voltage at the sending end (N_s), R and X are the resistance and reactance of the branch, (P_r) and (Q_r) are the summation of the real power loads and reactive power loads at the node r.
Automatic Generation Control under False Data Injection Attack [121]	$ACE_i = (P_{tie} - P_{sch}) + \beta_i(f - 60)$	where ACE represents the Area Control Error, P_{sch} represents the scheduled tie-line power exchange between the balancing areas, β_i represents the frequency bias for the balancing area i, P_{tie} and f represents the power flow in the tie-line and system frequency measurements fabricated by a false data injection attack in order to force the miscalculation of ACE.
Real-pricing under data integrity attacks [122]	$\lambda_1 = \frac{\sum_{j\epsilon M}\frac{b_j}{2a_j} + \sqrt{\left(\sum_{j\epsilon M}\frac{b_j}{2a_j}\right)^2 + 4\sum_{j\epsilon M}\frac{1}{2a_j}\sum_{i\epsilon N} w_{i1}}}{\sum_{j\epsilon M}\frac{1}{a_j}}$, and $\lambda_2 = \frac{\frac{n}{2m} + \sqrt{\left(\frac{n}{2m}\right)^2 + 4\frac{1}{2m}\sum_{i\epsilon N} w_{i2}}}{\frac{1}{m}}$	λ_1 and λ_2 represents the prices of renewable energy and conventional power sources; m, n, a_j, b_j are the coefficients of the cost function, $w_{i1}$and w_{i2} represents the preference factors for renewable energy and conventional power consumption for demand user i, and M, N represents the number of supply users and demand users, respectively.
DC State Estimation under False Data Injection Attack [123]	$Z = h(X) + e$ $\Vert Z_a - h\widehat{X_{bad}}\Vert^2_{R^{-1}} = \Vert Z - H\hat{X}\Vert^2_{R^{-1}}$ $\widehat{X_{bad}} = \hat{X} + C$ $Z_a = Z + a$	where $Z = (z_1, z_2, \dots z_m)^T$ represents the original measurement vector, $X = (x_1, x_2, \dots x_n)^T$ represents the state vector, $e = (e_1, e_2, \dots e_m)^T$ represents the measurement error vector, $h(X)$ is a nonlinear vector function, $\hat{X}$ represents the original estimates, C represents the malicious errors added to the original estimates, $a = (a_1, a_2, \dots a_m)^T$ be the nonzero attack vector, Z_a be the observed sensor measurements vector.
AC State Estimation under False Data Injection Attack [125]	$Z = h(X) + e$ $\Vert Z_a - h\widehat{X_{bad}}\Vert = \Vert Z + a - h(\hat{X} + C)\Vert$ $= \left\Vert \begin{pmatrix} Z_1 \\ Z_2 + a_2 \end{pmatrix} - \begin{pmatrix} h_1(\widehat{X_1}) \\ h_2(\widehat{X_1}, \widehat{X_2} + C \end{pmatrix} \right\Vert$ $= \left\Vert \begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} - \begin{pmatrix} h_1(\widehat{X_1}) \\ h_2(\widehat{X_1}, \widehat{X_2}) \end{pmatrix} \right\Vert$ $= \Vert Z - h(\widehat{X})\Vert < \tau$ $a_2 = h_2(\widehat{X_1}, \widehat{X_2} + C) - h_2(\widehat{X_1}, \widehat{X_2})$	Where τ represents the predetermined threshold, if it is violated, then there is at least one faulty measurement. The difference with the dc analysis is, an attacker when using an ac analysis must also know the estimated value of the state variables that appear in h_2.
Kalman Filtering under False Data Injection Attack [124]	$\left\lvert \frac{z_{k,i} - h_i(\widehat{X_k^-}, 0)}{\rho_{k,i}} \right\rvert \leq \lambda_{max}$	where $z_{k,i}$ represents the malicious measurement, $h_i(\widehat{X_k^-}, 0)$ represents the predicted measurement, $\widehat{X_k^-}$ represents the predicted state, $\rho_{k,i}$ represents the intermediate variable and λ_{max} represents the value for detecting anomaly condition.
Data attacks on network topology of a smart grid [69]	$\bar{s} = s + b$ $\bar{z} = z + a(z),\ a(z)\epsilon\mathcal{A}$	where $\bar{s}$ represents the modified network data, $b\epsilon\{0,1\}^d$ represents the modifications on the network data s, $a(z)\epsilon R^m$ represents the attack vector added to the meter data z, and $\mathcal{A} \subset R^m$ denotes the subspace of feasible attack vectors.

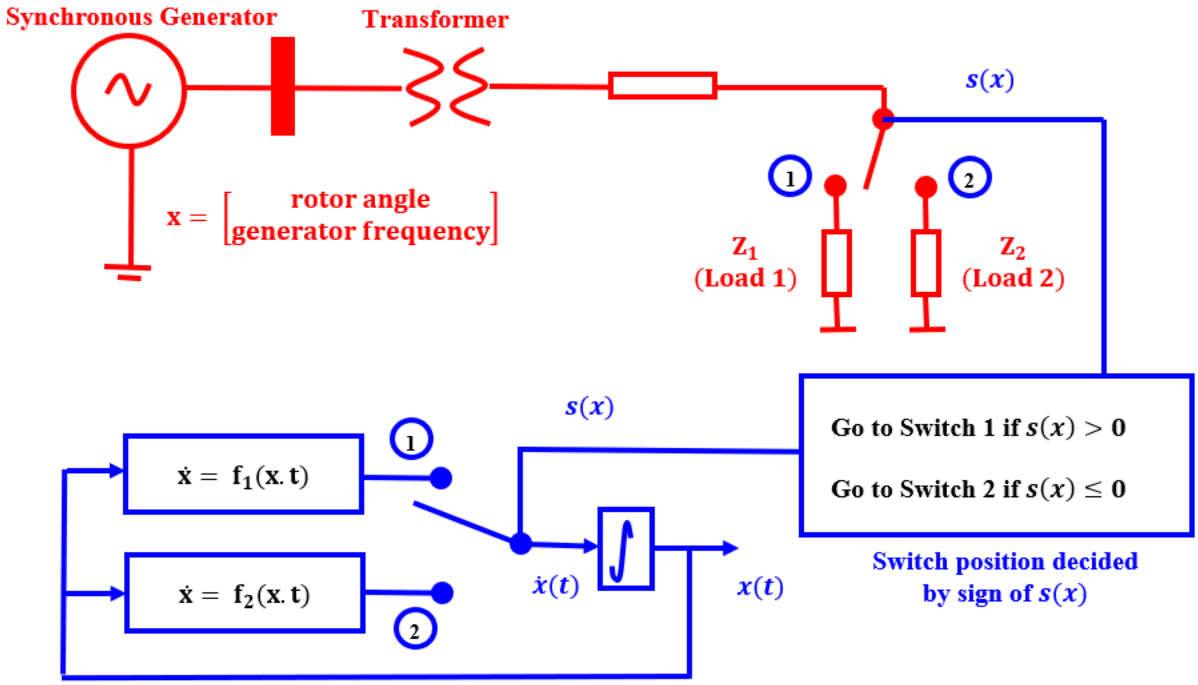
Synchronous Generator
Transformer
$x = \begin{bmatrix} \text{rotor angle} \\ \text{generator frequency} \end{bmatrix}$
$s(x)$
1
2
Z_1 (Load 1)
Z_2 (Load 2)
$s(x)$
Go to Switch 1 if $s(x) > 0$
Go to Switch 2 if $s(x) \leq 0$
Switch position decided by sign of $s(x)$
$\dot{x} = f_1(x.t)$
$\dot{x} = f_2(x.t)$
1
2
$\dot{x}(t)$
$\int$
$x(t)$

FIGURE 16. Elementary variable structure system example. (a) Elementary power system. (b) Block diagram.

It utilizes the measurements from PMU, but the communication delays between the PMU and the control centre are significant, which affects the CPPS stability. In [127], [128], the authors have utilized the delay-dependent stability analysis method for eigenvalue analysis of CPPS. The CPPS is modelled by the directed graph method, and using the dynamic system equation, the state information of each power node is determined [73]. If the cyber-attacks have triggered in CPPS, the state variation of the power node can be evaluated by numerical simulation.

c: VARIABLE STRUCTURE SYSTEM MODEL

The status of the circuit breaker switches decides the topology of CPPS. If the attacker attacks the power system switches the topology of the power grid is changed continuously, and its dynamics depend upon the value of switching signals. The variable structure theory is used to identify the weakness of the CPPS when the switching attack signals reconfigure the grid. It captures the interactions between the cyber and physical systems in CPPS effectively and demonstrate how the switching vulnerability disrupts the operations of CPPS within a short period. In the Fig. 16 it represents when the power system switches change its position between $Z_1(load1)$ and $Z_2(load2)$ it stimulates the effect of changing system dynamics between $f_1(x, t)$ and $f_2(x, t)$ respectively [129].

In [130], the authors have demonstrated the distributed smart grid attack on CPPS to destabilize the power system components using variable structure system theory. The attacker controls the multiple circuit breaker within a power system through cyber intrusion to destabilize the synchronous generator by state-dependent breaker switching. They utilize the localized state information to identify the sliding surface of the CPPS then destroy the stability condition of a particular sliding mode, which triggers the transient instability condition of the targeted synchronous generator. The attacker intrudes through a single breaker then reaches multiple and coordinated switch-case attacks, which leads to a stealthier and wide-area cascading failure. In [32], the authors have designed the optimal partial feedback based switching data injection attacks for CPPSs. The goal of an attacker is to manipulate the control signals, and alter the attack locations persistently to degrade the CPPS performance with a minimum cost. Using convex relaxation and pontryagin's maximum principle the authors have proved that for all the optimal switch inputs a switching condition can be derived to select the optimal attack locations.

d: MULTI-AGENT SYSTEM MODEL

With the increasing number of integrations of DERs into CPPS, the distribution characteristics of the CPPS become very clear, the power system operators exchanging the data among them very, and the control scheme becomes of great significance. The traditional centralized mode of control is very difficult and inefficient to control the different types of DERs in the CPPS. The centralized control scheme requires the complete mathematical model of the CPPS. With the continuous expansion of the modern CPPS, the design of a single centralized controller for various DERs have a chance to failure, since no other sources to control the system, the CPPS becomes unstable. The cost of implementing the centralized controller is very high [16]. This motivates to develop a multi-agent-based control for CPPS, which solves the cooperative optimization problem of various DERs integration into CPPS. In the multi-agent system model, each physical entity is monitored by an agent and communicates with other agents for interchanging the information to attain the common objective.

In [131], the authors had investigated the goal-based Holonic Multi-Agent System (HMAS) for optimal operation of CPPS by reactive power control method at solar photovoltaic installations. Using the same HMAS, the state estimation of CPPS can also be performed by leveraging the different measurements from smart meters. In [132], the authors have presented the multi-agent-based security enhancement of protection schemes in CPPS by detecting and identifying the cyber threats on protection systems of power grids. The multi-agent model utilizes the properties of physical and cyber systems in CPPS to distinguish the cyber-attacks from the physical faults and thereby to improve the cybersecurity and stability. In [55], the authors have proposed the multi-agent-based cyber-physical control framework for transient stability enhancement. In this framework, a cyber-physical delay resilient controller is designed, which adapts its structure depending on the value of latency and the state of the cyber component in CPPS. In [133], the authors have investigated the application of a distributed averaging based integral (DAI) controller for CPPS. The uncertainties of the cyber and communication layer and their effect on robustness and performance were considered. Based on these uncertainties, a delay-dependent condition for robust stability of DAI controlled CPPS concerning communication delays, link failures, and packet loss is derived.

6) PROBABILISTIC MODEL

The probabilistic models are classified into two types, such as uncertainty model and the game-theoretic model. In CPPS, both physical and cyber systems events are probabilistic in nature. These events occurring in the physical and cyber systems cannot be narrated exactly. In such a situation, the uncertainty model can be used to describe the behaviour of CPPS. Meanwhile, the CPPS operation involves various stakeholders, making important decisions under uncertain conditions. If the interactions exist among the multiple decision-making stakeholders for the operation of CPPS, each one of them implements their strategy for their benefits depending upon the existing information. The game-theoretic type models are used to describe this kind of probabilistic situation.

a: UNCERTAINTY MODEL

The interactions between the physical and cyber systems in CPPS are uncertain, which includes the direct and indirect impacts of cyber system unreliability through cyber-attacks on power systems [137] as well as through the malfunctioning of the cyber systems [135], [138], [139] in wide-area monitoring and protection systems. The degradation of the performance of the cyber system may be due to many reasons such as failure of power source to cyber systems, time synchronization error among the cyber systems, breakdown of ICTs and improper configuration of SCADA, etc.

The cyber systems can be modelled by three methods, namely Reliability Block Diagram (RBD) method, discrete Markov Decision Process (MDP), and Semi Markov Process (SMP). The RBD method is a practical method for constructing the reliability model for cyber systems. In [134], the RBD method is used to calculate the cyber system reliability quantitatively, and a multi-state Markov chain method is used to analyze the effects of cyber systems failures on the power system components. In [30], the cyber-attacks are modelled by the discrete MDP and generate all the possible attack scenarios. The attacker uses the same Markov process to perform the state transition. Once it is successful, the attacker gets the rewards with a certain probability. Then estimating the current security state of the system using this Markov process model and combined with cyber intrusion and detection system alerts. In [117], the cyber-attacks on SCADA systems are modelled as SMP. In addition to that, the time delay and time-varying delay in the communication system, including the traffic delay with Probability Distribution Function (PDF), minimum deterministic delay, and processing delay with PDF, are adopted deeply into the modelling of the communication system [18]. In [134], the impacts of cyber layer failure (protection and monitoring failure) are added to the reliability evaluation of the power system components. A multi-state Markov chain model is used to build the structure of electrical components considering the topology of the cyber layer with its reliability functions and actual protection and monitoring strategies simultaneously. From the complete model of CPPS, the reliability information of each component and subsystems in CPPS are collected. Then the probability table (P–Table) is used to express the system reliability [137], [138], and the state transition diagram is used to model the state transition probability of each component in the CPPS [135], [139]. In addition to that, a Bayesian structure can also be used for reliability assessment of CPPS by Bayesian network probabilistic reasoning [136].

b: GAME-THEORETIC MODEL

In recent years the cyberattacks on the physical power system are increasing the attention worldwide. The attackers target the ICTs of CPPS through cyberattacks, and the defenders tried to protect the power system using a cyber-attack detection and mitigation scheme. The attack detection and mitigation game-theoretical model is used to model the cyber-physical interaction process and also applied for risk, vulnerability, and threat analysis. The defenders involved in the operation of CPPS makes their decisions for their benefits in a competitive situation by allocating limited resources. The competitive relationship among the participants of CPPS can be modelled as a Colonel Blotto Game [117], Zero-Sum Game [142], and Stochastic Game [141]. In [143], the authors investigated the vulnerability analysis of CPPS under terrorist threat, assuming the attacker knows the complete information about CPPS. The problem is formulated as a mixed-integer nonlinear bilevel program with upper and lower level optimization. In the upper level of optimization, the terrorist tries to maximize the damage to the power systems, which is measured in terms of the level of load shedding. On the other hand, in the lower level of optimization, the power system operator tries to minimize the damage by optimal operation of the power system and capable of modifying the network topology in case of severe cyber-attacks. In [144], the authors analysed the bi-level model of coordinated cyber-physical attacks on power systems. This two-step cyber-attacks comprising topology-preserving attacks and load redistribution attacks, ensuring the bad data measurements are undetectable. In [145], the authors investigated the security assessment of electricity distribution networks with vulnerable DERs nodes. The game-theoretical model is used to model a 3-stage defender-attacker-defender (DAD) tri-level optimization problem. In stage 1, the defender chooses the cybersecurity measures to secure a subset of DERs node; in stage 2, the attacker compromises the vulnerable DERs nodes, and, in stage 3, the defender responds by taking a controlling action by the rescheduling of loads [146].

From the past research works, the game-theoretic model assumes that the level of attacker and defender are the same, and their actions also similar. Practically this assumption is invalid; the attacker observes the defender cybersecurity framework then decides the attack countermeasures. This asymmetric behavior between the attacker and defender can be modelled as a static infinite Stackelberg game-theoretic model [147]. Using this model, the interactions between the different security agents can be represented in the cyber layer, and for the physical layer, the full-information H-infinity min-max control with packet drops is modelled by the Stackelberg game model. In the dynamic attack detection and mitigation scheme, the game is not finished at once and using the same attack structure, the attack persists many times. In this regard, the attacker's history is recorded and analysed then the decisions can be taken based on the attacker's actions. This process be continued as long as the attacker and defender are opposed to each other in their long-term interest. This interaction between cyber attackers and physical defenders can be modelled as an iterated game model in CPPS, where the results are completely different from the one-time game [140]. Almost the previous game-theoretical model analysis assumes that the control is optimal, and the physical systems dynamics model is accurate. In CPPS, the dynamics of the physical systems are usually modelled by differential equations with energy flow, and the cyber systems are modelled by difference equations with information flow. In [126], the authors have proposed a differential game-theoretic model to demonstrate the worst-case attack by an attacker to disrupt the transient stability of CPPS by leveraging the control over DERs, with the consideration of full dynamics of the power system.

7) SIMULATION MODEL

The continuous nature of the physical system and the discrete nature of the cyber system complicates the research in CPPSs. The simulation model supports the power system operators to realize the integrated modelling of the dynamic behaviour of the continuous system and static behaviour of the discrete system. The software used for building the simulation model of the power system is discussed in detail in Section III.

C. CPPS INTERDEPENDENT MODELLING (DEGREE OF PHYSICAL AND CYBER SYSTEMS DEPENDS ON EACH OTHER)

The CPPS consists of a large number of physical devices and cyber devices which form a large-scale interdependent complex system. The interface relationship between the cyber and physical devices is modelled as interdependent modelling of CPPS, which changes over time. The interdependent CPPS is divided into the three-layer structure, namely the physical layer, cyber layer, and interface-mapping layer, as shown in Fig. 17. The physical layer node represents the generator, transformer, substation, etc., and the transmission lines in the electric power grid network are represented as a physical layer edge. The cyber layer nodes composed of computational systems, communication equipment's and control algorithms where its main function is to monitor and control CPPS. The network edges represent the communication links between the cyber nodes. There are two types of interdependencies in CPPS based on cyber layer nodes, namely one-to-one interdependency and one-to-multiple interdependency [148]. In the one-to-one interdependency, each physical node is monitored (sensing the status of the physical node) and controlled (issuing the control commands) by the single cyber node [149]. Then the control centre collects the information from the distributed cyber nodes. In the one-to-multiple interdependencies, each physical node is monitored by more than one cyber node, which is very much useful for securing the data against cyber-attacks [150].

In [151], the interdependent modelling of CPPS is used to analyze the effects of cyber-attack and defense in smart city applications. A smart city integrates several interdependent CPS that operate in a coordinated manner to achieve the global objective of the city's residents. These large-scale interdependent CPS are more vulnerable to cyber-attacks due to these interdependencies, which can be lead to cascading failures and serious effects on the city. A novel approach is proposed to allocate the security resources for the various cyber components of an interdependent CPS to protect the system against cyber-attacks. In case the attacker not aware of the CPS interdependencies, the defender can have a higher payoff compared to the case in which the attacker knows the complete information. In [152], a realistic model called HINT (Heterogeneous Interdependent NeTworks) is proposed to study the evolution of cascading failures in the interdependencies between the power grid and the communication network taking into account the heterogeneity of

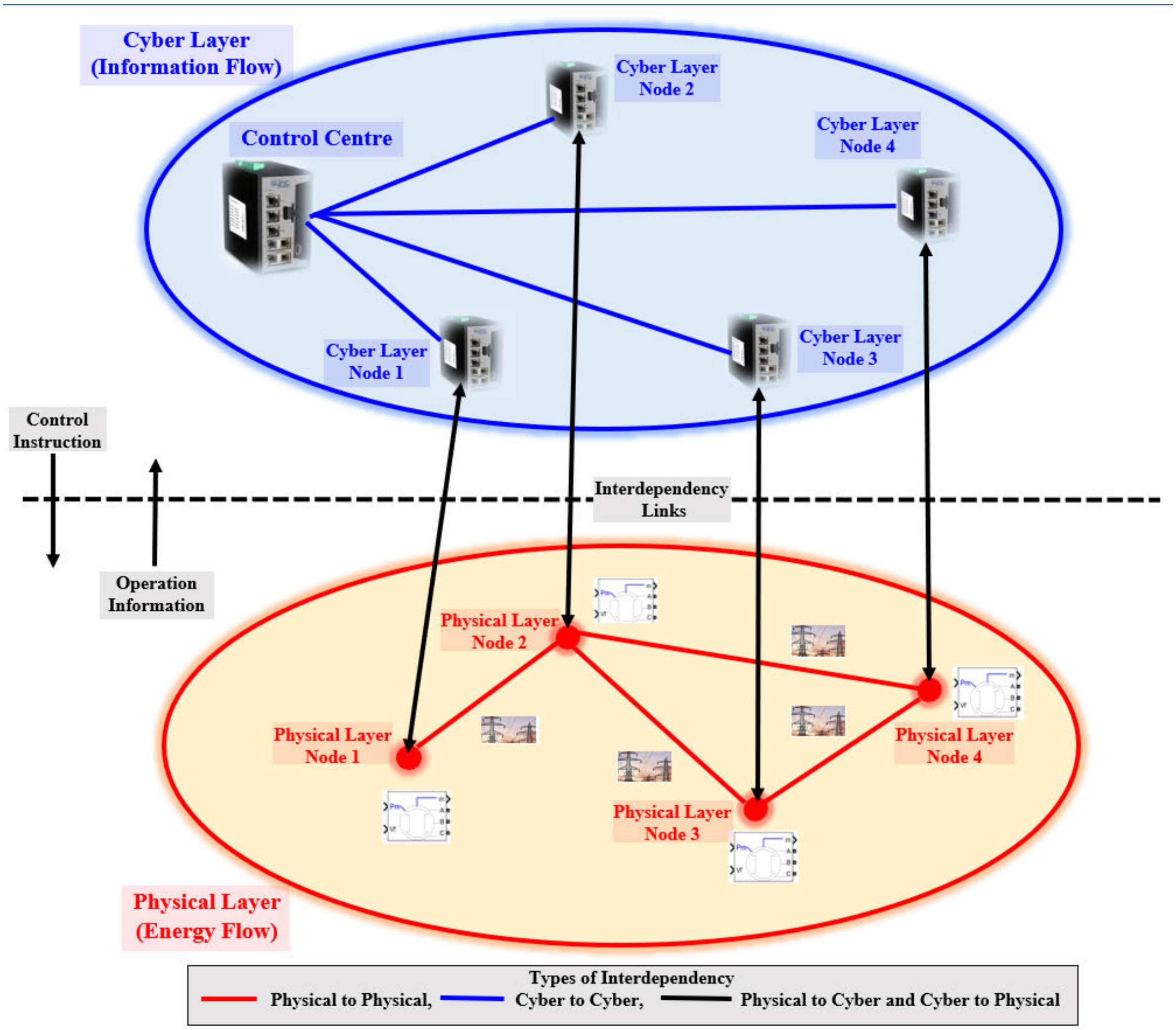

FIGURE 17. Interdependencies within CPPS.

the networks as well as their complex interdependencies. Using this model, the failure propagation is accurately forecasted and improved the network robustness. A quantitative analysis of the impact of interdependency on power system vulnerability is proposed in [153] considering the strong coupling between the power grid and the communication system. A reliability modelling of the smart grid is developed considering the cyber-physical interdependencies among the components and shown that the flawed cyberinfrastructure results in lower reliability of the smart grid compared to the conventional power grid with less advanced control [154]. In [268], based on the interdependence between the cyber and physical networks, a risk area prediction model for CPPS is developed using dependent markov chain. Then the cross-adaptive gray wolf optimization algorithm is utilized to optimize the prediction model to accurately reflect the actual system risk propagation process. In [155], based on the network interdependencies relation and physical layer operation, the modelling of cascading failures and its mitigation in the CPPS is presented. The CPPS is modelled as an interdependent complex network-based model incorporating the physical layer power flow analysis, cyber layer information, edge capacity checks, delay analysis, transmission analysis, and indirect interaction mechanism between the two layers. The physical and cyber layer usually operates without the interdependencies from the other. Since the two layers are different in topology and operational relations, it is necessary to consider the interdependency effect and should apply the mitigation strategies simultaneously in both layers.

The cyber-physical coupling failure in the strong interdependent CPPS increases the risk of smart grids when the physical outages remedial control is failed due to a simultaneous cyber-side failure. In this situation, to enhance the robustness of smart grids concerning the possible cyber-physical coupling failures, the critical information about the CPPS should be transmitted through a reliable path to ensure its accessibility. A CPS robust routing model with cyber-physical sensitivity-based information flow is proposed.

It improves the performance and robustness in power flow corrective control on comparing with conventional routing based shortest-path model [156].

III. SOFTWARE TOOLS FOR MODELLING AND SIMULATION OF CPPS

The CPPS is a complex system with the large-scale integration of renewable sources (e.g., PV, Wind), Controllable Loads (e.g., Smart Building, Electric Vehicle (EV), Batteries, Heat Pumps, etc.), Digitization of Power System (e.g., AMI), Multi-domain grid (ICT, Heat, Gas, Electricity) with strong interconnection and interaction effects. The efficient operation of CPPS depends upon the close interactions between the power system and cyber systems [157]. A holistic approach for CPPS is needed for a comprehensive analysis of interdependent subsystems. The inclusion of the cyber system model with the power system model is important for the analysis of complex CPPS involving the dynamics of both the systems for reliable power delivery to the critical infrastructure [158]. The individual domain of the CPPS can be modelled and simulated by continuous-time based power system simulation tools and discrete-event based cyber system simulation tools, as listed in Table 5. However, the CPPS necessitates an integrated system design for an in-depth analysis of the interdependencies of ICTs and power systems, which can be done by the co-simulation tools.

The co-simulation framework involves the joint simulation of simulations in the power system domain and the cyber system domain in a holistic test-case. It shows the realistic behavior of CPPS in faulty and extreme conditions with strict considerations on latency and stability. Using the co-simulation tool, we can understand the impact of cyber-attacks on the physical power system operation, whereas the independent simulation tool supports either the communication network or the power system but not both together. Thus, the cyber-physical co-simulator supports exploring the effects of cyber-attacks on power system dynamics and operation. The cyber-physical co-simulation tools listed in Table 5 are useful for the assessment of the cyber-physical security for CPPS, which simulates the power system and communication system together. This tool identifies the vulnerable states of CPPS, bad measurements, and then aids the power system operator at the control center to take appropriate actions to minimize the effect of the cyber-attack on smart grid operation.

Much industrial-grade software tools are available for electric power systems and cyber system simulation, as listed in Table 5. A wide range of power system simulation tools are available for various aspects of power systems, and the cyber systems are generally modelled as a computer network for simulation purposes; therefore, network simulation tools are used for cyber system simulation. The researchers can use the open-source simulators for CPPS, e.g., OMNeT++, NS-2, and NS-3, or commercial simulators, e.g., OPNET.

In [159], the researchers had developed the co-simulation framework by combining OpenDSS and OMNeT++ for power system simulations and communication networks to examine the wide-area monitoring and control applications. In [160], the co-simulation framework is developed for

TABLE 5. Simulation tools.

Power System Simulation Tools	1. MATLAB – Simpower systems
	2. PSCAD/EMTDC
	3. PowerWorld Simulator
	4. OpenDSS
	5. DIgSILENT
	6. EMTP-RV
	7. OPAL-RT
	8.PSS/E
	9. ETAP
	10. GridLab-D
	11. PSLF
	12. MATPOWER
	13. EnergyPlus
	14. PowerFactory
	15. UWPFLOW
	16. TEFTS
	17. PST
	18. InterPSS
	19. OpenETran
	20. OpenPMU
	21. rapid61850
	22. Aspen
	23. PSCAD
	24. PLECS
	25. adevs
	26. NEPLAN
	27. EUROSTAG
	28. Homer
	29. RTDS
	30. PCFLO
	31. Psap
Cyber System Simulation Tools	1. OMNet++
	2. Java
	3. NS2
	4. RINSE
	5. OPNET
	6. Visual Studio
	7. NS3
	8. GridSim
	9. NeSSi2
	10. GridStat
	11. COOJA
	12. DeterLab
	13. WANE
	14. UPPAAL
	15.Stateflow
	16. TIMES-Pro
	17. MATLAB – SimEvents
	18. GLOMOSIM
	19. Cloonix
	20. GNS3
	21. IMUNES
	22. Shadow
Co-Simulation Tools	1. Modelica
	2. Dymola
	3. MathModelica
	4. MapleSim
	5. JModelica
	6. Ptolemy II
	7. Simantics
	8. Mosaik
	9. Mathworks
	10. Simscape
	11. EPOCHS
	12. Simulink
	13. LabVIEW

TABLE 6. Major cyber-physical attacks in the energy industry sector.

Year	Location	Attack Objects	Type	Impact
1982	Soviet Union (Russia)	Gas pipeline control software	Code Manipulation	3 kilotons TNT equivalent explosion
1999	Bellingham, USA	Slowdown of SCADA system of a gasoline pipeline	Code Manipulation	Huge fireball that killed 3 people and injured many others
2003	Ohio, USA	Slammer Worm penetrated the nuclear plant control system	Malware Injection	Parameter Display System was off for 5 hours
2007	Idaho National Laboratory, USA	Aurora Attack manipulated a circuit breaker of a diesel generator	False Data Injection	Exploded generator
2008	Turkey	Attackers manipulated control system parameters of the oil pipeline	False Data Injection	Oil explosion and 30k barrels are spelled in water
2012	Saudi Arabia & Qatar	Malware affected Aramco and RasGas	Malware Injection	Generation and delivery of energy have been affected.
2015	Kiev, Ukraine	Attack on the breaker's sittings in 3 distribution companies	False Data Injection	Blackout affecting 225k customers for a few hours

simulating the power routing algorithm in microgrid application by combining OMNeT++ with Real-Time Digital Simulator (RTDS). In [161], the authors presented the event-driven co-simulation scheme utilizing network simulator NS2 and OpenDSS for simulation of CPPS. In [162], the co-simulation environment INSPIRE (Integrated Co-simulation of Power and ICT systems for Real-Time Evaluation) with high-level architecture is proposed for realizing a combined simulation of both ICT and power systems. It focuses on analyzing the real-time performance of wide-area monitoring, protection, and control (WAMPAC) applications. It applies a co-simulation of a continuous time-based power system simulator (DIgSILENT PowerFactory), a communication network simulator (OPNET), and continuous time-based WAMPAC applications modelled in MATLAB, JAVA, GNU R, and C++. In [163], an information flow-based co-simulation model is proposed to analyze the interdependencies between information and energy flows and obtaining the quantitative relation between them. Using this quantitative relation, the planning and operation of cyber systems are performed. In [164], the co-simulation platform utilizes OpenDSS and OPNET for power system simulator and cyber network simulator for testing different communication technologies. Based on DIgSILENT Power Factory as a power system simulator and OMNeT++ and INET framework as a cyber network simulator, a co-simulation environment is developed in [165] for analyzing the impacts of communication delay and failure. Another co-simulation environment named Greenbench presented in [166], which utilizes PSCAD and OMNeT++ for power and cyber system simulation to evaluate the impact of data-centric threats. In [167], a power system and communication network co-simulation framework are proposed using a global event-driven mechanism (GECO) using PSLF and NS2 simulators. It improves the practical investigation of the smart grid and enhances the wide-area measurement and control schemes. The MATLAB Simulink and OPNET are integrated to study the ICT impacts on the reliability of WAMS applications [168]. In [169], the Virtual Test Bed (VTB) software is integrated with OPNET called VPNET for simulating the remotely controlled power electronic devices in the system. The electric power and communication synchronizing simulator (EPOCHS) [170] are a combination of PSLF (commercial electric simulator) and NS-2 (open-source communication network simulator) used for most of the smart grid co-simulation applications. EPOCHS are used to understand the impacts of a communication system on a smart grid relevant to wide-area monitoring, security, and management applications.

IV. CYBER ATTACKS AND CYBER SECURITY IN CPPS

The electric power grid is one of the most important critical infrastructures of the nation and also the best example of the cyber-physical system. It is fully monitored and controlled by advanced information and communication technologies, which involve the tight integration of computation, communication, control, and human factors. Even though the digital technologies monitoring and controlling the electric power grid more efficiently and reliably, the power grid is vulnerable to cybersecurity risk and involves the complex interdependency between cyber and physical systems. The cyber-attack on the physical power system affects the secure operation of the power system by changing the information flow. The initial physical attacks on the power system are difficult to detect in the large-scale CPPS once it is successfully coordinated with cyber-attacks. The subsequent cyber-attacks mask these physical attacks, which tend to trigger a cascading failure across the electric power grid system. Therefore, it is necessary to analyse the various cyber-attacks and cybersecurity measures in CPPS. The cyber-attack is a major concern to the critical infrastructure like the electric power grid in which most of the R&D activities are giving maximum priority to cybersecurity research globally. From the technical literature, it is inferred that there is a wide range of advanced cyber-attacks created for the system like a power grid with monitoring, controlling, and protecting function, as shown in Table 6.

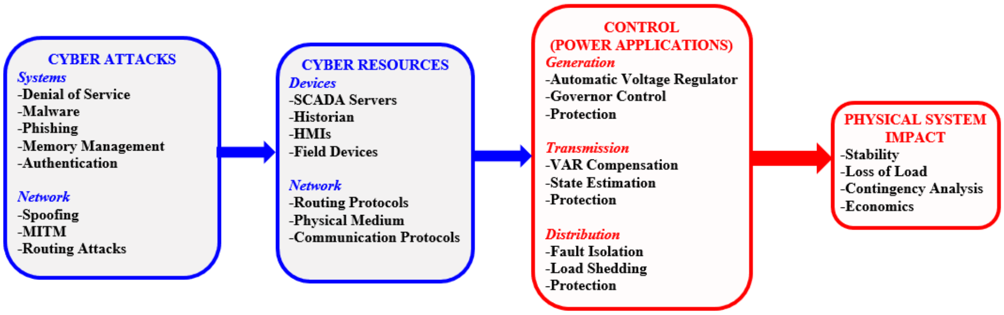

FIGURE 18. Mapping from cyber-attacks to control actions to system impacts.

A. HISTORY OF CYBER ATTACKS IN THE ENERGY SECTOR

Recently the various cyber-attack incidents that happened in the electric power grid around the world, for example, the Slammer worm of the David-Besse nuclear plant in Ohio, USA on 2003 [171], SCADA system in the nuclear power plant attacked by Stuxnet worm in Iran on 2009 & 2010 [172], Ukraine Cyber Attack in December 2015 leading to the loss of power for about 225,000 customers which were considered as the worst blackout caused by cyber-attack in power system history [173], Malware Triton in Saudi Arabian oil refinery on 2017 [174], U.S Cyber Attack in power utilities on March 5, 2019 [175], Cyber Attack in Kudankulam Nuclear Power Plant, India on 30 October 2019 [176], and Man-in-the-Middle attack in Nuclear Power Corporation of India Limited (NPCIL), India [177]. The world economic forum ranked large-scale cyber-attack as fifth among the risks to happen in the next ten years [178]. The history of the cyber-attacks alerts the entire world to protect their critical infrastructure of the nation. Table 6 lists out the major incidents reported in the energy sector [179]. The electric power grid is a big networked transmission and distribution system with a huge load that has a chance of entering of a cyberattack. The disruption of electricity creates a loss of billions of money in the country, which directly affects the economy of the nation and also the GDP growth in the modern global markets with private attackers. Therefore, it is necessary to develop the indigenous firewalls/cybersecurity measures against the cyber-attacks with innovative, resilient control algorithms.

B. CYBER SECURITY FOR CPPS

The CPPS needs cybersecurity at multiple levels, namely information security, ICTs infrastructure security, and application-level security [180]. From the past research works it is identified that the traditional information technology (IT) security features are not suitable for CPPS and certain research areas in cybersecurity for CPPS is identified as: (i) Cyberattack risk modelling and risk mitigation, (ii) Attack-resilient monitoring, protection and control algorithms, (iii) Defence against coordinated cyber-attacks, (iv) AMI infrastructure security, and (v) Simulation models. The cybersecurity of the power grid consists of Cyber-attack – Detection, Mitigation, Prevention, and Resilience, which is the most of R & D's need for the emerging CPPS. The main goal of cybersecurity research for the smart grid is to develop an integrated risk modelling framework that combines physical system dynamics as well as cyber system dynamics. Then the model is utilized to assess the impact of a cyberattack on the power system in terms of loss of load, stability problem, economic loss, or equipment damage. Following the risk assessment, the next important task is to develop indigenous cybersecurity algorithms to protect the power system from various cyber-attacks, including intrusion-based attacks, denial-of-service attacks, malware-based attacks, and coordinated attacks. The risk from the cyberattack is evaluated by the product of threats, system vulnerabilities, and their resulting impact, as shown in equation (24).

$$Risk = [Threat] \times [Vulnerability] \times [Impact] \qquad (24)$$

The *threat* can be defined as the presence of potential attacks, their motivation, and available resources. The *vulnerability* of the CPPS depends on the grid's cyber advanced supporting infrastructure. Typically, it consists of software, protocols, networks, and other resources to support the monitoring, protection, and control functions. The *impact* on the CPPS is determined by how the various cyber vulnerabilities impact the grid's various power applications to control the physical system.

The cyber-attack on CPPS greatly differs from the traditional cyber-attack on IT systems. While attacker techniques have closely resembled traditional attacks, their ability to impact the grid is heavily dependent on the power system applications or control functions supported by those systems. Fig. 18 shows how the cyber-attack would impact the CPPS [180]. The first step of an attacker is to degrade the availability, integrity, or confidentiality of some portion of the cyber system supporting for CPPS. The degradation impacts some of the power applications/control functions used to support the grid. The attackers ability to manipulate the control functions would then directly lead to the physical system impact.

The power system is generally divided into three major domains, namely, Generation, Transmission, and Distribution. Each domain has its control of specific machines/

TABLE 7. A taxonomy of control loops in the power grid.

Power – Cyber-Physical Systems Control Taxonomy								
		Control Attributes						
Domain	**Control**	**1. Physical Parameter**	**2. Measurements & Inputs**	**3.Data Acquisition**	**4. Control**	**5. Computation**	**6. Machine/ Device**	**7. Control Action**
Generation	Automatic Voltage Regulator	Terminal Voltage	Measured and Reference Terminal Voltage	Local Measurement from Terminal	Local Message to Exciter Control	Calculation of Excitation Current	Generators	Increase/Decrease Exciter Current
	Governor Control	Rotor Speed	Measured and Reference Rotor Speed	Local Measurement from Rotor Speed Sensor	Local Message to Prime Mover Controller	Valve Position	Prime Mover	Open/Close Valve
	Automatic Generation Control	Frequency	Frequency & Tie-Line Power Measurement	Wide-Area Communication (IEC 61850)	Point to Point Communication (DNP 3.0)	Area Control Error (ACE) Calculation	Generators	Raise/Lower Generation
	Security-Constrained Economic Dispatch	Power Generation	Demand, Network Topology, and Line Limits	Wide-Area Communication (IEC 61850)	Point to Point Communication (DNP 3.0)	Generation Set Points	Generators	Generation Re-Dispatch
Transmission	State Estimation	Power Generation and Network Topology	Voltage & Power, VAR or Current-Flow	Wide-Area Communication (IEC 61850)	Point to Point to Switchyards and Generation Stations	System Voltage and Phase Angle Calculation	Generators and Switching Devices	Generation Re-Dispatch and Open/Close Breakers
	VAR Compensation	Voltage	Reference Voltage, Measured Voltage & VAR Device	Local Measurement	Local Message to FACTS Devices	Reactive Power Level Calculation	FACTS	Absorb/Supply Reactive Power
	HVDC Transmission Control	DC Voltage and Current	Reference Voltage & Measured Voltage	Local Measurement of Voltage	Local Message to Converters	Firing Angle	Power Electronic Converters	Increase/Decrease Firing Angle
Distribution	Demand Side Management	Load Scheduling	Demand, Conventional and Alternate Resources Availability	Power Demand Request	Allotted Schedule to Factories and Homes	Load Schedule Computation	Loads	Turn ON/OFF Load
	Load Shedding	Load connected to System	Generation Limit, System Frequency, and Current Generation	Local Frequency Measurement & Generation Level from Control Center	Trip Message to Relays on Distribution Feeder	Load Amount and Location	Distribution Feeder	Open Feeder Breaker
	Advanced Metering Infrastructure	Consumer Load	MDMS/Headend Instructions	NA	Disable/Load Shed	Meter Function	Consumer Meter	Disable Meter/Shed Load

devices, protocols, and communication signals. Therefore, each control system has its threats, vulnerabilities, and impact on CPPS operations. Table 7 presents the classification of control loops based on the domains in CPPS [180].

Fig. 19 shows the cybersecurity life-cycle model for attack resilient Wide-Area Monitoring Protection and Control (WAMPAC) applications in the power grid through a hub-and-spokes model integrating attack deterrence, attack prevention, attack detection, attack mitigation, attack resilience, and attack forensics [56].

Attack Deterrence: The ability of the defender to positively influence the potential adversary not to carry out attacks.

Attack Prevention: The ability of the defender to prevent attacks on the system through risk assessment, risk mitigation, cybersecurity technologies, etc.

Attack Detection: The defender should detect the attack in online/offline mode.

Attack Mitigation: The defender should apply the suitable mitigation technique to maintain the operational status of the system without any violation or degradation in the performance, security, or stability of the grid.

Attack Resilience: If an attack occurs in the system, the system must have adequate resiliency to maintain the operational status of the system, perhaps at a degraded level of performance, security, or stability.

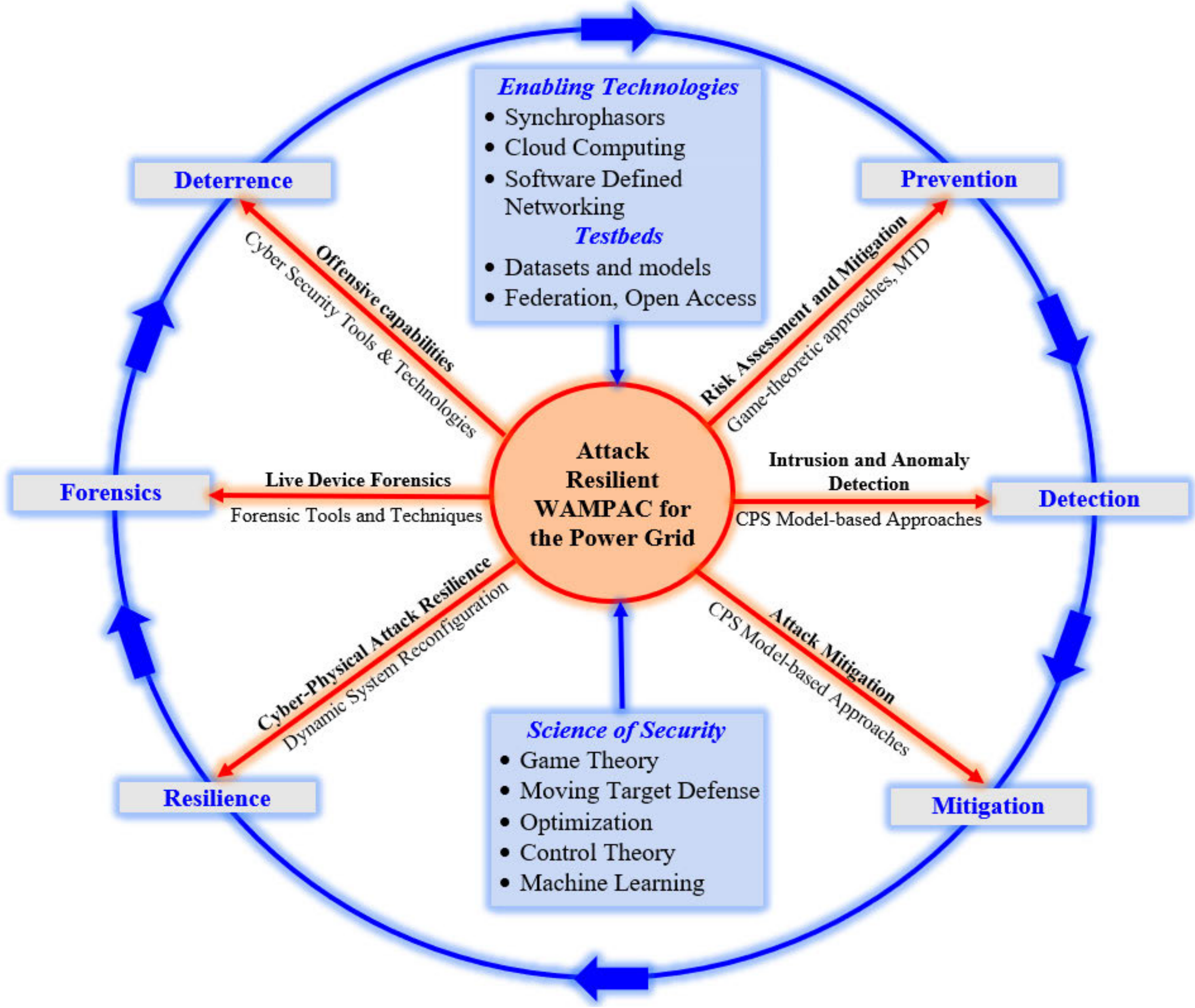
Enabling Technologies
• Synchrophasors
• Cloud Computing
• Software Defined Networking
Testbeds
• Datasets and models
• Federation, Open Access
Deterrence
Prevention
Offensive capabilities
Cyber Security Tools & Technologies
Risk Assessment and Mitigation
Game-theoretic approaches, MTD
Attack Resilient WAMPAC for the Power Grid
Forensics
Live Device Forensics
Forensic Tools and Techniques
Intrusion and Anomaly Detection
CPS Model-based Approaches
Detection
Cyber-Physical Attack Resilience
Dynamic System Reconfiguration
Attack Mitigation
CPS Model-based Approaches
Resilience
Mitigation
Science of Security
• Game Theory
• Moving Target Defense
• Optimization
• Control Theory
• Machine Learning

FIGURE 19. Cyber security life-cycle model.

Attack Forensics: Forensic analysis is useful to determine the originator and source of the attack, which helps to determine future attacks.

Finally, each spoke of the hub-and-spoke model highlights the innovative cyber-security approaches with efficient technologies and enabling scientific tools to prevent the succession of attacks along the cybersecurity life cycle.

Fig. 20 presents the research issues and potential solutions for attaining attack resilience at the infrastructure layer for WAMPAC [56]. Fig. 21 presents the research issues and potential solutions for attaining attack resilience at the application layer for WAMPAC [56]. For both the layers, various issues are listed across the various domains, namely online attack detection, mitigation, resilience, and offline risk assessment & attack prevention. Table 8 lists out the taxonomy of cyber-attack and cybersecurity in CPPS. It should be noted that a coordinated attack also possible where the multiple attacks are combined to enhance the attacking behaviour in CPPS further.

V. CPPS IN THE DEVELOPED COUNTRIES

The CPPS is considered as a next-generation power grid that allows the two-way flow of electricity and information to create a wide distributed automated electrical power delivery network. The CPPS grid is also called a smart power grid, future grid, intelligent grid, inter grid is an enhancement of the 21st-century power grid of the world [248]. The CPPS uses two-way flow, computational intelligence and cyber-secure communication technologies in an integrated manner across the generation, transmission, distribution, and utilization of the electrical power capable of delivering the power in more efficient ways and responds to the wide range of events & conditions anywhere in the grid for the safe, resilient, reliable, sustainable and efficient operation of the power grid. The concept of CPPS started from the idea of a smart grid with the abstraction of AMI that helps to improve the energy efficiency, Demand Side Management (DSM), developing self-healing grid, and resilient grid protection, etc. However, the new demand requirements urged

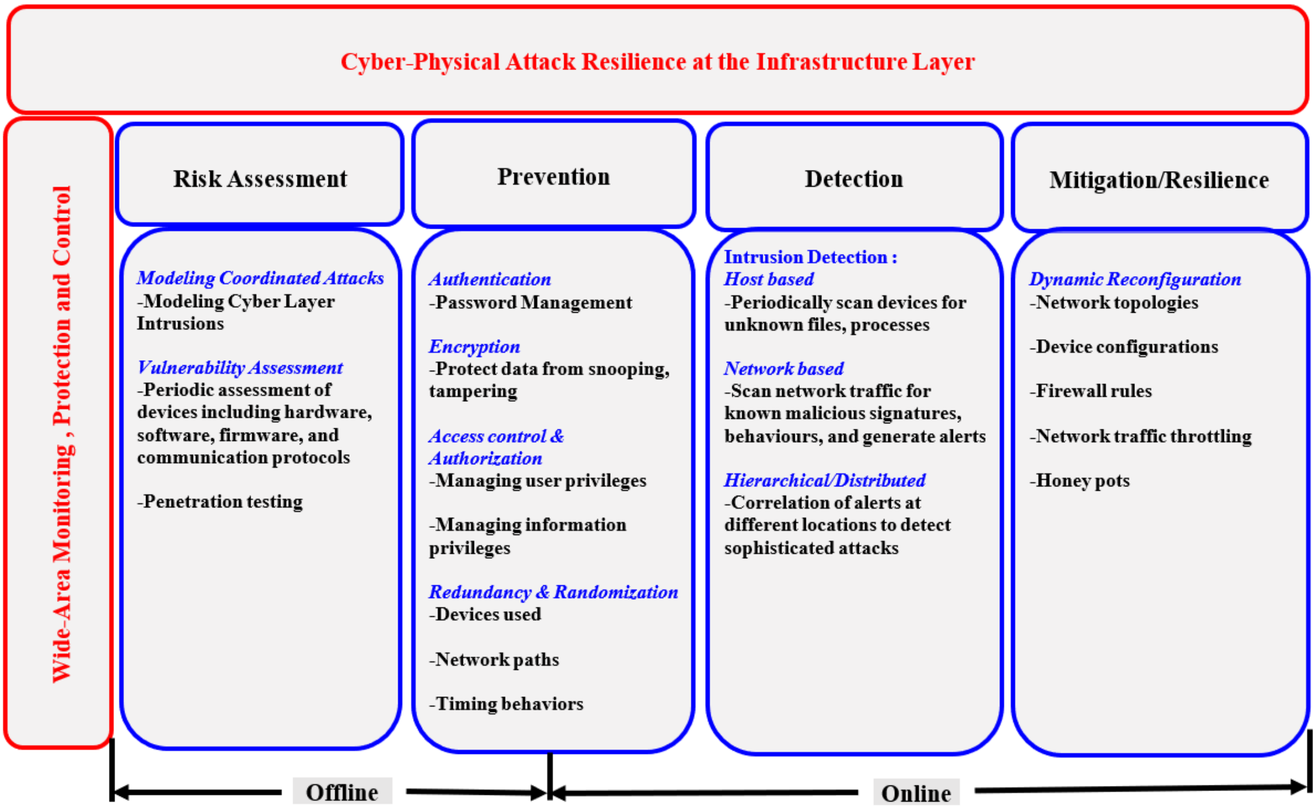
Cyber-Physical Attack Resilience at the Infrastructure Layer
Wide-Area Monitoring , Protection and Control
Risk Assessment
Modeling Coordinated Attacks
-Modeling Cyber Layer Intrusions
Vulnerability Assessment
-Periodic assessment of devices including hardware, software, firmware, and communication protocols
-Penetration testing
Prevention
Authentication
-Password Management
Encryption
-Protect data from snooping, tampering
Access control & Authorization
-Managing user privileges
-Managing information privileges
Redundancy & Randomization
-Devices used
-Network paths
-Timing behaviors
Detection
Intrusion Detection :
Host based
-Periodically scan devices for unknown files, processes
Network based
-Scan network traffic for known malicious signatures, behaviours, and generate alerts
Hierarchical/Distributed
-Correlation of alerts at different locations to detect sophisticated attacks
Mitigation/Resilience
Dynamic Reconfiguration
-Network topologies
-Device configurations
-Firewall rules
-Network traffic throttling
-Honey pots
Offline
Online

FIGURE 20. Infrastructure layer attack resilience.

the power industries, government, and research organizations to rethink and expand the scope of the smart grid to CPPS. The United States Energy Independence and Security Act of 2007 directed to the National Institute of Standards and Technology (NIST) to coordinate the research activities to attain the objectives of smart grid systems and devices. According to the report from NIST [249], the requirements and benefits of the smart grid are the following:

- Enhancing power quality and reliability;
- Effective utilization of facility and preventing construction of back-up power plants;
- Improving the efficiency and capacity of existing electric power networks;
- Enhancing resilience and reliability to disturbances;
- Enabling predictive maintenance and self-healing responses to system disruption;
- Facilitating the expanded deployment of renewable power sources;
- Accommodating centralized and distributed power sources;
- Automating operation and maintenance;
- Enabling EV and renewable power sources to reduce greenhouse gas emissions;
- Avoiding the operation of the inefficient power plant during peak usage periods to reduce oil consumption;
- Presenting opportunities for grid modernization;
- Enabling the transition to new energy storage options and plug-in EVs;
- Increasing customer choice;
- Enabling new services, products, and markets.

With the above benefits of the smart grid, the NIST released another report [250] on the CPS by joint work between the smart grid working group and CPSs working group for the energy domain. From this report the main characteristics of CPS that support for the efficient operation of CPPS that goes beyond conventional product, system, and application are

- The combination of the physical and the cyber, and their interconnectedness, is essential to CPS.
- A CPS maybe a System of Systems (SoS).
- Emergent behaviours are to be expected of CPS due to the heterogeneous nature of CPS composition.
- CPS needs a methodology to ensure interdependency, dealing with prominent effects, and managing evolution.
- CPS may be designed for multi-purpose applications.
- CPS is noted for enabling cross-domain applications.
- CPS potential impact on the physical system and their interconnectedness with them raised the concern about trustworthiness.
- CPS should be freely composable.
- CPS must be able to accommodate continuous and discrete computational models.

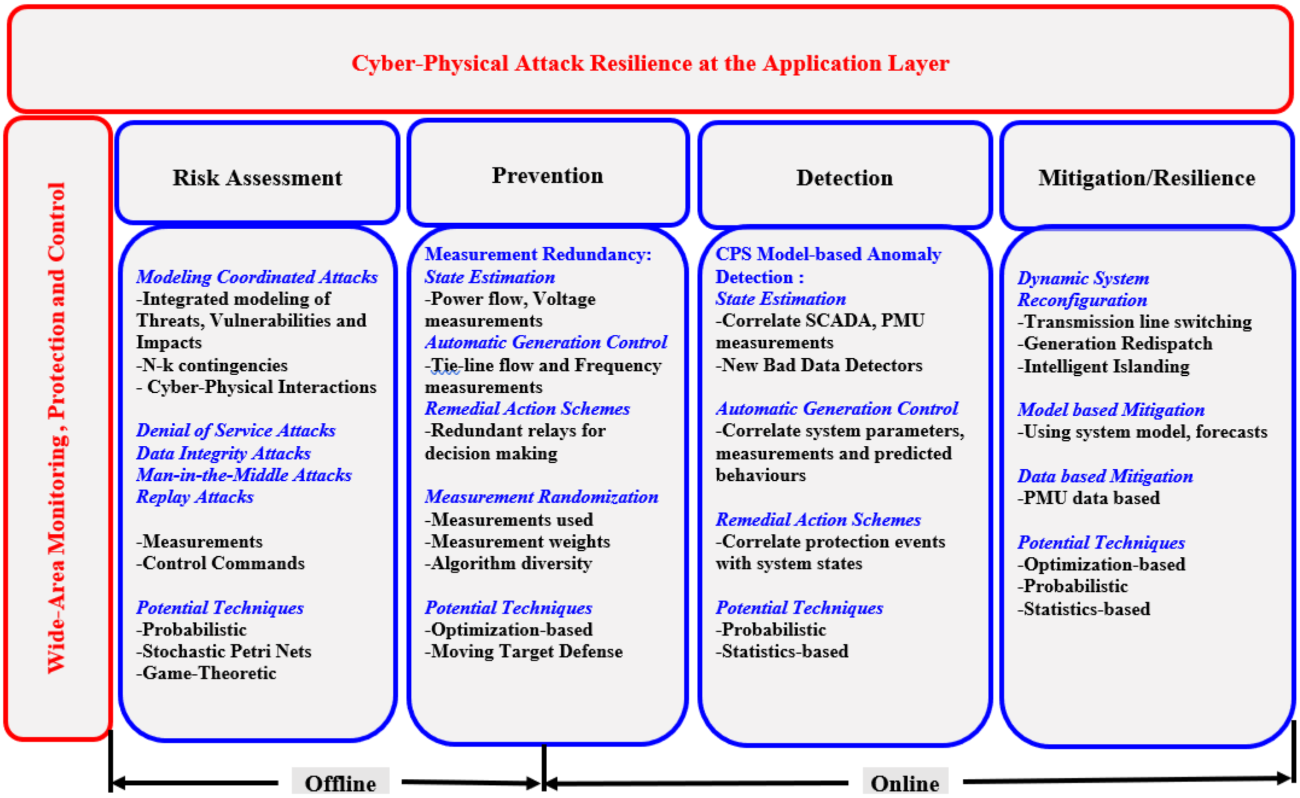
Cyber-Physical Attack Resilience at the Application Layer
Wide-Area Monitoring, Protection and Control
Risk Assessment
Prevention
Detection
Mitigation/Resilience
Modeling Coordinated Attacks
-Integrated modeling of Threats, Vulnerabilities and Impacts
-N-k contingencies
- Cyber-Physical Interactions
Denial of Service Attacks
Data Integrity Attacks
Man-in-the-Middle Attacks
Replay Attacks
-Measurements
-Control Commands
Potential Techniques
-Probabilistic
-Stochastic Petri Nets
-Game-Theoretic
Measurement Redundancy:
State Estimation
-Power flow, Voltage measurements
Automatic Generation Control
-Tie-line flow and Frequency measurements
Remedial Action Schemes
-Redundant relays for decision making
Measurement Randomization
-Measurements used
-Measurement weights
-Algorithm diversity
Potential Techniques
-Optimization-based
-Moving Target Defense
CPS Model-based Anomaly Detection :
State Estimation
-Correlate SCADA, PMU measurements
-New Bad Data Detectors
Automatic Generation Control
-Correlate system parameters, measurements and predicted behaviours
Remedial Action Schemes
-Correlate protection events with system states
Potential Techniques
-Probabilistic
-Statistics-based
Dynamic System Reconfiguration
-Transmission line switching
-Generation Redispatch
-Intelligent Islanding
Model based Mitigation
-Using system model, forecasts
Data based Mitigation
-PMU data based
Potential Techniques
-Optimization-based
-Probabilistic
-Statistics-based
Offline
Online

FIGURE 21. Application layer attack resilience.

- CPS must also support different modes of communication.
- The heterogeneity and interdependency of CPS lead them to exhibit a wide range of complexity.
- Cyber and Physical system time synchronization is a sensitive component to CPS, and its centralized architecture is a major concern.
- CPS is characterized by the interaction between the cyber and physical systems with their operating environment.

To promote the smart grid/CPPS deployment activities, government, industry, academia, and research organizations had spent a lot of money and efforts in pilot projects, smart grid programs, and field studies. To help the readers about the recent progress in CPPS, we summarized the major projects, programs & trials related to the smart grid/CPPS is presented in Table 5. It covers Smart Meter, AMI, Transmission Grid, Micro Grid, DERs, EV, and Integrated Systems, etc. From Table 9, it is inferred that most of the countries had spent a significant investment for deployment of Smart Grid/CPPS technologies and applications, but their integration is the new challenge.

VI. OUTLOOK OF THE FUTURE CPPS

In general, the CPPS is a complex networked system that has impacted the way electrical energy generated, transmitted, and utilized. The electrical energy systems have evolved through the years from the conventional power systems to the smart grid and further explored CPSs in energy (CPSE) with the consideration of primary energy and end-use energy phases, as shown in Fig. 22 [265].

The future energy systems need a holistic approach (systems-of-systems) for modelling, simulation, and analysis. The various power grid blackouts occurred in worldwide are due to the malfunctioning of the grid components (generator, transmission lines, load buses, communication facilities, etc.) and the increasingly stringent constraints on carbon emissions regulations, market volatility. To prevent the system-wide blackouts, it requires ICTs at a level higher than the existing smart grid can offer. The CPPS has already advanced than the smart grid environment and serves to be more reliable for the holistic (systems of systems) approaches to the smart grid problem, but it has not gone far enough. The future energy systems should consider the coordination of various generalized environmental factors, social factors, economic factors, human behaviors, as well as hybrid research framework with different time and scales. This involves the varieties of large data with hidden relationships in the complex economical, technological, social, and environmental dimensions.

The economic and societal potential of CPPS can be realized by a new concept of Cyber-Physical-Social Systems (CPSS). The CPSS lies at the intersection of the *physical* electric power systems, *the cyber* system market and

TABLE 8. Taxonomy of cyber-attack and cyber security in CPPS.

Taxonomy of CPPS	
Cyber Attack Types	1. Data Tampering Attack [181][191][46] 2. Man-in-the-Middle Attack (MITM) [181][169][200][46][205][220] 3. Replay Attack [181][195][199][46][207][209][217][221][227] 4. Denial of Service (DoS) Attack [181][169][200][46][205][212][220][227] 5. False Data Injection Attack [87][184][188][190][191][197][198][199][211][214][217][220][52] 6. Switching Attack [32][129][134][145] 7. Data Integrity Attack [184][187][188][46] 8. Data Availability Attack [184][188][46] 9. False Negatives Attack [188] 10. False Alarm Attack [188] 11. Stealthy Attack [193][198][204][211][217] 12. Masquerade Attack [195] 13. Time Delay Attack [196][169][206] 14. Disordered Data Attack [196] 15. Dropped Data Attack [196] 16. Communication Line Outage (CLO) Attack [196][205] 17. Spoofing Attack [200][46][194] 18. Repudiation Attack [194] 19. Information Disclosure Attack [194] 20. Elevation of privilege Attack [194] 21. Load Altering Attack [242] 22. Eavesdropping Attack [200][46][221][227] 23. Modification Attack [46] 24. Reconnaissance Attack [46] 25. Confidentiality Attack [46] 26. Load Redistribution Attack [197][208][149][226] 27. Economic Attack [197] 28. Energy Deceiving Attack [197] 29. Device-Failure Attack [203] 30. Password-Cracking Attack [203] 31. Authentication-Identifying Attack [203] 32. Worm Attack [203] 33. Communication Congestion Attack [192] 34. Noise-Injection Attack [207][210] 35. Destabilization Attack [210] 36. Topology Preserving Attack [208][149] 37. Malware-Induced Attack [182][87][209][243] 38. Covert Attack [217] 39. Command-Injection Attack [207][210] 40.Aurora Attack [207] 41. Jamming Attack [219] 42. Smurf Attack [216] 43. Neptune Attack [216] 44. Teardrop Attack [216] 45. Pod Attack [216] 46. Mail Bomb Attack [216] 47. Upstorm Attack [216] 48. Apache Attack [216] 49. Probing Attack [216] 50. User-to-Root Attack [216] 51. Remote-to-login Attack [216] 52. Data Spoofing Attack [200] 53. Compressed Key Attack [221] 54. Privacy Attack [221][241] 55. Unauthorized Access Attack [182][201] 56. Spear Phishing Attack [182] 57. Data Deception Attack [199][212] 58. Payload Attack [229] 59. Ransomware Attack [229] 60. GPS Spoofing & Jamming Attack [229] 61. Theft of Cryptographic Key Attack [229] 62. Time-Synchronization Attack [229] 63. Stuxnet Attack [172][201]
Cyber Attack Detection Methods	1. State Estimation Based Detection [188][191][197][211][52][246] 2. Machine Learning Based Detection [189][191] 3. Time Series Prediction Based Detection [191] 4. Bad Data Detection [188][197][211][52][227]

TABLE 8. ***(Continued.)*** **Taxonomy of cyber-attack and cyber security in CPPS.**

	5. Dynamic Model Based Detection [203] 6. Correlation Based Detection [203] 7. Distributed Detection [203][217] 8. Anomaly Detection Using Machine Learning [213][214][222][56] 9. $\mathcal{X}^2$ Detector [239][246] 10. Binary Hypothesis Method [246] 11. Model-Free Detection Method [246] 12. Watermarking method [246] 13. Attack Space Search Method [246] 14. Convex Relaxation Method [246] 15. Kalman Filter-Based Method [239][246] 16. Observer-Based Method [246] 17. Intrusion Detection System [186][202] 18. Gaussian Mixture Model-Based Method [187] 19. Variable Mode Decomposition and Online Sequential ELM (OS-ELM) [189] 20. Margin Settling Algorithm [190] 21. Security Threat Analysis in CPS [1] 22. Adaptive CPS Attack Detection [199] 23. Game-Theoretic Attack Detection [46] 24. Cooperative Vulnerability Framework (CVF) Attack Detection [204] 25. Anti-Malware Scanning [209] 26. Anomaly-Based Attack Detection and Identification [215] 27. Model-Checking Based Detection Algorithm [216] 28. Centralized and Distributed Attack Detection System [217] 29. Hybrid Attack Detection System [223] 30. Attack Resilient WAMPAC [56] 31. Cyber-Physical Attacks and Defences [226] 32. DDOA Model-Based Threat Detection Method [234] 33. Dynamic Characteristics Analysis Based Attack Detection [235] 34. Mixture Gaussian Distribution Learning Method Based Attack Detection [236] 35. Graph Signal Processing Based Attack Detection [238] 36. Kalman Filter-Based Attack Detection [239] 37. Area Control Error (ACE) Based Cyber-Attack Detection and Mitigation Platform (CDMP) [240] 38. Moving Target Defence Approach [244]
Cyber Attack Mitigation Methods	1. Data Analytics Approach to FDIA [190] 2. Cyber Defence to FDIA [203] 3. Cyber-Physical Fusion Defence [203] 4. Replay and Masquerade Attack Mitigation [195] 5. Defence-in-Depth Approach [184][232] 6. SNR Estimation [184] 7. Dynamic Watermarking-Based Defence [210] 8. Moving Target Defence [211][232] 9. ARCADES: Analysis of Risk from Cyber Attack Against Defensive Strategies [247] 10. Game-Theoretic Graph Colouring Technique [185] 11. Game-Theoretic Analysis [145] 12. Real-Time and Adaptive Defence Mechanisms Based on Data Aggregation [193] 13. Real-Time Assessment and Mitigation [206] 14. Attack Detection and Mitigation Using Machine Learning [214] 15. Stochastic Game-Based Analysis [218] 16. Cognitive Risk Control for Mitigating Cyber Attack [52] 17. Attack Resilient WAMPAC [56] 18. Cyber-Physical Attacks and Defences [226] 19. Highly Resilient Communication Architecture for a Smart Grid [227] 20. Multiple Level Cyber Defence Model for Attack Mitigation [231] 21. PMU Based Attack Mitigation [237] 22. Area Control Error (ACE) Based Cyber-Attack Detection and Mitigation Platform (CDMP) [240] 23. Attack-Mitigation Dynamic Game-Theoretic Scheme for Security Vulnerability Analysis in CPPS [245]
Cyber Attack Risk Analysis	1. STRIDE Risk Analysis – Spoofing, Tampering, Repudiation, Information Disclosure, Denial-of-Service, Elevation of Privilege [194] 2. DREAD Risk Ranking – Damage, Reproducibility, Exploitability, Affected Users, Discoverability [194] 3. Cyber Security Insurance Model [183] 4. Attack Resilient WAMPAC [56]

TABLE 8. ***(Continued.)*** **Taxonomy of cyber-attack and cyber security in CPPS.**

	5. Competitive Markov Decision Process [225] 6. Security Threat Analysis in CPS [1] 7. Attack Resilient WAMPAC [56] 8. Assessment and Management of Security Risk in Network Control Systems [230]
Cyber Attack Threat Modelling	1. Cyber-Physical Modelling and Assessment (CPMA) Framework [87] 2. Game-Theoretic Graph Colouring Technique [185] 3. Gaussian-Mixture Model-Based Detection Scheme (GMMD) [187] 4. STRIDE Threat Model [194] 5. System Theoretic Approach [201] 6. Security Threat Analysis in CPS [1] 7. Real-Time Assessment and mitigation [206] 8. Stochastic Game-Based Analysis [218] 9. Holistic Attack-Resilient Framework [57] 10. DDOA Model-Based Threat Detection Method [234]
Cyber Attack Vulnerability Assessment	1. Cyber-Physical Modelling and Assessment (CPMA) Framework [87] 2. Game-Theoretic Graph Colouring Technique [185] 3. Margin Setting Algorithm [190] 4. Component-Wise Vulnerability Analysis to System-Wide Impact Analysis [46] 5. Anomaly-Based Attack Detection and Identification [215] 6. Resilient Control Formulation [220] 7. CPINDEX – A Security Oriented Stochastic Technique [48] 8. Testbed Based Vulnerability Assessment [224] 9. Cyber-Physical Attacks and Defences [226] 10. Control Loop Vulnerabilities in the Electric Power Grid [228] 11. Cyber Vulnerabilities in Distributed Electric Power Systems [232] 12. Vulnerabilities in General CPS [233] 13. Attack-Mitigation Dynamic Game-Theoretic Scheme for Security Vulnerability Analysis in a CPPS [245]

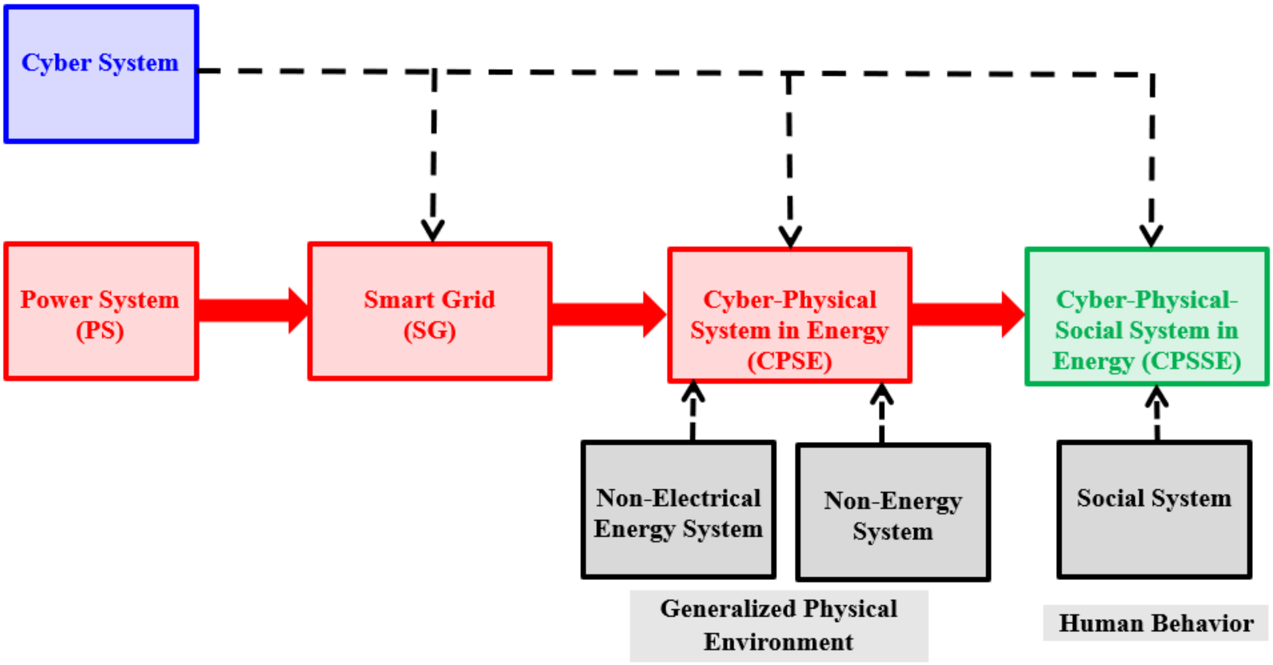
Cyber System
Power System (PS)
Smart Grid (SG)
Cyber-Physical System in Energy (CPSE)
Cyber-Physical-Social System in Energy (CPSSE)
Non-Electrical Energy System
Non-Energy System
Social System
Generalized Physical Environment
Human Behavior

FIGURE 22. **Evolution of energy systems.**

control layer, and *social* residential end-users, as shown in Fig. 23 [266]. The CPSS encompasses the physical system, ICTs infrastructure, human behavior, and changes the way people interact with the complex interdependent systems. The general concepts of CPSS are shown in Fig. 23, in which the Social System plays a critical part in such an interdependent system. Social Systems include customer behaviors, policy, regulation, and economics. The new concept of CPSS in the energy sector comprises primary energy, secondary energy, and end-user energy in a broader framework but not limited to, other essential factors to be considered such as intermittent DERs, influence of market operations, transition in primary energy sources and end-user behaviors [265]. The enabling technologies for CPPS development are the Internet

TABLE 9. A summary of major projects/programs/trials related to smart grid/CPPS.

SI. NO	Project/Program Name	Organization	*Country	Period	Description of the Project / Program / Trial	Project/Program/Trial Category
1.	NSGM Smart Grid Projects and Smart Grid Pilot Projects [251]	National Smart Grid Mission (NSGM)	IN	From 2015	To accelerate smart grid deployment in India through smart meters, AMI, Medium-sized microgrids, Distributed generation by rooftop PVs, Real-time monitoring and control, Power quality improvement measures, and Creation of EV Charging Infrastructure, etc.	Smart meter and AMI
2.	Energia AG Smart Metering Project AMIS [252]	NETZGMBH	AT	From 2005 to 2013	To implement efficient process automation for saving money and gain additional revenues.	Smart meter and AMI
3.	Smart Grids for Industry (Smart Energy Solutions) [252]	Smart Grid Flanders	BE	From 2012 to 2014	To awaken the consciousness of the utility and the consumer about the benefits of modernization of grid infrastructure.	Smart Grid Structure
4.	Power Shift Atlantic- Phase I [252]	Maritime Electric, New Brunswick Power, Saint John Energy, Nova Scotia Power	CA	From 2010 to 2012	Designed the world's first fully grid-integrated Virtual Power Plant (VPP) to allow more integration of wind power.	Integrated system
5.	Power Shift Atlantic- Phase II [252]	Maritime Electric, New Brunswick Power, Nova Scotia Power, Saint John Energy,	CA	From 2012 to 2015	Designed the world's first fully grid-integrated VPPs to allow more integration of wind power.	Integrated system
6.	Green Button: Enabling Consumer Empowerment in Ontario [252]	Ministry of Energy and MaRS Discovery District	CA	From 2012	With the help of innovative smart grid technology, the energy usage data is given to the families and business direct, through a secure data communication transfer from their utility's website.	Integrated system
7.	Consumer engagement in the future power ISGAN system: EcoGrid [252]		DK	From 2011 to 2015	The objective of this project is to allow small-scale/residential consumers to participate in the power market by active demand response for balancing renewable power generation.	Smart meter and AMI
8.	Power Matching City Phase II [252]	DUTCH COMPANIES	DK	From 2011 to 2014	To implement the decentralized power production through modernized smart grid infrastructure and democratizing the energy market.	Smart Grid Structure
9.	(S3C) : Smart Consumer - Smart Customer - Smart Citizen [252]	Vito, European Union	EU	From 2012 to 2015	To encourage the smart energy behaviour of households via active end-user participation.	Smart Grid Structure
10.	Large-Scale Demonstration of European Smart Distribution Networks GRID4EU [252]	Électricité Réseau Distribution France (ERDF)	EU	From 2011 to 2016	To integrate the massive decentralized DERs (photovoltaic generation) on the low voltage grid.	Integrated system
11.	Smart Electric Lyon [252]	EDF	FR	From 2012 to 2016	To test the smart grid applications in realistic conditions with real clients to assess their conditions of acceptance.	Smart Grid Structure
12.	Nice Grid the French Demonstrator of GRID4EU [252]	Electricitre Research Distribution France (ERDF)	FR	From 2011 to 2016	To test the impact of DERs on a low voltage grid to improve the quality of service and efficiency in the smart grid (voltage).	Smart Grid Structure
13.	Modelec [252]	DIRECT-ENERGIA	FR	From 2011 to 2014	To test the impact of retail customer's DR on the times of peak demand consumption.	Smart meter and AMI
14.	Millener [252]	French Government and EDF	FR	From 2011 to 2014	To encourage DSM and control in individual households.	Smart meter and AMI
15.	Greenlys [252]	ERDF	FR	From 2012 to 2016	To develop advanced technological applications for the widespread deployment of smart grids by 2016.	Smart meter and AMI
16.	Energy Pool [252]	Delmarva Power	FR	From 2012 to 2015	To create an energy pool with balanced generation and load demand and making it smarter and cleaner.	Integrated system

TABLE 9. ***(Continued.)*** **A summary of major projects/programs/trials related to smart grid/CPPS.**

17.	Venteea [252]	Électricité Réseau Distribution France (ERDF)	FR	From 2012 to 2016	To create the best environment for technically and economically efficient integration of renewable energy sources, particularly wind power plants in rural medium voltage distribution networks.	Integrated system
18.	Smart Operator [252]	RWE Deutschland & Lechwerke AG	GE	From 2012 to 2015	To enable smart grid control for smart household appliances.	Integrated system
19.	Achieving sustainability with Advanced Metering Infrastructure – my energy Program [252]	CLP Power Hong Kong Ltd.	HK	From 2013 to 2015	To install AMI systems in Hong Kong that works from the billing system to customer payment through mobile and web channel.	Smart meter and AMI
20.	Consumer Reward Scheme [252]	Tata Power Pvt Ltd	IN	From 2014 to 2015	To offer value-added services to TATA power consumers under the consumer reward scheme.	Smart meter and AMI
21.	ADSM-(Automated Demand Side Management) Expansion Project with Reliance Energy [252]	Innovari & Reliance Infrastructure Limited	IN	From 2014 to 2015	To introduce utility-owned automated demand management assets.	Smart meter and AMI
22.	DS3 - Delivering A Secure, Sustainable Electricity System [252]	EirGrid Group	IR	From 2011 to 2020	To enable a secure and sustainable electricity delivery system programme in Ireland and Northern Ireland.	Smart Grid Structure
23.	Lambrate Smart Grid Project [252]	A2A Reti Elettriche	IT	From 2011 to 2015	To implement automatic fault detection and isolation system, with the objective of reducing the number of long and short interruptions (SAIFI &SAIDI).	Smart Grid Structure
24.	Development And Control Of Hybrid Gen. Set In Smart Microgrids [252]	University of Cagliary	IT	From 2014 to 2015	To realize the hybrid generation system by the integration of DERs for off-grid applications and grid-connected end-users based on the exploitation of traditional renewables, diesel generators, and storage.	Integrated system
25.	Incentive type DR pilot project in Japan [252]	Tokyo Electricity & Power Company & Ministry of Economic Trade and Industry of Japan	JP	From 2013 to 2014	To research and evaluate the effectiveness and economics of distributed renewables, including the performance of the generating system.	Integrated system
26.	Eco-Megane Plus [252]	NTT Smile Energy Inc. (NSE)	JP	From 2014 to 2015	To analyze the data to detect any malfunctioning of PV facilities.	Integrated system
27.	Keihanna Eco City Project (KECP) [252]	Kyoto Prefectural Government	JP	From 2014 to 2015	To verify the effect of energy-saving measures and CO2 emission reduction.	Integrated system
28.	AMI Polanco [252]	Comision Federal de Electricidad	ME	From 2011 to 2012	To deploy smart meters for reducing the technical and non-technical losses during transmission.	Smart meter and AMI
29.	Your Energy Moment (Jouw Energie Moment) [252]	ENEXIS	NL	From 2013 to 2016	To optimize the methodology for households to shift the electricity demand in time to match supply conditions.	Smart meter and AMI
30.	Smart Meter Deployment Project [252]	Nma (Dutch Energy Regulator), NL Agency	NL	From 2012 to 2014	To develop and integrate an Act which mandates net operators to offer small businesses and households with minimal technical and functional requirements of a smart meter.	Integrated system
31.	InovGrid [252]	EDP Distribuição	PT	From 2011 to 2014	To implement the smart grid technology in the distribution grid system for more efficient and better network management with enhanced consumer awareness in electrical grid information.	Integrated system

TABLE 9. ***(Continued.)*** **A summary of major projects/programs/trials related to smart grid/CPPS.**

32.	Shinan Microgrid Project [252]	KEPRI (KEPCO)	SK	From Feb.2014 to Nov.2014	To verify the operation of a microgrid by controlling the Energy Storage System (ESS) with grid-independent (GI) and grid-connected (GC) mode.	Integrated system
33.	Smart Grid Station of KEPCO [252]	Korea Electric Power Corporation (KEPCO)	SK	From Jan.2014 to Dec.2014	To set the target of reducing 30% greenhouse gases by 2020 and response to climate change.	Integrated system
34.	Construction of Gapado Carbon Free Island [252]	Jeju Special Self-Governing Province	SK	From 2011 to 2013	To implement smart grid technology for standalone power system development.	Integrated system
35.	Zem2All (Zero Emission Mobility to All) [252]	NEDO (Japan), City of Malaga and CDTI (Spain)	SP	From 2012 to 2015	To understand the impact and management of urban electric mobility.	Integrated system
36.	EMPOWERING [252]	GEG(France), LinZAG(Austria), El Gas(Spain), IREN(Italy), Intelligent Energy Europe Programme of European Union	SP	From 2013 to 2015	To help the customers by informing them about the meter reading and billing information frequently for saving energy and money.	Smart meter and AMI
37.	Smart Kund Gotland- Smart Grid Gotland [252]	Gotlands Energi AB and Swedish Energy Authority	SE	From 2012 to 2016	To be excellent in smart grid consumer empowerment and engagement through smart pricing and control.	Smart meter and AMI
38.	Karehamn_ Increasing Feed-In of Renewables [252]	E.ON	SE	From 2013 to 2014	Integration of E.ON’s power grid with 48MW Karehamn wind farm for more generation of power.	Smart Grid Structure
39.	Siemens Smart Multi-Dwelling Unit Solution- Phase I [252]	SIEMENS	UK	From 2012 to 2014	To facilitate the smart-metering facilities and improve metering connectivity for consumers living in multi-dwelling units across the UK.	Smart meter and AMI
40.	Siemens Smart Multi-Dwelling Unit Solution- Phase II [252]	SIEMENS	UK	From 2012 to 2014	Locating different MDUs and its capacities in the UK.	Smart Grid Structure
41.	PG&E Optimal Time-Varying Pricing [252]	PG&E	USA	From 2012 to 2015	PG&E has created a program for their customers to have an ability during critical peak days to opt-in for variable and time of day pricing.	Smart meter and AMI
42.	PG&E Company’s My Energy Tool [252]	PG&E	USA	From 2012 to 2015	PG&E has created a program for the customers to make personal decisions about their energy usage.	Smart meter and AMI
43.	Pacific Gas & Electric’s Smart Grid [252]	PG&E	USA	From 2012 to 2015	PG&E SmartMeter	Smart meter and AMI
44.	JUMPSmart Maui Project (JSM) [252]	NEDO, County of Maui	USA	From 2011 to 2015	To implement the smart grid technology for the development of EV and efficient use of DERs for low CO2 emissions.	Integrated system
45.	A capacity market that incentivizes smart and Green Technology investment [252]	PJM	USA	From 2011 to 2012	To develop the generation, transmission, and demand-side resources by creating long term price signals to stimulate investments.	Integrated system
46.	Know Your Own Power [252]	Central Maine Power (CMP)	USA	From 2012 to 2015	To suggest the most cost-effective programs, based on the price comparison report, which compares the costs from standard and time of use (TOU) pricing programs.	Integrated system
47.	Peak Energy Savings Credit (PESC) [252]	Delmarva Power	USA	From 2012 to 2015	To help the customers by reducing their energy consumption during peak demand period.	Smart meter and AMI
48.	Vermont Weather Analytics Center Project [252]	Vermont Electric Power Company (VELCO)	USA	From 2014 to 2016	To utilize the data-driven based analytical model for optimal integration of DERs and increase the grid reliability.	Integrated system
49.	USA-Japan Demonstration Smart Grid Project In Los Alamos, New Mexico [252]	Los Alamos County Department of Public Utilities	USA	From 2012 to 2015	To analyze the performance of 1 MW PV array solar panels from 10 different manufacturers for various operating conditions.	Integrated system

TABLE 9. ***(Continued.)*** **A summary of major projects/programs/trials related to smart grid/CPPS.**

50.	Grid-Tied Solar System For Green School [252]	Energy Conservation Center Ho Chi Minh City	VI	From Oct.2014 to Dec. 2014	To improve the student awareness on energy savings and make them understand the growing energy requirements whilst creating a showcase of a 2240Wp grid-tier solar system.	Integrated system
51.	Acea Distribuzione Smart Metering in Rome [253]	Acea Distribuzione	IT	From 2004	To improve the energy efficiency in Italy's capital through efficient operation control and the ability to monitor medium and low voltage line status automatically.	AMI and Smart meter
52.	ATC PMU Project [254]	American Transmission Company (ATC)	US	2010-2012	The main objective is to build the fibre optics communication network for high-speed transmission of PMU data across ATC transmission system	Transmission grid
53.	Austin Energy Smart Grid [255]	Austin Energy	US	From 2003	The first fully operational smart grid deployment in the US. By the on-line and real-time meter readings, it offers improved customer services, smart management of customer appliances and remote service turn-on and turn-off.	Integrated system
54.	CERTS Microgrid Test Bed Demonstration [256,257]	American Electric Power	US	From 2006	To enhance the smooth integration of DERs into the microgrid.	Microgrid and Integrated system
55.	DLC+VIT4IP [258]	Kema Nederland BV	AT, GE, UK, IT, NL, IL, BE	From 2010 to 2013	To develop, verify, and test the advanced power line communication using Internet Protocol (IP) for power system applications.	Communication and information systems
56.	EU-DEEP [258]	GDF Suez	GR, FR, GE, UK, ES, BE, SE, LV, PL, HU, AT, IT, CY, FI, TR, CZ	From 2004 to 2009	To enhance the smooth integration of DERs in Europe.	Integrated system and distributed resources
57.	Fenix [258]	Iberdrola Distribution '	UK, ES, SI, GE, AT, NL, RO, FR	From 2005 to 2009	To maximize the integration of DERs in the grid through aggregation into large-scale VPPs and decentralized energy management.	VPP and Integrated system
58.	Grid4EU [258]	ERDF	GE, ES, SE, IT, CZ, FR	From 2011 to 2015	To test the technologies and real innovative system concepts for smart grid deployment.	Integrated system
59.	INOVGRID [258]	EDP Distribution SA	PT	From 2007 to 2011	To replace the traditional low voltage meters into electronic devices with automated meter management standards.	Integrated system and home application
60.	IntelliGrid [259,260]	Electric Power Research Institute	US	From 2001	The main objective is to develop the new advanced electrical power delivery infrastructure that integrates computing, communication, and control to meet future energy demands.	Other
61.	Large-scale demonstration of charging of EVs [258]	ChoosEV A/S	DK	From 2011 to 2013	To develop the environment-friendly electric vehicle charging station.	Integrated System, EV, and Smart meter & AMI
62.	Model City Manheim [258]	MW Energie	GE	From 2008 to 2012	To develop the E-Energy project for urban area development through a large extent of distributed energy resources integration.	Integrated system
63.	More Microgrids [258]	National Technical University of Athens/ ICCS	GR, ES, NL, PT, DK, IT, GE, MK	From 2006 to 2009	The main objective is 1) To develop the advanced control techniques for DGs 2) To integrate the microgrids into the existing operational power grid 3) To test the control strategies in the actual microgrid and 4) To quantify and analyze the impact of microgrid operation on the power grid.	Integrated system, Microgrid, Smart meter, and AMI, Distribution Grid and Home application
64.	Pacific Gas and Electric Company's Smart Meter Program [261]	Pacific Gas and Electric Company	US	From 2006	To upgrade California's energy infrastructure with automated metering technology.	Smart meter and AMI

TABLE 9. ***(Continued.)*** **A summary of major projects/programs/trials related to smart grid/CPPS.**

65.	Pacific Northwest Smart Grid Demonstration Project [262]	Bonneville Power Administration	US	From 2010 to 2014	The main objective is 1) To validate the new smart grid technologies and business models 2) To provide two-way communication in the existing grid infrastructure 3) To quantify the smart grid costs and benefits and 4) To develop the standards for cybersecurity in power systems.	Integrated system
66.	Smart Grid City, Boulder, Colo [263]	Xcel Energy	US	2008-2010	The main objective is to explore the different smart grid tools for real-world problems.	Integrated system, smart meter and AMI
67.	Smart Grid Demonstration Project in Sino-Singapore Tianjin Ecocity [264]	Tianjin Electric Power Company	CN	2010-2011	To build a smart power supply network with 110kV and 220kV transmission grid, 380V/220V low voltage distribution grid, and 10-35kV distribution lines.	Integrated systems

*Country Codes: AT-Austria, BE-Belgium, CA-Canada, CN-China, CY-Cyprus, CZ-Czech Republic, DK-Denmark, EU – European Union, FI-Finland, FR - France, GE – Germany, GR-Greece, ES-Spain, Hong Kong – HK, HU-Hungary, IL-Israel, Ireland – IR, IN-India, IT-Italy, JP – Japan, LV-Latvia, MK-Macedonia, ME - Mexico, NL-Netherlands, RO-Romania, PL-Poland, PT-Portugal, SE-Sweden, Sl-Slovenia, SK – South Korea, SP – Spain, TR-Turkey, UK-United Kingdom, US-United States, VI – Vietnam.

of Things, Big data, Cloud Computing, Network Systems, etc. For the CPSSE, the additional enabling technologies includes economics, social science, environmental science, cognitive science, psychology, and political science. This enhances the CPSS in the energy system, and it can be seen as a part of the journey from the power system to the smart grid, CPSE to CPSSE, as shown in Fig. 21. The driving force in CPSSE is induced by the interaction between them, which is much more powerful than the individual and internal driving forces of energy systems, information systems, and human societies. All these factors are critical for the successful implementation of CPSS in energy future.

VII. CURRENT ISSUES AND RESEARCH DIRECTIONS

- The impact of the communication network effects such as latency, outliers, missing data, etc on performance, reliability, and security of the CPPS may be considered. This area of research is emerging and likely to see more contributions in the near future.
- The traditional CPPS communication networks have been designed to cover separate parts rather than the whole power grid. Therefore an interconnected communication network for generation, transmission, and distribution to be designed and its network topology should be optimized considering 5G technology.
- The traditional deterministic type N-1 contingency analysis was not suitable for CPPSs. Therefore stochastic cyber-physical contingency analysis should be developed and analysed for the CPPS. More research is needed in this area.
- In cybersecurity for CPPS, fast authentication is an open problem and there is a wide scope for this research work.
- Developing the testbed for CPPS to analyse the effects of cyber events such as communication failures and cyber-attacks due to single or coordinated failures on the physical power system for the specific application is another emerging research area. The testbed 5G technology can be demonstrated for future CPPSs and also we can include other types of energy systems such as heat, gas, etc.
- Estimating the cost of cyber attacks on CPPS at the national level for critical infrastructure protection is an important research area in the economic analysis of power systems.
- An advanced data-driven method with machine learning applications for CPPS in power system control area is emerging. It includes the hybrid data fusion of cyber and physical systems to monitor the stability of CPPS.
- Analysing the impact of the integration of renewable energy systems and electric vehicles in CPPS. Based on this a cyber-physical security analytics should be developed for the holistic cyber-physical transactive energy systems.
- Cyber resilience is the ability of CPPS to prepare, respond, and recover when cyber attacks happen. In addition to power system resilience the cyber system resilience also should be considered for developing control and operation methods and planning strategies to improve power grid resilience against physical and cyber events. A cyber-physical resilience metrics, evaluation methods, development of universally accepted standard definitions are needed for CPPS and there is a wide-scope for this research topic.

VIII. CONCLUSION

CPPS is a new technology that integrates cyber systems and physical power systems to achieve high efficiency and performance. In recent years, research studies on CPPS modelling, simulation, and analysis have gained considerable attention. A grand challenge in CPPS research is the development of models that elegantly interface the continuous-time characteristics of the physical system with the discrete-time characteristics of the cyber system. A review on modelling methods, simulation tools, cyber-attack types, cyber-attack detection and mitigation countermeasures in CPPS are summarized in this paper.

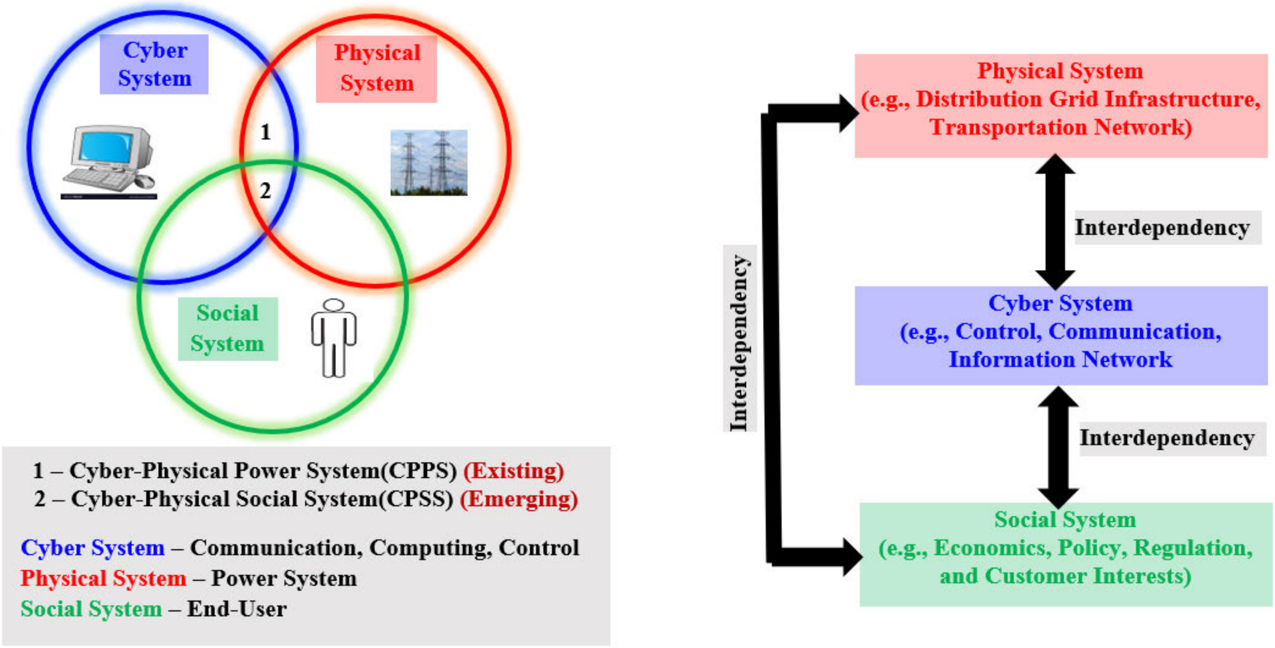
Cyber System
Physical System
1
2
Social System
1 – Cyber-Physical Power System(CPPS) (Existing)
2 – Cyber-Physical Social System(CPSS) (Emerging)
Cyber System – Communication, Computing, Control
Physical System – Power System
Social System – End-User
Physical System (e.g., Distribution Grid Infrastructure, Transportation Network)
Interdependency
Cyber System (e.g., Control, Communication, Information Network
Interdependency
Social System (e.g., Economics, Policy, Regulation, and Customer Interests)
Interdependency

FIGURE 23. Cyber-physical-social system.

The major contributions to the review of CPPS are highlighted as follows:

- This study mainly summarizes the CPPS modelling methods considering the impacts of cyber-attacks on power system control, power system stability, types of cyber-attacks, from the viewpoints of topology, mechanism, probability, and simulation. The unified framework for modelling of physical and cyber components in the CPPS is presented in Section II.
- The softwares corresponding to the CPPS for modelling and simulation of a physical system and cyber system and co-simulation tools are discussed elaborately. Different types of software for modelling and simulation of complex CPPS are presented in Section III. The co-simulation software includes and combines knowledge in multiple domains to consider the CPPS holistically.
- Cyber-physical security is the core of modern CPPS. In Section IV, we have presented a systematic and comprehensive review of the state-of-the-art in the field, ranging from cyber-attack types, defense strategies, to a wide range of challenges and opportunities. As CPPS has become one of the economic and technological developments around the globe, this survey provides critical insights into enhancing cybersecurity for CPPS by maintaining the integrity of the CPPS under complex cyber-attacks. To this end, we have reviewed the cyber-security issues in CPPS, which included attack detection, mitigation techniques, risk analysis threat modelling, and vulnerability assessment for cyber systems.
- We have surveyed the recent ongoing and completed research projects on CPPS in world-wide countries and briefly discussed in the Section V.
- The outlook of future CPPS focuses on CPSS with the integrated modelling framework utilizing a unified computing framework that is discussed elaborately in Section VI.
- Finally we have presented the current issues and research directions for the researchers those who are working in the CPPS research areas in Section VII.

The modelling methods, simulation softwares, cyber-attacks, and cybersecurity measures discussed in this paper imparts strong support for the secure and safe operation of the CPPS. An intensive analysis of simultaneous attacks on multiple targets is discussed elaborately. All the three modelling methods of CPPS considered both the power flow and information flow. In summary, there is no doubt that the emergence of CPPS leads to more efficient power system operations in the future, provides better services, and eventually revolutionize our daily lives. From the survey result, it was seen that this CPPS research area is growing exponentially in terms of publications, especially in recent years; this confirms that the researchers are more interested in exploring results, theories, and technologies. We hope this survey welcomes the other researchers to enter this emerging area. The future of CPPS addressed CPSSs associating CPSs with the social world, which is an important research topic that contributes to the construction of the future smart power system. It should be noted that only crucial research works are reviewed and summarized in this paper. However, there are some shortcomings in these modeling, simulation, and analysis. For instance, the specific topology of the communication network and transmission mechanism types in the information and communication network are not considered. By neglecting the steady-state and transient characteristics of CPPS subsystems the current research has only a theoretical significance. The modeling methods, simulation tools, cybersecurity applications, and performance evaluation are simulation-based approaches. To understand the complex behavior of CPPS, it is very difficult to model all the subsystems in simulation platforms. Therefore the construction of the CPPS testbed will further help the researchers, academicians, and industrialists to explore the in-depth knowledge of CPPS. Therefore, developing a testbed for CPPS that takes the actual power flow and information flow into consideration is the main problem to be solved in the near future. Based on this CPPS testbed, it is more appropriate to analyze and evaluate the three different types of modeling methods of CPPSs. In addition to that, cyber-attacks, cybersecurity algorithms, digital forensic analysis, risk assessment, attack modeling and defense can be demonstrated by organizing a co-simulation setup for CPPS and it becomes relatively crucial. Also, the major challenge is the design of large-scale CPPS and its implementation in real-world applications like the Wide-Area Monitoring and Control System (WAMCS).

REFERENCES

[1] E. F. Orumwense and K. Abo-Al-Ez, "A systematic review to aligning research paths: Energy cyber-physical systems," *Cogent Eng.*, vol. 6, no. 1, pp. 1–21, Dec. 2019.

[2] L. Shi, Q. Dai, and Y. Ni, "Cyber–physical interactions in power systems: A review of models, methods, and applications," *Electr. Power Syst. Res.*, vol. 163, pp. 396–412, Oct. 2018.

[3] S. Suryanarayanan, R. Roche, and T. M. Hansen, "Cyber-physical-social systems and constructs in electric power engineering," Inst. Eng. Technol., London, U.K., Tech. Rep., 2016.

[4] Y. Cao, Y. Li, X. Liu, and C. Rehtanz, *Cyber-Physical Energy and Power Systems*. Singapore: Springer, 2020.

[5] C. Dong, H. Jia, T. Jiang, L. Bai, Q. Hu, L. Wang, and Y. Jiang, "Effective method to determine time-delay stability margin and its application to power systems," *IET Gener., Transmiss. Distrib.*, vol. 11, no. 7, pp. 1661–1670, May 2017.

[6] H. Bevrani, M. Watanabe, and Y. Mitani, *Power System Monitoring and Control*. Hoboken, NJ, USA: Wiley, 2014.

[7] C. Li, G. Li, C. Wang, and Z. Du, "Eigenvalue sensitivity and eigenvalue tracing of power systems with inclusion of time delays," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 3711–3719, Jul. 2018.

[8] W. Yao, L. Jiang, J. Wen, Q. H. Wu, and S. Cheng, "Wide-area damping controller of FACTS devices for inter-area oscillations considering communication time delays," *IEEE Trans. Power Syst.*, vol. 29, no. 1, pp. 318–329, Jan. 2014.

[9] M. Mokhtari, F. Aminifar, D. Nazarpour, and S. Golshannavaz, "Wide-area power oscillation damping with a fuzzy controller compensating the continuous communication delays," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1997–2005, May 2013.

[10] J. Li, Z. Chen, D. Cai, W. Zhen, and Q. Huang, "Delay-dependent stability control for power system with multiple time-delays," *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 2316–2326, May 2016.

[11] F. Zhang, L. Cheng, and W. Gao, "Prediction based hierarchical compensation for delays in wide-area control systems," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3897–3899, Jul. 2018.

[12] F. Zhang, Y. Sun, L. Cheng, X. Li, J. H. Chow, and W. Zhao, "Measurement and modeling of delays in wide-area closed-loop control systems," *IEEE Trans. Power Syst.*, vol. 30, no. 5, pp. 2426–2433, Sep. 2015.

[13] D. Cai, Q. Huang, J. Li, Z. Zhang, Y. Teng, and W. Hu, "Stabilization of time-delayed power system with combined frequency-domain IQC and time-domain dissipation inequality," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 5531–5541, Sep. 2018.

[14] F. Milano, "Small-signal stability analysis of large power systems with inclusion of multiple delays," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 3257–3266, Jul. 2016.

[15] M. Liu, I. Dassios, G. Tzounas, and F. Milano, "Stability analysis of power systems with inclusion of realistic-modeling WAMS delays," *IEEE Trans. Power Syst.*, vol. 34, no. 1, pp. 627–636, Jan. 2019.

[16] R. V. Yohanandhan and L. Srinivasan, "Decentralised wide-area fractional order damping controller for a large-scale power system," *IET Gener., Transmiss. Distrib.*, vol. 10, no. 5, pp. 1164–1178, Apr. 2016.

[17] H. Ye, Y. Liu, and P. Zhang, "Efficient eigen-analysis for large delayed cyber-physical power system using explicit infinitesimal generator discretization," *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 2361–2370, May 2016.

[18] J. Zhang, S. Nabavi, A. Chakrabortty, and Y. Xin, "ADMM optimization strategies for wide-area oscillation monitoring in power systems under asynchronous communication delays," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2123–2133, Jul. 2016.

[19] J. Duan, H. Xu, and W. Liu, "Q-learning-based damping control of wide-area power systems under cyber uncertainties," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6408–6418, Nov. 2018.

[20] H. Ye, K. Liu, Q. Mou, and Y. Liu, "Modeling and formulation of delayed cyber-physical power system for small-signal stability analysis and control," *IEEE Trans. Power Syst.*, vol. 34, no. 3, pp. 2419–2432, May 2019.

[21] H. Ye, Q. Mou, X. Wang, and Y. Liu, "Eigen-analysis of large delayed cyber-physical power system by time integration-based solution operator discretization methods," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 5968–5978, Nov. 2018.

[22] Q. Mou, H. Ye, and Y. Liu, "Enabling highly efficient eigen-analysis of large delayed cyber-physical power systems by partial spectral discretization," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1499–1508, Mar. 2020.

[23] H. Ye, Q. Mou, and Y. Liu, "Calculation of critical oscillation modes for large delayed cyber-physical power system using pseudo-spectral discretization of solution operator," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4464–4476, Nov. 2017.

[24] H. Ye, T. Li, and Y. Liu, "Time integration-based IGD methods for eigen-analysis of large delayed cyber-physical power system," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1376–1388, Mar. 2020.

[25] W. Gao, H. Ye, Y. Liu, L. Wang, and W. Ci, "Comparison of three stability analysis methods for delayed cyber-physical power system," in *Proc. China Int. Conf. Electr. Distrib. (CICED)*, Xi'an, China, 2016, pp. 1–5.

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

[27] Z. Su, S. Xin, L. Xu, W. Li, Z. Shi, Q. Guo, and H. Sun, "A compensation method based assessment of cyber contingency for cyber-physical power systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Portland, OR, USA, Aug. 2018, pp. 1–5.

[28] K. Chen, F. Wen, and I. Palu, "Cyber contingencies impacts analysis in cyber physical power system," in *Proc. IEEE Int. Conf. Energy Internet (ICEI)*, Nanjing, China, May 2019, pp. 37–41.

[29] G. Cao, W. Gu, P. Li, W. Sheng, K. Liu, L. Sun, Z. Cao, and J. Pan, "Operational risk evaluation of active distribution networks considering cyber contingencies," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 3849–3861, Jun. 2020.

[30] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 3–13, Jan. 2014.

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

[32] G. Wu, G. Wang, J. Sun, and J. Chen, "Optimal partial feedback attacks in cyber-physical power systems," *IEEE Trans. Autom. Control*, early access, Mar. 19, 2020, doi: 10.1109/TAC.2020.2981915.

[33] L. Wang, Z. Qu, Y. Li, K. Hu, J. Sun, K. Xue, and M. Cui, "Method for extracting patterns of coordinated network attacks on electric power CPS based on Temporal–Topological correlation," *IEEE Access*, vol. 8, pp. 57260–57272, 2020.

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

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

[36] A. Patel and S. Purwar, "Switching attacks on smart grid using non-linear sliding surface," *IET Cyber-Phys. Syst. Theory Appl.*, vol. 4, no. 4, pp. 382–392, Dec. 2019.

[37] H. M. Khalid, S. M. Muyeen, and J. C.-H. Peng, "Cyber-attacks in a looped energy-water nexus: An inoculated sub-observer-based approach," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2054–2065, Jun. 2020, doi: 10.1109/JSYST.2019.2941759.

[38] Q. Wang, W. Tai, Y. Tang, and M. Ni, "Review of the false data injection attack against the cyber-physical power system," *IET Cyber-Phys. Syst. Theory Appl.*, vol. 4, no. 2, pp. 101–107, Jun. 2019.

[39] L. Yu, X.-M. Sun, and T. Sui, "False-data injection attack in electricity generation system subject to actuator saturation: Analysis and design," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 8, pp. 1712–1719, Aug. 2019.

[40] S. Ahmadian, X. Tang, H. A. Malki, and Z. Han, "Modelling cyber attacks on electricity market using mathematical programming with equilibrium constraints," *IEEE Access*, vol. 7, pp. 27376–27388, 2019, doi: 10.1109/ACCESS.2019.2899293.

[41] X. Lyu, Y. Ding, and S.-H. Yang, "Bayesian network based C2P risk assessment for cyber-physical systems," *IEEE Access*, vol. 8, pp. 88506–88517, 2020, doi: 10.1109/ACCESS.2020.2993614.

[42] D. J. S. Cardenas, A. Hahn, and C.-C. Liu, "Assessing cyber-physical risks of IoT-based energy devices in grid operations," *IEEE Access*, vol. 8, pp. 61161–61173, 2020, doi: 10.1109/ACCESS.2020.2983313.

[43] M. Z. A. Bhuiyan, G. J. Anders, J. Philhower, and S. Du, "Review of static risk-based security assessment in power system," *IET Cyber-Phys. Syst. Theory Appl.*, vol. 4, no. 3, pp. 233–239, Sep. 2019.

[44] X. Lyu, Y. Ding, and S.-H. Yang, "Safety and security risk assessment in cyber-physical systems," *IET Cyber-Phys. Syst. Theory Appl.*, vol. 4, no. 3, pp. 221–232, Sep. 2019.

[45] A. K. Srivastava, T. A. Ernster, R. Liu, and V. G. Krishnan, "Graph-theoretic algorithms for cyber-physical vulnerability analysis of power grid with incomplete information," *J. Mod. Power Syst. Clean Energy*, vol. 6, no. 5, pp. 887–899, Sep. 2018.

[46] X. Huang, Z. Qin, and H. Liu, "A survey on power grid cyber security: From component-wise vulnerability assessment to system-wide impact analysis," *IEEE Access*, vol. 6, pp. 69023–69035, 2018, doi: 10.1109/ACCESS.2018.2879996.

[47] Y. Zhu, J. Yan, Y. Tang, Y. Sun, and H. He, "Joint substation-transmission line vulnerability assessment against the smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 1010–1024, May 2015.

[48] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 566–575, Mar. 2015.

[49] C. Roberts, A. Scaglione, M. Jamei, R. Gentz, S. Peisert, E. M. Stewart, C. McParland, A. McEachern, and D. Arnold, "Learning behavior of distribution system discrete control devices for cyber-physical security," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 749–761, Jan. 2020.

[50] V. Venkataramanan, A. Hahn, and A. Srivastava, "CP-SAM: Cyber-physical security assessment metric for monitoring microgrid resiliency," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1055–1065, Mar. 2020.

[51] Y. Zhang, V. V. G. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn, and S. Suresh, "Cyber physical security analytics for transactive energy systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 931–941, Mar. 2020.

[52] M. I. Oozeer and S. Haykin, "Cognitive risk control for mitigating cyber-attack in smart grid," *IEEE Access*, vol. 7, pp. 125806–125826, 2019, doi: 10.1109/ACCESS.2019.2939089.

[53] M. U. Tariq, J. Florence, and M. Wolf, "Improving the safety and security of wide-area cyber–physical systems through a resource-aware, service-oriented development methodology," *Proc. IEEE*, vol. 106, no. 1, pp. 144–159, Jan. 2018.

[54] Q. Hu, D. Fooladivanda, Y. H. Chang, and C. J. Tomlin, "Secure state estimation and control for cyber security of the nonlinear power systems," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 1310–1321, Sep. 2018.

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

[56] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389–1407, Jul. 2017.

[57] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Phys. Syst. Theory Appl.*, vol. 1, no. 1, pp. 28–39, Dec. 2016.

[58] R. Danda, R. Joel, and S. Ivan, "Cyber-physical systems from theory to practice," in *Analysis and Design of Cyber-Physical Systems: A Hybrid Control Systems Approach*, G. R. Sanfelice, Ed. Boca Raton, FL, USA: CRC Press, 2015, ch. 1.

[59] G. R. Sanfelice, "Control of hybrid systems: An overview of recent advances," in *Hybrid Systems with Constraints*. Hoboken, NJ, USA: Wiley, May 2013, ch. 6.

[60] A. R. Teel, R. G. Sanfelice, and R. Goebel, "Hybrid control systems," in *Encyclopedia of Complexity and Systems Science*, R. Meyers, Eds. New York, NY, USA: Springer, 2009.

[61] R. Goebel, R. G. Sanfelice, and A. Teel, "Hybrid dynamical systems," *IEEE Control Syst. Mag.*, vol. 29, no. 2, pp. 28–93, Apr. 2009.

[62] R. G. Sanfelice, "On the existence of control Lyapunov functions and state-feedback laws for hybrid systems," *IEEE Trans. Autom. Control*, vol. 58, no. 12, pp. 3242–3248, Dec. 2013.

[63] R. G. Sanfelice, "Interconnections of hybrid systems: Some challenges and recent results," *J. Nonlinear Syst. Appl.*, vol. 2, nos. 1–2, pp. 111–121, 2011.

[64] R. G. Sanfelice, R. Goebel, and A. R. Teel, "Generalized solutions to hybrid dynamical systems," *ESAIM Control, Optim. Calculus Variat.*, vol. 14, no. 4, pp. 699–724, 2008.

[65] R. G. Sanfelice, D. Copp, and P. Nanez, "A toolbox for simulation of hybrid systems in matlab/simulink: Hybrid equations (HyEQ) toolbox," in *Proc. 16th Int. Conf. Hybrid Syst. Comput. Control (HSCC) Assoc. Comput. Machinery*, New York, NY, USA, 2013, pp. 101–106.

[66] R. Goebel, R. G. Sanfelice, and A. R. Teel, *Hybrid Dynamical Systems: Modelling, Stability, and Robustness*. Princeton, NJ, USA: Princeton Univ. Press, 2012.

[67] Y. Wang, Z. Lin, X. Liang, W. Xu, Q. Yang, and G. Yan, "On modelling of electrical cyber-physical systems considering cyber security," *Frontiers Inf. Technol. Electron. Eng.*, vol. 17, no. 5, pp. 465–478, 2016.

[68] M. Parandehgheibi, E. Modiano, and D. Hay, "Mitigating cascading failures in interdependent power grids and communication networks," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Dec. 2015, pp. 242–247.

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

[70] X. Lou, D. K. Y. Yau, H. H. Nguyen, and B. Chen, "Profit-optimal and stability-aware load curtailment in smart grids," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1411–1420, Sep. 2013.

[71] S. Soltan, M. Yannakakis, and G. Zussman, "Power grid state estimation following a joint cyber and physical attack," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 499–512, Mar. 2018.

[72] M. A. Williams, J. P. Koeln, H. C. Pangborn, and A. G. Alleyne, "Dynamical graph models of aircraft electrical, thermal, and turbomachinery components," *J. Dyn. Syst., Meas., Control*, vol. 140, no. 4, Apr. 2018.

[73] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. B. Purry, "Towards modelling the impact of cyber attacks on a smart grid," *Int. J. Secur. Netw.*, vol. 6, no. 1, p. 2, 2011.

[74] S. Korotunov, G. Tabunshchyk, K. Henke, and H. Wuttke, "Analysis of the verification approaches for the cyber-physical systems," CMIS, Zaporizhzhia, Ukraine, Tech. Rep. ISSN 1613-0073, 2019, vol. 2353, pp. 950–961, Paper 75.

[75] E. A. Lee and S. A. Seshia, *Introduction to Embedded Systems: A Cyber-Physical Systems Approach*. Cambridge, MA, USA: MIT Press, 2017.

[76] W. Li, L. Xie, Z. Deng, and Z. Wang, "False sequential logic attack on SCADA system and its physical impact analysis," *Comput. Secur.*, vol. 58, pp. 149–159, May 2016.

[77] C. Spagnolo, S. Sumsurooah, C. I. Hill, and S. Bozhko, "Finite state machine control for aircraft electrical distribution system," *J. Eng.*, vol. 2018, no. 13, pp. 506–511, Jan. 2018.

[78] K. Schneider, C. C. Liu, and J. P. Paul, "Assessment of interactions between power and telecommunications infrastructures," *IEEE Trans. Power Syst.*, vol. 21, no. 3, pp. 1123–1130, Aug. 2006.

[79] O. Gursesli and A. A. Desrochers, "Modelling infrastructure interdependencies using Petri nets," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, Oct. 2003, pp. 1506–1512.

[80] J.-C. Laprie, K. Kanoun, and M. Kaâniche, "Modelling interdependencies between the electricity and information infrastructures," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.*, 2007, pp. 54–67.

[81] J. P. Fortier and E. H. Michel, *Petri Nets, Computer Systems Performance Evaluation and Prediction*. Digital Press, 2003, pp. 279–303.

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

[83] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2435–2443, Sep. 2015.

[84] X. Liu, J. Zhang, and P. Zhu, "Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory," *Int. J. Crit. Infrastruct. Protection*, vol. 16, pp. 13–25, Mar. 2017.

[85] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 741–749, Dec. 2011.

[86] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2464–2475, Sep. 2015.

[87] P. A. Khand, "System level security modeling using attack trees," in *Proc. 2nd Int. Conf. Comput., Control Commun. (IC4)*, 2009, pp. 1–6.

[88] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Trans.*, vol. 46, no. 4, pp. 583–594, Oct. 2007.

[89] C. W. Ten, C. C. Liu, and M. Govindarasu, "Vulnerability assessment of cybersecurity for SCADA systems using attack trees," in *Proc. IEEE Power Eng. Soc. Gen. Meeting PES*, 2007, pp. 1–8.

[90] G. C. Dalton, R. F. Mills, J. M. Colombi, and R. A. Raines, "Analyzing attack trees using generalized stochastic Petri nets," in *Proc. IEEE Inf. Assurance Workshop*, Jun. 2006, pp. 116–123.

[91] Y. Wadhawan, A. AlMajali, and C. Neuman, "A comprehensive analysis of smart grid systems against cyber-physical attacks," *Electronics*, vol. 7, no. 10, p. 249, Oct. 2018.

[92] N. Liu, J. Zhang, H. Zhang, and W. Liu, "Security assessment for communication networks of power control systems using attack graph and MCDM," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1492–1500, Jul. 2010.

[93] Y. F. Wang, K. L. Gao, T. Zhao, and J. Qiu, "Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph," *Proc. CSEE*, vol. 36, no. 6, pp. 1490–1499, 2016.

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

[95] D. Olifer, N. Goranin, A. Cenys, A. Kaceniauskas, and J. Janulevicius, "Defining the minimum security baseline in a multiple security standards environment by graph theory techniques," *Appl. Sci.*, vol. 9, no. 4, p. 681, Feb. 2019.

[96] K. Kaynar and F. Sivrikaya, "Distributed attack graph generation," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 5, pp. 519–532, Sep. 2016.

[97] P. Johnson, A. Vernotte, M. Ekstedt, and R. M. Lagerstr, "pwnPr3d: An attack-graph-driven probabilistic threat-modelling approach," in *Proc. 11th IEEE Int. Conf. Availability, Rel. Secur. (ARES)*, Salzburg, Austria, Aug./Sep. 2016, pp. 278–283.

[98] K. Kaynar, "A taxonomy for attack graph generation and usage in network security," *J. Inf. Secur. Appl.*, vol. 29, pp. 27–56, Aug. 2016.

[99] H. S. Lallie, K. Debattista, and J. Bal, "An empirical evaluation of the effectiveness of attack graphs and fault trees in cyber-attack perception," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1110–1122, May 2018.

[100] C. R. Taylor, K. Venkatasubramanian, and C. A. Shue, "Understanding the security of interoperable medical devices using attack graphs," in *Proc. 3rd Int. Conf. High Confidence Netw. Syst. (HiCoNS)*, Apr. 2014, pp. 31–40.

[101] K. Karray, J. L. Danger, S. Guilley, and M. A. Elaabid, "Attack tree construction and its application to the connected vehicle," in *Cyber-Physical Systems Security*. Cham, Switzerland: Springer, 2018, pp. 175–190.

[102] O. B. Fredj, "A realistic graph-based alert correlation system," *Secur. Commun. Netw.*, vol. 8, no. 15, pp. 2477–2493, Oct. 2015.

[103] P. Luckett, J. T. McDonald, and W. B. Glisson, "Attack-graph threat modelling assessment of ambulatory medical devices," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, Waikoloa Village, HI, USA, Jan. 2017, pp. 3648–3657.

[104] O. Stan, R. Bitton, M. Ezrets, M. Dadon, M. Inokuchi, Y. Ohta, Y. Yamada, T. Yagyu, Y. Elovici, and A. Shabtai, "Extending attack graphs to represent cyber-attacks in communication protocols and modern IT networks," 2019, *arXiv:1906.09786*. [Online]. Available: http://arxiv.org/abs/1906.09786

[105] K. Pei, Z. Gu, B. Saltaformaggio, S. Ma, F. Wang, Z. Zhang, L. Si, X. Zhang, and D. Xu, "HERCULE: Attack story reconstruction via community discovery on correlated log graph," in *Proc. 32nd Annu. Conf. Comput. Secur. Appl.*, Los Angeles, CA, USA, Dec. 2016, pp. 583–595.

[106] F. Jia, J. B. Hong, and D. S. Kim, "Towards automated generation and visualization of hierarchical attack representation models," in *Proc. IEEE Int. Conf. Comput. Inf. Technol. Ubiquitous Comput. Commun. Dependable, Autonomic Secure Comput. Pervasive Intell. Comput.*, Liverpool, U.K., Oct. 2015, pp. 1689–1696.

[107] H. Kure, S. Islam, and M. Razzaque, "An integrated cyber security risk management approach for a cyber-physical system," *Appl. Sci.*, vol. 8, no. 6, p. 898, 2018.

[108] N. Agmon, A. Shabtai, and R. Puzis, "Deployment optimization of IoT devices through attack graph analysis," in *Proc. 12th Conf. Secur. Privacy Wireless Mobile Netw.*, Miami, FL, USA, May 2019, pp. 192–202.

[109] M. Ge and D. Seong Kim, "A framework for modeling and assessing security of the Internet of Things," in *Proc. IEEE 21st Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Melbourne, VIC, Australia, Dec. 2015, pp. 776–781.

[110] A. Singhal and X. Ou, "Security risk analysis of enterprise networks using probabilistic attack graphs," in *Network Security Metrics*. Cham, Switzerland: Springer, 2017, pp. 53–73.

[111] S. Noel and S. Jajodia, "A suite of metrics for network attack graph analytics," in *Network Security Metrics*. Cham, Switzerland: Springer, 2017, pp. 141–176.

[112] A. Ekelhart, E. Kiesling, B. Grill, C. Strauss, and C. Stummer, "Integrating attacker behavior in IT security analysis: A discrete-event simulation approach," *Inf. Technol. Manage.*, vol. 16, pp. 221–233, 2015.

[113] K. Durkota, V. Lisý, B. Bošanský, and C. Kiekintveld, "Optimal network security hardening using attack graph games," in *Proc. 24th Int. Joint Conf. Artif. Intell.*, Buenos Aires, Argentina, vol. 31, pp. 526–532, Jul. 2015.

[114] J. B. Hong, D. S. Kim, C.-J. Chung, and D. Huang, "A survey on the usability and practical applications of graphical security models," *Comput. Sci. Rev.*, vol. 26, pp. 1–16, Nov. 2017.

[115] L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala, "Interval vs. point temporal logic model checking: An expressiveness comparison," *ACM Trans. Comput. Log.*, vol. 20, pp. 4–41, Dec. 2018.

[116] M. Ibrahim, Q. Al-Hindawi, R. Elhafiz, A. Alsheikh, and O. Alquq, "Attack graph implementation and visualization for cyber physical systems," *Processes*, vol. 8, no. 1, p. 12, Dec. 2019.

[117] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4379–4394, Nov. 2016.

[118] M. Husák, J. Komárková, E. Bou-Harb, and P. Celeda, "Survey of attack projection, prediction, and forecasting in cyber security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 640–660, 1st Quart., 2019.

[119] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013.

[120] A. Anwar, A. N. Mahmood, and Z. Tari, "Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid," *Inf. Syst.*, vol. 53, pp. 201–212, Oct. 2015.

[121] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[122] X. Zhang, X. Yang, J. Lin, G. Xu, and W. Yu, "On data integrity attacks against real-time pricing in energy-based cyber-physical systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 1, pp. 170–187, Jan. 2017.

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

[124] Q. Yang, L. Chang, and W. Yu, "On false data injection attacks against Kalman filtering in power system dynamic state estimation," *Secur. Commun. Netw.*, vol. 9, no. 9, pp. 833–849, Jun. 2016.

[125] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[126] P. Srikantha and D. Kundur, "A DER attack-mitigation differential game for smart grid security analysis," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1476–1485, May 2016.

[127] T. J. Mary and P. Rangarajan, "Delay-dependent stability analysis of microgrid with constant and time-varying communication delays," *Electr. Power Compon. Syst.*, vol. 44, no. 13, pp. 1441–1452, Aug. 2016.

[128] H. Ye, W. Gao, Q. Mou, and Y. Liu, "Iterative infinitesimal generator discretization-based method for eigen-analysis of large delayed cyber-physical power system," *Electr. Power Syst. Res.*, vol. 143, pp. 389–399, Feb. 2017.

[129] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013.

[130] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, "A coordinated multi-switch attack for cascading failures in smart grid," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1183–1195, May 2014.

[131] A. Pahwa, S. A. DeLoach, B. Natarajan, S. Das, A. R. Malekpour, S. M. S. Alam, and D. M. Case, "Goal-based holonic multiagent system for operation of power distribution systems," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2510–2518, Sep. 2015.

[132] M. S. Rahman, M. A. Mahmud, A. M. T. Oo, and H. R. Pota, "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 436–447, Apr. 2017.

[133] J. Schiffer, F. Dörfler, and E. Fridman, "Robustness of distributed averaging control in power systems: Time delays & dynamic communication topology," *Automatica*, vol. 80, pp. 261–271, Jun. 2017.

[134] Y. Han, Y. Wen, C. Guo, and H. Huang, "Incorporating cyber layer failures in composite power system reliability evaluations," *Energies*, vol. 8, no. 9, pp. 9064–9086, Aug. 2015.

[135] H. Lei, C. Singh, and A. Sprintson, "Reliability modeling and analysis of IEC 61850 based substation protection systems," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2194–2202, Sep. 2014.

[136] M. Eliassi, A. K. Dashtaki, H. Seifi, M.-R. Haghifam, and C. Singh, "Application of Bayesian networks in composite power system reliability assessment and reliability-based analysis," *IET Gener., Transmiss. Distrib.*, vol. 9, no. 13, pp. 1755–1764, Oct. 2015.

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

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

[139] H. Lei and C. Singh, "Power system reliability evaluation considering cyber-malfunctions in substations," *Electric Power Syst. Res.*, vol. 129, pp. 160–169, Dec. 2015.

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

[141] L. Wei, A. I. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 684–694, Mar. 2018.

[142] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160–169, Mar. 2013.

[143] A. Delgadillo, J. M. Arroyo, and N. Alguacil, "Analysis of electric grid interdiction with line switching," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 633–641, May 2010.

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

[145] D. Shelar and S. Amin, "Security assessment of electricity distribution networks under DER node compromises," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 23–36, Mar. 2017.

[146] S. H. I. Libao and J. I. A. Zhou, "Vulnerability assessment of cyber physical power system based on dynamic attack-defense game model," *Autom. Electr. Power Syst.*, vol. 40, no. 17, pp. 99–105, 2016.

[147] Y. Yuan, F. Sun, and H. Liu, "Resilient control of cyber-physical systems against intelligent attacker: A hierarchal stackelberg game approach," *Int. J. Syst. Sci.*, vol. 47, no. 9, pp. 2067–2077, Jul. 2016.

[148] J. Guo, Y. Han, C. Guo, F. Lou, and Y. Wang, "Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties," *Energies*, vol. 10, no. 1, p. 87, Jan. 2017.

[149] X. Ji, B. Wang, D. Liu, Z. Dong, G. Chen, Z. Zhu, X. Zhu, and X. Wang, "Will electrical cyber–physical interdependent networks undergo first-order transition under random attacks?" *Phys. A, Stat. Mech. Appl.*, vol. 460, pp. 235–245, Oct. 2016.

[150] Z. Huang, C. Wang, S. Ruj, M. Stojmenovic, and A. Nayak, "Modelling cascading failures in smart power grid using interdependent complex networks and percolation theory," in *Proc. IEEE 8th Conf. Ind. Electron. Appl. (ICIEA)*, Jun. 2013, pp. 1023–1028.

[151] A. Ferdowsi, W. Saad, B. Maham, and N. B. Mandayam, "A colonel blotto game for interdependence-aware cyber-physical systems security in smart cities," in *Proc. 2nd Int. Workshop Sci. Smart City Oper. Platforms Eng. (SCOPE)*, 2017.

[152] A. Sturaro, S. Silvestri, M. Conti, and S. K. Das, "A realistic model for failure propagation in interdependent cyber-physical systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 2, pp. 817–831, Apr. 2020.

[153] H. Zhang, M. Peng, J. M. Guerrero, X. Gao, and Y. Liu, "Modelling and vulnerability analysis of cyber-physical power systems based on interdependent networks," *Energies*, vol. 12, no. 18, p. 3439, Sep. 2019.

[154] K. Marashi, S. S. Sarvestani, and A. R. Hurson, "Consideration of cyber-physical interdependencies in reliability modeling of smart grids," *IEEE Trans. Sustain. Comput.*, vol. 3, no. 2, pp. 73–83, Apr. 2018.

[155] Y. Han, C. Guo, S. Ma, and D. Song, "Modeling cascading failures and mitigation strategies in PMU based cyber-physical power systems," *J. Mod. Power Syst. Clean Energy*, vol. 6, no. 5, pp. 944–957, Sep. 2018.

[156] L. Xu, Q. Guo, T. Yang, and H. Sun, "Robust routing optimization for smart grids considering cyber-physical interdependence," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5620–5629, Sep. 2019.

[157] A.-S. K. Pathan, *Securing Cyber-Physical Systems*, 1st Ed. Boca Raton, FL, USA: CRC Press, 2016.

[158] M. El Hariri, T. Youssef, M. Saleh, S. Faddel, H. Habib, and O. A. Mohammed, "A framework for analyzing and testing cyber–physical interactions for smart grid applications," *Electronics*, vol. 8, no. 12, p. 1455, Dec. 2019.

[159] D. Bhor, K. Angappan, and K. M. Sivalingam, "Network and power-grid co-simulation framework for smart grid wide-area monitoring networks," *J. Netw. Comput. Appl.*, vol. 59, pp. 274–284, Jan. 2016.

[160] K. Boroojeni, M. H. Amini, A. Nejadpak, T. Dragicevic, S. S. Iyengar, and F. Blaabjerg, "A novel cloud-based platform for implementation of oblivious power routing for clusters of microgrids," *IEEE Access*, vol. 5, pp. 607–619, 2017.

[161] G. Celli, P. A. Pegoraro, F. Pilo, G. Pisano, and S. Sulis, "DMS cyber-physical simulation for assessing the impact of state estimation and communication media in smart grid operation," *IEEE Trans. Power Syst.*, vol. 29, no. 5, pp. 2436–2446, Sep. 2014.

[162] H. Georg, S. C. Muller, C. Rehtanz, and C. Wietfeld, "Analyzing cyber-physical energy systems:The INSPIRE cosimulation of power and ICT systems using HLA," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2364–2373, Nov. 2014.

[163] Y. Cao, X. Shi, Y. Li, Y. Tan, M. Shahidehpour, and S. Shi, "A simplified co-simulation model for investigating impacts of cyber-contingency on power system operations," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4893–4905, Sep. 2018.

[164] X. Sun, Y. Chen, J. Liu, and S. Huang, "A co-simulation platform for smart grid considering interaction between information and power systems," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2014, pp. 1–6.

[165] J. H. Kazmi, A. Latif, I. Ahmad, P. Palensky, and W. Gawlik, "A flexible smart grid co-simulation environment for cyber-physical interdependence analysis," in *Proc. Workshop Modeling Simulation Cyber-Phys. Energy Syst. (MSCPES)*, Apr. 2016, pp. 1–6.

[166] M. Wei and W. Wang, "Greenbench: A benchmark for observing power grid vulnerability under data-centric threats," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2014, pp. 2625–2633.

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

[168] K. Zhu, M. Chenine, and L. Nordstrom, ''ICT architecture impact on wide area monitoring and control Systems' reliability,'' *IEEE Trans. Power Del.*, vol. 26, no. 4, pp. 2801–2808, Oct. 2011.

[169] W. Li, A. Monti, M. Luo, and R. A. Dougal, ''VPNET: A co-simulation framework for analyzing communication channel effects on power systems,'' in *Proc. IEEE Electr. Ship Technol. Symp. (ESTS)*, Apr. 2011, pp. 143–149.

[170] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, ''EPOCHS: A platform for agent-based electric power and communication simulation built from commercial Off-the-Shelf components,'' *IEEE Trans. Power Syst.*, vol. 21, no. 2, pp. 548–558, May 2006.

[171] T. L. Hardy, *Software and System Safety: Accidents, Incidents, and Lessons Learned*. Bloomington, IN, USA: Author House, 2012.

[172] *Stuxnet Work Attack on Iranian Nuclear Facilities*. Accessed: Jun. 25, 2020. [Online]. Available: http://large.stanford.edu/courses/2015/ph241/holloway1/

[173] *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Electr. Inf. Sharing Anal. Center, Washington, DC, USA, 2016.

[174] *Xenotime: Hackers Behind Triton Malware Turn to Power Grids*. Accessed: Jun. 25, 2020. [Online]. Available: https://tech.newstatesman.com/security/xenotime-triton-power

[175] *The Cybersecurity 202*. Accessed: Jun. 25, 2020. [Online]. Available: https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/05/06/the-cybersecurity-202-a-cyberattack-just-disrupted-grid-operations-in-the-u-s-but-it-could-have-been-far-worse/5ccf61eda7a0a46cfe152c3e/

[176] *Cyber-Attack On Kudankulam Nuclear Power Plant*. Accessed: Jun. 25, 2020. [Online]. Available: http://www.infraline.com/Details/Cyber-Attack-On-Kudankulum-Nuclear-Power-Plant-Underlines-The-Need-For-Cyber-Deterrent-Strategy-360488.htm

[177] *NPCIL Accepts Cyber-Attack On Kudankulam*. Accessed: Jun. 25, 2020. [Online]. Available: http://www.infraline.com/Details/NPCIL-Accepts-Cyber-Attack-On-Kudankulam-358940.htm

[178] *The Global Risks Report 2019, 14th Edition*. Accessed: Jun. 25, 2020. [Online]. Available: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

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

[180] M. Govindarasu, A. Hann, and P. Sauer, *Cyber-Physical Systems Security for Smart Grid*. New York, NY, USA: PSERC Publication, 2012.

[181] B. Hu, C. Zhou, Y.-C. Tian, Y. Qin, and X. Junping, ''A collaborative intrusion detection approach using blockchain for multimicrogrid systems,'' *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 8, pp. 1720–1730, Aug. 2019.

[182] Y. Wadhawan, A. AlMajali, and C. A. Neuman, ''Comprehensive analysis of smart grid systems against cyber-physical attacks,'' *Electronics*, vol. 7, no. 10, p. 249, 2018.

[183] P. Lau, W. Wei, L. Wang, Z. Liu, and C. Ten, ''A cybersecurity insurance model for power system reliability considering optimal defense resource allocation,'' *IEEE Trans. Smart Grid*, early access, May 6, 2020, doi: 10.1109/TSG.2020.2992782.

[184] A. Farraj, E. Hammad, and D. Kundur, ''A distributed control paradigm for smart grid to address attacks on data integrity and availability,'' *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 4, no. 1, pp. 70–81, Mar. 2018.

[185] M. Touhiduzzaman, A. Hahn, and A. K. Srivastava, ''A diversity-based substation cyber defense strategy utilizing coloring games,'' *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5405–5415, Sep. 2019.

[186] M. El Hariri, T. Youssef, M. Saleh, S. Faddel, H. Habib, and O. A. Mohammed, ''A framework for analyzing and testing cyber–physical interactions for smart grid applications,'' *Electronics*, vol. 8, no. 12, p. 1455, Dec. 2019.

[187] X. Yang, X. Zhang, J. Lin, W. Yu, and P. Zhao, ''A Gaussian-mixture model based detection scheme against data integrity attacks in the smart grid,'' in *Proc. 25th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Waikoloa, HI, Aug. 2016, pp. 1–9.

[188] H. Tu, Y. Xia, C. K. Tse, and X. Chen, ''A hybrid cyber attack model for cyber-physical power systems,'' *IEEE Access*, vol. 8, pp. 114876–114883, 2020.

[189] C. Dou, D. Wu, D. Yue, B. Jin, and S. Xu, ''A hybrid method for false data injection attack detection in smart grid based on variational mode decomposition and OS-ELM,'' *CSEE J. Power Energy Syst.*, pp. 1–10, Apr. 2020, doi: 10.17775/CSEEJPES.2019.00670.

[190] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, ''A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids,'' *IEEE Access*, vol. 5, pp. 26022–26033, 2017.

[191] J. Cao, D. Wang, Z. Qu, M. Cui, P. Xu, K. Xue, and K. Hu, ''A novel false data injection attack detection model of the cyber-physical power system,'' *IEEE Access*, vol. 8, pp. 95109–95125, 2020.

[192] T. B. Rasmussen, G. Yang, A. H. Nielsen, and Z. Dong, ''A review of cyber-physical energy system security assessment,'' in *Proc. IEEE Manchester PowerTech*, Manchester, U.K., Jun. 2017, pp. 1–6.

[193] P. Srikantha, J. Liu, and J. Samarabandu, ''A novel distributed and stealthy attack on active distribution networks and a mitigation strategy,'' *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 823–831, Feb. 2020.

[194] D. Seifert and H. Reza, ''A security analysis of cyber-physical systems architecture for healthcare,'' *Computers*, vol. 5, no. 4, p. 27, Oct. 2016.

[195] T. S. Ustun, S. M. Farooq, and S. M. S. Hussain, ''A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard,'' *IEEE Access*, vol. 7, pp. 156044–156053, 2019.

[196] H. Haggi, R. R. Nejad, M. Song, and W. Sun, ''A review of smart grid restoration to enhance cyber-physical system resilience,'' in *Proc. IEEE Innov. Smart Grid Technol. Asia (ISGT Asia)*, Chengdu, China, May 2019, pp. 4008–4013.

[197] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, ''A review of false data injection attacks against modern power systems,'' *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[198] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, and Z. Han, ''A stealthy attack against electricity market using independent component analysis,'' *IEEE Syst. J.*, vol. 12, no. 1, pp. 297–307, Mar. 2018.

[199] W. Ao, Y. Song, and C. Wen, ''Adaptive cyber-physical system attack detection and reconstruction with application to power systems,'' *IET Control Theory Appl.*, vol. 10, no. 12, pp. 1458–1468, Aug. 2016.

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

[201] A. Nourian and S. Madnick, ''A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet,'' *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 1, pp. 2–13, Jan. 2018.

[202] P. Singh, S. Garg, V. Kumar, and Z. Saquib, ''A testbed for SCADA cyber security and intrusion detection,'' in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, Shanghai, China, Aug. 2015, pp. 1–6.

[203] D. Wang, X. Guan, T. Liu, Y. Gu, Y. Sun, and Y. Liu, ''A survey on bad data injection attack in smart grid,'' in *Proc. IEEE PES Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Kowloon, China, Dec. 2013, pp. 1–6.

[204] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragicevic, ''A stealth cyber-attack detection strategy for DC microgrids,'' *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

[205] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, ''Analyzing the cyber-physical impact of cyber events on the power grid,'' *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015.

[206] X. Lou, C. Tran, R. Tan, D. K. Y. Yau, Z. T. Kalbarczyk, A. K. Banerjee, and P. Ganesh, ''Assessing and mitigating impact of time delay attack: Case studies for power grid controls,'' *IEEE J. Sel. Areas Commun.*, vol. 38, no. 1, pp. 141–155, Jan. 2020.

[207] U. Adhikari, T. H. Morris, and S. Pan, ''Applying hoeffding adaptive trees for real-time cyber-power event and intrusion classification,'' *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4049–4060, Sep. 2018.

[208] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, ''Analyzing locally coordinated cyber-physical attacks for undetectable line outages,'' *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 35–47, Jan. 2018.

[209] S. Xu, Y. Xia, and H. Shen, ''Analysis of malware-induced cyber attacks in cyber-physical power systems,'' *IEEE Trans. Circuits Syst. II, Exp. Briefs*, early access, Jun. 4, 2020, doi: 10.1109/TCSII.2020.2999875.

[210] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, ''An online detection framework for cyber attacks on automatic generation control,'' *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6816–6827, Nov. 2018.

[211] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and J. Chen, ''Analysis of moving target defense against false data injection attacks on power grid,'' *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2320–2335, Jul. 2020.

[212] D. Du, X. Li, W. Li, R. Chen, M. Fei, and L. Wu, ''ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks,'' *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 8, pp. 1698–1711, Aug. 2019.

[213] M. Keshk, E. Sitnikova, N. Moustafa, J. Hu, and I. Khalil, ''An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems,'' *IEEE Trans. Sustain. Comput.*, early access, Mar. 25, 2019, doi: 10.1109/TSUSC.2019.2906657.

[214] G. Ravikumar and M. Govindarasu, "Anomaly detection and mitigation for wide-area damping control using machine learning," *IEEE Trans. Smart Grid*, early access, May 18, 2020, doi: 10.1109/TSG.2020.2995313.

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

[216] M. Deng, H. Cao, W. Zhu, H. Wu, and Y. Zhou, "Benchmark tests for the model-checking-based IDS algorithms," *IEEE Access*, vol. 7, pp. 135479–135498, 2019.

[217] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[218] W. Liao, S. Salinas, M. Li, P. Li, and K. A. Loparo, "Cascading failure attacks in the power system: A stochastic game perspective," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2247–2259, Dec. 2017.

[219] Z. Lu, W. Wang, and C. Wang, "Camouflage traffic: Minimizing message delay for smart grid applications under jamming," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 31–44, Jan. 2015.

[220] S. Sahoo, T. Dragicevic, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters–challenges and vulnerabilities," *IEEE J. Emerg. Sel. Topics Power Electron.*, early access, Nov. 14, 2020, doi: 10.1109/JESTPE.2019.2953480.

[221] C. K. Keerthi, M. A. Jabbar, and B. Seetharamulu, "Cyber physical Systems(CPS):Security issues, challenges and solutions," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCIC)*, Coimbatore, India, Dec. 2017, pp. 1–4.

[222] A. Ahmed, V. V. G. Krishnan, S. A. Foroutan, M. Touhiduzzaman, A. Srivastava, Y. Wu, A. Hahn, and S. Sindhu, "Cyber physical security analytics for anomalies in transmission protection systems," in *Proc. IEEE Ind. Appl. Soc. Annu. Meeting (IAS)*, Portland, OR, USA, Sep. 2018, pp. 1–8.

[223] C.-H. Lo and N. Ansari, "CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 1, pp. 33–44, Jun. 2013.

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

[225] A. Clark and S. Zonouz, "Cyber-physical resilience: Definition and assessment metric," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1671–1684, Mar. 2019.

[226] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber-Phys. Syst. Theory Appl.*, vol. 1, no. 1, pp. 13–27, Dec. 2016.

[227] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

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

[229] J. Wang and D. Shi, "Cyber-attacks related to intelligent electronic devices and their countermeasures: A review," in *Proc. 53rd Int. Universities Power Eng. Conf. (UPEC)*, Glasgow, Scotland, Sep. 2018, pp. 1–6, doi: 10.1109/UPEC.2018.8542059.

[230] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 20–23, Feb. 2015.

[231] C.-S. Cho, W.-H. Chung, and S.-Y. Kuo, "Cyberphysical security and dependability analysis of digital control systems in nuclear power plants," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 46, no. 3, pp. 356–369, Mar. 2016.

[232] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.

[233] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[234] B. Li, R. Lu, W. Wang, and K.-K.-R. Choo, "DDOA: A dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2415–2425, Nov. 2016.

[235] W. Bi, K. Zhang, Y. Li, K. Yuan, and Y. Wang, "Detection scheme against cyber-physical attacks on load frequency control based on dynamic characteristics analysis," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2859–2868, Sep. 2019.

[236] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method," *IET Cyber-Phys. Syst. Theory Appl.*, vol. 2, no. 4, pp. 161–171, Dec. 2017.

[237] M. Ghafouri, M. Au, M. Kassouf, M. Debbabi, C. Assi, and J. Yan, "Detection and mitigation of cyber attacks on voltage stability monitoring of smart grids," *IEEE Trans. Smart Grid*, early access, Jun. 22, 2020, doi: 10.1109/TSG.2020.3004303.

[238] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in smart grids based on graph signal processing," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1886–1896, Jun. 2020.

[239] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[240] S. D. Roy and S. Debbarma, "Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2023–2031, Jun. 2020.

[241] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 746–789, 1st Quart., 2020.

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

[243] J.-M. Lee and S. Hong, "Keeping host sanity for security of the SCADA systems," *IEEE Access*, vol. 8, pp. 62954–62968, 2020.

[244] J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, "Moving target defense approach to detecting Stuxnet-like attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 291–300, Jan. 2020.

[245] B. Gao and L. Shi, "Modeling an attack-mitigation dynamic game-theoretic scheme for security vulnerability analysis in a cyber-physical power system," *IEEE Access*, vol. 8, pp. 30322–30331, 2020.

[246] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J. C. Vasquez, "Brief survey on attack detection methods for cyber-physical systems," *IEEE Syst. J.*, early access, May 20, 2020, doi: 10.1109/JSYST.2020.2991258.

[247] M. Touhiduzzaman, A. Hahn, and A. Srivastava, "ARCADES: Analysis of risk from cyberattack against defensive strategies for the power grid," *IET Cyber-Phys. Syst. Theory Appl.*, vol. 3, no. 3, pp. 119–128, Sep. 2018.

[248] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.

[249] National Institute of Standards and Technology. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*. Accessed: Jun. 25, 2020. [Online]. Available: http://www.nist.gov/publicaffairs/releases/upload/smartgridinteroperabilityfinal.pdf

[250] *Framework for Cyber-Physical Systems: Volume 1, Overview Version 1.0*. Accessed: Jun. 25, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf

[251] Projects and Pilot Projects. *National Smart Grid Mission-Ministry of Power. Government of India*. Accessed: Jun. 25, 2020. [Online]. Available: https://www.nsgm.gov.in/en/sg-projects

[252] (2015). *Indian Smart Grid Forum (ISGF)—Smart Grid Project Book—A Global Snapshot*. Accessed: Jun. 25, 2020. [Online]. Available: https://indiasmartgrid.org/document/ISGFSmart%20Grid%20Project%20Book%20%20A%20Global%20Snapshot.pdf

[253] *Smart Grid Information Clearinghouse*. Accessed: Jun. 25, 2020. [Online]. Available: http://www.sgiclearinghouse.org

[254] American Transmission Company. *American Transmission Company Phasor Measurement Unit Project Description*. Accessed: Jun. 25, 2020. [Online]. Available: http://www.smartgrid.gov/sites/default/files/09-0282-atc-projectdescription-07-11-11.pdf

[255] Austin Energy. *Austin Energy Smart Grid Program*. Accessed: Jun. 25, 2020. [Online]. Available: http://www.austinenergy.com/About%20Us/Company%20Profile/smartGrid/index.htm

[256] (2010). *Value and Technology Assessment to Enhance the Business Case for the Certs Microgrid*. Accessed: Jun. 25, 2020. [Online]. Available: http://certs.lbl.gov/pdf/microgrid-final.pdf

[257] Lawrence Berkeley National Laboratory. *CERTS Microgrid Laboratory Test Bed*. Accessed: Jun. 25, 2020. [Online]. Available: http://certs.lbl.gov/pdf/certs-mgtb-app-o.pdf

[258] V. Giordano, F. Gangale, G. Fulli, M. S. Jiménez, I. Onyeji, A. Colta, I. Papaioannou, A. Mengolini, C. Alecu, T. Ojala, and I. Maschio, "Smart Grid projects in Europe: Lessons learned and current developments," Publications Office of the European Union, The Hague, The Netherlands, JRC Reference Tech. Rep. JRC 65215, 2011, doi: 10.2790/32946.

[259] R. E. Brown, "Impact of smart grid on distribution system design," in *Proc. IEEE Power Energy Soc. Gen. Meeting Convers. Del. Electr. Energy 21st Century*, Jul. 2008, pp. 1–4.

[260] *IntelliGrid*. Accessed: Jun. 25, 2020. [Online]. Available: http://intelligrid.epri.com/

[261] *Pacific Gas and Electric Company's SmartMeter Program*. Accessed: Jun. 25, 2020. [Online]. Available: http://www.pge.com/smartmeter/

[262] *Pacific Northwest Smart Grid Demonstration Project*. Accessed: Jun. 25, 2020. [Online]. Available: http://www.pnwsmartgrid.org/

[263] Xcel Energy. *SmartGridCity*. Accessed: Jun. 25, 2020. [Online]. Available: http://www.xcelenergy.com/smartgridcity

[264] *Sino-Singapore Tianjin Eco-City*. Accessed: Jun. 25, 2020. [Online]. Available: http://www.eco-city.gov.cn

[265] Y. Xue and X. Yu, "Beyond smart grid—Cyber–physical–social system in energy future [point of view]," *Proc. IEEE*, vol. 105, no. 12, pp. 2290–2292, Dec. 2017.

[266] F. A. Silva, "Cyber-physical-social systems and constructs in electric power engineering [Book News]," *IEEE Ind. Electron. Mag.*, vol. 11, no. 4, pp. 50–55, Dec. 2017.

[267] Z. Zhang, S. Huang, F. Liu, and S. Mei, "Pattern analysis of topological attacks in cyber-physical power systems considering cascading outages," *IEEE Access*, vol. 8, pp. 134257–134267, Jul. 2020.

[268] Z. Qu, Q. Xie, Y. Liu, Y. Li, L. Wang, P. Xu, Y. Zhou, J. Sun, K. Xue, and M. Cui, "Power cyber-physical system risk area prediction using dependent Markov chain and improved grey Wolf optimization," *IEEE Access*, vol. 8, pp. 82844–82854, 2020, doi: 10.1109/ACCESS.2020.2991075.

RAJAA VIKHRAM YOHANANDHAN (Member, IEEE) received the M.Tech. degree in control and instrumentation engineering and the Ph.D. degree in electrical engineering from the Thiagarajar College of Engineering, Madurai, India, in 2017. He is an Assistant Professor with the Department of Electronics and Instrumentation Engineering, SRM Institute of Science and Technology at Kattankulathur Campus (formerly known as SRM University), India. He was selected for the Council of Scientific and Industrial Research (CSIR)–Senior Research Fellowship (SRF) Scheme of the Ministry of Human Resource Development Group (HRDG), Government of India, New Delhi, in 2012. He was a gold medalist of the master's degree. He has authored five international journals and coauthored four international journals. His research interests include cyber-physical power systems, power system stability and control, the modeling and simulation of large-scale power systems, the modeling and simulation of FACTS devices, the wide-area monitoring and control of power system, intelligent control, and system identification. He is a member of the IEEE Power and Energy Society, the IEEE Control Systems Society, and the IEEE Computational Intelligence Society.

RAJVIKRAM MADURAI ELAVARASAN received the B.E. degree in electrical and electronics engineering from Anna University, Chennai, India, and the M.E. degree in power system engineering from the Thiagarajar College of Engineering, Madurai. He worked as an Associate Technical Operations at the IBM Global Technology Services Division. He was a gold medalist of the master's degree. He worked as an Assistant Professor with the Department of Electrical and Electronics Engineering, Sri Venkateswara College of Engineering, Chennai. He currently works as a Design Engineer with the Electrical and Automotive Parts Manufacturing Unit, AA Industries, Chennai. He has published papers in international journals, and international and national conferences. His areas of interest include solar PV cooling techniques, renewable energy and smart grids, wind energy research, power system operation and control, artificial intelligence, control techniques, and demand-side management. He is a member of the IEEE Power and Energy Society.

PREMKUMAR MANOHARAN received the B.E. degree in electrical and electronics engineering from the Sri Ramakrishna Institute of Technology, Coimbatore, India, in 2004, the M.E. degree in applied electronics from Anna University, Coimbatore, India, in 2010, and the Ph.D. degree from the Department of ICE, Anna University, Chennai, India, in 2019. He is currently working as an Assistant Professor with the GMR Institute of Technology, Rajam, India. He has more than ten years of experience in teaching, and he has published more than 60 technical papers in various national/international peer-reviewed journals such as the IEEE, Elsevier, and Springer. His current research fields include solar PV micro inverters, solar PV parameter extraction, modern solar PV MPPTs (optimization technique based), PV array faults, and non-isolated/isolated dc-dc converters for PV systems. He is serving as an Editor/Reviewer of leading journals such as the IEEE, IET, Wiley, Taylor & Francis, and Springer.

LUCIAN MIHET-POPA (Senior Member, IEEE) was born in 1969. He received the bachelor's degree in electrical engineering, the master's degree in electric drives and power electronics, and the Ph.D. and Habilitation degrees in electrical engineering from the Politehnica University of Timisoara, Romania, in 1999, 2000, 2002, and 2015, respectively. Since 2016, he has been working as a Full Professor in energy technology with Østfold University College, Norway. From 1999 to 2016, he was with the Politehnica University of Timisoara. He has also worked as a Research Scientist with Danish Technical University from 2011 to 2014 and Aalborg University, Denmark, from 2000 to 2002, and held a postdoctoral position at Siegen University, Germany, in 2004. He is also the Head of the Research Lab "Intelligent Control of Energy Conversion and Storage Systems" and is one of the Coordinators of the Master's degree Program in "Green Energy Technology" with the Faculty of Engineering, Østfold University College. He has published more than 130 papers in national and international journals and conference proceedings, and ten books. He has served as a scientific and technical program committee member of many IEEE conferences. He has participated in more than 15 international grants/projects, such as FP7, EEA, and Horizon 2020, and has been awarded more than ten national research grants. His research interests include modeling, simulation, control, and testing of energy conversion systems, and distributed energy resources (DER) components and systems, including battery storage systems (BSS) [for electric vehicles and hybrid cars and vanadium redox batteries (VRB)] and energy efficiency in smart buildings and smart grids. He was invited to join the Energy and Automotive Committees by the President and the Honorary President of the Atomium European Institute, working in close cooperation with—under the umbrella—the EC and EU Parliament, and he was appointed as the Chairman of AI4People, Energy Section. Since 2017, he has been a Guest Editor of five special issues of *Energies* (MDPI), *Applied Sciences*, *Majlesi Journal of Electrical Engineering*, and *Advances in Meteorology* journals.