Cyber–physical perspective on smart grid design and operation

Bo Chen1,2, Jianhui Wang2, Mohammad Shahidehpour3
1Energy Systems Division, Argonne National Laboratory, Argonne, IL, USA
2Department of Electrical Engineering, Southern Methodist University, Dallas, TX, USA
3Department of Electrical and Computer Engineering, Illinois Institute of Technology, Dallas, TX, USA
E-mail: bo.chen@anl.gov

Abstract: Emerging computation and communication technologies ubiquitously deployed in smart grids introduce unprecedented opportunities by enabling vigorous development of innovative business models and applications that aim for improving system efficiency, reliability, resiliency, and interoperability. Smart grids are typical cyber–physical systems (CPSs). The heterogeneous and complex nature of smart grids presents significant challenges introduced by the tight coupling of computation, communication, and physical systems. Here, the authors first provide an overview of smart grids from a CPS perspective. Then, the authors discuss the opportunities and challenges in smart grid design and operation. Next, a co-design framework is introduced and used for designing wide-area damping controller as one of many CPS applications that can be abstracted from various power system layers. The authors conclude that developing a theoretical modelling framework is critical for understanding and managing the complexity and interoperability of smart grids.

1 Introduction

As one of the most complex human-made systems, power systems are engineered by billions of components and geographically interconnected across thousands of miles. Electricity is the most important energy carrier in modern human society since it can be transmitted over long distance and power many other critical infrastructures such as communication, information, and transportation systems [1]. Owing to the ease of use and access, electricity has become a fundamental necessity for people living in both developed and developing countries. In the past few years, many efforts have been devoted to developing advanced design, planning, and operation technologies and establishing viable business models to improve the system efficiency, reliability, resiliency, and interoperability. Modern power systems have been continuously evolving by accommodating emerging technologies from various domains. Particularly, the advancements in communication and information technologies unprecedentedly facilitate the development of innovative technologies and business models that fundamentally modernise and transform electric power grids into so-called ‘smart grids’. In the realm of smart grids, electricity generation, transmission, and distribution are performed in a way that the overall social and economic benefits are maximised. This is achieved by the seamless integration of communication, information, and computation technologies through a framework of standards dedicated to achieving a higher level of interoperability [2].

Cyber–physical systems (CPSs) are highly engineered systems with physical systems and computational control components interacted through communication systems [3]. In CPSs, cyber and physical elements are intertwined in a way that any changes in the physical world affect the behaviour of cyber world, or vice versa. As shown in Fig. 1, in a networked CPS, both sensors and actuators are connected to the communication system. The cyber part (i.e. communication and control layers) and the physical part are tightly coupled, and any changes to the CPS will result in a series of interactions between the two layers. The physical system can be represented by a single node representing a device or a network representing an interconnected system. The operation states of the physical system are monitored by the sensors installed at the physical layer. Then, the sensed data is transformed into digital signals and transmitted to the computation and control layer through the two-way communication links. In response to the sensor data, the control actions are generated by the control algorithms embedded in the controllers and transmitted back to the actuation units in physical systems. The physical system reacts to the control actions and changes the operation state, which in turn generate another set of sensing signals. This process will be carried out iteratively such that the physical system can be continuously supervised and controlled to achieve the expected performance. It is worth noticing that the communication layer contains multiple nodes that can be interpreted as different meanings depending on the network and protocols. Similarly, multiple control applications can exist in the control layer and can be implemented in a centralised or a distributed manner. These control applications can be coordinated to achieve a trade-off among multiple objectives by sharing the needed data over the communication layer. Human factors are also considered when human activities are involved in the CPS to assist with decision-making and manufacturing process. In some CPSs (e.g. smart eyewear devices, cardiac pacemakers), human body is considered to be a part of the physical system. Although the similar feedback control scheme shown in Fig. 1 can be traced back to the age of Industrial Revolution, the revolutionary advancements in information and communication technologies fundamentally change the landscape of control world. Just like the Internet has changed the way we communicate with each other, in the era of CPSSs, the widely deployed embedded systems not only feature local sensing and computing in real time, but also share the collected data and the computation capability with other embedded systems and centralised control systems through the communication system. The enhanced scalability and complexity further strengthen the interdependency between cyber and physical systems, and thus enable numerous enabling technologies to be invented so as to achieve various performance goals and serve diverse needs of different stakeholders.

Smart grids are typical CPSSs due to the extensive deployment of advanced technologies and applications that systematically interconnect centralised and distributed controllers, sensors, physical devices, and various stakeholders involved in many processes [4]. The convergence of power systems, communication systems, and computing systems will enable numerous intelligent CPS applications that change the way we interact with both cyber
and physical worlds. On the other hand, the heterogeneity among these systems impedes the development of these applications and raises many challenges on CPS design and operation. Therefore, advanced CPS-based methodologies that can fundamentally change the way of designing and operating smart grids must be adopted to handle the challenges introduced by the inherent heterogeneity and concurrency of smart grids. In this paper, we will present an overview of smart grids from a CPS perspective.

The remainder of this paper is organised as follows. Section 2 introduces smart grids from a perspective of CPSs. Section 3 discusses the challenges and opportunities in the realm of smart grids. Section 4 presents a CPS co-design framework which can be used for designing and operating CPS applications in response to different cyber and physical events. Conclusions and envisions are discussed in Section 5.

2 Smart grids as CPSs

Smart grids are the next generation of electric power systems featured by the employment of smart grid technologies for delivering clean and affordable energy and achieving a higher level of system efficiency, reliability, resilience, and security [5]. The need for incorporating renewable energies and grid modernisation prompts the development of new intelligent technologies and business models to facilitate the evolution of traditional electric power systems towards smart grids.

To enable these technologies, numerous sensors and actuators, as well as associated networking technologies, are ubiquitously deployed in smart grids, hence qualifying smart grids as typical CPSs [6]. An example is the pervasive smart meter deployments in distribution systems. According to The Edition Foundation, smart meter deployments in the USA for the past 10 years have increased from 7 to 70 million, and expected to hit 90 million by 2020 [7]. Smart meters act as gateways between utilities and households. For each household installed with a smart meter, the energy usage will be sampled every few minutes. Through the advanced metering infrastructure (AMI), all the smart meter data can be integrated and used for facilitating applications built in distribution management system (DMS) and home energy management system (HEMS), such as load disaggregation, modelling, and forecasting [8, 9]. The predicted aggregated load curves can be further used for demand response, volt/var control, power loss minimisation, fault detection isolation and restoration etc. [10]. In this example, different applications directly or indirectly share the smart grid data and perform feedback control through actuators (e.g. smart appliances, electrical vehicles, voltage regulators). Fig. 2 provides a glimpse of smart grids from a CPS perspective. Physical components in generation, transmission, distribution, and customer (i.e. residential, commercial, and industrial) domains are shown in blue blocks. Communication technologies used for networking and transmitting sensing and actuating signals are shown in yellow blocks. Applications, which are performed based on the sensed information of physical systems, are shown in green blocks. Service provider, operations, and markets domains are shown in pink blocks as they are not directly interacting with physical systems. It can be seen that many CPSs can be found under each subdomain or entity. For example, HEMS in residential households can act as a centralised controller that coordinates smart appliances (e.g. refrigerator, washer/dryer, dishwasher, oven), home energy storage, plug-in vehicle, and photovoltaic solar panels in response to the real-time energy use and the energy market prices [11], through a dedicated communication network [12]. Also, each smart appliance by itself can be seen as a CPS as well. In the distribution domain, residential, commercial, industrial, and substation entities are interconnected by the field devices such as transmission lines and switches, thus forming a large-scale physical system. Based on the data collected from SCADA and other data sources, DMS and other grid applications perform advanced control strategies to optimise the system performance. Similarly, in the transmission and generation domains, system operation states are supervised by SCADA through wide area network and controlled by energy management system (EMS) to ensure stability and reliability. Service providers, operations, and markets can actively participate in the control loops. Communication systems are critical for ensuring interoperability between any two of the domains due to the time-critical requirements posed by the continuously time-changing system demand and renewable profiles.

3 Challenges and opportunities

The convergence of power systems, communication systems, and computing systems will enable numerous intelligent smart grid CPS applications that will change the way we interact with both cyber and physical worlds. On the other hand, the heterogeneity among these systems impedes the development of these applications and raises many challenges on CPS design and operation. In this section, we will discuss the challenges on current design and operation processes, as well as some progresses towards the modelling and simulation of smart grids.

3.1 CPS architecture and abstractions for smart grids

Conventional design and operation for power systems, communication systems, and computing systems are concern-separated considering limited interactions, resulting in less cost-efficiency and insufficient capability of interoperability [13]. The increasing stringent requirements for real-time applications force a full integration of all the domain systems during the design and operation process. The major challenge on smart grid design and operation arises from the heterogeneity among these systems. The concurrency, which is the intrinsic nature of physical power systems, cannot be fully realised in the abstractions in today's communication and computing systems [14]. However, timing is not included in the semantics of programming languages used in software-based systems, and thus further hidden from higher levels of abstractions. Lack of timing properties in the abstractions may result in failure of abstractions, since the successful execution of a piece of code cannot guarantee to meet the timing deadlines [14]. Therefore, the heterogeneity rooted in CPSs requires multiple layers of abstractions with sufficiently defined interfaces to be created during the design process [15].

A CPS reference architecture that can be used for developing a common taxonomy of smart grids is the key for achieving seamless interoperability among different heterogeneous systems. To serve this purpose, a smart grid architecture model (SGAM) framework is introduced by CEN/CENELEC/ETSI Smart Grid Coordination Group Reference Architecture working group under EU mandate M/490 [16], as shown in Fig. 3. The SGAM framework enables a comprehensive methodology for facilitating the decomposition of business processes and associated functions, so as to understand, assess, and manage the smart grid use cases [18]. The interoperability is achieved by identifying and mapping interrelated and interoperable processes in specific domains, zones, and layers. Given a smart grid CPS architecture and properly designed abstractions, numerous smart grid business models and technologies can be designed, developed, and validated. Advanced communication and networking technologies are critical to successfully realising the seamless information exchange within and between cyber and physical domains. Many efforts have been made towards developing standard data models and information models. For example, the IEC 61850 series of standards are used to provide substation-level data models, information exchange requirements and protocols, and common information model.
3.2 Modelling and simulation

As a system of CPS systems, smart grid contains many applications that are designed for achieving various purposes, such as enhancing small-signal stability and transient stability, improve voltage profiles, reduce system power losses, and minimise the probability of cascading failures. Some of these applications require the data to be sampled and transited as soon as possible (i.e. time-critical), otherwise the expected performance may be deteriorated [19]. In this sense, the characteristics of communication networks (e.g. time delay, packet loss, link failure, and topology) should be properly considered in the CPS model. For some applications that allow slower data sampling rates (i.e. non-time-critical), these characteristics may have minor impact, and thus can be simplified or neglected in the CPS model. However, the control algorithms of these applications are normally much more complicated than time-critical applications. The challenges usually lay on how to develop a scalable model that can handle a high volume of heterogeneous data sources. Also, the information confidentiality, integrity, and availability (i.e. CIA triad) become a priority [20]. Dedicated models with reasonable assumptions for each class of control application may be more preferred. For example, CPS dynamics should be considered for most time-critical applications (e.g. wide area controllers (WACs), dynamic state estimation). Whereas steady-state model may be sufficient for non-time-critical applications (e.g. steady-state voltage and power flow control). The CPS modelling and simulation are the core-enabling processes for designing, developing, and validating smart grid applications. In the context of CPS, an integrated framework is desired to model and simulate different elements at different interoperability layers, domains, and zones that are depicted in the SGAM framework, such that the requirements on the performance including the interoperability, reliability, and security can be fully considered. Current practice for power system design and operation cannot fully meet the stringent requirements posed by the aforementioned factors. Next, several aspects of CPS modelling and simulation are introduced, including testbed development, combined cyber–physical formulation, and cyber–physical security.

3.2.1 Cyber–physical testbed: In the literature, some work has been done on modelling and simulating cyber–physical smart grids. Specifically, initial attempts were made by developing CPS testbeds, which feature the capability of simulating communicating systems and power systems simultaneously, or co-simulation [21]. Existing modelling and simulation methods must be fundamentally reconstructed to support advanced optimisation and control applications, and a good interdisciplinary knowledge is required to develop reasonable abstractions in the modelling phase and the simulation phase. A co-simulation framework for developing a CPS testbed is shown in Fig. 4. Communication and power systems are modelled and simulated separately in dedicated commercial or open source software/hardware. For example, OPNET [22], NS-2 [23, 24], NS-3 [25], and OMNET++ [26] are used as network simulators that support most commonly used industrial and customised protocols. Power systems can be modelled in PSCAD [23], PSLF [27], MATLAB/Simulink [28], OpenDSS [29], RTDS [17, 30], and Opal-RT [31] for transient and steady-state simulations in real time or offline. In addition, a data middleware should be developed for bridging and synchronizing the cyber part and physical part modelled in software and hardware. Various protocols can be implemented for different applications, such as IEEE C37.118 Synchronized Phasor Protocol [32], IEC 61850 Sampled Values [17], MODBUS [30], and DNP3 [33]. Smart grid testbeds enable proof-of-concept prototyping, performance analysis, vulnerability evaluation, and many other useful functionalities. It is
worth noticing that some real-time CPS testbeds can be used for hardware-in-the-loop simulation by connecting real-world sensors and controllers through communication links or analogue/digital converters [34].

3.2.2 Cyber–physical combined state formulation: In CPS systems, computing systems normally employ powerful computers or programmable logic controllers that are typical discrete-time systems processing control laws by sequentially executing the embedded codes (e.g. C++). Communication systems normally use digital networking technologies for transmitting discrete data packets, which also present stochastic characteristics since the timing for the arriving packets is not deterministic [35]. On the contrary, physical power system components are interconnected and changing continuously and concurrently. The theories and tools for modelling and analysing cyber systems are completely different from physical systems. Therefore, it is desired to formulate the behaviours of both cyber and physical systems within an integrated model [36]. For example, in [37], a cyber–physical model is introduced for modelling power system hierarchical control systems using directed graph theory with data nodes and directed branches representing the data processing units and information flow. Hybrid automata models can be used for precisely modelling continuous dynamic behaviours of physical systems and discrete digital computational processes of cyber systems using differential equations to describe the system behaviours in response to discrete events, and can be categorised as a type of finite state machine. In the context of CPS, some new challenges are introduced by the networked and distributed hybrid systems and complex processes. A compositional model was proposed in [38] for control networks implemented on multi-hop networks, and a complicated modelling framework including the formal syntax and semantics for the composed system was introduced.

3.3 Cyber–physical security

Cyber–physical security is a critical concern in smart grids due to the ubiquitous adoption and interconnection of computer-based information systems, which inevitably introduce vulnerabilities that can be leveraged by malicious hacking activities and unintentional misoperations [39]. Power grids are often targeted by terrorism and sabotage activities. Although rarely happen, successfully conducted cyber and physical attacks can deteriorate the performance of a broad spectrum of applications and thus potentially jeopardise the system stability and security [40]. Coordinated cyber–physical attacks may cause power outages and even disastrous cascading failures [41, 42]. Unfortunately, cyber security is often overlooked by device manufacturers as they are building computing and networking capabilities into their products. Without sufficient protection, all the access points, which are created by wide area measurement system (WAMS) and AMI infrastructures, as well as numerous field intelligent electronic devices and smart appliances, can be potentially hacked by malicious parties [43]. For example, the SCADA system of Ukrainian power system was successfully hacked by foreign attackers in December 2015. Thirty substations were remotely disconnected through the DMS system, and 225,000 customers lost power access for 3 h [44]. According to the US Department of Homeland Security (DHS), cyber attacks against power grids are still increasing in both frequency and sophistication. A trustworthy framework should be developed to detect and mitigate cyber threats at the earliest possible time.

Traditional passive defence practices (e.g. firewalls, anti-virus software, access control, update patching, and response tools) are not adequate for preventing all the attacks, especially when it is used for against denial of service (DoS) and distributed DoS attacks and zero-day attacks [45]. On the other hand, active defence, which can proactively hunt down malicious attackers and malware that are identified by intrusion detection systems, is gaining attractions [46].

In response to cyber attacks, adaptive routing solutions can be used for determining network routing protocols based on equality of service (QoS) provisioning in packet delay, packet loss, and throughput using fast route reconfiguration. A QoS-aware adaptive routing method for hierarchical software defined networks (SDN) is introduced in [47], in which the delays in large SDNs are minimised using configurable controllers. Routing problem for cyber–physical power systems has been studied in [48], in which a dynamic routing solution is introduced for standby EMS communication routing. Similar work can be also found in [49, 50]. In addition, physical power grids (e.g. substations, lines, transformers) are inevitably exposed to nature environment since they are geographically dispersed. Therefore, protecting smart grids from being severely affected by physical damages (e.g. physical attacks, natural disasters, and equipment failures) is equivalently important. The aforementioned CPS testbeds can be used for evaluating various types of cyber and physical attacks and mitigation methodologies. A systematically integrated defence framework is desired to guarantee the confidentiality, integrity, and availability of cyber networks, while preserving the intact of physical systems.

4 CPS co-design framework for smart grids

In this section, we will introduce a framework to facilitate the analysis, co-design, and co-simulation of WAMS-based applications, which are one type of typical smart grid applications.

4.1 WAMS-based applications

The control loop of WAMS-based controllers is shown in Fig. 5. There are two plants (i.e. plant 1 and plant 2) representing energised equipment (e.g. generators, transformers, ESSs) with the capability of remote supervision and control. Each plant is installed with a sensor unit [i.e. phasor measurement unit (PMU)] and an actuator unit. Both units can communicate with the controllers (i.e. controller A and controller B) through a set of communication nodes [e.g. routers, phasor data concentrators (PDCs), gateways, and bridges] in the communication network. The solid lines represent sensor data flows and the dashed lines represent control data flows. For example, in Fig. 5, controller A receives the data...
sent from sensor 1 in plant 1, whereas controller B receives the data from both sensor 1 and sensor 2. The control actions generated by the controllers are transmitted back to the actuators. Different control laws may be implemented in different controllers using different data sets. For example, a single controller may be needed for achieving a centralised control scheme, and distribution control scheme can be implemented among multiple controllers. The sensor and control data flows can travel along different routing paths, even if the sensor and the actuator are installed on the same plant (e.g. controller B and plant 2). In addition, since it will take a certain amount of time for the data packets to transit from the sensor to the controller through the network, the controller will always receive delayed information. Similarly, control packets will also experience a time delay when being transferred from the controller to the actuator. Time delay (or latency) is always a critical concern for design of operation of time-critical applications. In addition, packet loss due to link congestion and software/hardware failure is also an important concern, especially for WAMS using wireless networks.

4.2 Model of physical system dynamics

Physical systems normally feature continuous dynamics, which can often be described by a set of differential and algebraic equations:

\[
\begin{align*}
\dot{x}(t) &= f(x(t), y(t), t, u(t)) \\
0 &= g(x(t), y(t))
\end{align*}
\]

(1)

where \(x(t)\) is the vector representing the physical system state variables, \(t \in \mathbb{R}\) represents the continuous time evolution, \(y(t)\) is the vector representing the physical system algebraic variables, \(u(t)\) represent a set of general time-varying functions of the system states, algebraic variables, inputs, and time.

Power systems can be modelled as a transmission line network interconnecting synchronous generators and customer loads. The dynamics follow the Newton’s law of motion and Kirchoff's law. Assuming there are \(n\) synchronous generators in the system, the state-space form of the dynamic of generator \(g \in G := \{1, \ldots, n\}\) (i.e. swing equation) can be expressed by two differential equations [51]:

\[
\begin{align*}
\delta_g &= \omega_g - \omega_b \\
\dot{\omega}_g &= -\frac{1}{M_g} (P_{mg} - D_g (\omega_g - \omega_b) - P_{e,g} + u_{c,g})
\end{align*}
\]

(2)

where \(\delta_g\) represents the generator phase angle in radians, \(\omega_g\) is the rotor speed in rad/s, \(\omega_b\) is the nominal rotor speed in rad/s, and \(\omega_b = 120\pi\) for 60 Hz operated system. \(D_g\) is the generator inertia in seconds. \(D_g\) is the damping coefficient in seconds. \(P_{mg}\) is the mechanical power input by the turbine in megawatts. \(P_{e,g}\) is the electric power output by the generator in megawatts. \(u_{c,g}\) is the active power injected by the entities (e.g. ESSs) installed at the same bus with generator \(g\). If the generator excitation control scheme can be implemented among multiple controllers. The control laws may be implemented in different controllers using different destinations for various application purposes, and can be identified through a user-assigned IDCODE [61]. PMU data packets are generated by PMUs, routed by communications nodes, and the load demand of load \(d\) as \(P_d + j Q_d\) then:

\[
\begin{align*}
P_i &= \sum_{g \in G} P_{e,g} \\
Q_i &= \sum_{g \in G} Q_{e,g} + \sum_{d \in D} V_d^2 (1 - \cos(2(\delta_{ik} - \theta_{ik}))
\end{align*}
\]

(4)

where \(u_{c,i}\) and \(u_{k,i}\) are active and reactive power generated by devices that can be controlled by the controllers.

4.3 Model of WAMS communication system

The PMU/PDC data is usually transmitted in the WAMS network in the form of time-synchronised packets. A WAMS network can be implemented on dedicated and public networks using any media, such as fibreoptic, analogue/digital microwave, telephone line, and power line. Multiple PMUs, PDCs, and application controllers are interconnected by communication devices. Multiple data streams can be transmitted by a single PMU or PDC. Each stream can be independently configured and transmitted to different destinations for various application purposes, and can be identified through a user-assigned IDCODE [61]. PMU data packets are generated by PMUs, routed by communications nodes,
and received by PDC and controllers. Specifically, PMU packets usually arrive at communication nodes in a sequential manner and thus form a queue, for which the queuing theory is usually used for analysing the queue lengths and waiting times [58, 62].

The complexity of the stochastic behaviours of communication networks may prohibit from developing an effective model for CPS design and operation. Therefore, to simply the analysis, we assume the data streams seen from the controllers and the actuators are continuous, since the WAMS normally features high fidelity and high sampling rate [63]. The impact of communication systems is usually represented as a range of time delay that is considered in the process of controller designing. Most wide area controllers are designed to withstand the worst-case delays, and thus, the control performance may be compromised to some extent. Therefore, many researchers have developed a variety of models to estimate the time delay based on a set of parameters [19, 64–66]. In these models, the network topology and routing strategies are either ignored or fixed. However, to enable the coordinated design and operation, these factors should be properly modelled and considered.

**4.3.1 Model of communication system topology:** A communication system can be modelled as a graph $G = (V, E)$, with $V := \{1, \ldots, N\}$ as the set of vertices (i.e. communication nodes) and $E := \{1, \ldots, n\}$ as the set of edges (i.e. communication links). We assume there are $N_a$ actuators, $N_s$ sensors, $N_c$ controllers, and $N_l$ communication nodes in the WAMS network. Denote sensor nodes $\delta \subseteq V$, actuator nodes $\alpha \subseteq V$, controller nodes $\beta \subseteq V$, and communication nodes $\gamma \subseteq V$. If there is a communication link from node $i$ to node $j$, then this link is denoted as $(i, j)$. The set of communication links is denoted as $\mathcal{L} = \{(i, j) ; i \in V, j \in V, i \neq j\}$. Specifically, assuming there are $N_p$ routing paths and $N_l$ communication links, we denote a routing path as a list of links that connects the sending node and the receiving node. The routing paths can be categorised into two types: routing paths between sensors and controllers $\mathcal{P}_{\text{SC}} \subseteq \mathcal{P}$, and routing paths between controllers and actuators $\mathcal{P}_{\text{CA}} \subseteq \mathcal{P}$.

![Fig. 5 Control loop of WAMS-based controllers](image)

**4.3.2 Model of control-loop delay:** The control-loop delay in a WACS refers to the sum of time required to transit a PMU packet from a PMU to a controller or PDC, and from the controller to the actuators [19]. We denote the control-loop delay of PMU-based WAMS as $T_{cl}$, which is determined by many factors such as network topology, routing paths, packet size, sampling rate, line capacity, and queuing delay [64, 66]. $T_{cl}$ can be estimated by [19, 64, 66]:

$$T_{cl} = T_s + T_{ac} + T_{ca} + T_c + T_a$$  \hspace{1cm} (6)

where $T_s$ is the delay required by the sensors to convert the analogue signals from the potential and current transformers (i.e. PT and CT) to PMU packets based on the C37.118 format [32]. $T_{ac}$ and $T_{ca}$ are the time delays required for transmitting the data from the sensor to the controller, and from the controller to the actuator, respectively. $T_c$ is the delay required by the controller to carry out the control strategy. $T_a$ is the delay required by the actuators to perform the control actions. Fig. 6 shows each domain that each delay term in (6) is related to, as well as the causes of the delay. It is worth noticing that $T_s$, $T_c$, and $T_a$ are assumed to be fixed, as long as the control strategy, PMU packet size, sampling rate, and discrete Fourier transform (DFT) window for each PMU are predetermined. $T_{ac}$ and $T_{ca}$ are mainly determined by propagation delay, serial delay, firewall screening, and routing delay. For a routing path $p \in \mathcal{P}$ between the sensor $s \in \delta$ and the actuator $a \in \alpha$, assuming there are total $N_p$ links and $N_\gamma$ routers in $p$, the communication delay for this path can be estimated as [66]:

$$T_{cl}^{\delta} + T_{cl}^{\gamma} = T_{act}^{\text{act}} + \sum_{i=1}^{N_p} (T_{\text{prop},i} + T_{\text{proc},i}) + \sum_{j=1}^{N_\gamma} T_{\text{queue},j} + T_{\text{act},a}$$  \hspace{1cm} (7)

where $T_{act}^{\text{act}}$ and $T_{act}^{\text{act}}$ are terminal delays for sensor $s$ and actuator $a$ required by firewalls and servers and assumed to be fixed. $T_{\text{prop},i}$ is the propagation time used for transmitting data through link $i$, and it can be determined based on the distance between the two end nodes of link $i$ (denoted as $l_i$) and the travel speed of the media $(v_i)$:

$$T_{\text{prop},i} = \frac{l_i}{v_i}$$  \hspace{1cm} (8)

where $T_{\text{proc},i}$ is the serial delay required for processing sequential bits of packets, and it is determined by the packet size ($L_i$ in bits/packet) and the data rate of link $i$ ($R_i$ in bits/s):

![Fig. 6 Control-loop time delay in a PMU-based WAMS network](image)
where $T_{\text{queue},j}$ is the routing delay required for a packet to wait for being serviced in a queue at a routing node. If WAMS is implemented in a dedicated network that is operated in light traffic conditions, $T_{\text{queue},j}$ can be ignored without significantly affect the estimated delay. However, $T_{\text{queue},j}$ should be considered if the network traffic is heavy. In [19], a simple model to estimate the routing delay based on the M/M/1 queue assumption:

$$T_{\text{queue},j} = \frac{\lambda_j}{\lambda_j - \lambda_j}$$

where $\lambda_j$ is the rate of packets arriving at the routing node $j$ in packets/s. $\lambda_j$ is the processing rate of packets of the routing node $j$ in packets/s.

We can see that the control-loop delays can be variable for routing paths with different sensors and destinations, as well as many other factors. Therefore, it is necessary to develop a model that can conveniently account for the changes in the communication systems. Next, we introduce a matrix-based model for formulating the time delays in a WAMS network.

### 4.3.3 Matrix-based model of control-loop delays:

For a communication system represented by a graph $S(V,E)$, the incidence matrix is usually used to describe the connectivity between the vertices and the edges. We define the link-node incidence matrix $I_S \in \mathbb{R}^{N_p \times N_s}$ with the entries defined as:

$$I_S(i, j) = \begin{cases} 1 & \text{if node } i \text{ is an end node of link } j, \quad i \in \mathcal{S} \cup \mathcal{A} \\ 0.5 & \text{if node } i \text{ is an end node of link } j, \quad i \in \mathcal{E} \cup \mathcal{R} \\ 0 & \text{otherwise} \end{cases}$$

(11)

We define the path-link incidence matrix $I_{\mathcal{PL}} \in \mathbb{R}^{N_p \times N_l}$ to denote all the routing paths:

$$I_{\mathcal{PL}}(i, j) = \begin{cases} 1 & \text{if path } i \text{ contains the link } j \\ 0 & \text{otherwise} \end{cases}$$

(12)

Then the path-node incidence matrix $I_{\mathcal{PN}} \in \mathbb{R}^{N_p \times N_s}$ can be derived from:

$$I_{\mathcal{PN}} = I_{\mathcal{PL}} I_G$$

(13)

To formulate the time-delay terms in (7) for each node and link, we define a series of vectors: $T_s, T_a, T_c, T_{\text{queue}} \in \mathbb{R}^{N_c \times 1}$, and $T_{\text{prop}}, T_{\text{proc}} \in \mathbb{R}^{N_c \times 1}$. Their entries are defined as:

$$T_s(i) = \begin{cases} T_{s,i} + T_{\text{sen},i} & \text{if } i \in \mathcal{S} \\ M & \text{otherwise} \end{cases}$$

(14)

$$T_a(i) = \begin{cases} T_{a,i} + T_{\text{act},i} & \text{if } i \in \mathcal{A} \\ M & \text{otherwise} \end{cases}$$

(15)

$$T_c(i) = \begin{cases} T_{c,i} & \text{if } i \in \mathcal{C} \\ M & \text{otherwise} \end{cases}$$

(16)

$$T_{\text{queue}}(i) = \begin{cases} T_{\text{queue},i} & \text{if } i \in \mathcal{R} \\ M & \text{otherwise} \end{cases}$$

(17)

$$T_{\text{prop}}(i) = \begin{cases} T_{\text{prop},i} & \text{if } i \in \mathcal{L} \\ \text{max}(0, \text{min}(U_{\text{SC}}(j,i) + \tau_c, T_{\text{act}})) & \text{if } \text{max}(U_{\text{SC}}(j,i)) \leq T_{\text{act}} \\ \text{min}(0, \text{min}(U_{\text{SC}}(j,i) + \tau_c, T_{\text{act}})) & \text{otherwise} \end{cases}$$

(18)

$$T_{\text{proc}}(i) = \begin{cases} T_{\text{proc},i} & \text{if } i \in \mathcal{L} \\ T_{\text{prop},i} & \text{otherwise} \end{cases}$$

(19)

where $M$ is a large number representing an equivalent big delay. It is worth noticing that all the vectors defined in (14)–(19) can be assumed to be constant with a conservative margin [19]. However, if a more detailed model is required, some of these vectors should be formulated using a dedicated model.

The control-loop delay $T_{cl} \in \mathbb{R}^{N_c \times 1}$ for all the routing paths can be written in the matrix-form based on (6):

$$T_{cl} = \begin{bmatrix} I_{\mathcal{PL}}(T_{\text{prop}} + T_{\text{proc}}) + I_{\mathcal{PL}} T_s + T_a + T_c + T_{\text{queue}} \end{bmatrix}$$

(20)

Substitute (13) into (20), we have:

$$T_{cl} = \begin{bmatrix} I_{\mathcal{PL}}(T_{\text{prop}} + T_{\text{proc}} + I_s(T_s + T_a + T_c + T_{\text{queue}})) \end{bmatrix}$$

(21)

Denote $D \in \mathbb{R}^{N_c \times 1}$, we have:

$$T_{cl} = \begin{bmatrix} I_{\mathcal{PL}} D \\ D = T_{\text{prop}} + T_{\text{proc}} + I_s(T_s + T_a + T_c + T_{\text{queue}}) \end{bmatrix}$$

(22)

From (22), we can see that the control-loop delay can be manipulated by changing the routing paths and parameter configurations of the communication network. Similarly, we can estimate the delays between sensors and controllers (denoted as $T_{SC}$), and between controllers and actuators (denoted as $T_{CA}$). Note that if the controllers are installed at the same location with the actuators, then the delay between them can be ignored and all the entries in $T_{CA}$ are zeros.

Additionally, we can derive the origin–destination (OD) close-loop delay matrix $U_{cl} \in \mathbb{R}^{N_s \times N_s}$:

$$U_{cl} = h(I_D^T \text{diag}(T_{cl}) I_D)$$

(23)

where $I_0 \in \mathbb{R}^{N_s \times N_s}$ is the origin incidence matrix with the entries $I_0(i,j)$ being 1 if the sensor node $i$ is an end node of the $j$th link, and being 0 otherwise. $I_0 \in \mathbb{R}^{N_s \times N_s}$ is the destination incidence matrix with the entries $I_0(i,j)$ being 1 if the sensor node $j$ is an end node of the $i$th link, and being 0 otherwise. diag$(\bullet)$ is a function used for transforming $T_{cl}$ into an $N_p \times N_p$ matrix with diagonal terms being the entries of $T_{cl}$. $h(\bullet)$ is a linear mapping function to transform the delay matrix from the communication dimension ($\mathbb{R}^{N_s \times N_s}$) to the controller dimension ($\mathbb{R}^{N_s \times N_s}$). Similarly, we can derive the delay matrices between sensors and controllers (denoted as $U_{SC} \in \mathbb{R}^{N_s \times N_s}$), and between controllers and actuators (denoted as $U_{CA} \in \mathbb{R}^{N_s \times N_s}$).

It is worth noticing that most control applications are relying on the data from the local PDCs, which is responsible for time alignment for multiple PMU channels. Two time alignment methods, namely absolute time alignment and relative time alignment, can be implemented in PDC [67]. In both methods, a maximum waiting period (i.e. time alignment window) is used to collect PMU packets with the same timestamps from all the channels. Any late packets (i.e. packets arrive after the window is closed) will be discarded and considered as lost packets. Therefore, from the controller perspective, all the channels should have a same delay due to the time alignment. Take the relative time alignment as an example, the time alignment window is activated when the earliest packet arrives. Then the time delay seen by the controller $i \in \mathcal{E}$, denoted by $\tau_c$, can be modelled as:

$$\tau_c = \begin{cases} \text{max}(U_{\text{SC}}(j,i) + \tau_c, T_{\text{act}}) & \text{if } \text{max}(U_{\text{SC}}(j,i)) \leq T_{\text{act}} \\ \text{min}(U_{\text{SC}}(j,i) + \tau_c, T_{\text{act}}) & \text{otherwise} \end{cases}$$

(24)
where $T^{\text{max}}$ is the maximum waiting period. From (24), we can see that $\tau_i$ can be reduced by minimising the delay difference between any two of the incoming PMU channels. This can be achieved by strategically configuring routing paths and properly selecting routing devices and PDCs.

The delay vectors and matrices derived above can help formulate the design and operation problems for CPS controllers, which will be introduced in the next subsection.

4.4 Model of control systems

Three types of control strategies can be implemented based on how the remote data are incorporated, namely centralised control, distributed control, and decentralised control. Specifically, centralised controllers collect measurement values from multiple sensors and issue control signals to all the actuators in the system. Distributed controllers are implemented by distributing multiple controllers throughout the system, and each local controller can communicate with neighbouring controllers. A decentralised controller is operated independently and it does not communicate with other controllers. It is critical to choose the proper control scheme based on the specific requirements posed by the applications on stability, reliability, scalability, cost etc. For example, centralised control heavily depends on the performance of the associated communication networks and it is usually prone to cyber attacks. It is crucial to ensure the intact of the central controller, since the failure of the central controller will affect the whole system. Distributed and decentralised controllers have higher reliability and scalability, but need more time for achieving the computational convergence. Based on the aforementioned control strategies and taking the state of cyber systems into consideration, the control actions for each controller $i$ (denoted as $u_i$) in (1) can be modelled as [54]:

\[
    u_i = \begin{cases} 
        c_i(x, y, z) & \text{centralised control} \\
        c_i(x, y, x_i^>, y_i^<, z) & \text{distributed control} \\
        c_i(x, y, z) & \text{decentralised control}
    \end{cases}
\]

where $c_i(\cdot)$ is the control function of controller $i$. $x_i, y_i$ are the vectors of system states and algebraic variables required by the controller $i$. $x_i^>, y_i^<$ are the vectors of system states and algebraic variables of the neighbouring controllers. $z$ is the state vector of cyber systems (e.g. time delays, packet loss rate).

A critical concern for analysis and design of WAMS-based controllers is how to assess the impact of time delays, packet losses, and measurement noises induced by the sensors and communication systems on system stability, and how to stabilise the systems under varying network conditions through a coordinated design of controllers [68, 69]. These issues can be addressed by optimising the communication network configurations (e.g. protocols, throughputs) without considering time delays or packet losses in the controller design, or by explicitly modelling the delays, protocols, or traffics [70, 71].

By assuming the physical system described in (1) to be linear and time invariant (i.e. linear time invariant system), the physical system dynamics can be formulated in the state-space as:

\[
\begin{align*}
    x(t) &= Ax(t) + Bu(t) \\
    y(t) &= Cx(t)
\end{align*}
\]

where $A, B, C$ are $N_x \times N_x, N_x \times N_u$ and $N_y \times N_x$ matrices representing the state matrix, input matrix, and output matrix, respectively. $N_x$ is the number of system state variables. Note that in (26), $u(t)$ is a piecewise continuous variable vector, since it only changes values when a packet arrives at each actuator. Note the linear system (26) modelled in the controller is an estimate of the non-linear physical system described in (1). Next, we will introduce how to model the delay, which is estimated by (23), in the controller.

4.4.1 Model of time delays: Assume the delay $\tau$ is constant and the communication is lossless, the controller can be modelled as [90]:

\[
u(t) = -K y(t - \tau)
\]

where $K \in \mathbb{R}^{N_y \times N_z}$ is the linear feedback gain matrix representing the control strategies and should be properly designed and tuned. $t \in (kh + r: k = 0, 1, \ldots)$ represents the instances when the control actions are carried out by the actuators. $h$ is the sampling period. The actuators may receive different number of sampling packets depending on the length of $\tau$. For example, if $\tau < h$, only two sampling period $t \in \{(k - 1)h, kh\}$ need to be considered. If $\tau > h$, multiple sampling packets can be received during a single sampling period. The detailed analysis when $\tau < h$ and $\tau \geq h$ can be found in [70]. It is important to determine if the system with delayed control signals can maintain stability or not. Substitute (27) into (26), we have:

\[
\begin{align*}
x(t) &= Ax(t) - BKx(t - \tau) = Ax(t) - A_{\tau}x(t - \tau)
\end{align*}
\]

Equation (28) is a delay differential equation and its stability is studied in many works such as [72, 73].

Note that in (27), each row of $u$ can be seen as a control entity taking observations from $y$. Then, the entries of $B$ and $K$ in (28) indicate the origins and the destinations of the communication links between the actuators and the control entities, and between the control entities and the sensors. For example, $K_{ij} \neq 0$ if the output channel $j$ is needed by the control entity $i$. Therefore, in the designing stage, the elements of $K$ may be selected considering the availability of the communication links and the associated time delays, which are estimated in $U_{ij}$. For example, a multicast routing method is developed in [74] to realise a decentralised control scheme by solving an optimisation problem formulated based on the linear matrix inequalities, so as to determine the entries of $K$ and stabilise the system. In addition, given the origins and destinations, the routing paths $I_{jix}$ should be proactively optimised to minimise the time delay in each route. For centralised control, a properly selected location for the central controller may also help reduce the time delays.

Time delay issues can be addressed in several ways. Smith predictor and robust control are effective control schemes for time-delay systems [75, 76]. In [77], a stabilising control based on the unified Smith predictor is introduce to dampen the system using WAMS data. In addition, since PMU packets are all timestamped, one can estimate the system states at time $t$ [i.e. $x(t)$] to compute $u_i(t)$, based on the information received at time $t - t_w$ [78]. Another method is to construct a gain-scheduling design as introduced in [54], in which the feedback gain matrix is modelled as $K(\tau)$, which is a function of the time delay $\tau$. Thus, the entries of $K(\tau)$ change with $\tau$ to achieve a better performance under varying time delays.

4.4.2 Model of packet loss: In a lossy communication system (e.g. wireless system), data packets can be dropped occasionally or continuously. Packet losses in WAMS have been observed and reported in [79]. In some WAMS-based applications, for simplicity, the missing data due to packet loss can be estimated using linear or quadratic interpolation algorithms without significantly affecting the controller performance, since the sampling rate of PMU is high [80]. The loss of packet generated at $kh$ can also be modelled as a form of time delay, with the delay being the duration between the arrival packets generated at $(k - 1)h$ and $(k + 1)h$ [81]. Furthermore, a CPS with time delays and packet losses can be modelled as an asynchronous dynamical system constrained by event rates, and its stability can be analysed through Lyapunov stability theory and linear matrix inequality method [82].

4.5 Co-design framework

In this section, we present a framework for designing and operating WAMS-based applications. The framework employs a hierarchical...
architecture that performs various functionalities at different layers, as shown in Fig. 7. The CPS controller design and operation is carried out at the bottom layer. Depending on the specific requirements on the control performance as well as the communication system conditions [e.g. z(t)], one or more control modes (e.g. centralised, distributed, and/or decentralised control) will be determined, and the control strategy u(t) is designed based on various theories. Furthermore, the requirements on routing, data rate, maximum time delay, and packet loss rate are posed by the need of transmitting needed data while maintaining the system stability and considered in the middle layer for communication system design and operation.

Either design problem or operation problem can be solved in the middle layer. In the design phase, all the components including PMU units, routers, routing paths, and actuators are modelled as decision variables to minimise the time delay and packet loss rate in each route path, while ensuring the maximum time delay and packet loss rate requirements posed by the bottom physical controller layer. In the operation phase, only routing paths are modelled as decision variables. The routing control can be implemented through decentralised protocols or proactive routing control. The bottom physical controller layer and the middle communication system layer will interact iteratively until converging to an optimal design for both the communication system configuration and the physical controller.

In addition, a top layer is added to the co-design framework to provide real-time supervision and enable the design and operation to be more resilient to cyber and physical events. For example, if the communication system is compromised by the DoS attack and heavy traffic is observed in one or more communication links, the top layer can identify the attack and isolate the compromised links and nodes, and then generate alternative routing paths to mitigate the impact. The top layer can also estimate the system states and correct the controller model to improve the control performance.

4.6 Example case study

In large interconnected power systems, interarea oscillation is a common problem that may limit the power transfer capability through the tie-lines among multiple regions [75]. The WAMS-based wide-area damping controller (WADC) can provide supplementary damping by leveraging remote measurements and are proven to be able to achieve better performance. Many WADC models that are robust to time delays and packet losses have been proposed in the literature [76–78, 80, 81]. In this case study, we emphasise the co-design framework introduced in Fig. 7, in which the routing paths can be adaptively configured to control the time delays.

4.6.1 WADC design: Assuming the system is operated at an equilibrium operation point (δ0, ω0, Ego, Vgo, θ0), the system small-signal performance can be investigated by linearising (2)–(5) at the equilibrium point [51]:

\[
\begin{align*}
\Delta x &= \hat{A}\Delta x + \hat{B}\Delta u \\
\Delta y &= \hat{C}\Delta x
\end{align*}
\]

(29)

where Δx = x – x0, Δu = u – u0, and Δy = y – y0 represent the small derivations of the state variables, inputs, and outputs from the equilibrium point, respectively. A, B, and C are state, input, and output matrices calculated based on the given equilibrium point, respectively. In some data-driven approaches, these matrices can be estimated online based on the WAMS data, such that the parameters of the WADC can be updated adaptively. The stability of the state-space model described in (29) can be analysed through the eigenvalues and eigenvectors of A. Then the transfer function assuming Δu is a single input and Δy is a single output can be written as [51]:

\[
G(s) = \sum_{i=1}^{n} \frac{R_i}{s - \lambda_i}
\]

(30)

where \(\lambda_i\) is the ith eigenvalue, and \(R_i\) is the residue of \(G(s)\) at pole \(\lambda_i\).

The WADC is designed to add damping to the target oscillation mode such that the eigenvalue is moved to the left side of the complex plane. This is done by compensating the phase of the residue arg(Ri):  

\[
\phi_i = 180° - \arg(R_i)
\]

(31)

where \(\phi_i\) is the compensation angle for oscillation mode \(\lambda_i\). The transfer function used for compensating \(\phi_i\) should be determined according to [83].

---

Fig. 7 Hierarchical co-design and co-operation framework for CPS controller design and operation.
The transfer function used for compensating the time delay (i.e. \( \tau_{sc} \)) between the sensor and the WADC can be designed according to [84]. The block diagram of the excitation system of generator 1 is shown in Fig. 8 [81]. The summation of the measurement signal representing the generator terminal voltage \( E_t \) through a voltage transducer, the control signal from local PSS, and the control signal from the WADC is compared with the reference voltage \( V_{ref} \). Then the voltage deviation is input to the exciter, which generates the control signal \( E_{fd} \) to regulate the field voltage.

4.6.2 Case studies: Next, we present a WADC model subjected to cyber attacks on a commonly used four-generator two-area test system as shown in Fig. 9 [a]. The detailed parameters can be found in Fig. 9b. The topology of the WAMS shown in Fig. 9b represent the unused links. We use the WADC configuration introduced in [80], in which the rotor speeds of Gen 2 and Gen 4 are measured and transmitted to the WADC through PMU1 and PMU2, respectively. The control signals generated by the WADC are then transmitted to the excitation system installed on Gen 1. For study purposes, we specify the parameters used for estimating the time delays in Table 1. Then the voltage deviation is input to the exciter, which generates the control signal \( E_{fd} \) to regulate the field voltage.

The delay for all the routing paths in Fig. 9b can be calculated as summarised in Table 2. The propagation delay \( T_{prop} \) and the processing delay \( T_{proc} \) can be ignored due to the relatively short distance and the high bandwidth. From Table 2, we can calculate the control-loop delay. Considering the PDC time alignment, the delay of the control loop is 300 ms, according to (24). Fig. 9c shows the performance of the time-delay compensation scheme with the delay being 300 ms comparing with the scenario without delay. When the WADC is enabled and no delay is applied, the interarea oscillation can be quickly damped out. When the delay compensator is used, the phase shift caused by the delay is compensated and the resulted control performance is similar to the scenario without delay.

Limited by the capability of the delay compensator, the WADC controller can only handle a range of time delays while achieving satisfactory performance. The co-design framework introduced should be able to reconfigure the communication system to minimise the communication delay. We assume the communication system protocols always seek the shortest paths to minimise the time delays. In addition, we assume the WADC can switch between the centralised model and the decentralised mode. For example, if the measured time delay is too long (e.g. 1000 ms), the WADC should be disabled or reconfigured to damp local oscillation modes. If the sensor is failed, then the WADC can use the data from another sensor located within the same area with the failed sensor, since the generators in the same area normally oscillate with the same speed. Table 3 describes the two case studies and the mitigation actions.

In case 1, the communication node 6 is assumed to be flooded by DoS attack performed by malicious hackers. We assume the time delay is increased to 1000 ms due to the cyber attack, and it takes 5 s for identifying the DoS attacks and carrying out the mitigation actions.

---

**Table 1** Communication network configuration

| Variable | Notation | Value |
|----------|----------|-------|
| \( R \)  | data rate of the network | 50 Mbps |
| \( L \)  | packet size | 40 byte |
| \( \lambda \)  | packet arriving rate | 50 packets/s |
| \( T_a \)  | actuator operational delay | Gen 1: 10 ms |
| \( T_c \)  | controller operational delay | WADC: 120 ms |
| \( T_s \)  | sensor operational delay | PMU 1: 10 ms PMU 2: 30 msPMU 3: 40 ms |

**Table 2** Time delay for routing paths

| Origin/destination | Routing path | Delay, ms |
|--------------------|--------------|-----------|
| PMU1 to WADC       | \{(3,7), (7,9), (9,8), (8,11)\} | 140       |
| PMU2 to WADC       | \{(1,5), (5,6), (6,8), (8,11)\} | 160       |
| WADC to Gen 1      | \{(11,8), (8,9), (9,7), (7,4)\} | 140       |

**Table 3** Cases studied on the WADC system

| Case no. | Description | Mitigation |
|----------|-------------|------------|
| 1        | node 6 is flooded by denial-of-service attack | change routing path between PMU 2 and WADC |
| 2        | both node 6 and PMU 2 are attacked | use \( \omega_{gen3} \) from PMU 3 instead of \( \omega_{gen4} \) from PMU 2 |
actions are shown in Fig. 11b. From 0 to 5 s, only local PSSs are responsible for damping oscillations, since PMU 2 data is not available for the WADC. Starting from 5 s, the oscillation can be quickly damped down by using PMU 3 data in the WADC.

From the case studies, we can conclude that in a CPS co-operation framework, the limited capability of the studied WADC controller (e.g. only compensate fixed time delay) can be compensated by optimising the network configurations. Additionally, some issues in the communication systems (e.g. congested nodes) can be compensated by the flexibility of the WADC control schemes (e.g. using alternative data sources).

5 Conclusion

The evolving communication and computing technologies are transforming traditional power systems into cyber–physical smart grids, which unprecedentedly change the landscape of electric power systems and the way we interact with them. On the one hand, the interoperability of cyber–physical smart grids enables us to develop various intelligent CPS applications that can address the great challenges introduced by the increasing load demand and the ever-growing penetration of renewable energies. On the other hand, the heterogeneity and complexity featured in most CPS applications impede the conceptual understanding and model analysis, and thus require a general modelling framework to be developed. In this paper, we provided an insight into smart grids from a CPS perspective. The WAMS and AMI infrastructures were introduced as two of the most enabling technologies, based on which various applications can be developed to enhance the system performance. Next, we discussed the challenges and opportunities introduced by the convergence of power systems, communication systems, and computing systems. Specifically, current practices for development of cyber–physical smart grid architectures, modelling and simulation, and cyber–physical security were discussed. Then, we introduced a CPS model for smart grids. Finally, a hierarchical framework used for co-design and co-simulation was introduced, and a simple case study was presented.

6 Acknowledgments

This work is supported by the U.S. DOE Office of Electricity Delivery and Energy Reliability, Cybersecurity for Energy Delivery Systems (CEDS) Program.

7 References

[1] Moteff, J., Parfomak, P.: ‘Critical infrastructure and key assets: definition and identification’. Congressional Research Service, The Library of Congress, Washington, DC, 2004
[2] Bryson, J., Gallagher, P.D.: ‘NIST framework and roadmap for smart grid interoperability standards, release 2.0’. Technical Report NIST Special Publication 1108R2, National Institute of Standards and Technology (NIST), 2012
[3] Cyber Physical Systems Public Working Group: ‘CPS PWG draft framework for cyber-physical systems, release 1.0’ (National Institute of Standards and Technology (NIST), 2016)
[4] Yu, X., Xue, Y.: ‘Smart grids: a cyber-physical systems perspective’, Proc. IEEE, 2016, 104, (5), pp. 1058–1070
[5] Farhangi, H.: ‘The path of the smart grid’, IEEE Power Energy Mag., 2010, 8, (1), pp. 18–28
[6] Gungor, V.C., Sahin, D., Kocak, T., et al.: ‘Smart grid technologies: communication technologies and standards’, IEEE Trans. Ind. Inf., 2011, 7, (4), pp. 529–539
[7] Cooper, A.: ‘Electric company smart meter deployments: foundation for a smart grid’. The Institute for Electric Innovation (IEEE) Report, October 2016
[8] Uribe-Pérez, N., Hernandez, L., Vega, D., et al.: ‘State of the art and trends review of smart metering in electricity grids’, Appl. Sci., 2016, 6, (3), pp. 68–92
[9] NETL Modern Grid Strategy: ‘Advanced metering infrastructure’ (US Department of Energy Office of Electricity and Energy Reliability, 2008)
[10] Rashid Mohassel, R., Fung, A., Mohammadi, F., et al.: ‘A survey on advanced metering infrastructure’, Int. J. Electr. Power Energy Syst., 2014, 63, pp. 473–484
[11] Kuzlu, M., Pipattanasomporn, M., Rahman, S.: ‘Hardware demonstration of a home energy management system for demand response applications’, IEEE Trans. Smart Grid, 2012, 3, (4), pp. 1704–1711
[12] Niyato, D., Xiao, L., Wang, P.: ‘Machine-to-machine communications for home energy management system in smart grid’, IEEE Commun. Mag., 2011, 49, (4), pp. 53–59
[78] Lu, C., Zhang, X., Wang, X., et al.: ‘Mathematical expectation modeling of wide-area controlled power systems with stochastic time delay’, IEEE Trans. Smart Grid, 2015, 6, (3), pp. 1511–1519

[79] Liu, Y., Zhan, L., Zhang, Y., et al.: ‘Wide-area-measurement system development at the distribution level: an FNET/GridEye example’, IEEE Trans. Power Deliv., 2016, 31, (2), pp. 721–731

[80] Zhu, L., Liu, H., Pan, Z., et al.: ‘Adaptive wide-area damping control using measurement-driven model considering random time delay and data packet loss’. 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, 2016, pp. 1–5

[81] Wang, S., Meng, X., Chen, T.: ‘Wide-area control of power systems through delayed network communication’, IEEE Trans. Control Syst. Technol., 2012, 20, (2), pp. 495–503

[82] Hassibi, A., Boyd, S.P., How, J.P.: ‘Control of asynchronous dynamical systems with rate constraints on events’. Proc. of the 38th IEEE Conf. on Decision and Control, Phoenix, AZ, 1999, vol. 2, pp. 1345–1351

[83] Febres, C.A., Araujo, P.B., Furtin, M.: ‘Damping of low-frequency oscillations by supplementary control of power system stabilizers’, Trends Appl. Comput. Math., 2008, 9, (2), pp. 223–232

[84] Yuan, Y., Li, G., Cheng, L., et al.: ‘A phase compensator for SVC supplementary control to eliminate time delay by wide area signal input’, Int. J. Electr. Power Energy Syst., 2010, 32, (3), pp. 163–169