energies

Review

Exploring Cyber-Physical Energy and Power System: Concepts, Applications, Challenges, and Simulation Approaches

Le Nam Hai Pham

Department of Electrical Engineering, IT and Cybernetics, University of South-Eastern Norway, 3918 Porsgrunn, Norway; le.pham@usn.no

Abstract: With the advancement of data-acquisition systems, information technology, and network technologies, the energy and power system has entered the deep integration of the cyber and physical sides as known as cyber-physical energy and power system (CPEPS) leading to more attention from researchers and practitioners in industry. The feedback loops in which physical processes affect cyber parts and vice versa, therefore, can gain greater efficiency, resilience, and intelligence through the data exchange process between two layers. The concept of CPEPS has been existed for a long time and its applications are gradually increasing in the real world, however, there has been still many potential risks and challenges in the research and development process. Simulation method is a common and simple approach for the purpose of analyzing, evaluating, and considering solutions before actual implementation. For this purpose, this paper provides first the framework of CPEPS, and current applications and challenges that researchers are facing. Then, the next section is the overview of simulation methods with different software and tools in CPEPS research in order to provide researchers with an optimal approach to the ongoing and further research towards the transition of digitalization on energy and power system.

Keywords: cyber-physical energy and power system; cyber-physical simulation methods; CPEPS framework

Citation: Pham, L.N.H. Exploring Cyber-Physical Energy and Power System: Concepts, Applications, Challenges, and Simulation Approaches. *Energies* **2023**, *16*, 42. https://doi.org/10.3390/en16010042

Academic Editors: Valeria Boscaino, Giovanni Tinè and Nicola Panzavecchia

Received: 15 November 2022
Revised: 9 December 2022
Accepted: 19 December 2022
Published: 21 December 2022

1. Introduction

In the era of digitalization transformation, cyber system (control, computing, and communication) capabilities have been embedded in all types of objects and structures in the physical environment. A new technology with the integration of two layers, physical and cyber, is called Cyber-Physical System (CPS) leading to significant impacts and economic benefits that will be developed by harnessing these capabilities across both space and time [1]. With the same integration trend, the energy and power system are becoming increasingly complex in the development direction to utilize sustainable energies sufficiently and improve the safety, reliability, and efficiency of power grid. Indeed, electrical power grid is presently integrated with data devices, data acquisition devices and computing devices via the information communication technologies (ICT). The operation of the power system is dependent not only on energy flow but also on information flow. The integration of conventional energy and power systems with physical equipment as a core element and cyber system is called Cyber-Physical Energy and Power System (CPEPS).

Even though the concept of CPEPS has appeared for a long time, the deep study of smart grids or energy and power sectors have gradually increased over the years with examination of physical power grids and power communication networks in collaboration [2]. Research efforts have been made worldwide from industry, academia, and national laboratories in the field of CPEPS research to contribute the investigation of power system vulnerabilities, mitigation strategies and system behavior during different kinds of conditions. Accordingly, the annual publication in the sector of CPEPS is increasing gradually over the years as shown in Figure 1 demonstrating the high interest of research in this area.

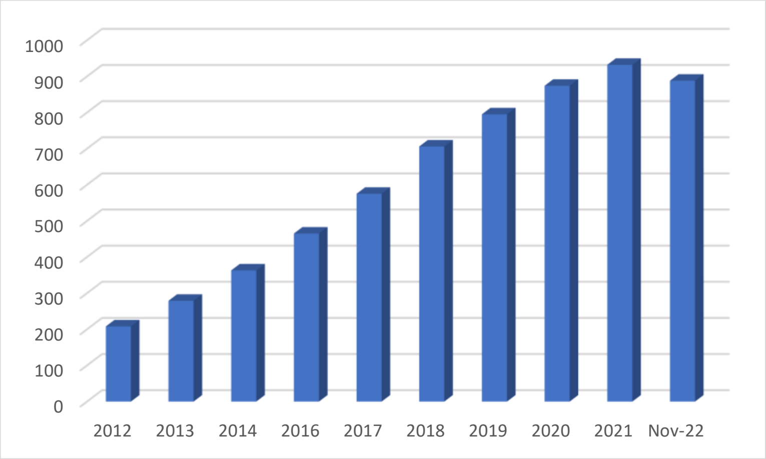


Figure 1. Annual publications in advanced search for CPEPS sector (Source: Google Scholar).

To develop a systematic, efficient, and all-encompassing approach to analyze the framework of CPEPS with energy and information flow in the day and age, it is important to understand the foundation concepts, and simulation methods. For this purpose, in the recent years, numerous and various review materials intend to provide overview and collect new research ideas, achievements in CPEPS. Cao et al. published a book named "Cyber-physical Energy and Power Systems" [3] in the motivation of reporting new results of modelling, analysis, and applications such as a CPEPS cascading failure model, a quantitative analysis method for substations with a cyber-physical interface matrix, a simplified co-simulation model for analyzing CPEPS interdependencies, or a CPEPS co-simulation architecture. Additionally, the document [4] provides a comprehensive review of different modelling, simulation, and analysis methods. Even though the digital technologies monitoring and controlling the energy and power system more efficiently and reliably, the dynamic consequence in cyber-system is opening high risk to cyber-security involving the complex interdependency between cyber and physical system. Therefore, taking integration and unification of the cyber and physical systems into consideration is important for configuration optimization and ensuring the safety and security of operation.

With the development of modelling and simulation environments, there has been lots of software, tools and integration modules support for researcher in CEPES sector, however, it is difficult to see the literature review about the software with its advantages and disadvantages. Therefore, the common simulation approaches used in CPEPS are summarized. This paper outlines as follows: the framework of CPEPS to describe the concept of CPEPS, then, the current CPEPS applications and challenges. The simulation approaches are given with advantages and disadvantages of common simulation software. Lastly, Sections 5 and 6, "Proposed Research Direction" and "Conclusions", will conclude this paper.

2. CPEPS Framework

The CPEPS mainly consists of two separated layers: energy and power system (physical layer), and communication network (cyber layer). In the physical layer, electrical and energy quantities (such as current or voltage measurement) in analog signals are converted into digital signals, then this data is transferred to the cyber layer through wired or wireless communication unit [2]. These signals are analyzed and processed via decision-making and computation unit of cyber layer and send the control signals back to the physical devices. Essentially, energy and power flows are optimized through information layer-based computation and control. The two layers are described detailly as following sections, physical energy and power system, and cyber system.

2.1. Physical Energy and Power System

The physical layer of CPEPS involves all the domains of energy and power system such as generation, transmission, distribution, or utilization, as shown in Figure 2. It may be defined as a huge structure made up of nodes and branches, with energy flowing between them. Other factors affecting to the energy flow such as temperature, humidity, wind speed, light intensity or other non-energy information influencing the functioning of equipment are also required. In addition, CPEPS can cooperate with other social system, such as transportation system, and with the environment to create a green economy and long-term development [3]. CPEPS has capabilities to monitor and operate power system in a secure, reliable and efficient manner, assisting in the achievement of the optimal balance between generation, distribution, and consumers [5]. The aforementioned fusion of power, information, and control can increase the safety, reliability, and efficiency of the power system by providing physical entities with functions of computing, communication, accurate control, coordination, and autonomy [6].

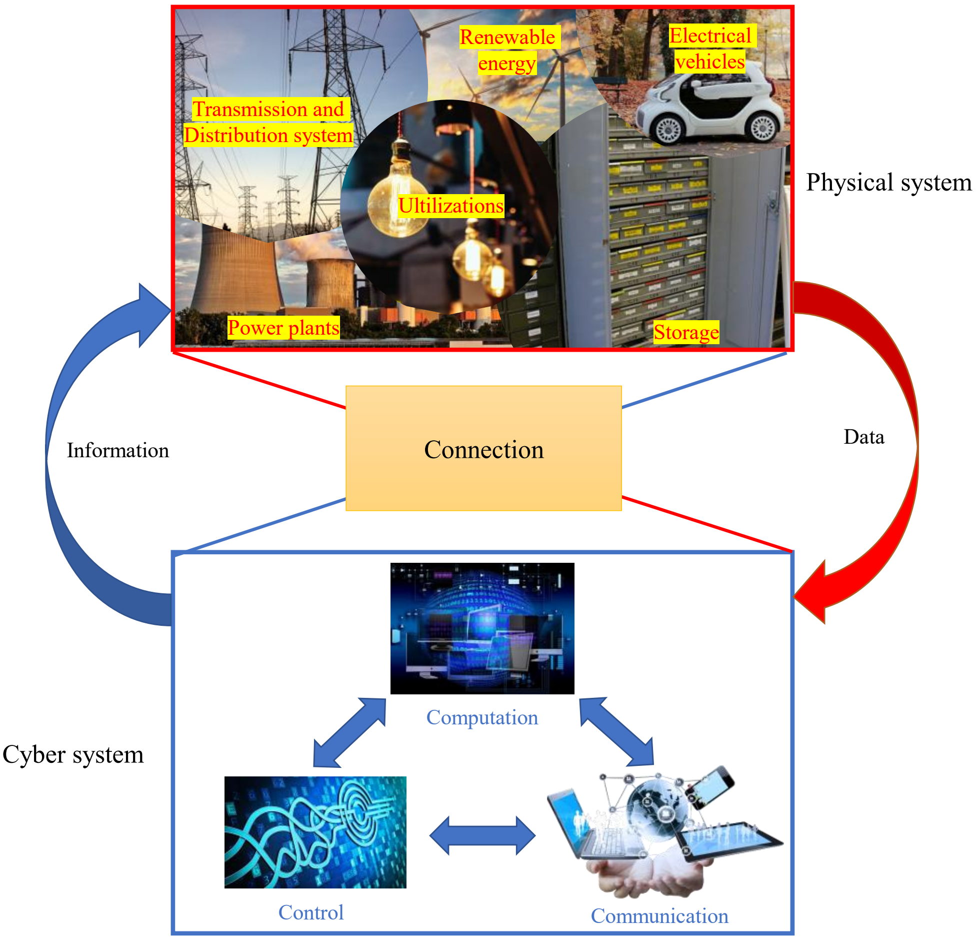


Figure 2. Structure of CPEPS.

The methods of modelling, analysis and simulate energy and power system, today, has been relative mature, but mainly using offline and static approach, these methods when applied in discrete event or synchronization time, they become imprecise. The impact of integration between physical and cyber system to each other is studied and developed in the future.

2.2. Cyber System

The cyber system contains three main features as known as 3C, control, computing, and communication. While the computing and control part are considered as the brain of the system with the task of analyzing and making decisions, the communication part is considered important with the task of exchanging information between the two layers, receiving data from the physical layer and return feedback from cyber layer. With different systems, the construction of computing and control parts is also different, however, the communication unit is based on basic working principle. Figure 3 shows the structure of cyber system with the communication part connecting with the physical system.

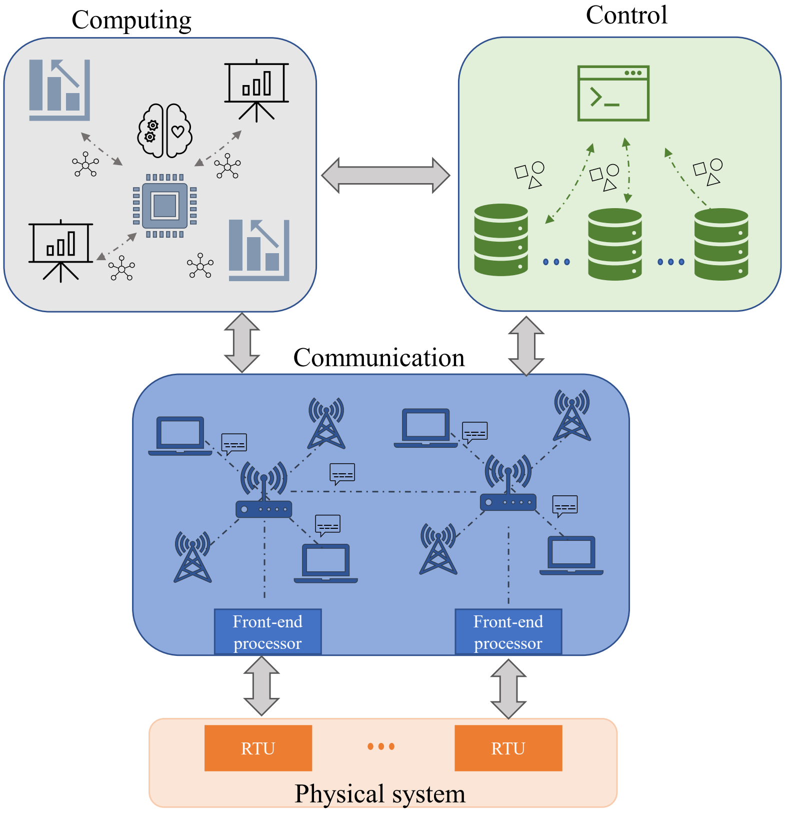


Figure 3. Framework of cyber system.

The communication feature consists mainly of equipment for information and data exchange such as terminal equipment, switching equipment and transmission link. The process of exchanging data and information of energy and electricity quantities is of primary interest in the research of CPEPS. The main purpose of communication layer in CPEPS is functionally to realize the measurement data of the energy and power system's flow and the control of operation equipment on the support of SCADA based on telecommunication control technology to completely receive the energy and power flow data, remotely indication and command, and remotely system adjustment. The remote terminal unit (RTU) at energy and power station and front-end process at the control center play an important role. The RTUs are responsible for collecting operation information of the physical system required from the dispatching center, and then sending it to the terminal processor of the dispatching center in the real-time process [2]. The front-end processor forward collected information from RTUs to the control center with two functions, computation for decision making and control signal feedback to the physical layers [2].

In energy and power industries, the automation of control systems of substations uses variety of specialized standards, technologies, and protocols, Among the most frequently used belong MODBUS [7], IEC 60,870 [8], DNP3 [9], and IEC 61,850 [10], the standard of communication in substations has resolved the interoperability between measurement equipment such as intelligence electronic devices (IEDs) from different vendors. However, these protocols still operate at the electronic utility level, the cyber system is usually adopted over the standards with the ultra-high speed and low loss latency communication environment [11]. It is difficult to describe fully structure of cyber system, this section gives the insight concept of cyber system and its operation, neglecting particular and complicated processes such as coding and modulation.

3. Current Applications and Challenges

3.1. Applications

Today, CPEPS are used as a new innovation of built-in control systems capable of monitoring and controlling physical energy and power systems in real-world scenarios. Many applications are being increasingly dependent on CPEPS. In this paper, common and trending applications of CPEPS research are given.

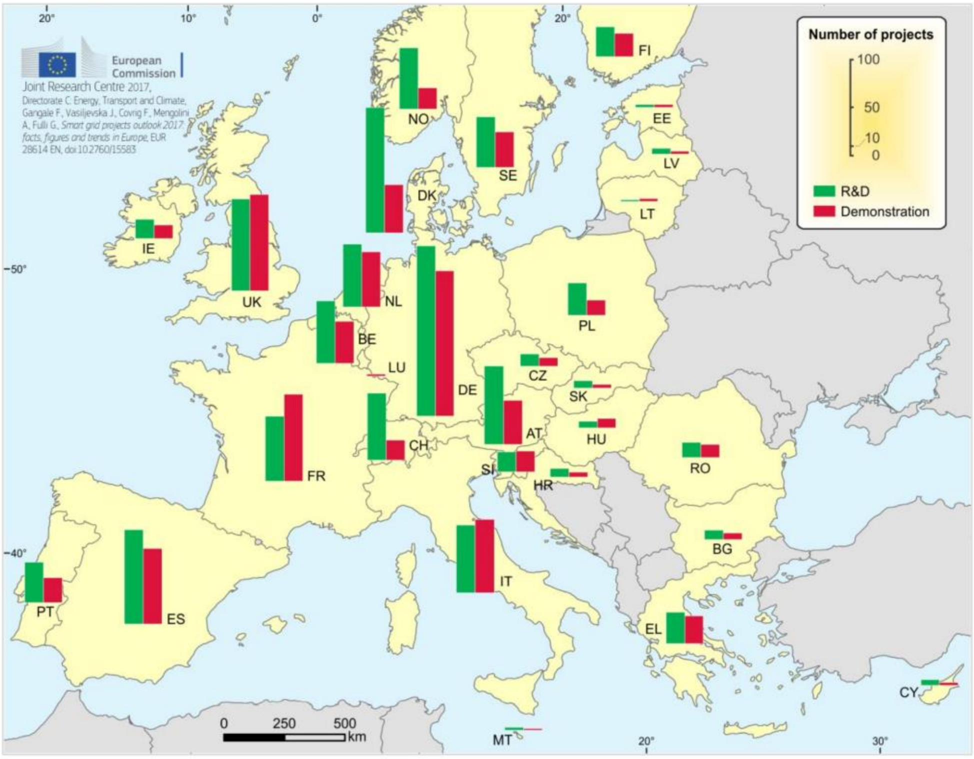
3.1.1. Management and Control Energy and Power

Applying integration of cyber and physical system for monitoring and control enhances controllability and energy flow in different operation situation and ensure the reliability, efficiency and resilience of physical energy and power stations. Sensors and actuators are being used to connect the electrical devices from physical world to communication network. Both communication capabilities via wired and wireless are set up in this system so that it can be utilized depending on the essence of the surrounding environment. Moreover, it has the ability to supervise and operate the activities in the control center by connecting it to the virtualization system. This application is being studied deeply to develop a large-scale integrated system to reduce the number of physical devices and achieve high efficiency in energy management and control. Automation optimization mechanism or self-healing after failure will be emphasized in the future developments.

3.1.2. Smart Grid

Even though power grids have been utilized for decades, smart grid is the new innovation of power grid that generates electricity with state-of-the-art features [12].

Smart grid is an ecosystem which will integrate its basis on information acquisition assessment and decision making as well as management. In general, it will control the connection of the network and the operational aspects in the electricity generation by two-way communication and control between power grid and consumers. The transition towards green energy leading to the high integration of renewable energy, it is where smart grid can play to its advantage through ability to receive measurement and respond optimal operation to physical power grid. Indeed, in recent years, the number of smart grid project has been gradually increased. Figure 4 shows the information of R&D (research and development) and demonstration project around European countries through the outlook of fact and trends in this area in 2017. The smart grid will receive more attention and focus on the future.



European Commission
Joint Research Centre 2017,
Directorate C Energy, Transport and Climate,
Gangale F., Vasiljevska J., Covrig F., Mengolini
A., Fulli G., *Smart grid projects outlook 2017: facts, figures and trends in Europe*, EUR
28614 EN, doi:10.2760/15583

Figure 4. Number of smart grid projects in the EU in 2017 [13].

3.1.3. Smart Vehicles

CPEPS provide an intelligent vehicle or smart vehicle that are vehicles that are more eco-friendly, more energy-efficient, safer, and have improved usability and convenience. Nowadays, smart vehicles can exchange data through various communication protocols in response to technological developments in smart transport system. As the IoT and data remaining fundamentally related, the virtual vehicle is possible in transport network's evolving design [14]. The smart vehicles are being developed presently to improve both carbon footprint as well as help reduce traffic congestion and maximize use of public transit.

3.2. Challenges

The existing challenges in CPEPS are proposed in this paper, which is ongoing research and encourage people to find out the solutions addressing these challenges. According to the existing technologies in the day and age, the devices currently are smart and connected to the Internet leading to challenges in (1) Cyber-physical attacks, (2) Data protection and data security. Therefore, it requires a system to predict and detect attacks as quickly as possible, challenge (3) Forecasting. Furthermore, the integration of cyber-system into existing conventional system with different vendors can bring challenge (4) Change management and conflicts in integrations, as well as the simulation-based in the future system–challenge (5) Model-based development. Overall, Figure 5 shows the current challenges of CPEPS.

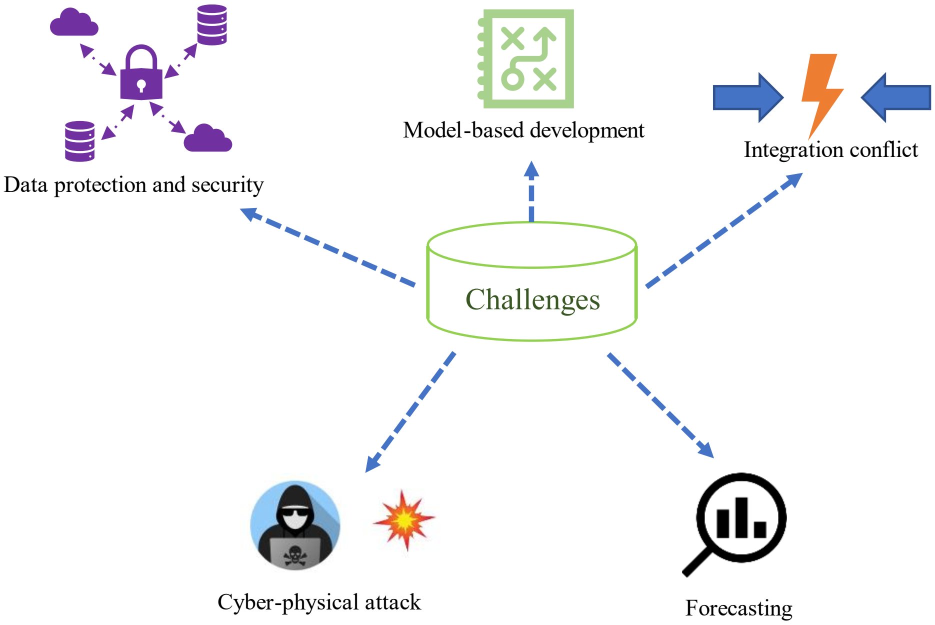


Figure 5. Current challenges of CPEPS.

3.2.1. Cyber-Physical Attack

In CPEPS, measurement data is collected from the physical system and transferred to the control system in the cyber layers. It makes higher efficiency and reliability of power and energy system related to the development of ICT. However, consolidated layers lead to new types of potential risks. On the one hand, the cyber system may adversely influence the physical system when cyber-attacks are involved. For example, untimely and/or fake commands may damage the facilities or even initiate a sequence of cascading events. On the other hand, many critical functionalities of the CPEPS require accurate information and measurements from the physical system. Failures of sensors, devices and communication lines lead to incomplete data, delays in computing and failures to deliver important commands. Consequently, the reliability of the physical system is compromised.

3.2.2. Data Protection and Data Security

Users are concerned about how their information and data will be used when registering to use the smart grid in the form of smart meters integrated into mobile devices, or remote monitoring devices. Since these devices connecting to Internet become more prevalent, this has become major issues for people. Customers 'data should not only be encrypted, but anonymization techniques should also be suggested to prevent attackers from deducing patterns or encrypted data to reveal private information. As a result, it is critical to ensure that the mechanism designed can both encrypt and safe data.

3.2.3. Forecasting

Detecting and responding to an attack is critical. Supervisory and monitoring systems are used to look for traces from invalid intrusions form a network or computer system. However, the algorithms become ineffective against attacks that tend to deceive the estimation and control mechanism. In addition, the control devices, and sensors, if physically attacked, are difficult to detect. As a result, the study of human–computer interaction is critical and difficult, because not only must recovery with a person-in-the-loop be considered, but also recovery without a person interface or self-healing. The unforeseen problems when people consider and develop a secure system after using autonomous real-time decision-making algorithm helping control the real-world cases, is being developed.

3.2.4. Change Management and Conflict in Integrations

The new integration also leading to the new equipment and software from different vendors, therefore, many conventional devices must be replaced, altered, or removed. To avoid problems, a CPEPS system update needs to be considered carefully. Furthermore, numerous investors can modify the security posture of the CPEPS system without their awareness, therefore the coordination in change management in avoiding and tracking security-related in the CPEPS should be taken into account. In order to avoid new security issues, new components can be safely integrated into existing systems. Notices that the power grid has been exist in a long time ago, therefore, the amount of old system can be vulnerable in integrations. It will require a lot of time, effort, and fund to replace them all with new, safer ones. As a result, short-term solutions need to be found to keep the system running smoothly without any major issues.

3.2.5. Model-Based Development

Model-based design is a power design technique for CPEPS that emphasizes the mathematical modelling to design, analyze, verify, and validate dynamics systems. Modelled systems may be tested and simulated offline, enabling developers to verify the logic to their application, assumptions about its environment, and end-to-end such as open-loop or closed-loop behavior. The design of open, large, and complex engineered system will be always challenge, the expectations of model-based is solving real-world problems.

4. Simulation Approach of CPEPS

Simulation is a typical and simple approach for evaluating CPEPS performance as well as solving existing challenges by modelling the CPEPS in simulation environment to analyze and evaluate before actual implementation. Therefore, this paper reviews simulation approach with two implementation manners classified as re-implementation and co-simulation. The first method is to re-implement the communication models in the power system simulator (or vice versa), while the second is to set up a co-simulation platform that incorporates both simulators and uses a simulation control module to achieve time synchronization and data interchange.

4.1. Re-Implementation Method

For simulating the entire CPEPS, re-implementation is a traditional method when implementing the communication models in power system simulator (or vice versa), with no integration of time synchronization and data exchange construction. In other words, this method uses the results of the simulation to perform another simulation. Therefore, in this approach, the power and energy system, and communication simulator lacks the connections and cannot support exhaustive functions from each other. The platform accomplished analysis of static power and energy system or communication network, and then uses the results to continue conducting simulations of the remaining system. For instance, an integrated development platform was setup by modelling the power system in MATLAB and then linking to OMNeT++, a discrete event simulator to assess the effectiveness of control mechanism by controlling storage and loads from available renewable energy [15]. By compiling the MATLAB files into .h, .lib, .ctf, and .dll files, and add these file into OMNET++, then, the integrated platform can be executed. In addition, the authors in [16] proposed an integrated simulation platform to analyze the impact of cyber system on power systems. The work in this paper includes three simulation modules, power system by TH-STBLT (a power system simulator designed by Tsinghua University), communication simulation with NS2, and the control simulation based on MATLAB. The authors also emphasized the difficulties to integrate different platform to simulate smart grid.

This conventional approach lacks the integration, connection and data exchange of two layers. Additionally, this method faces the challenge in selecting a communication network, power system or other platform as the basis for CPEPS, and implement the other components from scratch or link existing libraries or tools [17]. However, it contributes the concepts as well as fundamental buffer for simulation platform in the future.

4.2. Co-Simulation Method

When two or more models are used in a single simulation, the term "co-simulation" is used. In other words, co-simulation occurs when these two or more distinct models are run simultaneously and their variables or states depend on each other, then, these simulators are synchronized periodically.

Co-simulation is a viable and practicable method for ensuring simulation accuracy and efficiency by utilizing dedicated and readily accessible libraries for the integration of power and information communication system [18], and develop a collaborative simulation platform employing mature power system simulation software and communication system software to enable interaction under separate simulation conditions. The advantages of co-simulation approach can be listed as follows [19]:

- New models can be combined with legacy models already in use. Frequently, it is not possible to re-implement the given resources.
- A multidisciplinary problem can be broken down into pieces using specialized simulators. By doing so, models of one sub-model need to be duplicated in the simulator of another sub-problem. The model library and user interface of the specialized simulator are typically better and more tailored to the specific domain.
- The focus of the simulation study can have multiple foci. There is no need to simplify sub-problems, in contrast to a typical simulation. Since each sub-problem operates in a specialized environment, it is possible to model each one in detail.

The co-simulation consists mainly of the four sections as follows: power system simulation, communication network simulator/emulator, data measurement and collection simulator, and end user application simulator [3]. Simulators for digital power systems and communication systems are often discrete time based. The communication simulator/emulator must be used to mimic data measurement and collecting equipment in order to measure and export power system data to end user applications. There are two types of co-simulation methods: non-real-time and real-time.

4.2.1. Non-Real-Time Co-Simulation

The non-real-time co-simulation is using offline simulation based on discrete event. In other words, the discrete event can be described that the time step approach for a simulation model to advance time with fixed quantity, then, every state variable is updated according to the logic define by the model. There are a variety of simulation tools for modelling and simulating individual domains of CPEPS as well as integrated frameworks of power system domain and cyber system domain. Multi commercial software tools are available for CPEPS simulation as proposed by [4], as shown in Table 1. The power system and cyber system simulators in first and second column, respectively, are only capable for simulating power or cyber system, therefore, to perform co-simulation, users need to use concurrent links between these software. In the recent years, there has been many researchers performing the non-real-time co-simulation using integration of power and cyber simulator [20,21]. Yang et al. [18] provided a co-simulation for innovative integrated smart grid simulation framework by using MATLAB/Simulink for the distribution grid, through communication channels such as UDP and TCP socket, in order to consider computation and communication delays on the controller side. In the same interest of using co-simulation in smart grid scheme, the authors in [22] described a co-simulation framework by using Virtual Test Bed for dynamic simulation of the multi-physics power system and OPNET for realistic representation of communication network, with a wide range of protocols. The co-simulation framework in this paper is based on code generation that is implemented in C# and equipped with users interface to allow users to set a global co-simulation step time. Additionally, a global event-driven co-simulation framework is proposed in [23] by using PSLF and NS2 software. In this paper, the authors used global event-driven mechanism to create co-simulation framework to exchange the data between two simulators. It can be seen that the co-simulation framework between pure power, or cyber simulators requires much time and effort in finding a suitable way to connect these software/tools with each other. In addition, today's popular cyber system simulation tools with advantages and drawbacks that can be listed in Table 2.

Table 1. Simulation tools.

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

However, with the development of simulation technology, integrated model-based design of complex CPSs or called co-simulation tools (which mix physical dynamics with software and networks) are currently established to being able to model itself or integrate both systems in the same software that can be given in co-simulation tools part in Table 1. The MODELISAR project has released FMI—Functional Mockup Interface, a new open standard for model interchange and tool interoperability that simplifies whole product modeling [24]. FMI enables any modeling tool to generate C code or binaries that represent a dynamic system model, which can then be seamlessly integrated into another modeling and simulation environment [24]. FMI only specifies how the (co) simulation software interacts with the models, it is not in itself a simulation software. FMI is now supported by a plethora of simulation-based software/tools. Based on FMI, Modelica or Modelica-like simulation environments exist for modeling, compiling, and simulating Modelica models, such as Dymola, MapleSim, OpenModelica, Wofram SystemModeler, and others. These environments are responsible for transforming graphical models into efficient simulation code using symbolic algorithms for manipulating and simplifying resulting large-scale equation systems [25]. In the field of CPEPS, the paper [26] presented the electrical components adapted to Smart Grid simulation based on Modelica language and the FMI standards. In the similar topic, the authors in [27] emphasized the focus on possibilities to exploit Modelica and FMI technologies through the rapid toolbox and the power system library in Modelica for power system model identification. In addition, the authors in [28] proposed LabView as an oriented programming technology utilization for cyber-physical systems modelling and simulation purposes without integration with another software/tools.

Table 2. Common communication system simulation tools.

Simulation Tools	Applications	Advantages	Drawbacks	References
OMNET++	- Building network simulators based on C++ simulation library and framework. - Modelling communication networks, multiprocessors and other distributed or parallel system. - Real-time simulation, network emulation, hardware-in-the-loop functionality	- Structured and strong - Extremely adaptable - Not limited to network protocol simulation - Source code is freely accessible - Internet, IPV6, mobility simulation model is able available	- It does not provide a wide range of protocols - Users with significant background work - Poor standard performance analysis and management - The mobility extension is comparatively incomplete	[29–31]
OPNET	- Simulate any type of network's behavior and performance. - Potential working with OSI model	- Fast discrete event simulation engine - Element libraries with source code - Object-oriented modelling - Environment of hierarchical modelling - Support for scalable wireless simulations - Customizable wireless modelling - Discrete event, Hybrid, and Analytical simulation - Grid computing support	- Complex GUI operation - It does not allow a collection of nodes within a single connected device - The sample resolution limits the precision of the results - If nothing happens over lengthy periods of time, simulation is rendered ineffective	[31,32]
NS2	- Provide substantial support for simulation of different protocols over wired and wireless networks - Provide a highly modular platform for wired and wireless simulations supporting different network elements, protocols, traffic, and routing types	- Low cost and costly equipment is not required - Complex scenarios can be easily tested - Simple and quick way for correcting errors - Supported protocols - Supported platforms - Popularity and modularity	- Actual system is complicated to model - Unreliable bugs	[31,33]
NS3	- Provide and open, extensible network simulation platform for networking research and education - Provide models of how packet data networks work and perform and provides a simulation engine for users to conduct simulation experiments. - Modelling how Internet protocols and networks work.	- The system has been modularized - Modular libraries can be accessible - Individual modules are organized in a directory structure - The node to use external routing is enabled	- Suffers from lack of credibility - Modules, component based on NS2 - NS3 needs lot of maintainers - Active maintainers are necessary	[31,34]
GLOMOSIM	- Simulate network protocols - Simulate a large-scale wireless and wired networks	- It gives modular simulation for protocol stack	- The documentation is inadequate - No specific routing protocols for sensor network, no energy	[31,35]

	- Support Mobile adhoc networks and many major networking areas	- It is able of scaling up to networks with thousands of heterogeneous nodes - Parallel model execution is given to users in transparent manner - It is no cost for education and research	consumption models for transport layer and IP address support - It depicts the Random Waypoint mobility model, which may not be appropriate for all types of simulations - QualNet, the commercial version of GLOMOSIM, is primarily focused	
MATLAB SimEvent	- Model message-based communication in Simulink or any event-driven process with its discrete-event simulation engine and component library - Analyzing and optimizing event-driven system models	- Platform Independence - Predefined Functions - Device-Independent Plotting - Graphical user interface - MATLAB compiler	- Interpreted language - High cost - Difficult to develop real time applications	[36,37]

4.2.2. Real-Time Co-Simulation

In order to make the simulation behave exactly like real-world circumstances, real-time simulation refers to a model of a physical system that can run at the same speed as actual clock time. Comparing between non-real-time and real-time simulation, there has several research in recent years [38,39]. The authors in [40] proposed several experiments to calculate the time gap from the wall-clock time to verify the real-time behavior of a simulation run. The result in this paper demonstrated the difference in milliseconds between discrete event simulation with real-time simulation. As a result, when applied to the CPEPS sector, real-time simulation may be utilized to assess the dynamic power system by deriving the mathematical expression of numerous events originating in power and information systems. For simulating of CPEPS in real-time, according to [41], it was concerned with the creation and deployment of a complete cyber-power test bed comprised of simulation, emulation, and actual devices. Real-time co-simulation necessitates that the simulation software can run in real-time and the model be partitioned into several sub-models for parallel computing. This requires hardware-based real-time power system simulation platforms, such as Real Time Digital Simulator (RTDS) [42], OPAL-RT [43] and a new developing technology called Typhoon HIL [44] with the structure as shown in Figure 6. The real-time co-simulation is expensive and difficult because of hardware requirement; therefore, it is currently being developed and is mostly used for testing and exercising smart grid projects. However, Typhoon HIL developed and established Virtual HIL that is a true enabler or test-driven development processes where supports for users can deploy and run all real-time ready models without any actual hardware devices

At the same time, RTDS is commonly used to simulate the power system and sensor simulation as while network simulator-3 (NS3) is used to simulate the communication system according to [45]. The RTDS can be interfaced with external devices through dedicated analog and digital signal interface cards. In addition, phasor measurement units (PMUs) compliance, with the IEEE C37.118.1 standard [46], GOOSE messaging and IEC 61850-9-2 sampled value messaging for power system voltages and current are also used according to [47,48].

Related work about real-time CPEPS was conducted on suitable power system testbeds. The researchers at national SCADA testbed at Idaho National Laboratory investigated how a cyber-attack can cause damage to a physical system through an aurora generator test [49]. Similarly, the DIgEnSys-Lab [50] (a research group and a laboratory) at University of South-Eastern Norway is facilitated for real-time simulation research with OPAL-RT and Typhoon HIL as focus. The researchers at this lab proposed solutions to the most critical challenges to carbon-neutral energy system by showing the implementing a cyber-physical testbed for frequency analysis response in integration of two real-time simulators Typhoon HIL and Opal-RT [51].

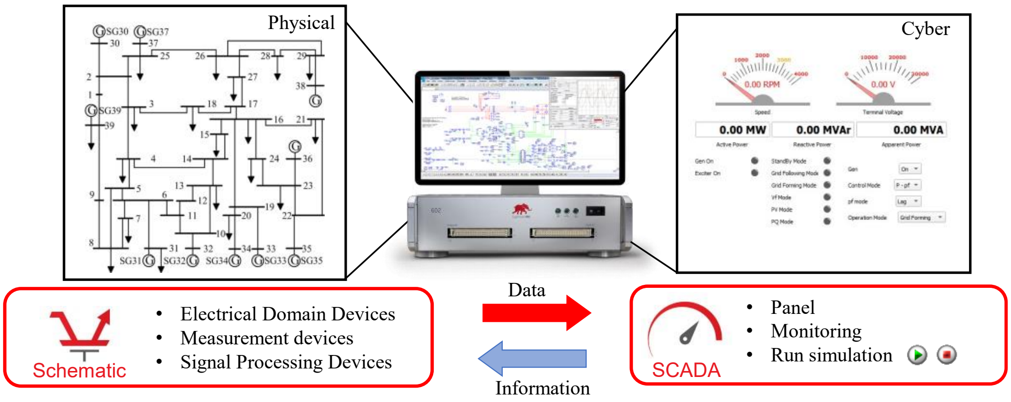


Figure 6. Real-time simulation using Typhoon HIL.

Focusing to a CPS testbed for cyber security issues, a testbed has been developed at University of Arizona using PowerWorld and MODBUS protocol to detect cyber-attacks on SCADA system [52]. In addition, a power system cyber-physical testbed was developed for intrusion detection and provides the platform for Hardware-in-the-Loop (HIL) simulation, cyber-attack and generated data sets for developing and validating an intrusion detection for monitoring power system events [53]. Researcher in [54] provided the development of a real-time cyber-physical system testbed for cyber security and stability control. The SEL 351S protection system with OPAL-RT including control functions and communications were used in that paper to analyze the impact of failures in experiment of knocking down two transmission lines. The high number of real-time CPEPS research demonstrates the major role in the development of the next-generation technology systems.

5. Proposed Research Direction

The large-scale deployment of networked CPEPS has been applied to address global needs in a variety of areas such as energy, water, health care and transportation during the recent decades. In the energy and power system major, CPEPS is considered as a smart power grid, future grid, intelligent grid, inter grid of the 21st century power grid of the world [55].

It allows two-way flow of electrical/energy and information to create a wide distributed automated power delivery network. According to the current challenges in the CPEPS research, the following research directions of CPEPS can be explored as follows:

(1) In CPEPS simulation methods, the time synchronization methods play a critical role in the efficiency of simulation, especially non-real-time-co-simulations. Therefore, creating and establishing and effective synchronization strategies will improve the accuracy of the simulation. Currently, physical energy and power, and communication network is analyzed, validated, and simulated in separated tools, so it is necessary to develop and platform capable of integrating features of these software, and satisfy the conditions of real-time simulation. In addition, real-time simulation software lacks specific analysis features such as specialized software for physical and cyber systems, the development of these features should be concerned.

(2) Digital twin is another concept associated with the cyber-physical integration that can creates a high-fidelity virtual model of physical objects in virtual space in order to simulate their behaviors in the real world and provide feedback. In terms of operating status and risk prediction, digital twin can propose an accurate equivalent method for physical entities and become an opportunity for the rapid development of CPEPS simulation methods in the future.

(3) The merged functionality to reduce physical equipment in the power station can be developed in the future. For example, the control devices such as silicon-controlled

rectifier (SCR) or DC-AC converters and protection devices such as circuit breaker or protection relays in the power system today are independent and unrelated to each other. These devices' functionality can be merged on the advancement of ICT, the control center receives data from the physical system, and then makes protection or control decisions. Figure 7 shows the diagram of cyber-physical convergent purpose for protection and control functionalities under ultra-high speed communication.

(4) Data and information transmission processes, from receiving data at the cyber layer to responding the control signals to the physical layers, are now being implemented according to communication protocols standards. However, with the increase of massive data nowadays, there is a need for a method out of standards limitation to speed up data processing between the two layers to improve the robustness of state perception, attack prediction, reliability assessment and CPEPS models.

(5) The cyber-security in communication network is necessary to enhance the anti-hacking capabilities toward the transition of digitalization of energy and power system. The cyber system should have self-healing and self-defense during cyber-attack. This direction should develop in the near future.

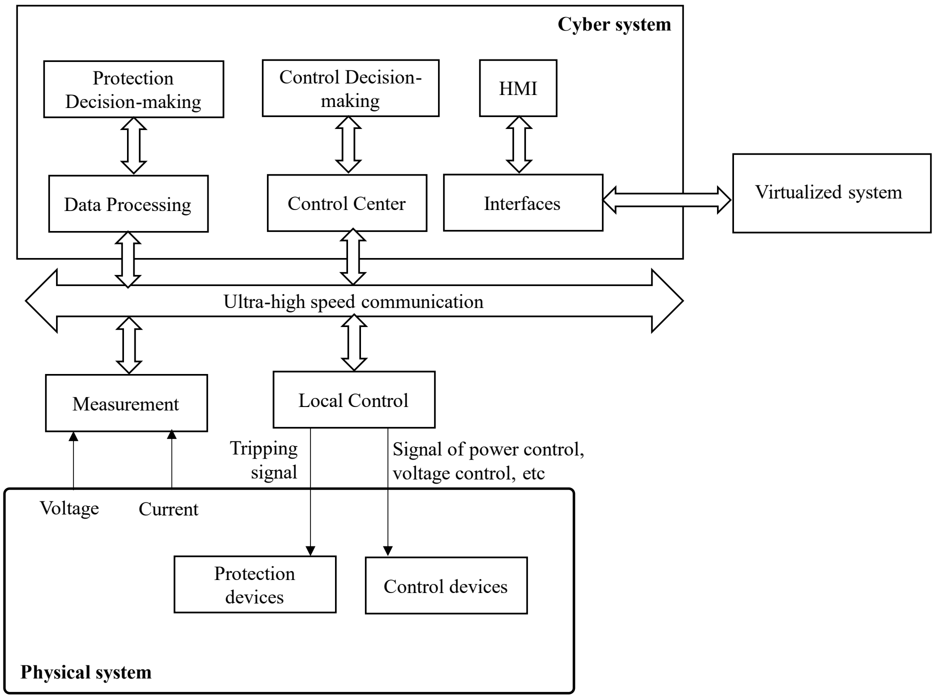


Figure 7. Ultra-high speed communication protocol together with convergent protection and control functionalities development.

6. Conclusions

In the transition toward digitalization with the respect to ICT advancement, power and energy systems gradually integrate digital processing technologies toward a new generation term called cyber-physical power and energy system aiming to the greater efficiency, reliability of the system. CPEPS has certain benefits and is being researched and developed with current applications such as smart grids, energy and power control and management or smart vehicles, however it still has many potential challenges and risks. These challenges can be addressed through simulation approaches, which help researchers simulate, analyze, and validate their logics and solutions before actual implementation. This paper gives two simulation manners including re-implementation, a traditional way, and co-simulations which are being applied commonly by many researchers. The review of research in the past years with overall simulation tools in CPEPS are also given in this paper with advantages and disadvantages. This paper helps ongoing and further research have accurate simulation approaches.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: The author would like to thank University of South-Eastern Norway, campus Porsgrunn for supporting during his PhD period.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Rajkumar, R.; Lee, I.; Sha, L.; Stankovic, J. Cyber-physical systems: the next computing revolution. In Proceedings of the 47th Design Automation Conference on—DAC '10, Anaheim, CA, USA, 13–18 June 2010; p. 731. https://doi.org/10.1145/1837274.1837461.
2. Fan, H.; Wang, H.; Xia, S.; Li, X.; Xu, P.; Gao, Y. Review of Modeling and Simulation Methods for Cyber Physical Power System. *Front. Energy Res.* **2021**, *9*, 642997. Available online: https://www.frontiersin.org/article/10.3389/fenrg.2021.642997 (accessed on 12 June 2022).
3. Cao, Y.; Li, Y.; Liu, X.; Rehtanz, C. *Cyber-Physical Energy and Power Systems: Modeling, Analysis and Application*; Springer: Singapore, 2020. https://doi.org/10.1007/978-981-15-0062-6.
4. Yohanandhan, R.V.; Elavarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications. *IEEE Access* **2020**, *8*, 151019–151064. https://doi.org/10.1109/ACCESS.2020.3016826.
5. Cai, Y.; Huang, T.; Bompard, E.; Cao, Y.; Li, Y. Self-Sustainable Community of Electricity Prosumers in the Emerging Distribution System. *IEEE Trans. Smart Grid* **2017**, *8*, 2207–2216. https://doi.org/10.1109/TSG.2016.2518241.
6. Cyber-Physical System. Wikipedia. 20 April 2022. Available online: https://en.wikipedia.org/w/index.php?title=Cyber-physical_system&oldid=1083735376 (accessed on 12 June 2022)
7. Fovino, I.N.; Carcano, A.; Masera, M.; Trombetta, A. Design and implementation of a secure modbus protocol. In *International Conference on Critical Infrastructure Protection*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 83–96.
8. Lin, C.-Y.; Nadjm-Tehrani, S. Understanding IEC-60870-5-104 traffic patterns in SCADA networks. In Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Incheon, Republic of Korea, 4–8 June 2018; pp. 51–60.
9. Amoah, R.; Camtepe, S.; Foo, E. Securing DNP3 broadcast communications in SCADA systems. *IEEE Trans. Ind. Inform.* **2016**, *12*, 1474–1485.
10. Brunner, C. IEC 61850 for power system communication. In Proceedings of the 2008 IEEE/PES Transmission and Distribution Conference and Exposition, Chicago, IL, USA, 21–24 April 2008; pp. 1–6. https://doi.org/10.1109/TDC.2008.4517287.
11. Horalek, J.; Matyska, J.; Sobeslav, V. Communication protocols in substation automation and IEC 61850 based proposal. In Proceedings of the 2013 IEEE 14th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, Hungary, 19–21 November 2013; pp. 321–326. https://doi.org/10.1109/CINTI.2013.6705214.
12. Tyagi, A.K.; Sreenath, N. Cyber Physical Systems: Analyses, challenges and possible solutions. *Internet Things Cyber-Phys. Syst.* **2021**, *1*, 22–33. https://doi.org/10.1016/j.iotcps.2021.12.002.
13. Gangale, F.; Vasiljevska, J.; Covrig, C.; Mengolini, A.M.; Fulli, G. *Smart Grid Projects Outlook 2017: Facts, Figures and Trends in Europe*; Publications Office of the European Union: Luxembourg, 2017.
14. Alshdadi, A.A. Cyber-physical system with IoT-based smart vehicles. *Soft Comput.* **2021**, *25*, 12261–12273. https://doi.org/10.1007/s00500-021-05908-w.
15. Mets, K.; Verschueren, T.; Develder, C.; Vandoorn, T.L.; Vandevelde, L. Integrated simulation of power and communication networks for smart grid applications. In Proceedings of the 2011 IEEE 16th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Kyoto, Japan, 10–11 June 2011; pp. 61–65. https://doi.org/10.1109/CAMAD.2011.5941119.
16. Wan, Y.; Cao, J.; Zhang, S.; Tu, G.; Lu, C.; Xu, X.; Li, K. An integrated cyber-physical simulation environment for smart grid applications. *Tsinghua Sci. Technol.* **2014**, *19*, 133–143. https://doi.org/10.1109/TST.2014.6787366.
17. Mets, K.; Ojea, J.A.; Develder, C. Combining Power and Communication Network Simulation for Cost-Effective Smart Grid Analysis. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1771–1796. https://doi.org/10.1109/SURV.2014.021414.00116.
18. Yang, C.; Zhabelova, G.; Yang, C.-W.; Vyatkin, V. Cosimulation Environment for Event-Driven Distributed Controls of Smart Grid. *IEEE Trans. Ind. Inform.* **2013**, *9*, 1423–1435. https://doi.org/10.1109/TII.2013.2256791.
19. Strasser, T.I.; de Jong, E.C.W.; Sosnina, M. (Eds.) *European Guide to Power System Testing: The ERIGrid Holistic Approach for Evaluating Complex Smart Grid Configurations*; Springer International Publishing: Cham, Switzerland, 2020. https://doi.org/10.1007/978-3-030-42274-5.
20. Godfrey, T.; Mullen, S.; Griffith, D.W.; Golmie, N.; Dugan, R.C.; Rodine, C. Modeling Smart Grid Applications with Co-Simulation. in 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 291–296. https://doi.org/10.1109/SMARTGRID.2010.5622057.

21. Lévesque, M.; Xu, D.Q.; Joós, G.; Maier, M. Communications and power distribution network co-simulation for multidisciplinary smart grid experimentations. In Proceedings of the 45th Annual Simulation Symposium, San Diego, CA, USA, 26–30 March 2012, pp. 1–7.
22. Li, W.; Monti, A.; Luo, M.; Dougal, R.A. VPNET: A co-simulation framework for analyzing communication channel effects on power systems. In Proceedings of the 2011 IEEE Electric Ship Technologies Symposium, Alexandria, VA, USA, 10–13 April 2011; pp. 143–149. https://doi.org/10.1109/ESTS.2011.5770857.
23. Lin, H.; Veda, S.S.; Shukla, S.S.; Mili, L.; Thorp, J. GECO: Global Event-Driven Co-Simulation Framework for Interconnected Power System and Communication Network. *IEEE Trans. Smart Grid* **2012**, *3*, 1444–1456. https://doi.org/10.1109/TSG.2012.2191805.
24. Functional Mock-Up Interface—FMI—OpenModelica User's Guide v1.11.0 Documentation. Available online: https://openmodelica.org/doc/OpenModelicaUsersGuide/v1.11.0/fmi.html (accessed 8 December 2022).
25. Elsheikh, A.; Awais, M.U.; Widl, E.; Palensky, P. Modelica-enabled rapid prototyping of cyber-physical energy systems via the functional mockup interface. In Proceedings of the 2013 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Berkeley, CA, USA, 20 May 2013; pp. 1–6. https://doi.org/10.1109/MSCPES.2013.6623315.
26. Chilard, O.; Boes, J.; Perles, A.; Camilleri, G.; Gleizes, M.P.; Tavella, J.P.; Croteau, D. The Modelica Language and the FMI Standard for Modeling and Simulation of Smart Grids. In Proceedings of the 11th International Modelica Conference, Versailles, France, 21–23 September 2015; pp. 189–196. https://doi.org/10.3384/ecp15118189.
27. Vanfretti, L.; Bogodorova, T.; Baudette, M. Power system model identification exploiting the Modelica language and FMI technologies. In Proceedings of the 2014 IEEE International Conference on Intelligent Energy and Power Systems (IEPS), Kyiv, Ukraine, 2–6 June 2014; pp. 127–132. https://doi.org/10.1109/IEPS.2014.6874164.
28. Szász, C. Benefits of Cyber-Physical Systems Modeling and Simulation with LabView. December 2021. Available online: http://hdl.handle.net/2437/327237 (accessed on 8 December 2022).
29. Varga, A.; Hornig, R. AN OVERVIEW OF THE OMNeT++ SIMULATION ENVIRONMENT. In Proceedings of the First International ICST Conference on Simulation Tools and Techniques for Communications Networks and Systems, Marseille, France, 3–7 March 2008. https://doi.org/10.4108/ICST.SIMUTOOLS2008.3027.
30. OMNeT++ Discrete Event Simulator. Available online: https://omnetpp.org/ (accessed on 6 June 2022).
31. Gayathri, C.; Vadivel, R. An overview: Basic concept of network simulation tools. *Int. J. Adv. Res. Comput. Commun. Eng.* **2017**, *6*, 19–22.
32. OPNET Network Simulator—Opnet Projects. Available online: https://opnetprojects.com/opnet-network-simulator/ (accessed on 6 June 2022).
33. Network Simulator—An Overview | ScienceDirect Topics. Available online: https://www.sciencedirect.com/topics/computer-science/network-simulator (accessed on 15 June 2022).
34. Introduction—Tutorial. Available online: https://www.nsnam.org/docs/tutorial/html/introduction.html (accessed on 15 June 2022).
35. GLOMOSIM SIMULATOR. PHD Projects. Available online: https://phdprojects.org/glomosim-simulator/ (accessed on 15 June 2022).
36. MATLAB—MathWorks. Available online: https://www.mathworks.com/products/matlab.html (accessed on 6 June 2022).
37. Advantages of MATLAB | Disadvantages of MATLAB. Available online: https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-MATLAB.html (accessed on 15 June 2022).
38. Earle, B.; Bjornson, K.; Ruiz-Martin, C.; Wainer, G. Development of a real-time DEVS kernel: RT-Cadmium. In Proceedings of the 2020 Spring Simulation Conference, Fairfax, VA, USA, 18–21 May 2020; pp. 1–12.
39. Buse, D.S.; Schettler, M.; Kothe, N.; Reinold, P.; Sommer, C.; Dressler, F. Bridging worlds: Integrating hardware-in-the-loop testing with large-scale VANET simulation. In Proceedings of the 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), Isola, France, 6–8 February 2018; pp. 33–36. https://doi.org/10.23919/WONS.2018.8311659.
40. Obermaier, C.; Riebl, R.; Al-Bayatti, A.H.; Khan, S.; Facchi, C. Measuring the Realtime Capability of Parallel-Discrete-Event-Simulations. *Electronics* **2021**, *10*, 636. https://doi.org/10.3390/electronics10060636.
41. Vellaithurai, C.B.; Biswas, S.S.; Liu, R.; Srivastava, A. Real Time Modeling and Simulation of Cyber-Power System. In *Cyber Physical Systems Approach to Smart Electric Power Grid*; Khaitan, S.K., McCalley, J.D., Liu, C.C., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 43–74. https://doi.org/10.1007/978-3-662-45928-7_3.
42. Home. RTDS Technologies. Available online: https://www.rtds.com/ (accessed on 15 November 2022).
43. Real-Time simulation—Real-Time Solutions. OPAL-RT. Available online: https://www.opal-rt.com/ (accessed on 15 November 2022).
44. Home Page. Typhoon HIL. Available online: https://www.typhoon-hil.com/(accessed on 15 November 2022).
45. Khaitan, S.K.; McCalley, J.D. Cyber physical system approach for design of power grids: A survey. In Proceedings of the 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, Canada, 21–25 July 2013; pp. 1–5. https://doi.org/10.1109/PESMG.2013.6672537.
46. IEEE Standard Association. *IEEE Standard for Synchrophasor Measurements for Power Systems, in IEEE Std C37.118.1-2011;* Revision of IEEE Std C37.118-2005; IEEE Power & Energy Society: Piscataway, NJ, USA, 2011; pp. 1–61. https://doi.org/10.1109/IEEESTD.2011.6111219.

47. Shariatzadeh, F.; Vellaithurai, C.B.; Biswas, S.S.; Zamora, R.; Srivastava, A.K. Real-Time Implementation of Intelligent Reconfiguration Algorithm for Microgrid. *IEEE Trans. Sustain. Energy* **2014**, *5*, 598–607. https://doi.org/10.1109/TSTE.2013.2289864.
48. Peirelinck, T.; Bratcu, A.I.; Besanger, Y. Impact of IEC 61850 GOOSE Communication Quality on Decentralized Reactive Power Control in Smart Distribution Grids—A Co-simulation Study. In Proceedings of the EPEC 2016—IEEE Electrical Power and Energy Conference, Ottawa, ON, Canada, 12–14 October 2016. Available: https://hal.archives-ouvertes.fr/hal-01347640 (accessed on 6 June 2022).
49. NHS Testing Facilities—INL. Available online: https://inl.gov/national-security-old/testing/ (accessed 7 June 2022).
50. fglongatt-Lab Cyber-Physical Experimenal Testbed. Available online: https://fglongattlab.fglongatt.org/Cyber-Physical.html (accessed on 11 June 2022).
51. Riquelme-Dominguez, J.M.; Gonzalez-Longatt, F.; Melo, A.F.S.; Rueda, J.L.; Palensky, P. Cyber-Physical Testbed Co-simulation Real-Time: System Frequency Response. In Proceedings of the 2022 IEEE International Conference on Environment and Electrical Engineering and 2022 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Prague, Czech Republic, 28 June–1 July 2022; pp. 1–5. https://doi.org/10.1109/EEEIC/ICPSEurope54979.2022.9854592.
52. Mallouhi, M.; Al-Nashif, Y.; Cox, D.; Chadaga, T.; Hariri, S. A testbed for analyzing security of SCADA control systems (TASSCS). In Proceedings of the ISGT 2011, Anaheim, CA, USA, 17–19 January 2011; pp. 1–7. https://doi.org/10.1109/ISGT.2011.5759169.
53. Adhikari, U.; Morris, T.H.; Pan, S. A cyber-physical power system test bed for intrusion detection systems. In Proceedings of the 2014 IEEE PES General Meeting | Conference & Exposition, National Harbor, MD, USA, 27–31 July 2014; pp. 1–5. https://doi.org/10.1109/PESGM.2014.6939262.
54. Poudel, S.; Ni, Z.; Malla, N. Real-time cyber physical system testbed for power system security and control. *Int. J. Electr. Power Energy Syst.* **2017**, *90*, 124–133. https://doi.org/10.1016/j.ijepes.2017.01.016.
55. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart Grid—The New and Improved Power Grid: A Survey. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 944–980. https://doi.org/10.1109/SURV.2011.101911.00087.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.