A Study on Cyber-Physical System Architecture for Smart Grids and Its Cyber Vulnerability

N. Rajeswaran, M. Lakshmi Swarupa, Rekharani Maddula, Hassan Haes Alhelou, and Vajjala Kesava Vamsi Krishna

Abstract Technological advances resulted in overwhelming usage of electronic gadgets across the world which further resulted in increased load demands. The obvious challenges are blackouts, overloads and voltage sags. One possible and trusted solution for these problems is Smart grid. A power network supported by digital communication technology is termed as Smart grid. But this solution is not that simple as it seems to be. There are few challenges associated with this solution like cyber vulnerabilities and cyber-attacks. Therefore, an effort is made here to review comprehensively the research work carried out till date, encompassing different heuristic detection and estimation techniques. It is a convenient factor that issues in Smart grid like relay protection, Power flow control, grid security and reliability can effectively be modelled and efficiently be analyzed. An effort is made to identify the dependencies among Cyber Physical System controls in this work. There is an immediate need to protect the communications and computations carried out by the digital communication equipment in Smart grids from cyber-attack. An overview of current research efforts in expanding the Smart grid applications and its infrastructure security is presented here. The conclusions submitted here present the further scope of the research work.

N. Rajeswaran (✉)
Electrical and Electronics Engineering, Malla Reddy Institute of Engineering and Technology, Maisammaguda, Secunderabad, Telangana, India
e-mail: rajeswarann@gmail.com

M. L. Swarupa
Electrical and Electronics Engineering, CVR College of Engineering, Hyderabad, Telangana, India

R. Maddula
Department of Physics, Gokaraju Lailavathi Womens Engineering College, Hyderabad, Telangana, India

H. H. Alhelou
Department of Electrical and Computer System Engineering, Monash University, Melbourne, Australia

V. Kesava Vamsi Krishna
Department of Physics, Malla Reddy Engineering College, Maisammaguda, Secunderabad, Telangana, India

H. Haes Alhelou et al. (eds.), *Power Systems Cybersecurity*, Power Systems,
https://doi.org/10.1007/978-3-031-20360-2_17

Keywords Smart grid · Cyber physical system · Cyber vulnerabilities · Cyber-attacks · Cyber security

1 Introduction

Cyber Physical Systems (CPS) are heterogeneous technologies that deal with interactions between computing and communications systems and the regulation of related physical dynamics [1, 2]. CPS involves leveraging the economy through the integration of computing and communication technology with physical systems. The CPS research is behind, however, because it is still in its early stages and as a result lacks the requisite standards and system design. Another difficulty is that CPS's integration with the public internet raises serious questions about its security. This analysis analyses expected cybersecurity issues in addition to focusing on architectural modelling by classifying CPS [3, 4]. Additionally, this research has attempted to separate out a number of the problems and difficulties facing CPS [5].

Broadly speaking, the term "Smart Grid" (SG) refers to the integration of emerging IT and other technologies with large-scale power networks with the goal of ensuring effective, efficient, commercially viable, and environmentally sustainable electricity generation, transmission, distribution, and use [6, 7]. The conceptual model recommended by the National Institute of Standards and Technology of the United States puts forth seven important domains: bulk generation, transmission, distribution, customers, service provider, operations, and markets. SG refers to the change of the electric business in the USA from a producer-controlled network to one that is somewhat customer interactive [8–10].

Modern SGs are made up of modern communications systems, energy storage devices, electric vehicle charging stations, and distributed renewable energy resources [11]. The typical electric grids, in contrast, were developed prior to any of these technological developments. As a result, a thorough restructuring is necessary to convert to a Smart Grid that includes computing resources and connected devices. Energy production, delivery, consumption, and storage were all optimized with the use of computing resources. The urgent and challenging task is to create diversified Smart Grid architecture that implements secure communication between various SG infrastructure tiers [12–14].

1.1 Issues in SG's

With the development of internet-connected applications in SGs, significant advancements are being seen on a variety of levels, including better consumption management, production optimization, and enabling utilities to provide power with better control and reduced costs (Fig. 1). On the other hand, the same internet that provided

the SGs with the benefits listed above has also opened up opportunities for cyberattacks that will disrupt the SGs [15]. The hazards vary from minor and imperceptible effects on SG caused by straightforward viruses to more significant attacks that could result in the animated freeze of the entire system. Nuclear facilities in particular are now vulnerable to everything from little viruses made by solitary people to massive and intricate cyberattacks coordinated by larger organizations [16].The development of networks and computing in recent years has made life for the average person much more comfortable. Information systems and physical objects are increasingly being integrated with more focus as a result of developing technologies like data science, the Internet of Things, cyber security, etc. [17–19]. The development of Cyber Physical Systems (CPS) was aided by these circumstances, which naturally caught the interest of governments, businesses, academic institutions, and universities.

Through the use of appropriate feedback loops, embedded computers and networks in CPS monitor and regulate the physical processes. As a result, both the computation and these physical processes have an impact. Computation, Communication, and Control are CPS's three primary building blocks (3C). Global academic academics began to pay attention to CPS, which also became an emerging topic in the industry [20].

CPS security is a critical issue because it affects the system's stability. As a result, the first focus of this work is on the CPS Security model, which also contains the

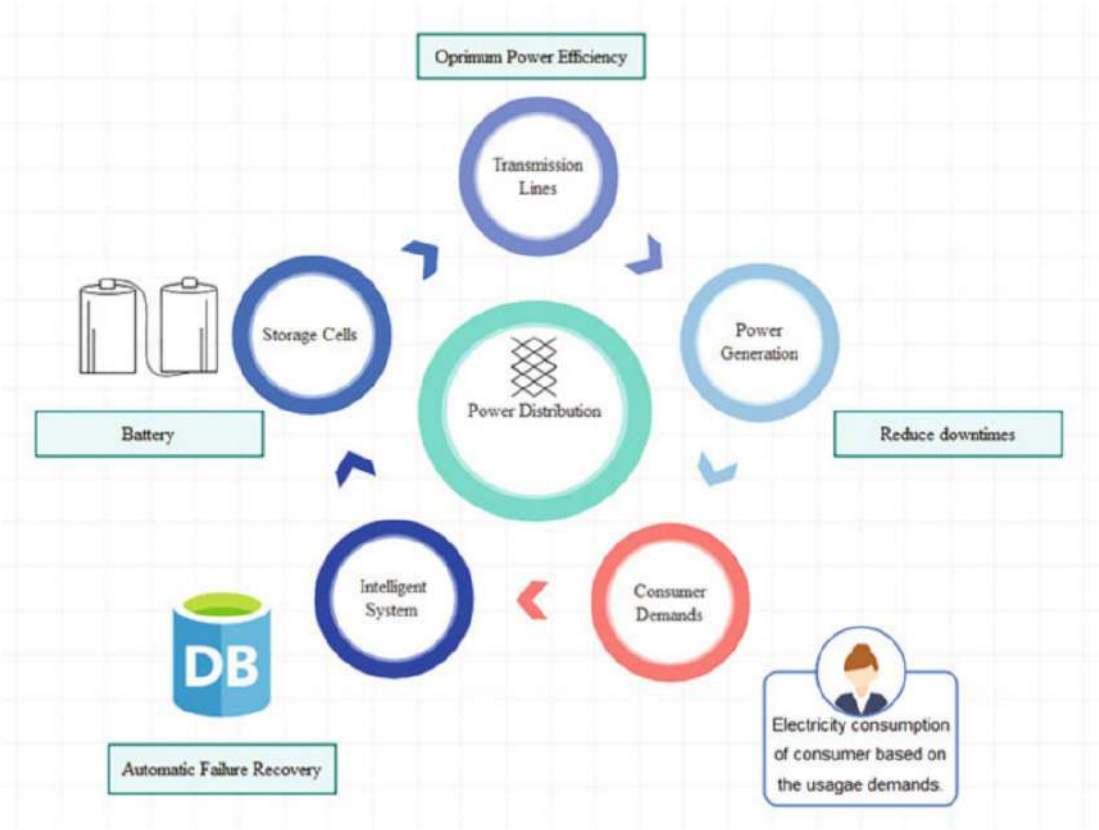

Fig. 1 Smart grid transmission network

2 CPS Architecture

The original CPS architecture included two layers: a physical layer and a cyber layer. While the cyber component handled the work of evaluating and processing the data from the physical part and sending the required orders, the physical part was responsible for sensing the physical environment, gathering data, and carrying out commands that it got from the cyber part. New CPS architectures that weren't hierarchical were introduced in a few papers. Three-tiered CPS architecture was attempted to be introduced [25] with a very hazy description. The three-layer CPS architecture, comprised of an execution layer, a transport layer, and a control layer, is depicted in Fig. 3 of this study. The execution layer is made up of several physical components, including sensors, actuators, RFID tags, readers, and more. The physical environment data collection and command execution are handled by this layer. Internet, LAN, and communication networks are all included in the transport layer [26]. In addition to handling data management and processing, this layer deals with real-time data transfer. The control layer serves as a link in the interaction between the cyber and physical components. The control layer gathers information from the execution layer's devices and uses that information to generate the appropriate commands. The control layer's application support layer uses middleware, entertainment platforms, cloud computing platforms, service support platforms, etc. Based on the suggested CPS architecture, this proposed design makes an effort to categories attacks for the execution, transport, and control layers [27].

Execution layer attacks target nodes such as sensors and actuators, whereas transport layer attacks target nodes such as those involved in large-scale data integration and leakage or destruction to data. Loss of user privacy, improper access control procedures, and insufficient security standards are all examples of control layer assaults. In terms of CPS application domains, researchers frequently concentrated on the SG, medical device, automotive, and aerospace industries [28]. Security is a crucial and essential key problem in the context of CPS. While administering CPS locally and on a smaller scale, it would appear that security is not a serious problem. However, if the same system implementation is expanded via the internet, several security flaws may be exposed. Borg claims that hackers are increasingly focusing their attacks on industrial machinery, particularly process control devices like Programmable Logic Controllers and local networks.

Due to a potential quality control failure, this may have an impact on the stock price of the impacted company. As a result, business executives are increasingly coming under cyber hackers' attention. When compared to the money made by cybercriminals by manipulating a company's stock price, credit card fraud is a relatively insignificant source of income. With the development of the Internet of Things, these security threats are growing and causing difficulties. When more physical infrastructures are connected to the internet, systems will become even more vulnerable.

The networks for the Internet of Things and Cyber-Physical Communication are vulnerable to the following six urgent problems:

- The sixth justification relates to connected devices in real-world settings, which are different from any IT system. For instance, in smart homes, there is no software expert or manager to update connected refrigerators.

The success of IoT/CPS operations in the Cyber Communication sector depends on tackling cybersecurity, which is crucial for preserving the aforementioned as well as protecting large plants, networks, and establishments.

3 CPS in Smart Grids

Smart grids can lower energy prices, assist in preventing blackouts, and thwart cyber-attacks. Smart grids are power systems that adjust to changes in demand and reconfigure as necessary to avoid overloads and other difficulties. They also provide novel, more difficult issues [29, 30]. Massive amounts of sensor data from stations must be efficiently transferred and properly evaluated in real time as power generation transitions from centralized power stations to distributed and heterogeneous systems.

3.1 Smart Grid Cyber Physical System

The SG is presented in the next part from the viewpoint of the CPS. The conventional power grid was not intended to be flexible enough to accommodate future changes like smart metering and monitoring, control, the integration of renewable energy sources, etc., whereas the SG modifies the current grid in a way that incorporates disciplines like generation, transmission, distribution, consumers, operation, and market in order to enable real-time grid monitoring. A example CPS-based SG is depicted in Fig. 3 [31]. SG-CPS plans to combine computational and physical components in order to monitor, process, and govern the Grid in real time. The SG-CPS consists of physical systems and cyber systems, with physical systems include power network infrastructures and sensors [32]. The customer domain, market domain, service provider domain, operational domain, bulk generating domain, transmission domain, and distribution domain are the seven linked domains that make up SG, according to NIST. The aforementioned domains cover sensors, actuators, intelligent electronic devices (IEDs), smart metres, distributed energy resources (DERs), and other physical and cyber components. The data exchange between the connected physical components is made possible by cyber components like software, communication networks, etc.

- Generation system
  Coal, thermal, nuclear, hydrothermal, and other conventional power-generating methods are used on a large scale. Small-scale non-conventional power-generating methods include wind, solar, geothermal, and biomass. Traditional and renewable generation sources will be integrated by SG-CPS in order to address the issue of natural resource depletion in traditional energy sources. Even the energy produced

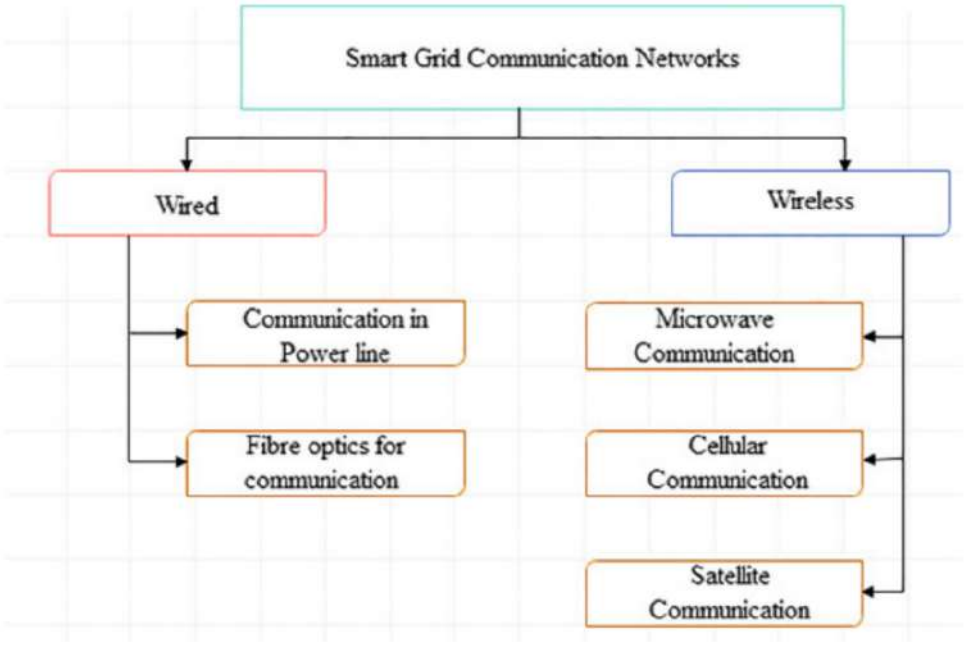

Fig. 4 SG communication network technologies

- Defense of many crucial SG components, including as the transmission, distribution, and generation infrastructures.

Figure 4 illustrates how the SG-CPS communication infrastructure needs differ from standard communication requirements. For instance, in addition to the needs of normal cellular-based commercial applications, the SG-CPS requires less delay, less packet drop, higher dependability, high resilience, better scalability, high availability, etc. [33]. The CPS communication infrastructure and its requirements are thoroughly surveyed [14]. One can infer that the communication network infrastructure in the context of SG-CPS is not extensively examined.

4 Modeling and Stability Analysis of Integrated Cps

The intricate relationships between software and hardware as well as the complex, ongoing interactions between the environment and the system in SG-CPS make it difficult to apply conventional testing methods. To lessen these difficulties, we suggest performing testing during the early stages and using executable models of the system and its surroundings. This does not imply that there aren't any challenges with the CPS model testing. Figure 5 illustrates how the complexity and variety of CPSs make it necessary to combine many modelling formalisms in order to create accurate models of each component. Additionally, the co-simulation process must be controlled, allowing it to accurately replicate the desired results, and quick, allowing thousands of simulations to be run in practical time. Mathematical modelling plays

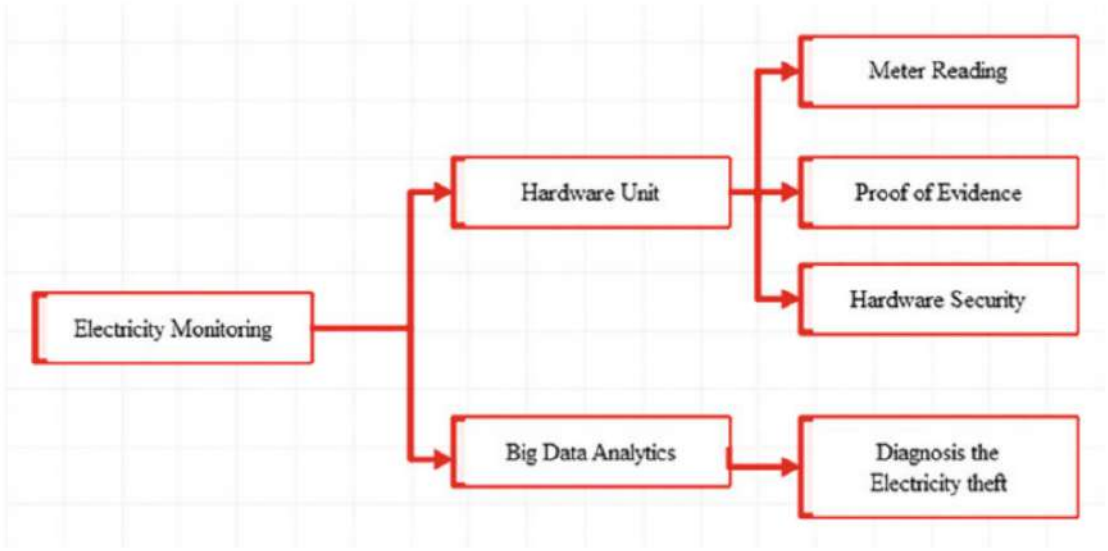

Fig. 5 A sample integrated CPS architecture

a crucial role in the design of any complex system because it generates simulation data that makes it possible to identify faults.

Mathematical modelling is crucial for the design of any complicated system, but it's especially crucial for physical systems because they can never be deterministic. Another significant worry is the system's stability. Due to the communication delays that may occur when CPS is used to manage and monitor a critical situation, packet loss during data transfer is another possibility. As a result, system stabilization would need to be given the attention it deserves in these system design concerns. The modelling and stability of CPS using the proposed Passivity Model have been studied in this research. When a storage function is present and the energy of the stored system is constrained by the.

4.1 Cyber-Attack System Modeling and Analysis

Control system networks that contain vital control systems are increasingly being connected to enterprise networks, which increases the risk of cyberattacks on those networks. In the current world, things are becoming integrated, and as the integration develops, protecting these systems becomes more crucial. Some particular examples of CPS are smart grids, pervasive healthcare systems, unmanned air vehicles, etc. The overall danger of the CPS would unquestionably be considerably higher than that of the component systems when systems are created and integrated to create it. Attacks on software have recently moved to embedded systems, and occurrences like the Stuxnet attack, which target automation systems, are quite likely since computational and physical dynamics are being connected to the internet these days.

Because the majority of CPS models employ their own proprietary protocols, there haven't been many attacks against CPS to date. However, as CPS becomes increasingly integrated with the internet, more attacks should become common place. With the link to the public internet, security would be more at risk; this would have been a much bigger worry with the new internet concept, i.e. the Internet of Things or the Internet of Everything. As more physical systems and facilities are connected to wireless sensor networks, IoT vulnerabilities are created (WSN). National infrastructure CPS systems, including national power grids, smart energy systems, sophisticated metering infrastructures, etc., are becoming more and more vulnerable as cyber security incidents have received more and more credibility as real concerns [34].

Attacks on CPS should receive considerable consideration because they involve physical systems, machinery, people, expensive establishments, and crucial infrastructures. As a result, the damage would undoubtedly be greater and might not be repairable [35]. Pervasive computing raises more security and safety concerns, although these concerns are still very important. Preschern et al. developed the one-out-of-two security model based on the study by Kai Hansen, which includes potential assaults, outcomes, and discusses attack scenarios from the attacker's perspective (Fig. 6).

Because the majority of CPS models employ their own proprietary protocols, there haven't been many attacks against CPS to date. However, as CPS becomes increasingly integrated with the internet, more attacks should become commonplace. With the link to the public internet, security would be more at risk; this would have been a much bigger worry with the new internet concept, i.e. the Internet of Things or the Internet of Everything. As more physical systems and facilities are connected to wireless sensor networks, IoT vulnerabilities are created (WSN).

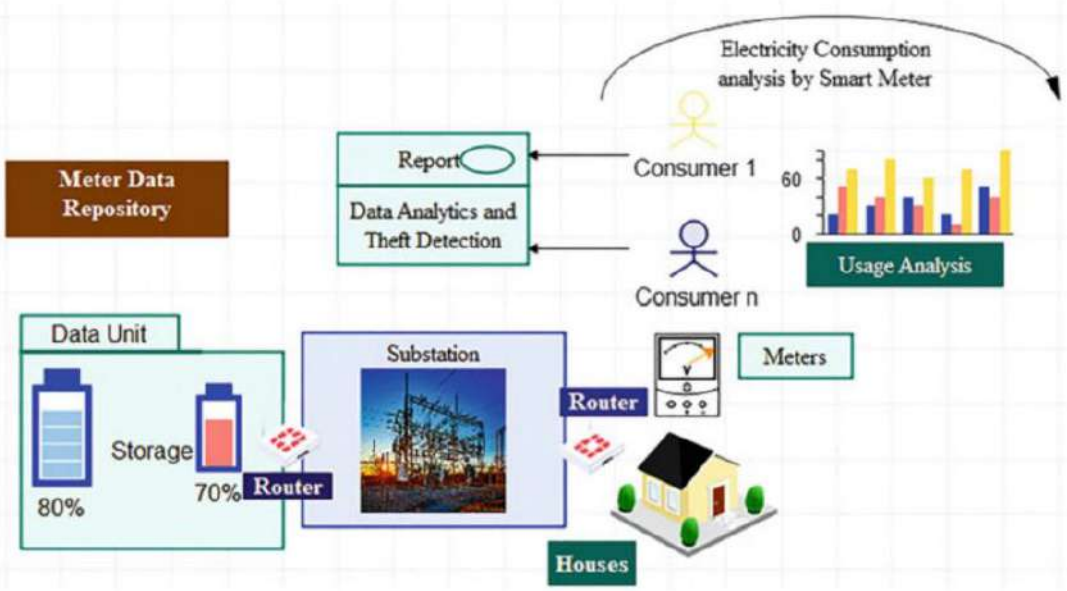

Fig. 6 Modeling of CPS based Smart Grid

As cyber security incidents have gained more and more recognition as legitimate issues, national infrastructure CPS systems, such as national power grids, smart energy systems, complex metering infrastructures, etc., are becoming more and more vulnerable. Figure 7 illustrates the necessity of interoperability, hybrid and heterogeneous modelling, operations, and simulation tools to meet system and network specifications. They ensure that the components can work together and that the large-scale network SG-CPSs can run flawlessly. Future SGs will provide dependable, affordable, open, and user-friendly options for energy and utilization. These options can be small-scale but widely dispersed sources or large-scale bases with massive distribution over great distances, supporting a variety of energy demands from electric vehicles, energy conservation, and market participation [36]. This obviously necessitates transdisciplinary and interdisciplinary work combining risk management, economic coordination, uncertainty analysis, and system security.

As of now, the operating conditions and disturbances for power network analysis have been provided based on offline experiences, so they cannot be realistically configured in accordance with the cutting-edge trends of external nonelectrical systems. This hinders the development of early warning systems as well as the adaptation of predecisions about external settings. Future analyses of power networks must take the environment and energy into account as a whole. The limitations on emissions, primary energy, and the energy market can make even a physically safe power network unstable. Energy sources, financial systems, communication networks, transportation, and products delivery networks must all work in harmony to prevent widespread blackouts. Modeling and simulation of needs a new generation framework, which will be adopted in future SG's.

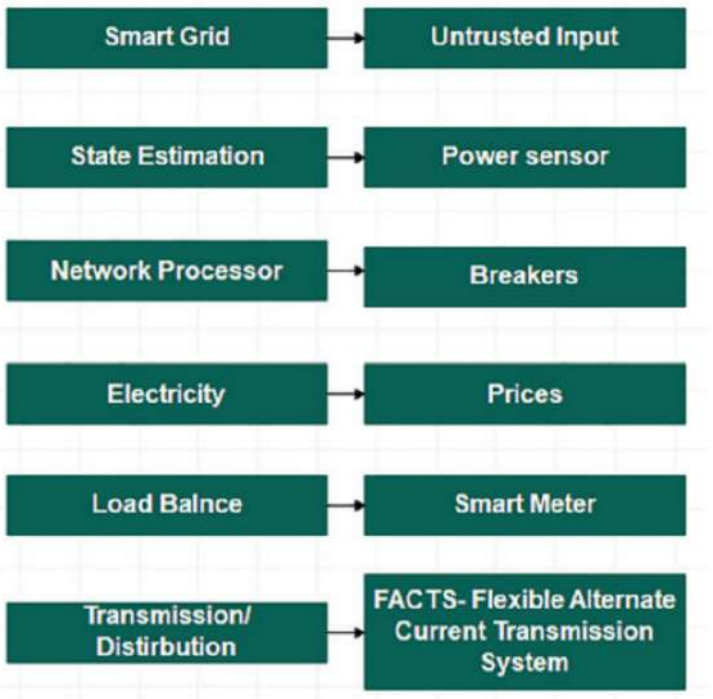

Fig. 7 Block diagram of state process

2. M. You, Q. Liu, H. Sun, New communication strategy for spectrum sharing enabled smart grid cyber-physical system. IET Cyber-Phys. Syst.: Theory Appl. **2** (2017). https://doi.org/10.1049/iet-cps.2017.0051
3. I. Horv´ath, B. Gerritsen, Cyber-physical systems: Concepts, technologies and implementation principles, in *TMCE* (2012), pp. 19–36
4. C. A. Macana, N. Quijano, E. Mojica-Nava, A survey on cyber physical energy systems and their applications on smart grids, in *Proceeding IEE PES Conference Innovative Smart Grid Technology* (2011), pp. 1–7
5. A. Sheela, S. Revathi, A. Iqbal, Cyber risks assessment for intelligent and non-intelligent attacks in power system, in *2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC)*, (IEEE, 2019), pp. 40–45
6. M.H. Cintuglu, O.A. Mohammed, K. Akkaya et al., A survey on smart grid cyber-physical system testbeds. IEEE Commun. Surv. Tutorials **19**(1), 446–464 (2017)
7. Facilitating whole electricity system outcomes. nationalgrideso.com/sites/eso/files/ documents/WholeElectricitySystemfinal.pdf. Accessed on 19 March 2020
8. N. Uribe-Pérez, L. Hernández, D. Vega et al., State of the art and trends review of smart metering in electricity grids. Appl. Sci. **6**(3), 68–92 (2016)
9. A. Nelson, S. Chakraborty, D. Wang, P. Singh, Q. Cui, Q, L. Yang, S. Siddharth, Cyber-physical test platform for microgrids: combining hardware, hardware-in-the-loop, and network-simulator-in-the-loop, in *Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM)* (Boston, 2016)
10. G. Bedi, G. Kumar, R. Singh, R.R. Brooks, K.C. Wang, Review of Internet of Things (IoT) in electric power and energy systems. IEEE Internet Things J. **5**, 847–870 (2018)
11. K.-D. Kim, P.R. Kumar, Cyber-physical systems: A perspective at the centennial, in *Proceedings of the IEEE*, vol. 100 (Special Centennial Issue) (2012), pp. 1287–1308
12. X. Yu, Y. Xue, Smart grids: a cyber-physical systems perspective. Proc. IEEE **104**, 1058–1070 (2016)
13. L. Parolini, B. Sinopoli, B. Krogh, Z. Wang, A cyber physical systems approach to data center modeling and control for energy efficiency. Proc. IEEE **100**(1), 254–268 (2012)
14. Y. Mo, T.H.J. Kim, K. Brancik et al., Cyber physical security of a smart grid infrastructure. Proc. IEEE **100**(1), 195–209 (2012)
15. z. Su, L. Xu, S. Xin, W. Li, Z. Shi, Q. Guo, A future outlook for cyber-physical power system, in *Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)* (Beijing, China, 2017), pp. 1–4
16. F. Aghaee, N. Mahdian Dehkordi, N. Bayati, A. Hajizadeh, Distributed control methods and impact of communication failure in AC microgrids: a comparative review. Electronics **8**, 1265 (2019)
17. G.C. Konstantopoulos, A.T. Alexandridis, P.C. Papageorgiou, Towards the integration of modern power systems into a cyber-physical framework. Energies **13**, 2169 (2020). https://doi.org/10.3390/en13092169
18. J. Zhao, F. Wen, Y. Xue, Z. Lin, Cloud computing: Implementing an essential computing platform for future power systems, in Chinese. Autom. Electr. Power Syst. **34**(15) (2010)
19. P.P. Varaiya, F.F. Wu, J.W. Bialek, Smart operation of smart grid: Risk-limiting dispatch. Proc. IEEE **99**(1), 40–57 (2011)
20. D. Niyato, L. Xiao, P. Wang, Machine-to-machine communications for home energy management system in smart grid. IEEE Commun. Mag. **49**(4), 53–59 (2011)
21. X. Guan, B. Yang, C. Chen, W. Dai, Y. Wang, A comprehensive overview of cyber-physical systems: From perspective of feedback system. IEEE/CAA J. Autom. Sin. **3**(1) (2016)
22. B. Chen, J. Wang, M. Shahidehpour, Cyber–physical perspective on smart grid design and operation, (N. p, United Kingdom, 2018). Web. https://doi.org/10.1049/iet-cps.2017.0143.
23. Y. Wang, Research framework of technical standard system of strong and smart grid. Autom. Electr. Power Syst. **34**(22), 1–6 (2010)
24. F. Guo, L. Herrera, R. Murawski, E. Inoa, C.-L. Wang, P. Beauchamp, E. Ekici, J. Wang, Comprehensive real-time simulation of the smart grid **49**(2), 899–908 (2013)