JOIN (Jurnal Online Informatika)
p-ISSN: 2528-1682, e-ISSN: 2527-9165
Volume 9 Number 1 | June 2024: 119-127
DOI: 10.15575/join.v9i1.1344

A Mathematical Modelling and Behaviour Simulation of a Smart Grid Cyber-Physical System

Elvis Tamakloe[1], Klogo Selorm Griffith[2], Benjamin Kommey[3]
[1,2,3]Department of Computer Engineering, Kwame Nkrumah University of Science and Technology, KNUST-Kumasi, Ghana

Article Info

Article history:

Received May 1, 2024
Revised May 20, 2024
Accepted May 21, 2024
Available Online May 24, 2024

Keywords:

Cyber physical systems
Mathematical modelling
Operational technologies
Smart grids
Simulation

ABSTRACT

The significant contributions of information and communication technology (ICT) and other operational technologies (OTs) or cyber networks have had a tremendous impact on the real-time monitoring, management, and control of power or energy system facilities. This study aims to explore the integration of these technologies into the energy grid system, creating a smart, complex, and interdependent system known as a smart grid cyber physical power system (SGCPPS). The method used involves developing a mathematical model for an SGCPPS. The research has found that the performances of cyber physical systems are achieved via computation and communication, based on a real-time feedback mechanism. Monitoring and control of the grid systems are essential in ensuring efficient power supply, quality, reliability, stability, and resilience. However, their interdependence and integrated nature expose the grid to disturbances, leading to faults. Failure to know the grid conditions at a particular period can result in complete system collapse. Simulations were performed to study the behavior of the SGCPPS regarding monitoring and controlling the physical systems using the MATLAB Simulink tool to facilitate system awareness.

Corresponding Author:

Benjamin Kommey,
Computer Engineering Department, Faculty of Electrical and Computer Engineering,
College of Engineering
Kwame Nkrumah University of Science and Technology, KNUST-Kumasi, Ghana
Email: bkommey.coe@knust.edu.gh

1. INTRODUCTION

The emergence of information and communication technology, remote sensing, automated control systems and the application of internet-of-thing (IoT) technologies has dynamically altered the landscape of power systems engineering. The integration of these elements with the conventional power system has offered an efficient and robust method of monitoring and controlling all facets of the physical power system. This includes all aspects of power generation, transmission, distribution and usage. The combination and coordination of these important elements (cyber system) with the physical power system collectively forms the cyber physical power systems (CPPS). This system provides a more distributed architecture that allows flexibility, planning, system optimization, interoperability and many more. In this regard, cyber physical power systems are primarily the backbone of smart grids (SGs) which are considered as critical infrastructures [1], [2]. The architecture of smart grid cyber physical power systems therefore enables the bidirectional flow of electrical power and data or information as represented in Figure 1. That is, it relies on an established internet framework to compute, control and communicate through simultaneous feedback interactions. This allows for resource sharing and creates an environment to host complex interactions. However, it is vital to note that in the event of limited

resources, the interaction between these interdependent systems in the CPPS could be constrained, lead to system disruptions and in effect undermine its usefulness [3], [4], [5]. Therefore, to maximize the utilization of the CPPS, it is paramount to comprehend the behaviour and interaction of the connected components when limited resources are being shared. Similarly, the vulnerability of the CPPS to adversarial attacks such as denial of service (DoS) and its distributed variants requires solutions that provide absolute protection for the cyber physical power system [6], [7], [8], [9]. In relation to this, it is of utmost importance to develop models to address the afore-mentioned setbacks [10], [11]. In energy informatics, it is worth noting that numerous aspects ranging from grid control and management present an interdisciplinary platform that exploits machine learning algorithms formulated on mathematical principles to handle big data collected for forecasting and assessment of the smart grid system [12], [13], [14]. In this paper, a mathematical model for a smart grid cyber physical power system is developed. To ascertain and analyze the behavior of this system, simulations were performed accordingly in the subsequent sections using MATLAB Simulink software simulation tool.

Due to the immense benefits derived from smart grid CPPS, several studies have been conducted to mathematically model its behaviour to ensure efficient monitoring, management and control. Imperatively, numerous aspects of the smart grid CPPS can be modelled. In the quest to improve reliability in a cyber physical smart grid system, presented a model based on Markovian chain Imbeddable Structure that records the outcome of impairments obtained from the respective physical and cyber components [15]. The outcome of the interdependent cyber physical components was also categorized, taken and quantified. Based on these parameters, the model was expressed and populated with failure data. This technique was dependent on the Institute of Electrical and Electronics Engineers (IEEE) 14-bus test system. Simulated results via a quantitative analysis indicated that the reliability of the proposed smart grid system bearing 500 components degraded exponentially with the introduction of more interdependencies. Hence, this approach performed well with fewer components. However, the reliability of the systems was compromised based on the propagated failures recorded by the cyber-to-physical components.

The vulnerability of smart grids and other CPSs to attackers prompted the need to safeguard, defend and repel such attacks. A stochastic Petri net (SPN) is proposed as model based on the behavioral characteristics of an attacker and defender to analyze the safety and security of CPSs [16]. Established on the backbone of a semi-Markov model, the system's security (attacks factors and mitigation measures) was quantitatively analyzed based on the mean-time-to-fail (MTTF) and availability. The analyzed outcome after evaluation revealed that enormous technical comprehension of the level of attack, timing, working principles, failure conditions and implications is required by an attacker to physically disrupt the CPS. However, the results also indicated that the probability of false positives of the intrusion detection systems have an immense effect on the outcome of the attack and the resilience of the CPS components.

To curb the impact on cyber-attacks on smart grids, a linear mathematical model is proposed based on ordinary differential equations (ODEs) to comprehend attack scenario, analyze, confirm and evaluate the impact of the attack on the smart grid system [17]. Three distinct components were utilized by the model to achieve the stated objective. This included the attacker, smart grid and control center which were denoted by A, S and C respectively. The mathematical expression and relation between these components were established and simulations were performed to analyze the impact and effectiveness of cyber-attacks for various conditions using MATLAB. The stability of the model was tested and analyzed using polar plot to ascertain the intensity of the attacks.

Because of urbanization on the management of electrical energy, other research presents a home energy management (HEM) system which was modelled with the incorporation of photovoltaics (PVs) and energy storage systems (ESSs) [18]. More so, home to grid (H2G) energy exchange was integrated in this scheme with user preferences and system constraints equally considered. In reference to this, genetic algorithm was utilized to realize optimal scheduling of electrical loads. Based on the analyzed simulation results, the proposed modelled system achieved energy demand side management objectives via reduced energy cost, enhanced performance and reduced system uncertainty. However, analysis of the impact of faulty energy storage system on the overall system's stability was not provided.

An analytical channel modelling of a synchro phasor communication network (SCN) in a smart grid cyber physical system was proposed [19]. This model was based on discrete-time Markov chain and employed packet delivery ratio (PDR) and average-end-to-end delay (AE2ED) as its performance metrics. Upon validation with MATLAB, the behaviour of a realistic network was mimicked with PDR and AE2ED performance metrics against background traffic (B.T). The simulation results indicated that the performance of the SCN degraded when the background traffic exceeded 0.75 times the limited

p-ISSN: 2528-1682
e-ISSN: 2527-9165

capacity (C). Hence, the reliability of the network is assured to 75% of BT. This approach was cost effective, however, it only provided generic or quantitative outcomes.

Maintaining energy sustainability is critical in analyzing the behaviour of smart grid infrastructures. In this regard, modelled a smart grid cyber physical system and its respective components [20] is modelled to achieve efficient energy management under different operational scenario using MATLAB. The stability and security of the proposed smart grid system to faults and cyber-attacks was nonetheless not analyzed in this work. Therefore, several modernizations have been introduced into the grid system to increase the system resilience and optimal regulation of key domains of the grid [21], [22].

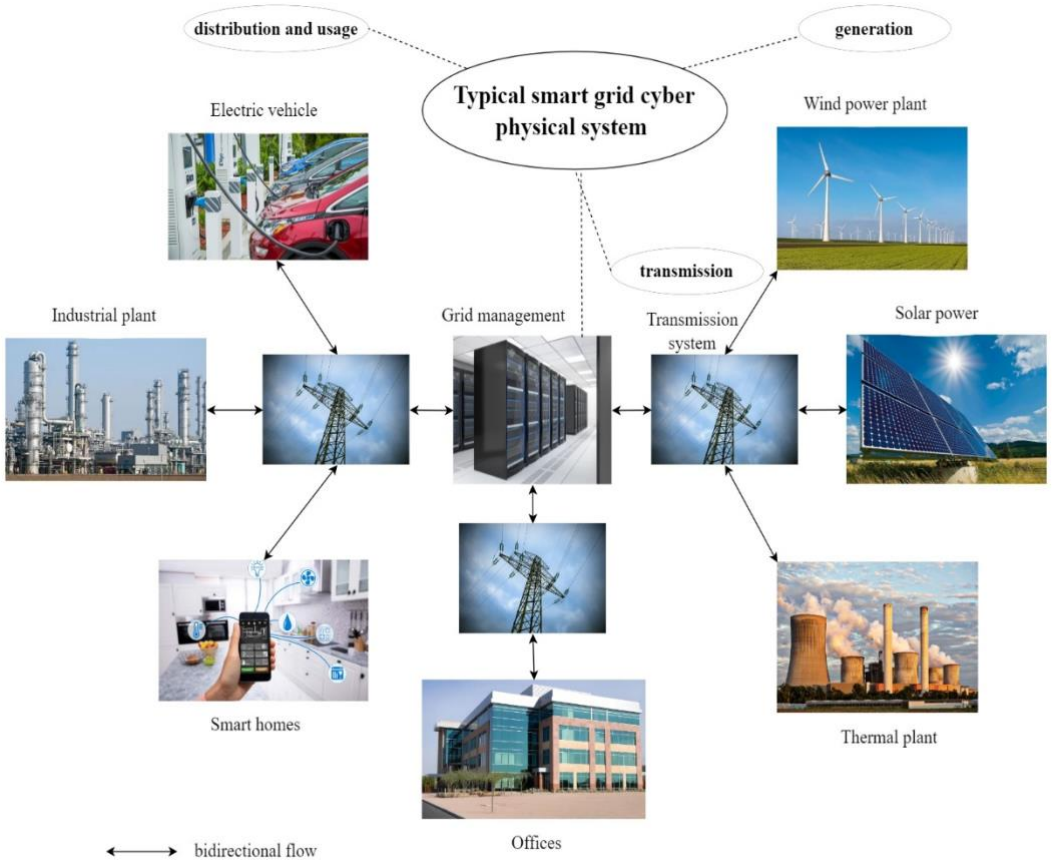

Figure 1. Smart grid cyber-physical power system (SGCPPS) architecture

2. THE COMPREHENSIVE THEORETICAL BASIS

2.1. SGCPPS feedback system

The architecture of the smart grid cyber physical power system (SGCPPS) is based on a feedback mechanism between the cyber and physical components. This is represented in Figure 2 as a framework of block diagrams to indicate the operation of the system.

The SGCPPS is composed of mainly two integral components: the physical power system (z) and the cyber system (η). To control the physical power system, the output signal (y) is measured via an analog-to-digital converter (ADC). This signal is then computed and analyzed to produce an input control signal (u) to the physical power system through a digital-to-analog converter (DAC) to realize the desired system results or objectives.

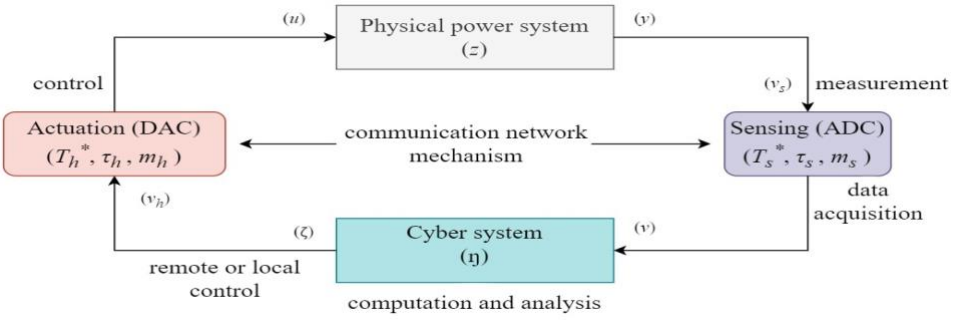

Figure 2. Smart grid cyber-physical power system (SGCPPS) feedback interaction

2.2. Mathematical modeling of the SGCPPS behavior

Modeling of the SGCPPS can be categorized into three groups namely: interconnection, interaction and interdependent modeling. As established, both the physical and cyber systems must be physically interconnected via the ADC and DAC. The behaviour of the physical and cyber system is mathematically modeled using the hybrid dynamical system theory. This implies the use of differential equations to depict the continuous-time behaviour of the physical system and difference equations on the other hand for the discrete behaviour of the cyber system.

2.3. Mathematical modeling of the physical power system

$$y = h(z,u) \ , \dot{z} \in F_P(z,u) \quad (1)$$
$$(z,u) \in C_P \subset R^{n_P} \times R^{m_P} \quad (2)$$

Equation (1) and (2) represent the mathematical modelling of the physical power system. Here, the state of the physical system and the Euclidean space with regards to state space are denoted by z and R^{n_P} respectively. The input control signal is represented by $u \in R^{m_P}$ and the output signal by $y \in R^{r_P}$. It is important to note that y is defined by the function h which is a function of the physical power system and the input control signal (z,u). In the event of specialized operations, a set of values C_P are employed to constrain or limit the state and input values of the physical power system.

2.4. Mathematical modeling of the cyber system

$$ŋ^+ \in G_C(ŋ,v) \ , \ \zeta = K(ŋ,v) \quad (3)$$
$$(ŋ,v) \in D_C \ \subset \Upsilon \times v \quad (4)$$

On the other hand, the cyber system is mathematically modelled in equation (3) and (4) where its state is represented by $ŋ \in \Upsilon$. The Euclidean space in relation to the state space of the cyber system is also denoted by R^{nc}. Both the input and output signals of the cyber system are denoted by $v \in V \subset R^{mc}$ and $\zeta \in R^{rc}$ respectively.

Additionally, the output signal is defined by K which represents the function of the input-signal and the state $(ŋ,v)$. Like the constraints in the physical power system, constraints in the cyber system are also provided in specific applications with values of limits in the set D_C. The cyber system is composed of components that are tasked with executing algorithms, performing computation, receiving and transmitting information over a digital network. Thus, these components can be mathematically modelled as either pure finite state machines (FSMs) or finite state machines with conditional structures as guards in equation (5) and (6) respectively.

$$q^+ = \delta(q,v) \ , \ \zeta = K(q)(q,v) \in Q \times \Sigma \quad (5)$$

In comparison with equations (3) and (4), it can be deduced that $\Upsilon = Q$, $G_C = \delta$, $ŋ = q$, $v = \Sigma$ and $D_C = \Upsilon = v$.

Hence, the difference equation (5) is like the mathematically modelled equation of the cyber system. Furthermore, the state, input and output of the FSM are essentially updated in discrete transitions.

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

This equation also shows similarities with equation (3) and (4) where $\Upsilon = Q, G_C = \delta, \mathfrak{y} = q, v = \Sigma$ and $D_C = \{(q, v) \in Q \times v : l(q, v, K(q)) \leq 0\}$.

Therefore, based on the conditional structure $\{l(q, v, K(q)) \leq 0\}$, a true condition creates an enabled transition while a false condition terminates the transition. The computations carried out by the cyber system can be modelled as one-shot or iterative. One-shot computations are mathematically modelled as:

$$\zeta = \widetilde{K}(v) \tag{7}$$

In reference to equation (7), v, ζ and $\widetilde{K}$ denotes the input, output and modelling computation respectively. It also bears similarity with equation (3) and (4) where $\mathfrak{y} = \emptyset, \Upsilon = \emptyset, v = \Sigma, \ D_C = v, G_C = \emptyset$ and $K = \widetilde{K}$.

$$\mathfrak{y}^+ = \begin{bmatrix} \widetilde{K}(m, k, v) \\ k + 1 \end{bmatrix}, \zeta = m, m \in R^{n_C - 1}, k \in \{0,1,2, \dots, k^* - 1\}, v \in V \tag{8}$$

Iterative computation is performed using equation (8) to provide the desired result needed to control the physical power system. When compared with the equation (3) and (4), $\mathfrak{y} = \begin{bmatrix} m \\ k \end{bmatrix}$, $\Upsilon = R^{n_C - 1} \times \{0,1,2, \dots, k^*\}, \ v = \Sigma, \ G_C = \begin{bmatrix} \widetilde{K}(m, k, v) \\ k + 1 \end{bmatrix}, \ K(\mathfrak{y}) = m \forall \mathfrak{y} \in \Upsilon, \ D_C = R^{n_C - 1} \times \{0,1,2, \dots, k^* - 1\}$.

Therefore, the difference equations are utilized to express the discrete-time algorithm in equation (9).

$$\mathfrak{y}^+ = G_C(\mathfrak{y}, v), \ \zeta = K(\mathfrak{y}) \tag{9}$$

2.5. Mathematical modeling of the ADC interface system

The primary role of the ADC interface system is to link the physical power system to the cyber system. This is achieved by converting and relaying measured or sampled analog data by the sensors to digital data for processing by the cyber system. In Figure 2, the output data (y) of the physical power system is sampled at a rate T_s^* and transferred to the cyber system as its input data (v). The mathematical model of the ADC interface system is represented as follows:

$$\dot{\tau}_s = 1, \ \dot{m}_s = 0, \ \text{on the condition that } \dot{\tau}_s \in [0, T_s^*] \tag{10}$$
$$\tau_s^+ = 0, \ m_s^+ = v_s, \text{ on the condition that } \tau_s \geq T_s^* \tag{11}$$

$\tau_s \in R_{\geq 0}$ represents the states of the timer, $m_s \in R^{r_P}$indicates the sample state and $v_s \in R^{r_P}$ depicts the input of the ADC.

2.6. Mathematical modeling of the DAC interface system

In contrast to the ADC, the DAC converts the computed digital data into analog data which controls the physical power system. It is mathematically modelled as the zero-order hold (ZOH) in equation (12) and (13).

$$\dot{\tau}_h = 1, \ \dot{m}_h = 0, \ \text{on the condition that } \dot{\tau}_h \in [0, T_h^*] \tag{12}$$
$$\tau_h^+ = 0, \ m_h^+ = v_h, \text{ on the condition that } \tau_h \geq T_h^* \tag{13}$$

Similarly, $\tau_h \in R_{\geq 0}$ represents the states of the timer, $m_h \in R^{r_C}$indicates the sample state and $v_h \in R^{r_C}$ depicts the input of the DAC.

2.7. Mathematical modeling of the digital communication network mechanism

The digital communication network serves as a medium for data exchange between the cyber and physical power system. This is modelled in equation (14), (15) and (16) by combining both the differential and difference equation due to the interface systems involved.

$$\dot{\lambda} \in F_A(\lambda, w) \text{ given that } (\lambda, w) \in C_A \quad (14)$$
$$\dot{\lambda} \in G_A(\lambda, w) \text{ given that } (\lambda, w) \in D_A \quad (15)$$
$$\psi = \varphi(\lambda) \quad (16)$$

In these equations, the state, input data and output data are represented by λ, w and ψ respectively. Likewise, the F_A indicates the continuous-time behaviour on C_A and G_A shows the discrete time behaviour on D_A of the interfaced digital communication network.

3. METHOD

The dynamic system of the SGCPPS is simulated as a hybrid system in MATLAB Simulink where the interaction between the cyber and physical power system presents a behaviour assessment of the entire system. This simulation enables visualization of the modelled interactions. The implementation of this hybrid SGCPPS in MATLAB Simulink is presented in Figure 3.

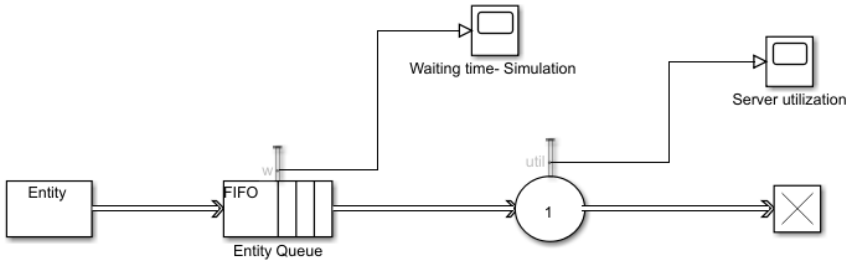

Figure 3. Implementation of the modelled SGCPPS for continuous and discrete behaviour analysis

From the mathematical description provided for both the differential and difference equation as shown in the previous section, an informed probe into their validity lies in ascertaining how well data from the physical power system is handled, processed and thoroughly delivered through the cyber space to effect a change (control) on the selected physical system via actuators. In relation to this, input data (w) from the physical system which are mostly analog in nature are converted into digital forms by the ADC. Upon arrival in the cyber system, an in-depth computation and analysis is performed on the received input data to release the appropriate output signal (ψ). The output signal which is in digital form is interpreted by an actuator to produce the desired outcome. However, in reference to the presence of multiple input data, a queuing system offers adequate and equitable access to the available resources. Several queuing modalities can be implemented based on the conditioned at hand nonetheless a first-in-first-out algorithm is primarily employed in this context. On this basis, the waiting time, server utilization and quality of service amongst other parameters can analyzed accordingly. Although a simplified case is presented in this context, transient behaviors which impose a degree of computational complexity are handled by more advanced and sophisticated models

4. RESULT AND DISCUSSION

The experiment conducted in MATLAB and Simulink simulated a the SGCPPS which encapsulated aspects of generation, transmission, distribution and usage. This is represented in Figure 4 by the generator speed, transmission line voltage and load current based on numerical parameters. This aspect covers the interaction between the physical systems in per unit value. Thus, the waveform in the first subplot depicted a gradual rise from the origin indicating the generator speed from start to the finish time. However, the speed became more pronounced after 5s which signifies increase in power generation. A similar observation was made in the second subplot in the transmission line voltage. A

p-ISSN: 2528-1682
e-ISSN: 2527-9165

steady and sustained voltage level was experienced at a period of 2s. Electrical current consumption as seen in the third subplot had a constant profile close to 0.8pu.

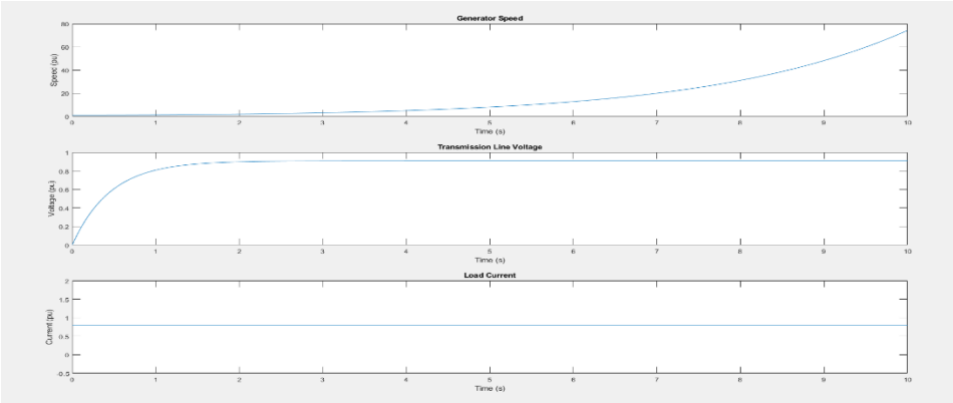

Figure 4. Simulation of the continuous behaviour of the physical system

The discrete behaviour of the cyber system was simulated over the same period as observed in Figure 5. Based on the simulated results, entity (data) from the ADC is queued at an interval of 1s because of the first-in-first-out (FIFO) scheduling strategy employed in this developed system. In signal communication, it is important to optimize lateness and prevent signal or data loss. Hence, to facilitate real time exchange of data, which is crucial for SGCPPS control and management, it is critical to ensure effective sharing of valuable resources (bandwidth) in order to avoid deadlocks. Therefore, the introduction of the aforesaid scheduling scheme provided the platform to successfully implement the discrete behavior mechanism.

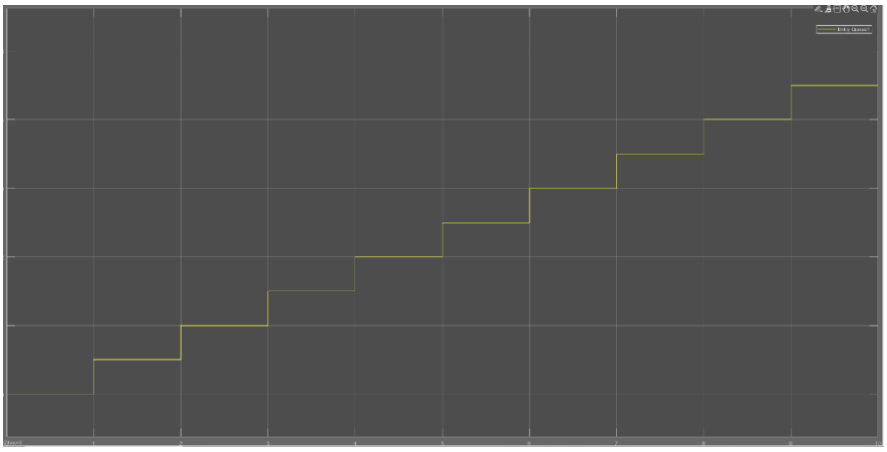

Figure 5. Simulation of the discrete behaviour of the cyber system

The server interaction in this smart grid cyber physical power system (SGCPPS) occurs at a periodic interval of 1s as depicted in Figure 6. This is integral in the establishment of the discrete behaviour of the system. The operation of this interaction is based on a single server system which provided a regular service time. It is imperative to note that the behaviour of the server interaction is subject to change based on the configuration of the parameters used and the FIFO scheduling scheme adopted in this context.

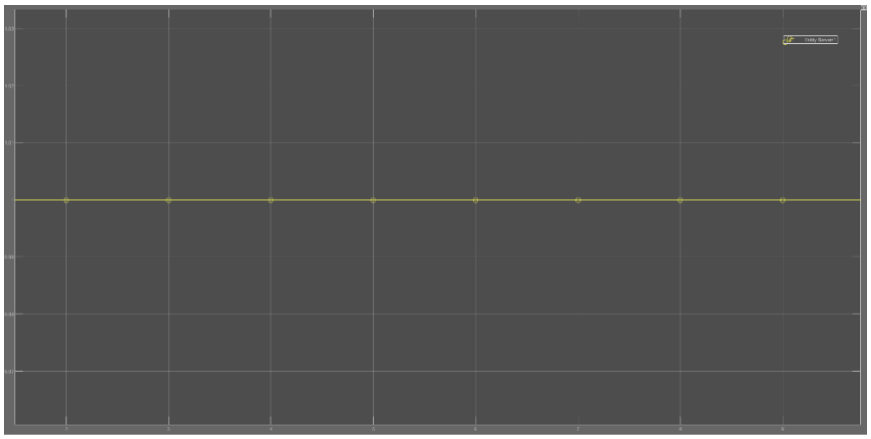

Figure 6. Simulation of the server interaction

5. CONCLUSION

A mathematical model for a smart grid cyber physical power system was developed in this paper and a model simulation was performed using MATLAB and Simulink software simulation tools to analyze the behaviour of the system. In order to exercise effective control and management over SGCPPS, knowing the grid conditions, their response to system disturbances that arise, and mitigating failures play a vital part towards achieving sustainable power supply, delivery and utilization. Given the economic benefits derived from this system it is imperative to establish behavioral awareness of the grid. The continuous and discrete behaviour of the physical and cyber systems were verified based on the simulations results. Within the specified simulation period, the graphical interactions captured between the hardware infrastructure and the cyber component provided a holistic insight into the control and management of the SGCPPS. In this regard, the formulation of this hybrid approach established from the mathematical model represented a steady relationship between the physical and cyber component. However, future works would investigate the effect of various system faults especially the implications of cyber-attacks (denial of service and distributed denial of service) on multi-server systems. Therefore, subsequent research would analyze the robustness and stability of the continuous and discrete behaviour in the face of privacy concerns, latency, packet loss and queuing.

REFERENCES

[1] Q. Wang, G. Zhang, and F. Wen, "A survey on policies, modelling and security of cyber-physical systems in smart grids," *Energy Conversion and Economics*, vol. 2, no. 4, pp. 197–211, Dec. 2021, doi: 10.1049/enc2.12051.

[2] X. Yu and Y. Xue, "Smart Grids: A Cyber–Physical Systems Perspective," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1058–1070, May 2016, doi: 10.1109/JPROC.2015.2503119.

[3] A. Nayak, R. Reyes Levalle, S. Lee, and S. Y. Nof, "Resource sharing in cyber-physical systems: modelling framework and case studies," *Int J Prod Res*, vol. 54, no. 23, pp. 6969–6983, Dec. 2016, doi: 10.1080/00207543.2016.1146419.

[4] S. Poudel, Z. Ni, and N. Malla, "Real-time cyber physical system testbed for power system security and control," *International Journal of Electrical Power & Energy Systems*, vol. 90, pp. 124–133, Sep. 2017, doi: 10.1016/j.ijepes.2017.01.016.

[5] B. Chen, J. Wang, and M. Shahidehpour, "Cyber–physical perspective on smart grid design and operation," *IET Cyber-Physical Systems: Theory & Applications*, vol. 3, no. 3, pp. 129–141, Sep. 2018, doi: 10.1049/iet-cps.2017.0143.

[6] R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, and V. Terzija, "A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid – Part – I: Background on CPPS and necessity of CPPS testbeds," *International Journal of Electrical Power & Energy Systems*, vol. 136, p. 107718, Mar. 2022, doi: 10.1016/j.ijepes.2021.107718.

[7] H. Zhang, B. Liu, and H. Wu, "Smart Grid Cyber-Physical Attack and Defense: A Review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021, doi: 10.1109/ACCESS.2021.3058628.

[8] Y. Wadhawan, A. AlMajali, and C. Neuman, "A Comprehensive Analysis of Smart Grid Systems against Cyber-Physical Attacks," *Electronics (Basel)*, vol. 7, no. 10, p. 249, Oct. 2018, doi: 10.3390/electronics7100249.

[9] F. Liberati, E. Garone, and A. Di Giorgio, "Review of Cyber-Physical Attacks in Smart Grids: A System-Theoretic Perspective," *Electronics (Basel)*, vol. 10, no. 10, p. 1153, May 2021, doi: 10.3390/electronics10101153.

[10] H. Mora, J. F. Colom, D. Gil, and A. Jimeno-Morenilla, "Distributed computational model for shared processing on Cyber-Physical System environments," *Comput Commun*, vol. 111, pp. 68–83, Oct. 2017, doi: 10.1016/j.comcom.2017.07.009.

[11] L. Arnaboldi, R. M. Czekster, C. Morisset, and R. Metere, "Modelling Load-Changing Attacks in Cyber-Physical Systems," *Electron Notes Theor Comput Sci*, vol. 353, pp. 39–60, Nov. 2020, doi: 10.1016/j.entcs.2020.09.018.

[12] C. Bordin, A. Håkansson, and S. Mishra, "Smart Energy and power systems modelling: an IoT and Cyber-Physical Systems perspective, in the context of Energy Informatics," *Procedia Comput Sci*, vol. 176, pp. 2254–2263, 2020, doi: 10.1016/j.procs.2020.09.275.

[13] F. Darbandi, A. Jafari, H. Karimipour, A. Dehghantanha, F. Derakhshan, and K. Raymond Choo, "Real-time stability assessment in smart cyber-physical grids: a deep learning approach," *IET Smart Grid*, vol. 3, no. 4, pp. 454–461, Aug. 2020, doi: 10.1049/iet-stg.2019.0191.

[14] A. Chakrabortty and A. Bose, "Smart Grid Simulations and Their Supporting Implementation Methods," *Proceedings of the IEEE*, vol. 105, no. 11, pp. 2220–2243, Nov. 2017, doi: 10.1109/JPROC.2017.2737635.

[15] K. Marashi, S. S. Sarvestani, and A. R. Hurson, "Consideration of Cyber-Physical Interdependencies in Reliability Modeling of Smart Grids," *IEEE Transactions on Sustainable Computing*, vol. 3, no. 2, pp. 73–83, Apr. 2018, doi: 10.1109/TSUSC.2017.2757911.

[16] H. Orojloo and M. Abdollahi Azgomi, "Modelling and evaluation of the security of cyber-physical systems using stochastic Petri nets," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 1, pp. 50–57, Mar. 2019, doi: 10.1049/iet-cps.2018.0008.

[17] N. K. Singh and V. Mahajan, "Mathematical Model of Cyber Intrusion in Smart Grid," in *2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia)*, IEEE, Mar. 2019, pp. 965–969. doi: 10.1109/GTDAsia.2019.8715946.

[18] M. M. Iqbal, I. A. Sajjad, M. F. Nadeem Khan, R. Liaqat, M. A. Shah, and H. A. Muqeet, "Energy Management in Smart Homes with PV Generation, Energy Storage and Home to Grid Energy Exchange," in *2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, IEEE, Jul. 2019, pp. 1–7. doi: 10.1109/ICECCE47252.2019.8940684.

[19] A. V. Jha, B. Appasani, and A. N. Ghazali, "Analytical Channel Modelling of Synchrophsor Communication Networks in a Smart Grid Cyber Physical System," in *2021 3rd Global Power, Energy and Communication Conference (GPECOM)*, IEEE, Oct. 2021, pp. 257–262. doi: 10.1109/GPECOM52585.2021.9587832.

[20] D. C. Devisree Chippada, "Mathematical modeling and simulation of energy management in smart grid," *International Journal of Smart Grid and Clean Energy*, pp. 746–755, 2020, doi: 10.12720/sgce.9.4.746-755.

[21] G. C. Konstantopoulos, A. T. Alexandridis, and P. C. Papageorgiou, "Towards the Integration of Modern Power Systems into a Cyber–Physical Framework," *Energies (Basel)*, vol. 13, no. 9, p. 2169, May 2020, doi: 10.3390/en13092169.

[22] R. Wagle, P. Sharma, C. Sharma, M. Amin, J. L. Rueda, and F. Gonzalez-Longatt, "Optimal power flow-based reactive power control in smart distribution network using real-time cyber-physical co-simulation framework," *IET Generation, Transmission & Distribution*, vol. 17, no. 20, pp. 4489–4502, Oct. 2023, doi: 10.1049/gtd2.12786.