Grid-Metaverse: The Path From Digital Twins and Prototype Tests on DC Microgrids

***Abstract*—With the development of cutting-edge technologies and the efforts of business giants, Metaverse is getting closer and closer to us. In addition to the fields of healthcare, education and cultural tourism, Metaverse will also have a profound impact on the power grid. The digital twin (DT) is regarded as the foundation of Metaverse, but its high cost hinders the wide application of DTs in power grids. In this paper, we propose a path to build the DTs in the DC microgrid, which is a representative block in the future power grid with the penetration of renewable energy sources, forming Grid-Metaverse that can significantly reduce the cost and improve the interactivity. A model-based DT, which is originated from the physical model, and a data-driven DT, using the graph neural network with the data from the model-based one, are built together to illustrate this path and to show their roles in the Grid-Metaverse. Moreover, in the prototype tests, the threats of denial-of-service (DoS) and false data injection (FDI) attacks are validated through the developed DTs.**

***Index Terms*—Grid-Metaverse, Digital Twin, DC Microgrid, Cyberattack, Graph Neural Network**

I. INTRODUCTION

There is no agreed-upon definition of the Metaverse, but it is frequently used to refer to a future scenario in which the virtual and physical worlds are closely intertwined [1]. Although the precise design of the future Metaverse is unknown, many tech behemoths, including Facebook, Microsoft, and NVIDIA, are trying to create it using cutting-edge technologies like augmented reality, artificial intelligence, blockchain, cloud, edge computing, etc. [2].

Metaverse can give users immersive experiences that transcend space and time, and it is also seen as the next generation of the Internet with a significant social dimension [3]. The applications of Metaverse will make it possible for human users to live and play in a self-sustaining, persistent and shared domain [4]. Possible applications of Metaverse are already being shown in the medical industry [5], [6], the education industry [7], and the cultural tourism [8], [9]. Research has also been done in the industry area to suggest a roadmap for an industrial Metaverse built based on ideas like Social-Cyber-Physical System (SCPS) and Industry 5.0, ultimately enabling the efficient use of resources and the delivery of goods and services to satisfy individual needs [10].

Metaverse will also enable a natural shift in the way people work to telecommuting. It has been demonstrated that telecommuting not only does not impair the work's quality but also boosts output [11]. In addition to office workers, the teleworker population will also consist of engineers, scientists, and technicians [12]. The convergence of the real and the virtual will lead to a greater flow of information [13], which, combined with closer collaboration and simulation, will make it easier to manage complex projects and reduce costs as the need for physical prototypes decreases [12]. Although the results of the massive investment of money are still limited [14], it is believed that the future of Metaverse is promising and Metaverse will be everywhere [15].

The main contributions of this paper are as follows.

- An overview is shown about the far-reaching impact that the introduction of Metaverse will have on the grid in all life cycle.
- One path to Grid-Metaverse from grid digital twin (DT) is proposed for solving the high cost and lack of interoperability. And model-based DT and data-driven DT are constructed for functional prototype tests to illustrate the path.
- Model-based DT is set up for security assessment, and direct impacts are found created by the hybrid attack.
- Graph neural network PIDeuG is migrated to the DC microgrid (DCmG), and the training function of this data-driven DT is shown.

This paper is organized as follows. In Section II, we will show the benefits Metaverse will bring to the grid throughout its life cycle and will give the path to Grid-Metaverse from grid DT to reduce the cost and improve the interactivity. In Sections III and IV, the realization of model-based DT and data-driven DT is introduced respectively. In Section V, we show the results of the experiment. Section VI gives the summary and prospects.

II. GRID-METAVERSE

A. When Metaverse meets power grids

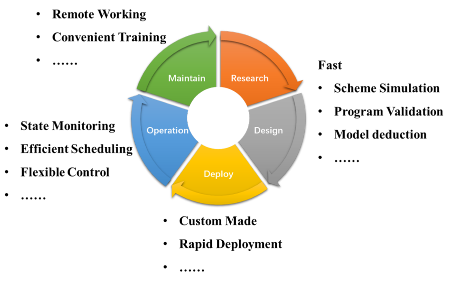

Fig. 1. Metaverse brings benefits to the grid throughout its life cycle.

Nowadays, the grid, moving towards a smart grid, is becoming increasingly large and complex under the influence of societal goals such as sustainability [16]. Some studies propose the introduction of Metaverse into the grid [17]. On the one hand, this accommodates the shift of the grid from a pure CPS to a SCPS [18], and on the other hand, it may bring benefits to the grid throughout its life cycle.

In the research and design stage, many models and theories either stay on paper or require much time and cost for testing because it is difficult to have an actual power system for experiments [19]. Metaverse, however, can provide powerful technical support for new power system modeling. It can help to realize rapid planning derivation, scheme simulation, and proposal verification of new power grid systems under virtual scenarios, so as to provide feedback to guide the control, optimization, and resource allocation of physical power grids, greatly improving the efficiency of design and research [20]. When the deployment is required, the previous design relying on the manufacturing link and transportation link in the industrial Metaverse can be quickly landed to shorten the deployment cycle [10].

In the operation stage, the physical entity of the power system and the virtual space of Metaverse realize the virtual reality through advanced sensing and high-speed communication. By establishing control and scheduling strategies for each power equipment in Metaverse, the flexible and optimal scheduling of the virtual power system in Metaverse is achieved, which in turn leads to more efficient and safer operation of the power system in reality [21]. In periods when maintenance is required, the use of technologies such as augmented reality can provide maintenance personnel with an accurate grasp of equipment principles, state parameters, and operational status [22], and if technologies such as remote collaborative robotics are used, safe remote maintenance beyond spatial limitations can also be achieved [23]. In addition, Metaverse can facilitate communication and collaboration between staff members to improve project efficiency, and can also be used to train grid staff at all stages, reducing training costs while improving training effectiveness [13].

Because the concept of Metaverse is relatively vague and its goals are not sufficiently clear, the path to its realization is also difficult to be completely explicit. But for this very reason, the possible changes that Metaverse will bring to the power grid will be far more than that and fascinating.

B. From DT to Metaverse

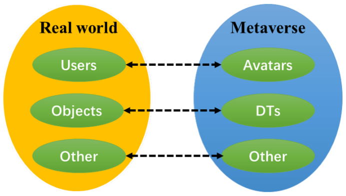

Fig. 2. A simplified relationship between Metaverse and DT.

DT is considered to be part of Metaverse and an important supporting technology [24]. Although, like Metaverse, DT lacks a uniform definition, the basic idea behind DT is a high-precision virtual model of physical entities [25]. DT serves as a solution to replicate the real world in Metaverse, allowing participants to experience physical entities as if they were interacting with them in the real world [26]. Currently, grid DT is still in its nascent stage [27] and the high cost is the main obstacle for the digital twin of the grid and any other general CPS [28]. However, it is foreseeable that grid DT is a necessary path in the evolution of the grid towards Metaverse. And the perspective of Metaverse will bring new insights to the development of grid DT.

DT behavior models can be built based on model or data [29]. The ANGEL DT framework proposed in [30] can be used to continuously track the power system and provide information about the grid dynamics. According to the ANGEL vision, model-based DT built in real-time simulation devices will play an important role in grid DT, but the high cost of these devices will hinder grid DT development. To address this problem, many data-driven approaches have been proposed in the fields of grid optimization, control, fault, and attack detection [31]–[33]. If the data is obtained based on the model-based DT, and then data-driven methods are used to obtain an approximate model of the physical dynamics, it will allow reducing the cost significantly. And considering that the current research related to grid DT is always proposed, designed, and tested on various small-size platforms [34], the relative separation of model-based DT and data-driven DT is conducive to the realization of interoperability in the future Metaverse, as well as the specialization of the division of labor and further reduction of cost [4].

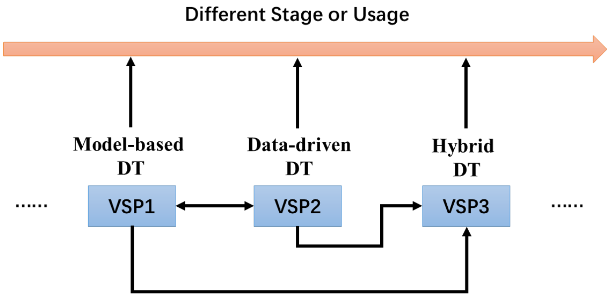

Fig. 3. VSPs' functions and the relationship between VSPs.

At that time, there will be different virtual service providers(VSPs), providing different virtual services to users, and VSPs can cooperate with each other. It should be noted that the boundary between VSPs and users will become increasingly indistinct in the future, and users can also become new VSPs, relying on the use of other virtual service providers to establish new own services [35].

In the Sections IV-VI, we will experiment with functional prototypes of model-based grid DT service providers, and data-driven grid DT service providers, respectively, in the context of Metaverse to further demonstrate their own roles and relationships with each other.

In the case, although not limited to specific scenarios, we chose a DC microgrid, which integrates distributed energy sources, energy storage units, and flexible loads [36]. On the one hand, DCmG is expected to be able to solve the increasingly prominent problem of grid integration of renewable energy sources as countries around the world accelerate their development and is very promising [38], on the other hand, it is simpler in control but representative as part of a microgrid which is the basis of the smart grid [39].

III. MODEL-BASED DT

The VSP that provides model-based DT is expected to provide users with a graphical or immersive model-building platform that, once built, calculates and returns real-time operational data about the grid at the user's command from its own computing center or other cloud platforms as needed. For that, the prototype device was built just as shown in the Fig. 4.

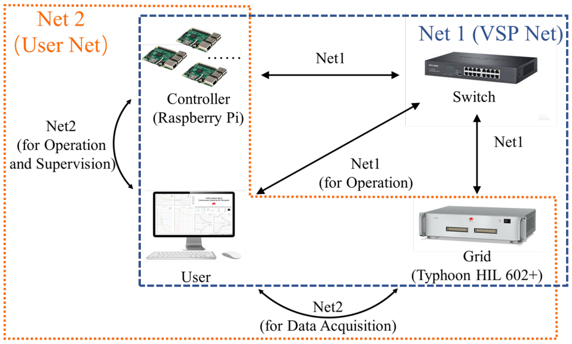

Fig. 4. Implementation overview of the model-baesd DCmG DT platform.

Abstractly, it can be divided into two information networks. Net1 is a microgrid model simulation network, which serves as the net of VSPs and is used for simulation, and Net2 is an operation and monitoring network, which serves as the net of users. Users can send operation instructions and collect simulation data through Net2. In our prototype, there are mainly four entities, namely, host, HIL simulator, controller and switch. They cover two information networks and play different roles.

In section IV, we will use the prototype device to do security assessment about a hybrid attack on the DCmG in the structure Fig. 5

A. HIL Simulator

HIL simulator serves as the computing center or cloud platform and is used to simulate power supply, load, line, actuator, sensor, and other objects. The Typhoon hardware in the loop (HIL) 602 + simulator can realize ultra-low delay and ultra-high fidelity real-time simulation of power electronic microgrid [37].

As shown in the Fig. 5, in each node, the DC voltage source represents the battery or conventional new energy and then is connected to the common coupling point of the power grid through the LC filter circuit and the voltage converter. The load of the node is represented by the current source. The voltmeter and the ammeter can measure the voltage of the common coupling point and output current of the node respectively. The nodes are connected through a certain cable resistance.

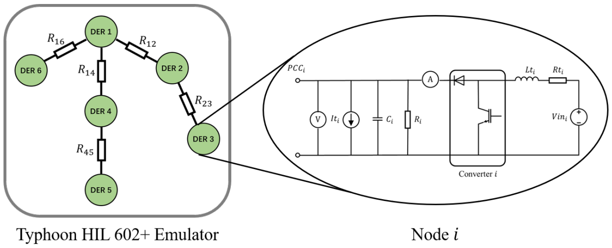

Fig. 5. Physical model and connection topology.

B. Controller

The controller is mainly responsible for executing the control program, including the communication between nodes, and the calculation and transmission of control signals. In the platform, the execution equipment transmitted to by the controller refers to the voltage converter. Any required control algorithm can be implemented in the controller, which is also the key to the more expansibility of the platform. A typical DCmG hierarchical control scheme is selected and used in this platform [40].

C. Host

The host serves as the user. On the one hand, the host is connected to the communication network of the microgrid and can implement the operation. On the other hand, the host is connected to the controller through Net2, just for example, which can realize the remote configuration and supervision of the controller. In addition, the host is connected to the Typhoon, which can make real-time monitoring and recording of the operation status of the microgrid on the Typhoon SCADA interface.

D. Switch

Switch the messages between the node controllers to simulate the real communication environment.

IV. DATA-DRIVEN DT

Some VSPs, as mentioned in Section III, can provide data-driven DT using the data from the model-based DT. In section IV, We will construct a date-driven DT for Metaverse training about grid attacks in this way.

A. Graph Neural Network

The traditional deep learning methods can be used in DTs, but their performance in processing non-Euclidean space data is still unsatisfactory. Therefore, the graph neural network came into being. The graph neural network makes full use of the information of the graph. It is flexible and powerful and can handle the graph data well [41]. Graph neural network has achieved rapid development in recent years and has achieved great success in the task of processing graph data, such as N-body dynamics [42], Hamiltonian mechanics [43], and particle dynamics [44]. Microgrid also has complex topological structure, but there are few reports of using graph neural network to try to solve microgrid-related problems. Yu *et al.* designed the PIDeuG network to predict the transient response of AC power grid load change [45]. However, the network has not been applied to DCmGs. We will use that to model the transient response of attack on the DCmG and the following is the network model.

B. Network Model

The input and output of the network and the design of the network structure in this method refer to PIDGeuN.

Let the state of the i^{th} node at moment k be $x_{gi}^{(k)} = [Vpcc_i, I_i]$, and let $x_i^{(k)} = [x_{gi}^{(k)}, It_i, Flag]$, where $Vpcc_i$ and I_i represents the voltage of the common coupling point and node output of node i respectively, It_i represents the current data in the node i server, and if there is attack in the system $flag = 1$, otherwise $flag = 0$. Let $X_g^{(k)} = [x_{g1}^{(k)}, x_{g2}^{(k)}, ..., x_{gi}^{(k)} ...]$, $X^{(k)} = [x_1^{(k)}, x_2^{(k)}, ..., x_i^{(k)} ...]$ and $\chi_C^{(k)} = [X^{(k)}, X^{(k-1)}, ..., X^{(k-C+1)}]$. Then the input of the system is $\chi_C^{(k)}$, and the output is $X_g^{(k+1)}$.

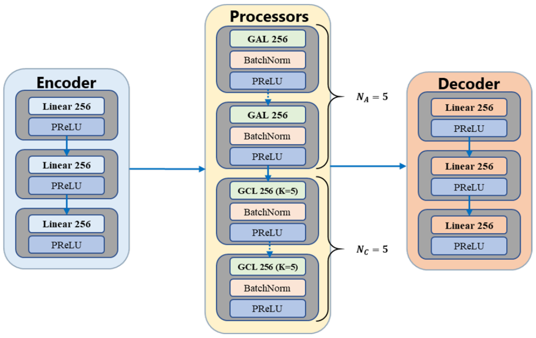

Fig. 6. Network model.

The network in Fig. 6 is mainly composed of three parts: encoder, processor, and decoder. The encoder increases the dimension of the original data and more fully expresses the Boolean value and other variables. The processor is composed of graph convolution layers and graph attention layers with stronger nonlinearity. The application of BatchNorm in the model reduces the risk of gradient disappearance and overfitting.

The network in this paper does not use the technology of constructing the new adjacency matrix and physical regularization mentioned in the original PIDGeuN, but from the following results, the model can still get good results.

V. TEST RESULTS

A. Basic Settings

The electrical parameters in Fig. 5 are shown in Table I, and the controll related parameters are in Table II. The current loads of nodes are set as in Table III. Besides, the control cycle is 0.05s and the communication cycle is 0.02s.

TABLE I
FUNDAMENTAL PARAMETERS

Item Name	Fundamental Parameters					
	Vin_i	Rt_i	Lt_i	R_i	C_i	$Rline_i$
Value	$68V$	0.2Ω	$0.002H$	200Ω	$0.0018F$	0.2Ω

TABLE II
CONTROLLER PARAMETERS

Item Name	Primary Controller			Second Controller	
	kp_V	kp_I	k_i	k_p	k_i
Value	0.85	0.01	2	0.1	0.15

TABLE III
LOAD

Node #	1	2	3	4	5	6
Value (A)	2.5	2.75	2	2.25	2.5	2.75

B. Attack Implementation

1) DoS: A denial-of-service (DoS) attack occurs when the information systems, devices, or other network resources are unable to access. There are many ways to implement DoS attacks like Smurf Attack and SYN flood [46]. In the following test, we just use ARP to achieve the equivalent attack effect. When ARP spoofing is applied to the controllers of nodes 1 and 2 simultaneously and the interacted data packets are discarded, then the communication link is selectively cut off.

2) FDI: A false data injection (FDI) attack is to inject a well-designed malicious value into a communication link. The man-in-the-middle attack is one way to implement FDI attacks [47]. In the following test, we just use ARP Spoofing to selectively eavesdrop, modify and forward. When ARP spoofing is applied to node 1 and node 2 at the same time, eavesdropping on the current information replied by node 1 to node 2, modifying and retransmitting, and only forwarding other data packets, node 1 will be normal and only node 2 will obtain the wrong current information.

3) Hybrid Attack: That is using different types of attacks, such as DoS attacks and FDI attacks.

C. Model-based DT

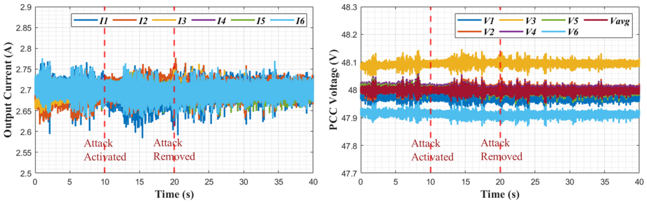

Fig. 7. Impact of DoS attack on the model-based DT.

Dos Attack: Within the range of $t = 10$s to $t = 20$s, the communication link of nodes 1 and 2 is cut off by ARP deception. For node 1, the information from node 2 is $I_{21}(t) = I_{21}(t_0), t_0 = 10$s, $t \in (10, 20)$. For node 2, the information from node 1 is $I_{12}(t) = I_{12}(t_0), t_0 = 10$s, $t \in (10, 20)$. It can be seen from Fig. 7 that there is no obvious change before and after the attack, as the disconnected link does not destroy the connectivity of the communication network [48].

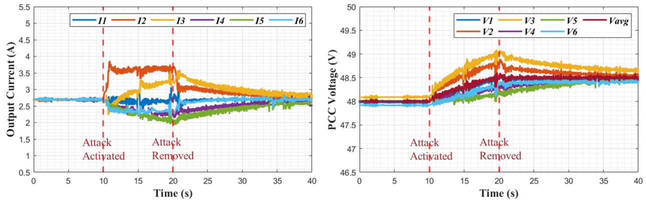

Fig. 8. Impact of FDI attack on the model-based DT.

FDI Attack: Within the range of $t = 10$s to $t = 20$s, the communication information obtained from node 3 to node 2 is modified as a fixed value, i.e., $I_{21} = 5$A, $t \in (10, 20)$. The results can be seen from the Fig. 8. The current of each node deviates from the equilibrium value. While the currents of nodes 2 and 3 raise a lot, the currents of nodes 4, 5 and 6 reduce correspondingly. The voltage of each node monotonously rises during the attack. This will destroy the grid a lot since nodes 2 and 3 have the risk of overvoltage and nodes 4, 5 and 6 will get impaired due to the current return. After the attack, the current sharing state can be restored under the action of the controller, but the average voltage after the attack does not return to the equilibrium voltage. So the risk of overvoltage still exists.

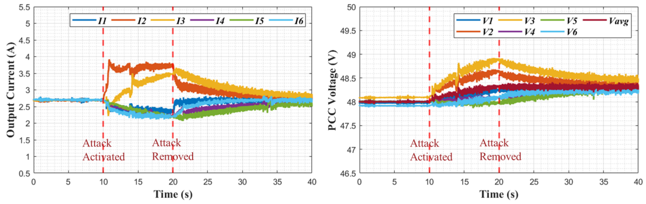

Fig. 9. Impact of hybrid attack on the model-based DT.

Hybrid Attack: Within the range of of $t = 10$s to $t = 20$s, the communication link of nodes 1 and 2 is cut off by ARP deception, and the communication information obtained by node 2 from node 3 is modified to a fixed value of 5A. Compared with the above-mentioned separate DoS attack (Fig. 7) and FDI attack (Fig. 8), the addition of DoS attack makes the impact of FDI attack on the current of node 1 severe. Under the condition of FDI attack, the impact of DoS attack seems no longer trivial.

It is demonstrated that the model-based DT can be used to simulate the microgrid in a real-time manner and we can use it as a security assessment tool for DCmG.

D. Data-driven DT

1) Using Data: The training data is from the model-based DT with six node topology as shown in Fig. 5, where a total of 350+ samples are collected. Each sample contains 80s of information (voltage, current, current in the server, attack flag, and time), of which the 40^{th} is the attack, that is, random false data injection is added to each server. There are 10 sampling points per second.

2) Results: In order to iterate the prediction, the predicted data can be combined with the data of the last two moments before inputting the network next. But when the output is $X_g^{(k+1)}$, the data of the server of each node is not known, so the predicted current value can only be used as the data in the server. However, due to the lag of the server data update in the actual situation, the value in the server at the same time is not the real-time value of the current, so this method can not get good results. Therefore, the model is retrained to enable the model to output the current value in the server. When there is an external attack, that is, when the flag is 1, the attack value will be automatically used.

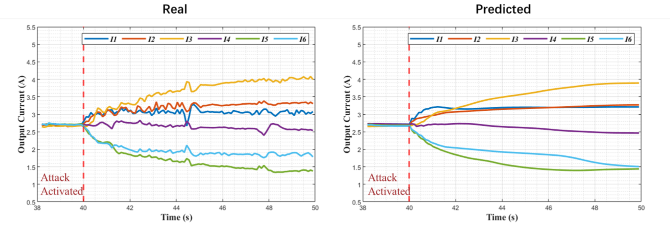

Fig. 10. Accuracy of the data-driven DT.

The mean absolute error of the current within 10s of attack is about 0.087A. So it can be seen that the data-driven DT can be used to predict the attack effect quickly and conveniently at any steady state as long as the user inputs the attack value. It can be used for grid operator training about attack effect.

VI. CONCLUSION AND FUTURE WORKS

In this paper, we envisioned the positive changes that Metaverse will bring to the grid, and starting from the view of Metaverse, a possible path from grid DT to Grid-Metaverse was proposed. Through the specialization of the division of labor among different VSPs, it is promising to reduce the cost of development and achieve the trend of interoperability. We built model-based and data-driven DTs as separate VSP prototypes. The model-based DT using HIL can play a role in the design and verification of control schemes and security analysis. The data obtained from model-based DT built by the specific VSP can be used to obtain an approximate model of physical dynamics through the data-driven method, which can expand the application scenarios of DT to other stages in the life cycle. The test results of security analysis indicate that both DoS and FDI attacks can significantly deteriorate the control performance of DCmG, and even induce overvoltage security accidents.

However, the prototype tests are incomplete, and more detailed experiments are still needed. Besides the function impact from Metaverse we mentioned, the application of blockchain may also have a great influence on grid safety and security. In the future, on the one hand, we will exploring more about grid DT from the perspective of Metaverse; on the other hand, we will focus on the research of collaborative FDI attacks at all levels with the help of the DTs. In addition, we will further study the application of graph neural networks in the security and control of the microgrid.

REFERENCES

[1] A. M. Al-Ghaili *et al.*, “A Review of Metaverse’s Definitions, Architecture, Applications, Challenges, Issues, Solutions, and Future Trends,” *IEEE Access*, vol. 10, pp. 125835–125866, 2022, doi: 10.1109/ACCESS.2022.3225638.

[2] Y. Wang *et al.*, “A Survey on Metaverse: Fundamentals, Security, and Privacy,” *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2022, doi: 10.1109/COMST.2022.3202047.

[3] T. Chen, H. Zhou, H. Yang, and S. Liu, “A Review of Research on Metaverse Defining Taxonomy and Adaptive Architecture,” in *2022 5th International Conference on Pattern Recognition and Artificial Intelligence (PRAI)*, Aug. 2022, pp. 960–965. doi: 10.1109/PRAI55851.2022.9904076.

[4] L.-H. Lee *et al.*, “All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda.” arXiv, Nov. 03, 2021. doi: 10.48550/arXiv.2110.05352.

[5] D. Yang *et al.*, “Expert consensus on the metaverse in medicine,” *Clinical eHealth*, vol. 5, pp. 1–9, Dec. 2022, doi: 10.1016/j.ceh.2022.02.001.

[6] S. Qiao *et al.*, “SPReCHD: Four-Chamber Semantic Parsing Network for Recognizing Fetal Congenital Heart Disease in Medical Metaverse,” *IEEE Journal of Biomedical and Health Informatics*, pp. 1–11, 2022, doi: 10.1109/JBHI.2022.3218577.

[7] B. Kye, N. Han, E. Kim, Y. Park, and S. Jo, “Educational applications of metaverse: possibilities and limitations,” *J Educ Eval Health Prof*, vol. 18, Dec. 2021, doi: 10.3352/jeehp.2021.18.32.

[8] C. I. Nwakanma, J. N. Njoku, J. Jo, C. Lim, and D. Kim, “‘Creativia’ Metaverse Platform for Exhibition Experience,” in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, Oct. 2022, pp. 1789–1793. doi: 10.1109/ICTC55196.2022.9952599.

[9] D. Gursoy, S. Malodia, and A. Dhir, “The metaverse in the hospitality and tourism industry: An overview of current trends and future research directions,” *Journal of Hospitality Marketing & Management*, vol. 31, no. 5, pp. 527–534, Jul. 2022, doi: 10.1080/19368623.2022.2072504.

[10] X. Yao *et al.*, “Enhancing wisdom manufacturing as industrial metaverse for industry and society 5.0,” *J Intell Manuf*, Nov. 2022, doi: 10.1007/s10845-022-02027-7.

[11] A. Ozimek, “The Future of Remote Work.” Rochester, NY, May 27, 2020. doi: 10.2139/ssrn.3638597.

[12] H. Pozniak, “Could engineers work in the metaverse?,” *Engineering & Technology*, vol. 17, no. 4, pp. 1–8, May 2022, doi: 10.1049/et.2022.0408.

[13] J. Lee and P. Kundu, “Integrated cyber-physical systems and industrial metaverse for remote manufacturing,” *Manufacturing Letters*, vol. 34, pp. 12–15, Oct. 2022, doi: 10.1016/j.mfglet.2022.08.012.

[14] Z. Allam, A. Sharifi, S. E. Bibri, D. S. Jones, and J. Krogstie, “The Metaverse as a Virtual Form of Smart Cities: Opportunities and Challenges for Environmental, Economic, and Social Sustainability in Urban Futures,” *Smart Cities*, vol. 5, no. 3, Art. no. 3, Sep. 2022, doi: 10.3390/smartcities5030040.

[15] Christensen, Lau, and Alex Robinson. ”The potential global economic impact of the metaverse.” Analysis Group. https://www.analysisgroup.com/globalassets/insights/publishing/2022-the-potential-global-economic-impact-of-the-metaverse. pdf (Accessed: Jul. 13, 2022), 2022.

[16] M. A. Judge, A. Khan, A. Manzoor, and H. A. Khattak, “Overview of smart grid implementation: Frameworks, impact, performance and challenges,” *Journal of Energy Storage*, vol. 49, p. 104056, May 2022, doi: 10.1016/j.est.2022.104056.

[17] R. Singh *et al.*, “Energy System 4.0: Digitalization of the Energy Sector with Inclination towards Sustainability,” *Sensors*, vol. 22, no. 17, Art. no. 17, Jan. 2022, doi: 10.3390/s22176619.

[18] Y. Xue and X. Yu, “Beyond smart grid—cyber–physical–social system in energy future [point of view],” *Proceedings of the IEEE*, vol. 105, no. 12, pp. 2290–2292, Dec. 2017, doi: 10.1109/JPROC.2017.2768698.

[19] N. Naval and J. M. Yusta, “Virtual power plant models and electricity markets - A review,” *Renewable and Sustainable Energy Reviews*, vol. 149, p. 111393, Oct. 2021, doi: 10.1016/j.rser.2021.111393.

[20] H. Ning *et al.*, “A Survey on Metaverse: the State-of-the-art, Technologies, Applications, and Challenges.” arXiv, Nov. 18, 2021. doi: 10.48550/arXiv.2111.09673.

[21] Y. Deng, Z. Weng, and T. Zhang, “Metaverse-driven remote management solution for scene-based energy storage power stations,” *Evol. Intel.*, Sep. 2022, doi: 10.1007/s12065-022-00769-0.

[22] A. Siyaev and G.-S. Jo, “Towards Aircraft Maintenance Metaverse Using Speech Interactions with Virtual Objects in Mixed Reality,” *Sensors*, vol. 21, no. 6, Art. no. 6, Jan. 2021, doi: 10.3390/s21062066.

[23] Y. Cao *et al.*, “V.Ra: An In-Situ Visual Authoring System for Robot-IoT Task Planning with Augmented Reality,” in *Proceedings of the 2019 on Designing Interactive Systems Conference*, New York, NY, USA, Jun. 2019, pp. 1059–1070. doi: 10.1145/3322276.3322278.

[24] M. Intizar Ali, P. Patel, J. G. Breslin, R. Harik, and A. Sheth, “Cognitive Digital Twins for Smart Manufacturing,” *IEEE Intelligent Systems*, vol. 36, no. 2, pp. 96–100, Mar. 2021, doi: 10.1109/MIS.2021.3062437.

[25] C. Semeraro, M. Lezoche, H. Panetto, and M. Dassisti, “Digital twin paradigm: A systematic literature review,” *Computers in Industry*, vol. 130, p. 103469, Sep. 2021, doi: 10.1016/j.compind.2021.103469.

[26] L. U. Khan, W. Saad, D. Niyato, Z. Han, and C. S. Hong, “Digital-Twin-Enabled 6G: Vision, Architectural Trends, and Future Directions,” *IEEE Communications Magazine*, vol. 60, no. 1, pp. 74–80, Jan. 2022, doi: 10.1109/MCOM.001.21143.

[27] Z. Jiang, H. Lv, Y. Li, and Y. Guo, “A novel application architecture of digital twin in smart grid,” *J Ambient Intell Human Comput*, vol. 13, no. 8, pp. 3819–3835, Aug. 2022, doi: 10.1007/s12652-021-03329-z.

[28] M. Eckhart and A. Ekelhart, “Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook,” in *Security and Quality in Cyber-Physical Systems Engineering: With Forewords by Robert M. Lee and Tom Gilb*, S. Biffl, M. Eckhart, A. Lüder, and E. Weippl, Eds. Cham: Springer International Publishing, 2019, pp. 383–412. doi: 10.1007/978-3-030-25312-7_14.

[29] T. G. Ritto and F. A. Rochinha, “Digital twin, physics-based model, and machine learning applied to damage detection in structures,” *Mechanical Systems and Signal Processing*, vol. 155, p. 107614, Jun. 2021, doi: 10.1016/j.ymssp.2021.107614.

[30] W. Danilczyk, Y. Sun, and H. He, “ANGEL: An Intelligent Digital Twin Framework for Microgrid Security,” in *2019 North American Power Symposium (NAPS)*, Oct. 2019, pp. 1–6. doi: 10.1109/NAPS46351.2019.9000371.

[31] G. S. Thirunavukkarasu *et al.*, “Role of optimization techniques in microgrid energy management systems—A review,” *Energy Strategy Reviews*, vol. 43, p. 100899, Sep. 2022, doi: 10.1016/j.esr.2022.100899.

[32] S. Kim, K.-J. Park, and C. Lu, “A Survey on Network Security for Cyber–Physical Systems: From Threats to Resilient Design,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1534–1573, 2022, doi: 10.1109/COMST.2022.3187531.

[33] T. B. Lopez-Garcia, A. Coronado-Mendoza, and J. A. Domínguez-Navarro, “Artificial neural networks in microgrids: A review,” *Engineering Applications of Artificial Intelligence*, vol. 95, p. 103894, Oct. 2020, doi: 10.1016/j.engappai.2020.103894.

[34] Md. M. H. Sifat *et al.*, “Towards electric digital twin grid: Technology and framework review,” *Energy and AI*, vol. 11, p. 100213, Jan. 2023, doi: 10.1016/j.egyai.2022.100213.

[35] Y. Han *et al.*, “A Dynamic Hierarchical Framework for IoT-Assisted Digital Twin Synchronization in the Metaverse,” *IEEE Internet of Things Journal*, vol. 10, no. 1, pp. 268–284, Jan. 2023, doi: 10.1109/JIOT.2022.3201082.

[36] S. Kakran and S. Chanana, “Smart operations of smart grids integrated with distributed generation: A review,” *Renewable and Sustainable Energy Reviews*, vol. 81, pp. 524–535, Jan. 2018, doi: 10.1016/j.rser.2017.07.045.

[37] M. Liu *et al.*, “Demo Abstract: A HIL Emulator-Based Cyber Security Testbed for DC Microgrids,” in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, May 2021, pp. 1–2. doi: 10.1109/INFOCOMWKSHPS51825.2021.9484453.

[38] IEA. ”Electricity information: Overview.” July 2022, https://www.iea.org/reports/electricity-information-overview.

[39] H. Lotfi and A. Khodaei, “AC Versus DC Microgrid Planning,” *IEEE Transactions on Smart Grid*, vol. 8, no. 1, pp. 296–304, Jan. 2017, doi: 10.1109/TSG.2015.2457910.

[40] M. Tucci, L. Meng, J. M. Guerrero, and G. Ferrari-Trecate, “Stable current sharing and voltage balancing in DC microgrids: A consensus-based secondary control layer,” *Automatica*, vol. 95, pp. 1–13, Sep. 2018, doi: 10.1016/j.automatica.2018.04.017.

[41] Z. Wu *et al.*, “A Comprehensive Survey on Graph Neural Networks,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 1, pp. 4–24, Jan. 2021, doi: 10.1109/TNNLS.2020.2978386.

[42] P. Battaglia, R. Pascanu, M. Lai, D. Jimenez Rezende, and koray kavukcuoglu, “Interaction Networks for Learning about Objects, Relations and Physics,” in *Advances in Neural Information Processing Systems*, 2016, vol. 29. Accessed: Jan. 17, 2023. [Online]. Available: https://proceedings.neurips.cc/paper/2016/hash/3147da8ab4a0437c15ef51a5cc7f2dc4-Abstract.html

[43] A. Sanchez-Gonzalez, V. Bapst, K. Cranmer, and P. Battaglia, “Hamiltonian Graph Networks with ODE Integrators.” arXiv, Sep. 27, 2019. doi: 10.48550/arXiv.1909.12790.

[44] A. Sanchez-Gonzalez *et al.*, “Learning to Simulate Complex Physics with Graph Networks,” in *Proceedings of the 37th International Conference on Machine Learning*, Nov. 2020, pp. 8459–8468. Accessed: Jan. 17, 2023. [Online]. Available: https://proceedings.mlr.press/v119/sanchez-gonzalez20a.html

[45] Y. Yu, X. Jiang, D. Huang, and Y. Li, “PIDGeuN: Graph Neural Network-Enabled Transient Dynamics Prediction of Networked Microgrids Through Full-Field Measurement.” arXiv, Apr. 18, 2022. doi: 10.48550/arXiv.2204.08557.

[46] CISA.”Understanding Denial-of-Service Attacks.” Oct. 2022, https://www.cisa.gov/uscert/ncas/tips/ST04-015.

[47] M. Conti, N. Dragoni, and V. Lesyk, “A Survey of Man In The Middle Attacks,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016, doi: 10.1109/COMST.2016.2548426.

[48] M. Liu, C. Zhao, R. Deng, P. Cheng, and J. Chen, “False Data Injection Attacks and the Distributed Countermeasure in DC Microgrids,” *IEEE Transactions on Control of Network Systems*, vol. 9, no. 4, pp. 1962–1974, Dec. 2022, doi: 10.1109/TCNS.2022.3181483.