Energy and AI 11 (2023) 100213

Contents lists available at ScienceDirect

Energy and AI

journal homepage: www.elsevier.com/locate/egyai

Review

Towards electric digital twin grid: Technology and framework review

Md. Mhamud Hussen Sifat [a], Safwat Mukarrama Choudhury [a], Sajal K. Das [a], Md. Hafiz Ahamed [a], S.M. Muyeen [b,*], Md. Mehedi Hasan [a], Md. Firoj Ali [a], Zinat Tasneem [a], Md. Manirul Islam [a], Md. Robiul Islam [a], Md. Faisal R. Badal [a], Sarafat H. Abhi [a], Subrata K. Sarker [a], Prangon Das [a]

[a] Department of Mechatronics Engineering, Rajshahi University of Engineering & Technology, Rajshahi, 6204, Bangladesh
[b] Department of Electrical Engineering, Qatar University, Doha, 2713, Qatar

ARTICLE INFO

Keywords:
Electric digital twin grid
Online analysis of grid
Cloud platform of grid
Real-time grid analysis
Self-healing
Cybersecurity

ABSTRACT

The major hindrances in the energy system are ecological consciousness, lack of clean and sustainable energy management, insufficient energy distribution–transmission–optimization, expensive power transfer costs, and increased customer knowledge of energy charges. Thus why, universal access to the grid with high cybersecurity, and reliability is needed to solve all these challenges. The digital twin concept turns a new dimension of technology into the world. Electric Digital Twin grid can perform online analysis of the grid in real-time and integrates all the past and present data and express the current grid status to the producers and consumers and also predicts the future grid status. Thus, the power grid transmission loss and location of the overheated line and power connection missing can be detected in addition decision-making and self-healing can possible. The future prediction saves the power grid from small to long accidents such as power outages and even blackout problems. The whole consumers and nation feel relief from these types of accidents and saves from large economic and business loss. The blockchain-enabled digital twin grid provides high security for the grid from cyberattacks. The paper conveys the framework of the electric digital twin grid and the concept of the DT grid processing and the way of serving the producer, prosumers, consumers even the whole nation in infrastructure, education, research, economic, business, and political development.

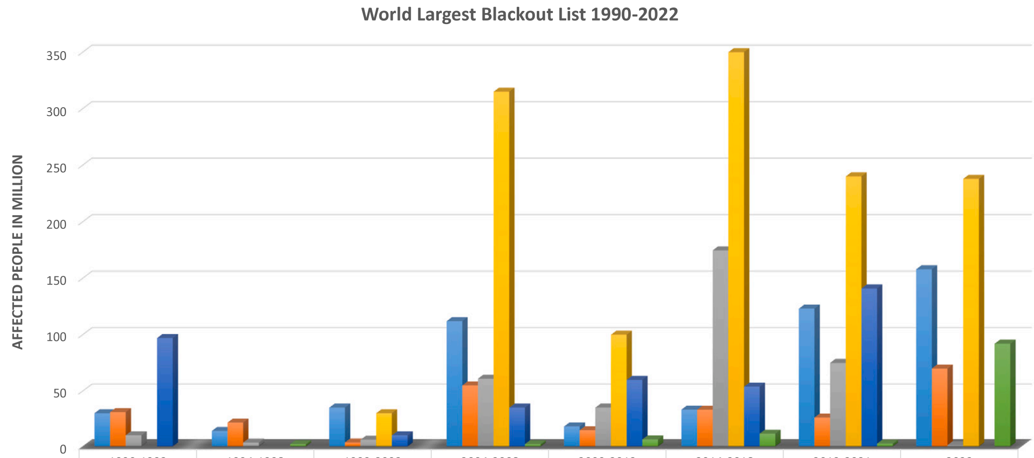
1. Introduction

The electric grid is a network between producer and consumer for power transmission over a large area even in a whole country or country to country. In the very first stage, the traditional grid transfer power over a long distance by centralized one-way power transmission which is produced from oil, coal, and natural gas. When fossil fuels are burned, large quantities of carbon dioxide, Sulphur dioxide, methane, nitrous oxide, and some other greenhouse gases (GHGs), are emitted and pollute the atmosphere. Owing to all this, the electricity sector generates a huge proportion of emissions per source when compared to other sectors, making it a major contributor to greenhouse gases (GHG) [1]. This trend lessens the sole reliance on conventional fossil fuel-based generating, which leads to a decline in the climate carbon dioxide (CO2) emissions. Microgrid alleviated the challenges of the traditional electric grid by introducing DER which confirms a large clean energy resource (solar, wind turbine, wave) and integrates a renewable energy grid. To ensure the use of renewables for the concern of environmental issues in the electrical system, the ideas of microgrid, smart grid, and virtual power plant (VPP) are being investigated in the 21st-century [2]. By the use of contemporary message schemes, intelligence knowledge, and keen campaigns, the microgrid is converted into a virtual power plant (VPP) or else SG in response to the growing demand for electricity and public understanding of the need to cut carbon emissions. Thus, it is crucial to maintain the current essence of these systems in order to guarantee security, enhance control procedures, and automate processes as well as keep these systems up to date. The future grid will be a major source of clean energy that is approachable to everyone and offers high-demand side management in addition to security, dependability, and resilience. The grid is controlled by centralized or decentralized communication along a two-way energy transmission system [3].

Along with these climate issues, world energy demands are increasing at a high rate day by day. Following a 6 percent increase in 2021, the recent analysis predicts that global energy consumption will rise by 2.4 percent in 2022 [4], reflecting the average growth rate of the decade prior to the Covid-19 epidemic. Although it is presently anticipated that the rise in electricity consumption will continue until 2023, the prognosis is complicated by the current economic situation

* Corresponding author.
E-mail address: sm.muyeen@qu.edu.qa (S.M. Muyeen).

https://doi.org/10.1016/j.egyai.2022.100213
Received 17 August 2022; Received in revised form 4 November 2022; Accepted 5 November 2022
Available online 14 November 2022



	1990-1993	1994-1998	1999-2003	2004-2008	2009-2013	2014-2018	2019-2021	2022
USA	30	14	35	112	18	33.2	123	157.9
Canada	31	21.5	3.5	55	14.6	33.1	26	70
Europe	10	3.4	6	61	35	174.7	75	1.1
Asia			30	315	100	350	240	237.8
Africa	97		10	35	60	54	140.94	
Australia		2		2	6.2	11.5	2.46	92

Fig. 1. The affected people rate due to blackout in recent and past few decades [5].

and the unknown consequences that the cost of fuel may have on the generating mix. The world has gone under many blackouts in the past year and even faced them in the last 3 years. Fig. 1 shows the largest blackout list from 1990–2022 in some continents. These blackouts are remained for a long time due to manual maintenance, and high restoring time.

Ecological conscience, inept energy distribution networks, high electricity transfer costs, and growing customer knowledge of energy costs are very common in energy systems [6]. Therefore, universal grid access with high cybersecurity and dependability is required to resolve all of these issues. Renewables are of the utmost importance for achieving clean energy growth. Existing renewable energies have a number of deficiencies, including electrical transmission losses, frequent power outages, electro-mobility, cyberattacks, and inadequate system protection [7]. Rolling blackouts and power shortages in China and the Winter Storm Uri power emergency in Texas were among the most severe interruptions to the energy supply, while additional disruptions exacerbated already problematic markets (nationwide blackout in Pakistan; rolling blackouts in Sri Lanka). In many global markets, the danger of an interruption in the power supply is heightened With the addition of new obstacles, the existing problem such as extreme weather problems such as snowfall, tornados, cyclones, lack of maintenance, low structure of optimization, and chronic underinvestment in generating and grid infrastructure [8–10]. A digital twin is a virtual depiction of a physical object or activity that serves as its digital version in real-time. Consequently, a digital twin grid is a virtual clone of physical infrastructure, processes, and systems that can perform intelligent data analysis, computer modeling, simulation, and machine learning to aid users in boosting traditional electric grid planning and decision-making procedures [11].

Dr. Grieves initially used the phrase “digital twin” in 2013 [19]. A thorough analysis of the most cutting-edge Digital twin applications in business, including product development, manufacturing, prognostics, and health management [20]. NASA’s DT adoption plan incorporated high-fidelity simulation with the onboard integrated medical management platform, service histories, and all accessible ancient and support ships data in order to replicate the life of its physical twin and achieve virtually unreleased levels of safety and predictability [16]. The development of modeling, simulation, and optimization by the digital twin provides an intelligent answer to the intricate power grid system. DT can be used to forecast the predicted behavior of the electric grid in addition to serving visual functions. The DT modeling approach may also be used in tools that help decision-making using real-time data and are based on simulation. The virtual model gathers, transmits, and often processes data from real space in real-time [19]. For decision support or closed-loop control purposes, information or the concept introduced is sent back to the real world. It also integrates the power grid’s past and present histories in real-time simulation, reveals its capability and performance, and can even predict the grid’s future. The digital twin grid, the virtual mirror of the physical grid provides a tremendous novel dimension in the world energy system. It begins a new era of energy distribution, transmission, optimization, management, and self-healing operation along with high cybersecurity [16]. Digital twin includes past and present data in real-time using high computation data analysis capability and decision-making processes provide the whole grid status and all the variation of the data with the comparison of past and smart and secured optimization, of electric grid creates a diversity of changes and reduces all the complexity of current and next-generation electric grid such as conventional online analysis, large-scale data acquisition, and analysis problem, manual monitoring, high demand side management. Fig. 1 shows the blackout history, which shows the current status of energy management and monitoring status. Digital twin grid provides the status of the whole electric grid in real-time and intelligent decision-making capability that predicts the future of the grid and saves the power systems from tiny to large-scale accidents by both manual and automatic operation was taken by twin grid. This high level of cybersecurity paves the way for realizing decision-making constructed on a virtual mirror. The three-dimensional prototype is changed into a five-dimensional prototype by connecting it to the virtual archetypal, service, combination data, and PE. The information, automation, and interaction of the power generation, transmission, transformation, distribution, consumption, and dispatch processes give a promising new view for enhancing the power grid [12].

All the relative research on digital twins have proposed, designed, test on a small scaled platform are shown in Table 1. Digital twin presented concepts such as real-time online data analysis and data acquisition capability, automatic control, cloud-based platformed system, power grid dispatching, communicational system from the physical body to the digital twin, power grid optimization, high-demand side management, CPS, SCADA display of twin body, cybersecurity is tested using IoT, big data analysis, machine learning, deep learning, blockchain, PLC, MATLAB, artificial neural networks, various cybersecurity models, and a good number of data communication protocols. All these papers proposed the digital twin notion that can be implemented

Table 1
Relative research of digital twin electric grid.

Ref.	Methodology	Platform	Outcome	Challenge
[12]	New online analysis architecture	Power grid analysis and dispatching	Digitization, large-scale data analysis	Complexity in real-time data analysis
[13]	Power distribution and optimization using DT	Smart university campus power distribution	Cloud-based customer/producer communication, smart energy distribution	Further research needed
[14]	IoT-based DT architecture	Cyber replica of the physical body	Smart manufacturing, transportation	CPS and cybersecurity challenges
[15]	Cybersecurity DT	Electric power system on smart home	Low cost, attractive security for grid	Relative difference lies in physical test and DT
[16]	DER optimization using real-time DT	PV inverter technology	High reliable monitoring and optimization with security	Power distribution imbalance may occur
[11]	Architecture of digital twin in smart grid	35 kV substation of the electric grid	Intelligent power grid controlling and decision-making from the DT body	Large-scale data real-time analysis complexity
[17]	Digital twin energy cybersecurity validation	Amazon web services	Physical shadow controlling (high and low bandwidth), highly secured cyber platform	Low bandwidth has relatively more mean-square error than high bandwidth system
[18]	Power system DT ontological analysis	Hybrid renewables power system	Renewable power system emphasized with DT	Insufficient data analysis

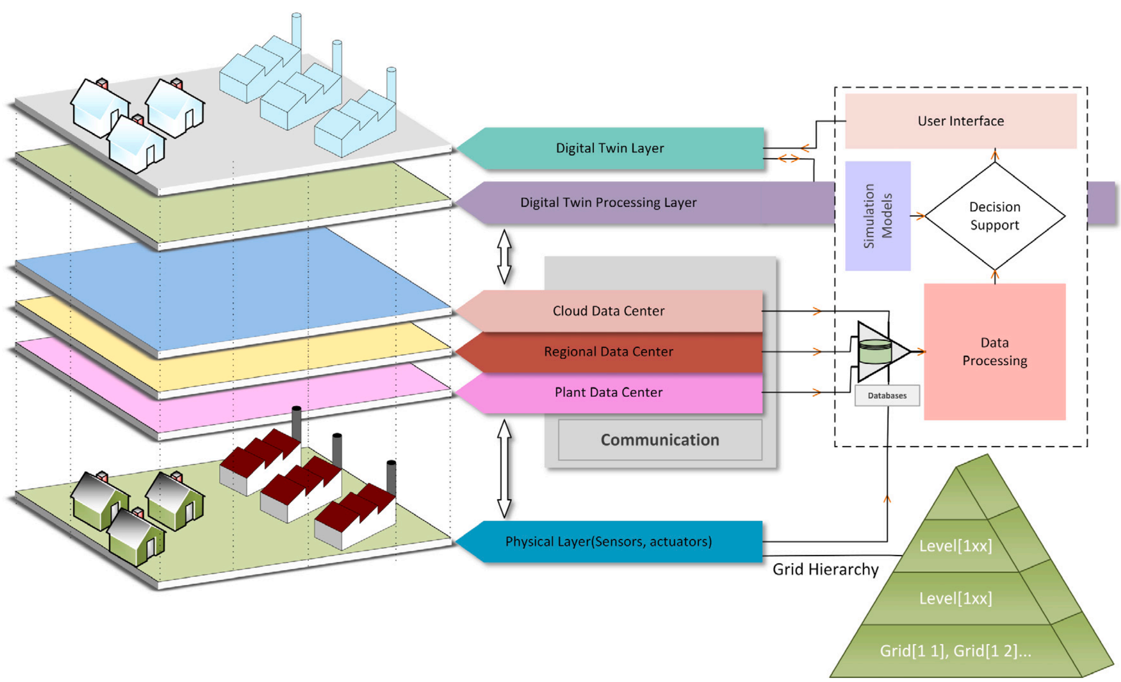


Fig. 2. The concept of the electric digital twin grid.

and solves the challenges by reducing the complexity of the current grid. The success rate of all the proposed concepts of the case studies is attractive by achieving high accuracy of 96–98 percent and a mean square error maximum of 3.2–3.7 percent.

The examination initially assesses the conventional grid, and the additional assessment demonstrates the requirement for a smarter power grid management system. The rationale for why the digital twin is going to be the right approach for future grid management. This paper conveys the electric grid transformation in the very first section and then Section 3 shows the electrical, computational, cybersecurity, optimization, management, and business challenges of the next-generation electric grid. Section 4, Why and how the Digital Twin concept has arisen and the conceptual framework of the electric digital twin grid, and the way serving the consumers, prosumers, and producers of energy. Finally, shortly mentioned some challenges of the DT electric grid and the road to the electric DT grid from currently operating grids. After taking an overview of this literature why and how digital twin is necessary for energy sectors are to be gathered.

Fig. 2 shows the concept of twining technology in electric grid management systems. The whole conceptual framework of the digital twin grid helps to visualize how the electric digital twin will be, the way of serving, optimizing, and managing the electric grid, the diversity of changes in the power system providing security of the grid, low transmission–distribution loss, low probability of power outages, smart demand side management, customer–prosumer–consumer in a cloud platform and very low restoring time if any outage occurred, high cybersecurity. This review shows the way to relief from the challenges of the power system at personal, business, economic, national, and international levels. It enters into the world of the dreamed smart distribution, optimization, and secured energy system via the digital twin grid. A comprehensive research comparison of recent works is shown in Table 1, the majority of which focused on one particular use of digital twin technology in electric grids. For instance, solely the DT framework was the focus of the study reported in [12,13]. Another work that was presented in [21] briefly discussed grid evolution and difficulties, but no framework or recommendations for future research were offered. In a similar vein, earlier publications indicated in Table 1

Table 2
Correlative works comparison.

Author (year)	Grid evolution	Challenges	DT opportunities	DT framework	Future research direction
(Zhou et al. 2019) [12]	✗	✗	✗	✓	✗
(Mourtzis et al. 2022) [13]	✗	✗	✗	✓	✗
(Qian et al. 2022) [14]	✗	✓	✓	✗	✓
(Kandasamy et al. 2022) [15]	✗	✗	✗	✓	✗
(Saad et al. 2020) [17]	✗	✓	✓	✓	✗
(Andryushkevich., 2019) [18]	✗	✗	✓	✓	✓
(Eckhart & Ekelhart, 2018) [21]	✗	✗	✗	✓	✗
(Wang et al. 2022) [22]	✓	✓	✓	✗	✗
(Zhang et al. 2022) [23]	✗	✗	✓	✓	✗
(Danilczyk et al. 2019) [24]	✗	✓	✓	✗	✗
(Atalay & Angin, 2020) [25]	✗	✓	✗	✓	✗
Current work	✓	✓	✓	✓	✓

also concentrated on individual qualities, however, the current work offers a circumstantial account of all the features described in Table 2. **The contribution of this paper is as follows:**

- This paper integrates the concepts of the digital twin in electric grid systems and defines a complete concept of the electric digital twin grid.
- The evolution of the electric grid from a traditional grid to an electric digital twin grid is thoroughly examined in this paper. Besides, it is also exhibited how each change in the electric grid leads to an increase in grid complexity.
- This work has demonstrated why and how the evaluation of the digital twin grid reduces the complexity and other challenges of next-generation electric grids.
- A conceptual framework of the digital twin grid is suggested and its components are pictured compactly. In addition, the framework layers are described briefly.
- This article provides a thorough road map for managing the next generation's energy internet taking recent research and technologies into account.

2. Electric grid framework and transformation

The electric grid is the network that provides electric power from power generation to the consumers enclosed a large area even in the whole country. The electric grid, the enormous network allows power generation from a diversity of resources and deals with a large number of prosumers and consumers even located far away providing electricity at the cheapest amount with anticipated and unanticipated losses [26] while meeting electricity demand. Electric grid transforms in various transformations Traditional Grid (TG), Smart Grid (SG), Microgrid (MG), Virtual Power Plant (VPP), and Internet of Energy (IoE). Fig. 3 displays a depiction of these transformations [27,28].

2.1. Traditional grid

The traditional electric grid constructs a network with a central power generation hub that interconnects transmission and distribution using the electromechanical infrastructure. The traditional grid provides electric power over a large-scale distribution area by centralized control one-way transmission–distribution line using electrically controlled and operated mechanical devices. The centralized energy infrastructure is one-way distribution equipped small amount of sensors which is difficult to control and so the power distribution and transmission monitoring are done manually and self-healing is not possible. The one-way centralized energy system has high power transmission and distribution loss and risk of grid overheating accidents. Due to manual monitoring, hardly pinpointed the fault which leads to transmission loss and frequent power outages and requires high restoring time, and creates economic harm and losses [29].

2.2. Microgrid

A microgrid, potentially expanding technology uses Distributed Energy Resources (DERs) and eliminates the challenges of the traditional electric grid. Distributed energy resources reduce the transmission and distribution of power loss and provide a highly efficient and secured energy system at a lower cost. DER introduces a renewable energy electric grid that eliminates the contribution of coal and natural gases and confirms a large clean energy resource (solar, wind turbine, wave) [30]. DER eliminates the challenges of the traditional centralized grid and converts the grid infrastructure into more complex also management and operational systems. A microgrid is a controlled entity of a grid that promises to eliminate the complexity of DER and provides potential, organized grid expansion in addition to improvision of quality, security, and efficiency of the grid [31]. Microgrid integrates a number of distributed power grids in a systematic way to reduce the complexity and controls optimally approaching PCC (Point of Common Coupling) that ensures a reliable power system [32–34].

An isolated or linked to the grid localized set of energy sources and loads is known as a microgrid. It is an advanced feature in that the microgrid has a dual mode that is connect-with-grid and another is an island. A "standalone microgrid" or "isolated microgrid" is one that runs entirely independently of the grid and is not able to be linked to a larger electrical power network [35]. A microgrid is capable of managing the transition between grid-connected and independent modes. In the grid-connected mode, microgrid-to-grid trade can be used to supply ancillary services. Microgrid provides standard power service to the consumers connecting or disconnecting using the PCC network to the main grid at the time of power deterioration and network contingencies [36]. It continually monitors small-scale power generators, the accompanying load, power storage elements, sensors-measurement unit, and control unit, and forms a single, controllable entity in relation to the power grid system. It introduces a number of DERs that work in two different ways. The grid-connected mode is the first one, and the second is the autonomous or islanded mode, which likewise continues to be an intermediate or transitional condition between these two modes [37]. It constructs small-scale or located area which possesses AC or DC even hybrid (AC and DC) distributed or remote providing necessary protection utilities. It presents both "plug and play" and "peer–peer" functionality to the distributed grid system. Although renewable distributed generation (DG), supply, and net measuring are supported, not entirely MG can make use of them. It is discouraged from implementing microgrids that use non-renewable, renewables, or a combination of renewable DG knowledge. In a normal energy distribution system, when one-way flow of current, protective devices such as reclosers, circuit breakers, fuses, and relays maintain fault isolation, with overcurrent relays usually fulfilling the earlier role. In dual mode operation of the microgrid, DG plants in a microgrid must be safeguarded when a leakage current varies substantially for switching modes [32,38].

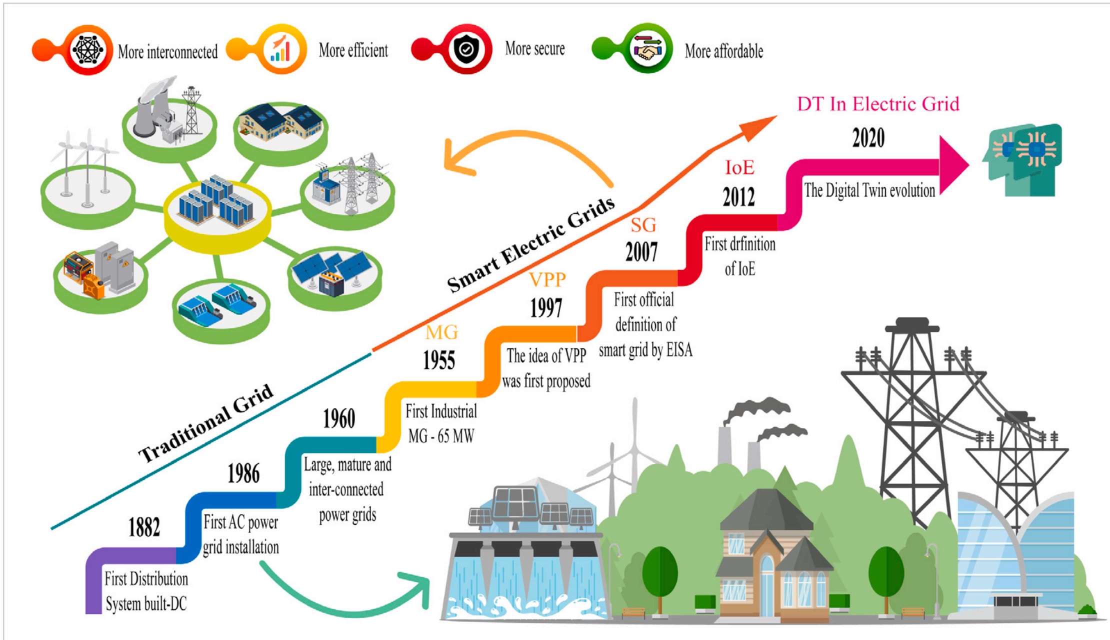


Fig. 3. Evolution of electric grids.

2.3. Smart grid

The smart grid has the capacity to communicate, store information, and analysis based decision-making capability. The smart grid transforms all the previously evaluated grids into one that operates more rapidly, intuitively, and collectively. This energy network successfully combines the behaviors of all attached people of this platform, including producers, consumers, and those who use twos, to deliver reliable, economical, and reliable power supplies [39,40]. The historical design of the grid, which may be described as supplying end users with centralized electricity generated and a conventional one-way high transmission loss system, is evolved into a more discrete, dynamic system that is defined by a two-way flow of information and power (both centralized and distributed). In Fig. 4, future smart grid concepts are presented.

Communications and information technology (IT) are crucial for the functioning of the smart grid [41]. Eventually, as part of the smart grid, a large number of sensors in both transmission–distribution infrastructure, remote monitoring, control devices including SCADA, lumbar systems, and domestic appliances that interact with the grid will be networked. Meters, sensors, and synchrophasors will produce a lot of data [42,43]. It will be essential to articulate systems for handling, investigating, and interim on this data. Intelligent electricity is produced by smart grids, which employ cutting-edge ICTs that are designed to bring benefits in a number of areas, including developing economies, renewables, the environment, efficiency, dependability, sanctuary, and protection. To advance the power system and analysis the whole system in real-time, deliberate to shorten principal times, the control hubs, and energy supply structures, are thought to interrelate and remotely monitor the power-driven campaigns [44]. They also use cutting-edge technologies and services to do this. The smart grid systems have the capacity to gather data, interconnect with processors to analyze the system, and advise the operator on the necessary actions based on it. The smart grid's capacity for self-awareness, self-optimization, and self-customization will allow various power grid components to function autonomously or with a smaller amount of humanoid controls to produce superior electricity [45]. An extremely adaptable electricity generating a model that will significantly increase energy competence and keenness in the electrical energy sectors will be built through this instantaneous communication amid schemes, employees, and customers. Smart Grids have certain drawbacks in addition to their many advantages. The price of converting conventional grids to smart grids is high and would severely affect the cost of industrial expenses [46]. Cybersecurity problems are more likely when a smart grid uses the internet for real-time information exchange [43]. From a different angle, using unlicensed software might result in data theft and criminal computer system attacks.

2.4. Virtual power plant (VPP)

A cloud-based energy plant called a virtual power plant integrates several forms of power resources [47]. Effective power delivery also involves the power distribution system. Eventually, VPPs will work on distributed energy resources (DERs) to improve the steadiness and intelligence of smart grids. The software system is what Virtual Power Plants rely on to automatically and remotely control, integrate, dispatch, and store the electricity. The substitute for integrating distributed energy resources is VPPs [48,49]. Each agent for a distributed energy resource uses VPP to combine, communicate, and behave like a neural network in a way like the Internet of Things. Utilizing VPPs makes difficult grid data processing simple and speeds up market price release [50]. Among the ideas of MG, SG, and VPPs, VPP is the one that is closest to DT.

By selling extra energy at an extreme charge and purchasing electric power deficiencies at an economical charge from the producers, VPP hopes to maximize its conveniences. Demand-side flexibility, or consumers' capacity to reduce demand during crowning periods and swing to off-crowing periods, is related to the production of excess profits from VPPs. In isolated wind generators in VPPs, they are utilized to reduce power production fluctuations that occur quickly and cause voltage and frequency ripples. ESSs that control the appropriate voltage level in the systems are used to manage the sensitive power drift in electric systems. Additionally, ESSs offer time shifting and well-suited time frames for transmission lines and other installations, stabilizing electrical networks. Large evidence transparency, scheme information security, and instantaneous demand-side data are built via blockchain-enabled VPPs [51]. Therefore, it is suitable for VPPs [47,52]. Although there are many issues with scalability, speed, and high regulatory costs that need to be resolved before blockchain technology can be

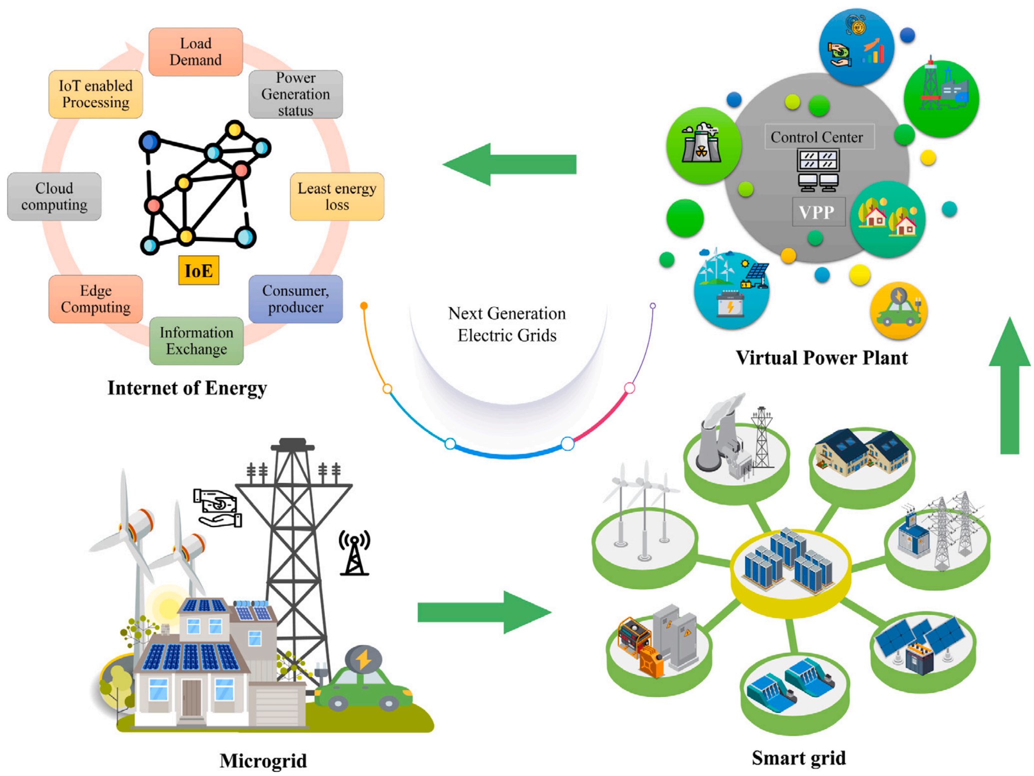


Fig. 4. Next generation electric grids.

implemented. They function as adaptable consumers that can be managed by certain software, and when all DERs and loads are combined, cloud computing becomes a crucial component of running VPPs. A significant obstacle to communication amongst DER units is universal acceptance. There can be just one standard used, and a set of guidelines must be developed. One standard for all data communication could be a smart way to encourage widespread adoption. VPP's operation presents numerous difficulties. A production unit will respond in a different way depending on the choice made by the owner or the VPP operator [53,54]. The system needs to be secured from external threats and have a service contract breakdown protocol. Safety requirements and web services criteria must be established. The DER portion contacts "Match Maker" to learn more about the novel affiliation by some other VPP if the assembly between it and the VPP operators is severed [55].

3. Next generation electric grid: Challenges and opportunities

3.1. Electrical point of view

3.1.1. Control challenges

There are three types of MG controls primarily: local controls, central controls, and dispersed controls [56]. For MG, Huge divergences amid production and loads are anticipated to result from switching from grid-connected mode and islanded modes of process, which will lead to momentous regularity and power management matters. Whether the controller is centralized or decentralized, the needed control deed with potentially lost model strictures will undoubtedly remain difficult. Additionally, there are secondary control techniques that assist main control, which then results in secondary control difficulties [57,58].

3.1.2. Grid integration

The use of transmission systems to transmit energy from far sites of origin, such as wind plants in countryside zones, to the sites of highest claim, such as metropolitan hubs, would be a problem with the combination of renewables and clean energy to the grid [59]. The complexity of the grid is further increased by the ongoing need for energy, which leads to the addition of new SGs and MGs to the parent grid. Smarter energy Big data has a great deal to do with natural laws, and advanced analytics might have a big impact on how safely system integration can be run in real-time [60]. Besides, the security mechanisms and the big data analytics for smart energy are currently built independently, which deteriorates the safety of the grid integration procedure. Again, there are additional challenges involved in taking part renewables and clean energy into the main grid. These challenges include the volatility, unpredictable nature, and reliance on the weather of renewables [61]. Consequently, of the abrupt and frequent instabilities in these resources' power production, managing the grid's electricity supply has become increasingly difficult. Also, a growing number of renewable energy sources might clog energy distribution networks [62]. Fig. 5 presents the issues with the next-generation electric grid in a single frame.

3.1.3. Reliability

Limitations in current control theories, failure to take into account the presence of a physical system, limits in standard SG cybersecurity models, and vulnerability evaluation limitations exacerbate reliability issues primarily [63]. In an IoE infrastructure, massive volumes of data are independently collected by smart meters and sent to utility companies, consumers, and service providers. Secluded purchaser data that may be accustomed to assuming a purchaser's actions [64]. Again, the size of the smart grid network makes network administration and monitoring increasingly challenging. To deal with the influence of renewable energy on fault currents, new protective devices and protection mechanisms must be created to rise the dependability of smart grids. Smart grid safety greatly depends on smart sensors' capacity to gather, analyze, and interpret quantitative measurements as well as to run optimization algorithms in their MPU. The dependability of the smart grid is increased by including more smart sensors, smart

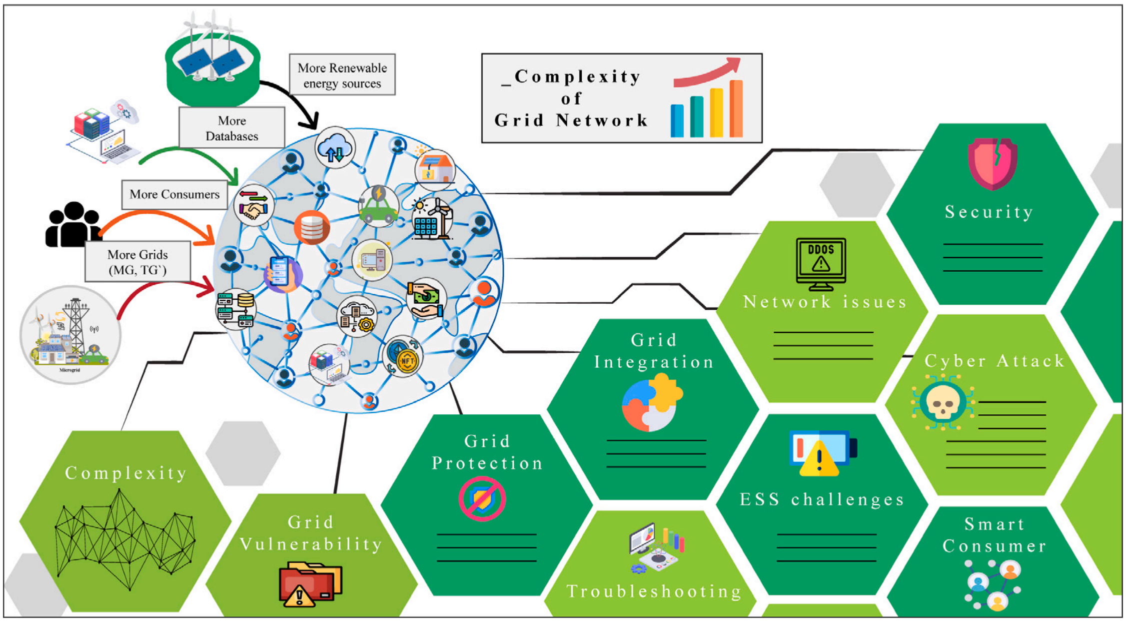


Fig. 5. Next generation electric grid challenges.

devices, and grid integrations since they shorten the time it takes for network breakers to activate [65]. Inconsistencies in power generation and consumption, internal component failures like insulation flaws, external reasons like broken cables, and vandalism incidents all have an impact on the grid and ultimately lead to reliability problems [66].

3.2. Communication point of view

3.2.1. Vulnerability

A big utility will have a lot of sub-distribution systems, each with its own hardware that has to be monitored and maintained. This number might rise to millions of devices with the implementation of sophisticated metering infrastructures. The primary grid must be expanded to accommodate future requirements, significantly escalating both the complexity and scale. Grid vulnerability is increased by complexity increment [57]. Several elements [67] need to be taken into consideration when determining whether an MG is feasible to operate. In the study, [68] many grid vulnerabilities are discussed, including those related to customer security, physical security, the lifespan of physical systems, IPs, grid integration, and many more.

3.2.2. Network and communication vulnerabilities

An SG or MG infrastructure's vulnerability is directly influenced by the communication protocols used, the vulnerability footprints of many communication protocols (IEC 61850, IEC 61850) are covered in [68] this study. Several security weaknesses are present in types of wireless network protocols and the corresponding protocol solutions used in Internet of Things communications, such as IEEE 802.11.x and IEEE 802.15.4x [69]. IoT has an influence on the IoE infrastructure when network segmentation is not used for a centralized control strategy, which further encourages grid failure and introduces latency in decision execution. Utilizing IP standards in smart grids has several benefits since it ensures compatibility across all of the parts. Though numerous IP-based attacks, including IP spoofing, bogus routing, teardrop, network, and others may be launched against IP-using devices

3.2.3. Grid communication

A noteworthy challenge for a dependable MG operation is the need for quick and precise computational devices and communication systems [70]. Grid network complexity results in communication issues such as low bandwidth failed bidirectional communications and delayed data updates. Besides, the hostile environs of the smart grid, such as the barriers and high-voltage electrical equipment, are causing serious interference problems for wireless communication [45]. Due to the growing number of services shared by the consumer market, the data exchange capability of cellular networks in emergency situations is declining quickly. In cellular networks, the range may be expanded in addition to the inter-cell interference by boosting the transmission strength, but the high data transfer speeds for SG applications stay the same.

3.2.4. Artificial intelligence

While the decentralized public log of blockchain may help to increase reliability, AI-enabled smart contracts may offer special benefits in the prompt reaction to new cyberthreats, such as a rapid response to a naturally occurring climate disaster or a cyber–physical fusion occurrence. Some power grid operations would become robust and automatic management as a result. A near instantaneous and simultaneous refuge retort to unauthorized efforts to modify formations or web and sensor sceneries might also be accomplished by combining AI with blockchain [71]

3.3. Security

A system of sensors, displays, campaigns, processes for data collecting and processing, and other components make up an SG, MG, and IoE and are all vulnerable to cyberattacks. Worms and viruses may spread swiftly because of the vast size and interconnection of the whole network, which is the main problem. Additionally, there are a ton of weak targets due to the network's spread design. For SG's cyber–physical system security solutions, the currently available cybersecurity is insufficient or ineffective. So, in order to uphold data security, domain-specific processes and solutions are needed [72]. In the framework of the SG, this [73] research has presented and explored data on security challenges. Additionally, numerous refuge protocols in the smart grid have been addressed collaboratively. These include significant administration, protected conveyance protocol, user and device verification, access and manipulator customer admittance control, etc.

3.3.1. Cyberattacks

Electric grid outages caused by targeted cyberattacks or unintentional repercussions of network abnormalities have been observed on a number of occasions [74]. Attacks on the grid might have a variety of motivations, such as cybercrime, hacking, cyberespionage, privacy theft, manipulating smart meters, and cyberwarfare [75].

The Davis-Besse nuclear power station in Oak Harbor, Ohio, had a computer network attacked by the Slammer worm assault in 2003. Due to high network traffic on the control system, the Brown Ferry nuclear power facility in Alabama collapsed in 2006. An event in 2009 showed that hackers might steal electricity by contravention of keen measurements and altering the measurement of power use. Additionally, phishing instances and virus illustrations that suggested a focused and classy attack were found at an electric bulk provider [75]. The control system of the Bushehr nuclear power plant was directly hacked by malware during the 2011 Stuxnet assault, leaving a destructed grid infrastructure [76]. It is a prime example of a cyber weapon that was the most lethal. The trojan Black Energy was found in the computer networks after the Ukrainian blackout [77,78] and is thought to have played a significant part in the incident, Havex is another known virus that has been created to target industrial control systems [79]. Dealing with these worm and malware attacks becomes more sophisticated as the grid complexity is rising with exponential demand. The enormous forthcoming security dangers will require a next-generation power infrastructure to manage them. It goes without saying that role-based access control (RBAC) can improve system dependability and get rid of any security risks [80]. But existing RBAC schemes do not satisfy the needs of safe operations across several domains since they are created for a single security domain, such as a regional network [81].

3.3.2. Physical network security

The physical network of an electric grid composed of numerous elements including actuators, sensors, controllers, data acquisition systems, and more sends data to the digital twin framework. These devices transport data from the physical layer to its twin layer using several network protocols. The network looses synchronization with its twin entity when terminals do not receive the desired data or signal. When such a phenomenon occurs, a threat is immediately declared according to its self-healing connective measures and the digital twin layer generates alerts [82]. Electric grid self-healing is a smart strategy for grid network troubleshooting in real time. The twin layer communicates with physical devices to make the self-healing process highly efficient as shown in Fig. 6. Data acquisition systems and other controllers collect field sensor data and actuator states in real time. When an intrusion is identified, the twin layer responds immediately and raises the troubleshooting priority value. The system recovery process is launched with the aid of fault-handling algorithms. To forecast grid performance and avert malfunctions, the log file serves as a database. In order to improve the speed of operation, the scope of application and overall effectiveness, several ML algorithms may be adopted [83–88]. The work presented in [89] makes recommendations and offers the test findings of a self-healing grid network's quick recovery scenario. Besides, a security evaluation method for digital environments is proposed in [90] concentrates specifically on the physical layer of security. Due to the real-time interconnectivity, each decision made by the twin grid flows into the physical layer with the help of incident response strategies [91].

3.3.3. Blockchain

The electrical network and an ICT infrastructure both facilitate the bidirectional flow of electricity via the future electric energy system, which is made up of a sizable network of associated parts. DERs, ESS, and dispatchable loads are significant players in such a smart grid system [92]. Blockchain might commoditize trust and perhaps facilitate inspectable miscellaneous dealings amid energy prosumers and consumers in the direction of a cyber-resilient energy system [93]. Blockchain might commoditize trust and perhaps facilitate inspectable miscellaneous dealings amid energy prosumers and consumers in the direction of a cyber-resilient energy system.

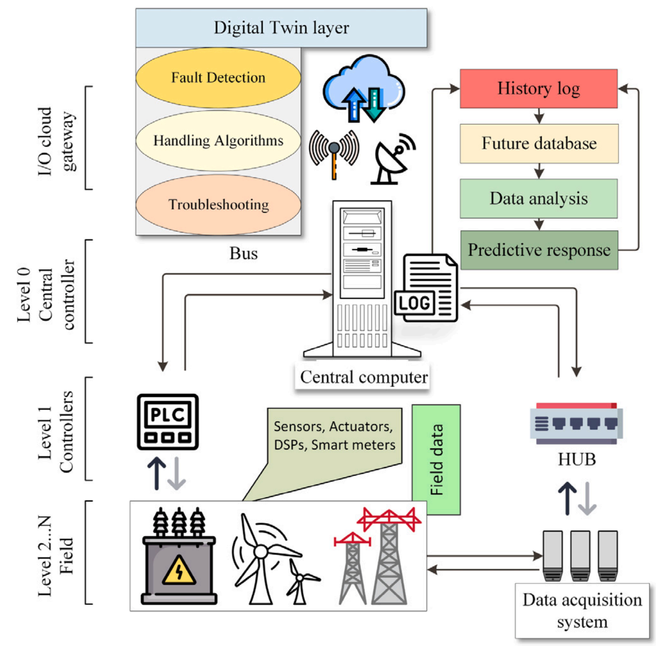


Fig. 6. Illustration of the self-healing process.

3.4. Optimization and management point of view

3.4.1. Grid protection

Unidirectional fault current flow has been used in traditional power system design and construction for radial distribution networks. However, the addition of DGs to the primary grid via microgrids causes a bidirectional shift in the direction of fault current flow [94]. Distributed generator integration, current fault level variations, sudden relay trips, relay miscoordination or decreased location, and unintentional interruptions are issues affecting MG operation [95].

3.4.2. Troubleshooting

Remote troubleshooting with computerized trials offers additional challenges such as synchronization, delay, intrinsic design security flaws, and so forth. There is generally no real bridge solution that can overcome the challenges using a unified, complete, and flexible architecture [96]. In order to confront these constraints modern machine learning algorithms are being developed for intrusion detection to impend remote analysis of multi-sensor, processor-based dynamic structures like a composite IoE containing enormous intelligent electronic devices (IEDs). For example, the work presented in [97] traditional ML algorithms have been assessed, while [98] proposed and evaluated a data fusion framework for anomaly detection. Such an advanced framework is expected to add up potential threats to protection and anticipatory warnings in the digital twin electric grid. Newer models with additional features may also be required to examine subsequent usages [83–88].

3.4.3. ESS (energy storage system) challenges

A review of the energy storage systems [99] shows different kinds of energy storage devices used as energy storage elements of MGs. Typically energy storage devices are supercapacitors (SC), superconducting magnetic energy storage (SMES), flywheel energy storage systems (FESS), batteries, hybrid ESS, thermal energy storage (TES), EESS, HFO, CES, Li-ion storage systems, etc. The need for safety and life cycle tracking as a complex network [100] is the ultimate concern. This [94] study's security analysis demonstrates the importance of ESS security solutions as the prime factor of MG's energy contribution to the parent grid.

3.5. Business point of view

3.5.1. Consumer interaction issues

The intelligent regulation of the power distribution system with the combination of energy consumer contact and feedback is one of the goals goalmouths of future power grids. Here customers will be in charge of setting their own energy use goals [101]. The future smart grid's customers are end users who actively participate in the challenge of balancing supply and demand. Each customer will choose which system support choices and services are best for their requirements. The connection between power distribution firms and consumers altered such that "power" became a marketable product for which customers will be allowed to choose the quantity and quality of the provided power. This transformation was especially a result of the liberalization of the energy market [102]. A paper [103] describes the smart customer requirements and future energy internet demands. The next-generation electric grid will need to manage the connectivity of billions of IoT devices and provide elevated critical communication for a prompt response. The bandwidth solution for this high-speed communication is described in [104] but the AMI expands the security flaws for potential SG interference, which might result in power failures or financial losses for the provider and the customer. This makes the SG more vulnerable to cyber assaults. Future energy trading will require regulations and procedures to address various assaults including DDoS, DoS, surveillance, and hijacking while allowing prosumers the freedom they need [105].

There are essentially two modes of operation when discussing digital twins: simulation or testing mode and operating mode. The digital twin is capable of making decisions based on algorithms or previous experiences. The security and other grid-related concerns are taken care of by this operation mode [21]. The twin layer produces alerts for urgent circumstances and occasionally performs interception of the troubled regions. Many security and optimization tests can be run in simulation mode and the tested strategies can be used to improve the welfare of the grid. By testing new algorithms in the simulation mode and putting them to use in operational mode, network handling performance is constantly boosted, as is the performance of the entire system. This guarantees cutting-edge technology, along with modern security infrastructures and optimization algorithms, to manage the entire system in real-time [106]. Hence, the conventional operating cost and time consumption are greatly reduced when the simulation and modeling procedures are carried out in a digital environment [15,22]. The digital twin grid system offers a cloud platform with many categories, including system administrators, suppliers, and customers [13]. By publishing the SCADA system, the supplier group and the system administrator group may input all parameter values onto the platform that updates in real-time which is 14 times greater than the present SCADA system. The DT grid's RTU measuring power can reflect the actual electrical grid while also monitoring changes to the grid in real-time [23]. The customer has received a profile broken down by sub-group, including commercial, residential, office, emergency connection, hospital, roadways, etc. Consumers can access the administrator-shared current status and repair actions of a grid using this profile [19,107]. The DT grid is monitored by a variety of sensors that are divided into several modules, each of which includes a high-memory device and data collection devices to address the problem of data mobility through machine learning big data analysis, and parallel computing. The virtual body of the DT grid gives all of the grid's status updates in real-time, incorporates all of the previous data, and forecasts the grid's future. The administrator may quickly optimize since the DT grid indicates which parameters need to be updated or which place needs to be repaired. The DT grid, which can identify when an item or parameter has exceeded the safety level, takes the appropriate action, such as performing a disconnection operation or self-healing operation.

4. Digital twin and electric grid: Conceptual framework and assessment

4.0.1. Digital twin

In spite of being widely believed to have been created in 2002, digital twin technology has really been a notion used since 1960. Then, NASA would service fundamental digital twin perceptions for space-purpose-related projects. After launch, oxygen tanks on the Apollo 13 mission in 1970 burst. The near 200,000-mile-distance technological issues were quite challenging to resolve. A digital twin of Apollo 13 was created by NASA and placed on earth, allowing engineers to test potential solutions from below. This can therefore be referred to as the first digital twin [108,109]. Despite the intense attention from business professionals, digital twins are not a novel concept. Its inspiration originated from "Mirror Worlds" by David Gelernter, published in 1991, "Product Lifecycle Management (PLM)" by Michael Grieves, published in 2002 at the University of Michigan, "Information Mirroring Model" published in 2006 which was changed from 'Mirrored Spaces Model' proposed by Michael Grieves, and finally mentioning the concept as "Digital Twin" in 2010 by NASA [110,111].

"Mirror Worlds" was conceived by David Gelernter in 1991 and uses software replicas to invent realism by means of data input from the real world [110]. Michael Grieves' "Mirrored Spaces Model" contains three portions. They are: actual space, virtual space, and a connecting mechanism for data or information transfer between the real and virtual world [112]. Fig. 7 illustrates the development of digital twin technology throughout time.

DT has developed as a technological flashpoint and has evolved quickly at both the hypothetical and applied stages hence the fast advance of modern novel technology, electric technology, and IT, particularly virtual simulation and information gathering [11]. A path has been followed by the electric grid to come to the digital twin technology. The route crosses smart grids, microgrids, and VPPs (Virtual power plants) in between.

A complex digital twin energy system provides real-time simulation of the grid state and performance of the grid by the smart energy management system. Digital Twin virtual body is presented with smart measuring and collection of data for smart electric grid management to reach the goal of standard energy efficiency along with safe management of the whole system.

4.1. Online analysis framework (OADT)

In 2016, "State of Grid, China" introduced an online analysis development project with real-time data analysis [12]. For Online Analysis Digital Twin (OADT), the data acquisition process starts with a state estimation of the electric grid. The state estimation functions are updated with the current status of the electric grid and the SCADA process is run by a loop periodically and updated continuously in real-time with fast DSA. The SCADA process runs dynamically and monitors the fluctuation of each data and analysis the data in real-time and describes the status of the electric grid. [11]. A 40 K-bus online network model is used to simulate China's State Grid Cooperation [12]. The D5000 EMS system in China employs this online analysis system. It operates using a relational data structure-based data processing pattern and a distributed active/passive data storage pattern. An in-memory database that supports SCADA and SE is used behind the scenes. A fast D5000 data bus is used to input the remote terminal unit (RTU) measurement data into the database. The term "periodic online analysis" refers to the current DSA analysis programs, which are periodically executed at 15-minute intervals. This method is proposed by Mike Zhou [23] (see Fig. 8).

The current online analysis method is immensely slow therefore a new online analysis framework is proposed in [113] which accelerates the procedure to produce a reaction time in the range of seconds. A novel real-time, incident-driven data dispensation and calculation

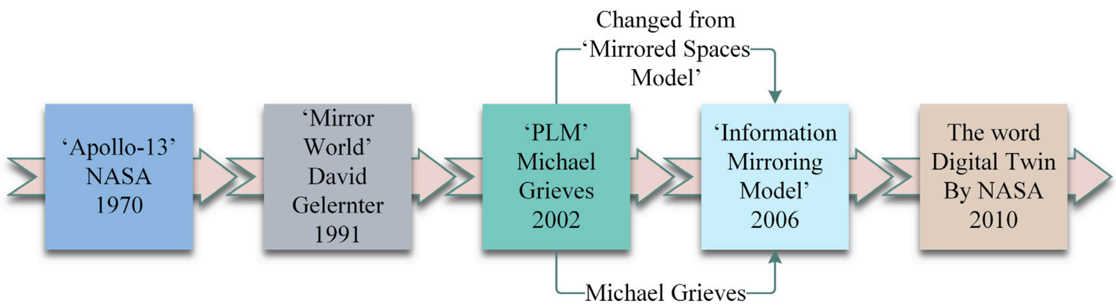


Fig. 7. Transformation of digital twin technology.

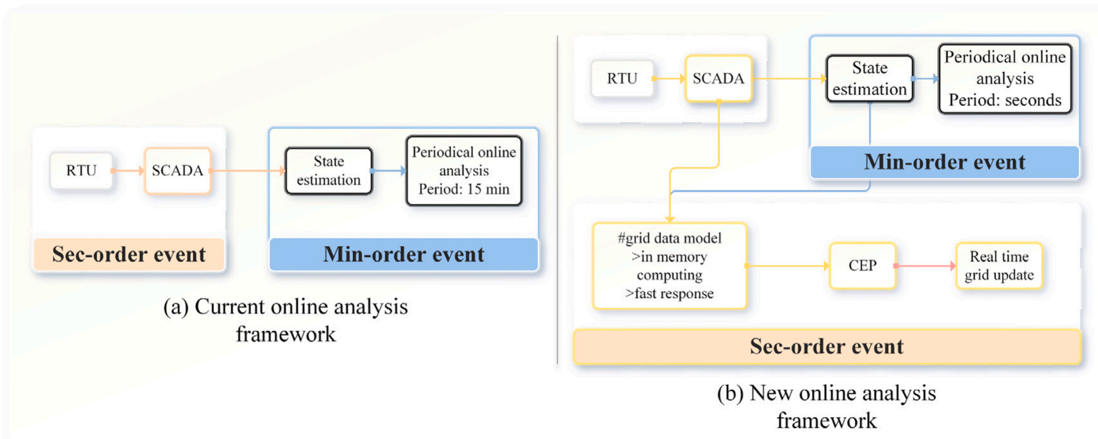


Fig. 8. Comparison between current and new online analysis framework.

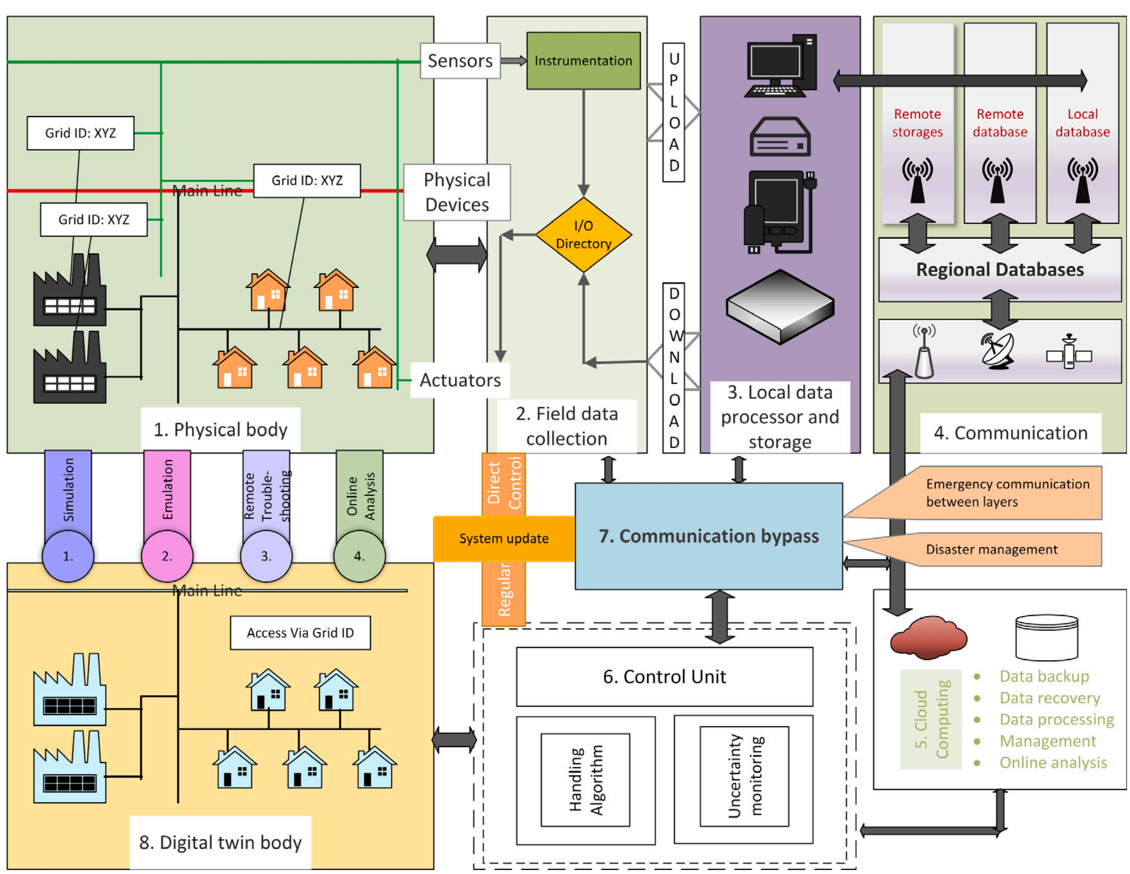


Fig. 9. The conceptual framework of electric digital twin grid.

track is announced in the architecture in addition to the present online analysis data processing and computing road. The new method is based on the master/slave digital storage template as well as the in-memory artificial intelligence pattern. In memory computing speeds up the computation process and generates a reaction within seconds [114].

4.2. Cloud platform of electric digital twin grid

A Cloud platform is needed in the electric digital twin grid to realize and monitor the energy status of the electric grid and also manage the demand side of power and energy consumers. The monitoring panel can show the energy status in real-time which can also provide energy supply status to each consumer [13,115]. As the cloud platform can provide the status of each consumer supply and also the whole electric grid status to the management unit in real-time analysis, the electric digital twin grid can handle both energy production and demand side management and can be escaped from undesirable problems. The consumer side of the platform can be categorized into domestic, industrial, office, educational institute, roads and highways, and other emergency connections and thus consumers can get extra benefits and high-quality energy service [116]. The management unit of the grid can be analysis the whole grid status and demand side status and analysis of all the updated statuses from the digital twin grid and apply effective decisions to avoid any type of mismanagement and unpredictable occurrences of the electric grid [115].

4.3. Communication of electric digital twin grid

The communication system of the electric digital twin grid is shown in Fig. 9, inter-connection each unit of the digital twin in a continuous process to ensure real-time analysis of the status and performance of the electric grid. Each of the sensors and other measuring and data collection devices is connected to a central data acquisition board [115]. All these sensing nodes are interconnected with wired/wireless connections using different communication topologies. The communication network management system collects and gathers all these data in a perfect formation and serves as the cloud platform of the digital twin grid [15]. The communication framework works as a central data acquisition board or SCADA workstation. As it is a SCADA workstation, it controls the whole digital twin body by providing a sorted collection of data in real time on the status of the grid. All sorted or gathered data are sent to the analyzing and decision-making and future prediction body digital twin grid, and all the sequence of collected and updated data are continuously sent to PLC and the controlling unit of the grid. The data processing in real-time of the digital twin electric grid goes through some data transferring protocol in each data bus of the digital twin grid for the security of data. The widely used large-scale data communication protocols are MQTT, MMS (IEC61850), GOOSE protocol, and OPC protocol [14]. Fig. 9 provides a thorough explanation of the conversion procedure from the physical grid to the digital twin grid including all the layers in between the physical and digital twin grid.

- **MQTT:** It is used in the Digital Twin data bus where a centralized data acquisition system is used such as a host in the cloud platform.
- **OPC protocol:** It is used in large-scale data transferring from the measuring node of the physical grid to SCADA of the electric Digital Twin grid.
- **MMS (IEC61850):** It is used to transfer data in real-time to the controlling end from the physical body measuring node or SCADA workstation to the controlling unit of the grid. It can transfer real-time data perfectly to multiple endpoints at a time in Digital Twin communication.
- **GOOSE Protocol:** MMS IEC61850 can transfer data from measuring nodes of the electric grid to the controlling unit through the SCADA workstation within 4 s. But GOOSE protocol can transfer data from the physical body to SCADA with high security in high critical communication and large-scale data processing in the Digital Twin grid [117,118].

Table 3 displays several features of various data transfer and communication methods. Given that DT requires highly fast communication to carry out real-time activities, it specifies the twining potential with regard to data transfer speed. Based on the model's adherence to security protocols, security measures are assigned. These [119–129] papers provide corresponding data of the protocols listed.

4.4. Automatic network guardian for electrical (ANGEL) system

The historical SCADA system has been used by power grid control centers for a long time to safeguard and manage the power grid. The new Smart Grid will serve as the cornerstone for the development of keen metropolises might profit from a more advanced refuge and control system. The ANGEL system has the capacity to continuously track the electricity system and offer information on the dynamics of the grid [24,130]. This [24] framework was proposed for microgrid security which can be used for digital twin grids as well. The ANGEL digital twin offers helpful feedback from the physical body which enables the possibility of precise control. The physics-based pattern, the digital twin's data analysis, DL, consumer–producer interference, and analytical package all leverage data from the physical network for the grid and microgrid communications. These are the processing and interaction elements of the ANGEL DT framework. In this approach a wide-area power distribution or transmission system's defects might be found and fixed using machine learning algorithms, enabling system monitoring to be done continuously and prevention of further system damage [131] (see Fig. 10).

4.5. Application framework of digital twin grid

An application framework of DT technology is proposed in [132] which primarily focuses on product lifecycle management (PLM). Physical space, virtual–digital interplanetary, and a film of data processing make up this structure. IoT is a rummage sale to move data from the physical grid to the information processing layer, which incorporates components for data processing and storage. Through two-way communication between the data processing and virtual layer, virtual space builds a model based on the physical layer that can interact with the physical one.

A DT architecture for Cloud-based Cyber–Physical Systems (C2PS) has been introduced in [133] which is supported by a cyber–Physical IoT architecture proposed in [134]. The described system makes use of data as updates or as a resource to other systems. The method assumed that every physical item in C2PS comes with a cloud-hosted digital twin that serves as a representation of it. Every twin cyber–physical object is directly connected to another object in a one-to-one relationship. Another CPS architecture is proposed in [135]. In this method, to synchronize the lively behavior of the corresponding corporeal apparatus and their real-time status data, virtual campaigns are created utilizing digital twin technology.

A study in [136] suggests a digital twin paradigm that integrates Building Information Modelling (BIM) and data mining. This is essentially a cutting-edge project management system that processes large amounts of physical twin data using data mining and a BIM methodology. The DT body is able to perform simulation, system diagnostics, and future prediction in real-time. Buildings Information Modeling (BIM), instead of being a straightforward virtual model or piece of software, is a method for quickly digitalizing the construction, engineering, architecture, and Operation industry by creating simulations with conceptually rich data in a common data environment (CDE) [137].

Table 3
Digital twin data transmission and communication protocols.

Protocol	Basement of protocol	Digital representation	Twining possibility	Transmission	Security measures
DTDL	Data representation	✓	✓	✓	✗
FIRMWARE	Data representation	✓	✓	✓	✗
OPC UA	Data representation	✓	✓	✓	✓
FDTF	Data representation	✓	✓	✓	✓
CoAP	Communication	✗	✓	✓	✓
MQTT	Communication	✗	✗	✓	✓
TCP/Ip	Communication	✗	✗	✓	✓
URLLC	Communication	✗	✓	✓	✓

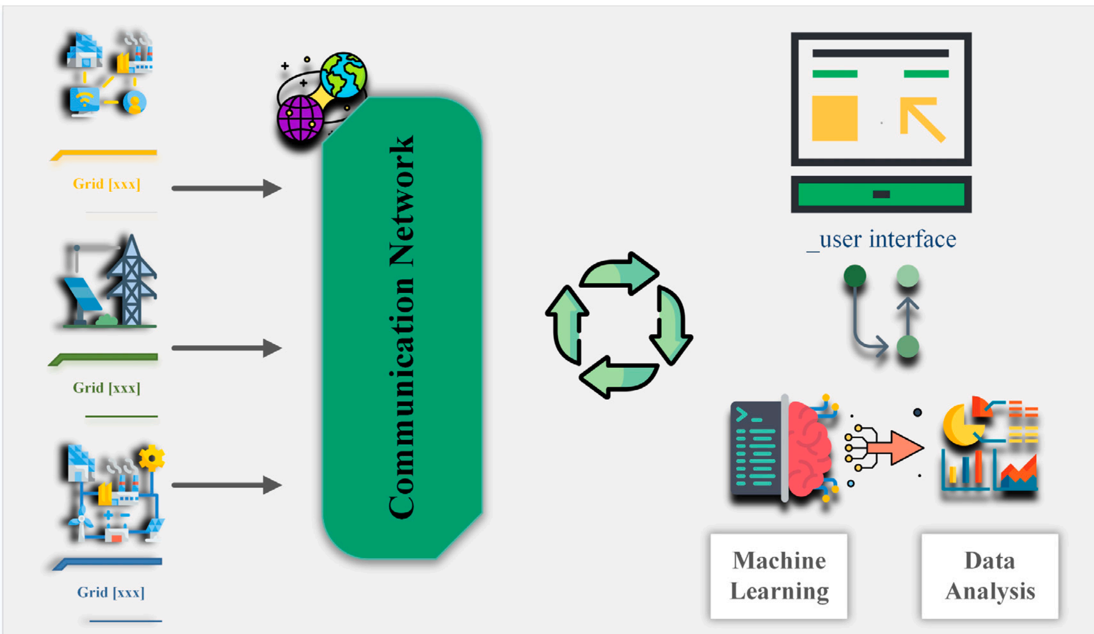


Fig. 10. ANGEL digital twin framework.

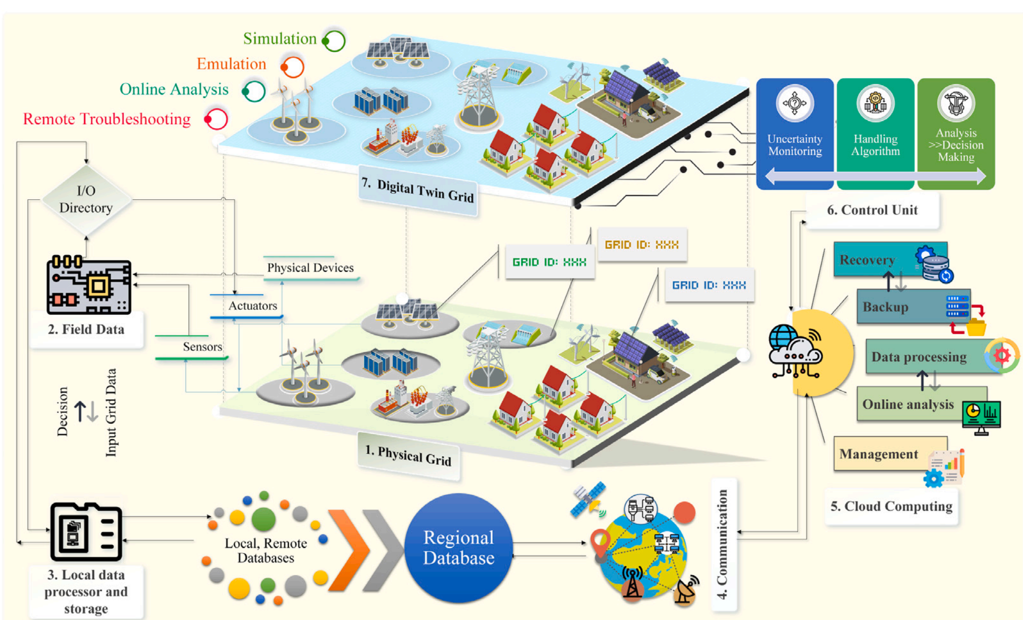


Fig. 11. The way of processing of electric digital twin grid.

4.6. Security framework

There have been some direct cyberattacks in recent years. The most notable examples of smart power systems are between 2005 and 2010, the Stuxnet malware [138], and the Ukrainian 2015 electrical grid assault [79]. When we discuss an electric grid's physical twin, we assume that it will be made up of a variety of microgrids, smart grids, power plants, and other components. These vital infrastructures must offer very high standards of dependability, accessibility, and privacy. Research in [25] suggests a DT approach for the security of this critical infrastructure of heterogeneous nature. With this method, a system is separated into its physical, virtual, and decision-making tiers. These layers will require a private cloud hub and a decision-making control center that can command PLCs and IoT gateways using the physical tier's bi-directional communication protocol. Fig. 11 depicts the layers between the physical and digital twin grids in three dimensions. The main difficulties in putting digital twin technology into practice are managing the cloud platform, data storage platforms, and data transit platforms depicted in Fig. 11.

4.7. Digital twin grid challenges

In addition to increasing CPS's potential to function more smartly, DT integration can help CPS deliver additional treasured services to customers. Remember that since DT is a digital representation of actual objects, it must be able to represent a range of objects quickly, accurately, and effectively. The networking, computation, control, and data analysis of IoT face several obstacles as a result of the reality of such a DT. Additionally, the design of DT must take into account all of the particular requirements of CPS (e.g., potential, steadfastness, security, scalability, sanctuary, and confidentiality). Designing DT presents a potential for original and integrative research endeavors to overcome such problems [139,140].

4.7.1. CPS challenges

CPS has severe presentation necessities in various project scenarios since it is a composite scheme that necessitates the synchronization of web, computation, and control. In general, CPS claims need to be very scalable, highly reliable, and have very low latency. Consider building apps for the power grid using the smart automatic control system. The electric grid must have the ability to swiftly gather important data, and continuous data processing is also required. This information is made up of sensor data that was sent over the internet of the grid and other networks [141]. The DT grid must then swiftly progress this information, excerpt illegal data, and manage, optimize, and regulates the electric grid in accordance with the determined grid state at the moment. The stability of the electric grid is without a doubt our top priority because it is accountable for continuously supplying energy to a sizable number of clients. Network failures, computer hardware failures, network congestion, highly sophisticated control algorithms, and many more problems need to be occupied in justification. The connections between various subsystems (network, computation, and control) inside the CPS are what determine the performance of the system as a whole. Due to this connection, even a small change in one subsystem's performance can have a combination of consequences on the presentation of other parts of the schemes, which can have a complicated impact on the presentation of the CPS system completely. Therefore, the concept is difficult to create a DT for CPS that not only satisfies all of these stringent presentation necessities nevertheless quickly captures the relations among the many parts of the schemes [142,143].

4.7.2. Data transmission and communication challenges

The perception of the digital twin is supposed to be complex to construct and challenging to model the whole grid system. To have a virtual clone of the complex electric grid system large-scale data, parameters, variables, and main factors are set in a complex mathematical model, and analysis in real-time is very much challenging. Extreme high data acquisition and analysis capabilities are needed to reflect the physical grid as described in CPS issues. The mathematical functions and strategies will be rather elaborate owing to the vast quantity of variables present in the CPS physical scheme, which frequently manifests traits like non-linearity, strong coupling, and time-variability. By employing a data-driven technique, we obtain a wealth of information from the physical system that represents its state throughout time [144].

There are numerous challenges involved in acquiring and selecting these data. In CPS all the data are not analyzed at the same time and another circumstance is that one quality of data is possible to accumulate from more than one found along all these foundations that have unique electrical–mechanical configurations. As a result of storing and transmitting this massive quantity of data, the system incurs a substantial overhead cost. For achieving an accurate portrayal according to the change with respect to the time of the physical scheme, sampled the status of the scheme with an actual high rate of recurrence. All the data necessitate a substantial amount of storage space and impose a substantial burden on communication and computer infrastructures with stringent performance requirements [145]. Therefore, a basic question in data analysis is the way of collecting the fewest information points possible deprived of dramatically and destructively affecting the efficiency of DT. The challenging challenge of quickly developing a digital twin for a complicated system with the smallest volume of information necessitates including both mathematical modeling and data science characteristics [146].

4.7.3. Security challenges

The concerns of privacy and security are now covered. The virtual twin grid would be susceptible to cyberattacks such as veracity assaults on hardware and sensors [147], communication, and numerical systems since DT must bring up-to-date the status of physical stuff in real-time through web infrastructures. In a data integrity attack, for instance, the adversary can target IoT devices directly and use them as data collectors, prompting them to upload false or inaccurate data [148]. A large amount of sensitive and confidential data of the whole electric grid and also the information of customers and demand for energy are integrated into the electric digital twin grid body. Despite of high cybersecurity system, the digital twin grid would be a high target to hackers as it is a potential digital clone of the vast energy system. If any cyberattacks occur, the whole electric grid would be crashed and large-scale end consumers such as house-hold, bank-office, industries, the confidential institution would be stopped to run which results in huge economical losses not only at the producer–prosumer–consumer levels but also at the national level of the country.

5. Road to digital twin electric grid

The complexity of the smart grid has grown, and the energy network is becoming more sophisticated day by day. To get the most out of this vast energy network, numerous ICT technologies are being put into the current system [149]. The smart grid is an intelligent service that helps producers and suppliers of energy manage their supplies more efficiently by giving them information about who is using their electricity [150]. The world is paying much attention to sustainable technology because of global climate change. Numerous nations are adopting renewable energy sources like solar power and water power as they look for new sources of energy [151]. Technologies that might improve energy efficiency are urgently being researched at the same time as renewable energy sources are being added to the existing grid.

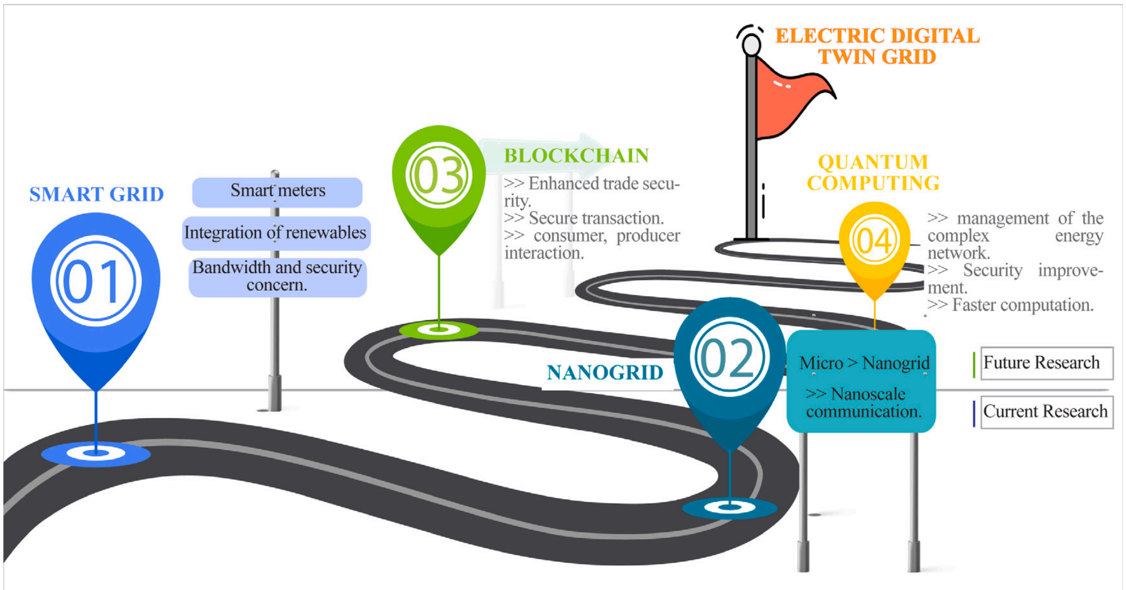


Fig. 12. Road to electric digital twin grid.

These problems led to the development of a more intelligent electric grid with the ability of real-time bidirectional communication, consumer security, and secure energy trade capability [152]. The United States (US) has encouraged grid modernization and the spread of smart meters as part of its recent "Grid 2030" national vision announcement, which aims to enhance the economy by updating old networks. Although SG meets contemporary demands adequately, it still lacks the key characteristics necessary to become the ultimate intelligent grid of the future. Therefore, the Energy Internet (EI), also known as the Internet of Energy (IoE) or Smart Grid 2.0, has been established by fusing the SG framework with Internet technology to improve and progress it and address the present restrictions [153,154]. Later, the grid technology developed in the direction of a decentralized smart grid system to connect DERs, EVs, V2G, prosumers, service providers, and integrated energy markets. This decentralized grid solution also integrates blockchain technology, which offers transaction and deep network security to electric grids [155]. It is quite difficult to accomplish all of the essential planning, security tests, grid evaluations, and troubleshooting for the massive network. Therefore, the future electric grid will be based on the emerging DT technology since has the necessary simulation flexibility, new security frameworks, consumer-utility connection schemes, and real-time data analysis capabilities [156]. Through the course of a product's lifespan, DTs may merge physical and virtual data, creating a vast amount of information that can be analyzed by progressive stats. The investigation findings can then be applied to enhance a process presented in a physical environment [157]. The DT technology has already begun the voyage as GE and Siemens own several patents for, respectively, to evaluate virtual wind turbine [158] farms and enable a human programming interface [159]. Additionally, the DT interface created by GE can simultaneously manage many digital models. The suggested interface uses a graphical user interface (GUI) to show a wind farm's digital image. The interface has a control icon that displays the most recent operational data for each wind turbine as well as certain control elements that may be adjusted to improve the wind farm's efficiency [20]. However, there are still a lot of issues to be resolved in order to realize service communication and collaboration. Some research has been done on the service application of digital twins in fatigue damage, real state detection, fault location tracking, and online monitoring. Further improvements and research will make this technology the ultimate future for managing more intelligent electric grids and complex EI (see Fig. 12).

6. Conclusions

The foundation for integrating the digital twin grids in practice is modeling and simulation. From the standpoint of simulation, the DT approach is the following wave in modeling, recreation, and optimization technologies. DT is useful for more than just depiction; it can also be used to forecast how a product will perform in the upcoming. The DT modeling approach can also be used in simulation-based decision assistance tools that use real-time data. Electric DT grid integrates all the real-time data of the grid with the past histories by real-time high parallel computation capability which supports the decision-making process and future prediction of the grid. The intelligence of the digital electric grid twin grid offers communication between the physical grid to human–machine interference by affording all the real-time data of the grid and the decision-making and future prediction capability using power grid situation based on the measurement data and the memorized limits and rules which helps the automatic operator to take effective and fruitful measures besides saving from any types of violations, outages, and blackout by self-healing.

This literature shows the overall perception of the electric digital twin grid framework. The new framework of the DT grid and some exciting technology introduce a new dimension of technology implemented on electric grid to reduce the complexity of the next-generation electric grid. To achieve clean energy growing up renewables are the most significant issue. It is a matter of regretting that there lies a lot of lagging in current renewable energies such as electricity transmission losses, frequent power outages, electromobility, cyberattacks, and the lack of grid protections. The DT online electric grid analysis, communication software, and protocols are advanced to real-time analysis, optimization, and management of the electric grid. The features of the electric digital twin grid enable it to solve all the complexity of large-scale power systems both the production and demand side management. DT online grid analysis software platform supports to access the current status of the grid from a remote position. The paper describes the features of OADT operation, data analysis, decision-making, and future prediction of the grid along with automatic management and self-healing. The cloud platform of the DT electric grid combines all the consumers, prosumers, and producers. Each consumer and prosumers can monitor the current grid status and monitor the whole energy supply and service. Digital Twin provides high cybersecurity for the whole decentralized system. The electric digital twin grid is a benchmark technology to change the whole energy production, transmission, and distribution system and provides a long-lasting development in the whole world's economic, social, political, communicational, and technological advancement. Despite all these advantages of the electric DT grid, the challenges also remain in the way of the advancement of the technology described in this paper based on different technological issues. Finally, the road to DT electric grid and future directions are shortly designated.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgment

The publication of this article was funded by Qatar National Library, Qatar.

References

[1] Gagnon P, Cole W. Planning for the evolution of the electric grid with a long-run marginal emission rate. Iscience 2022;25(3):103915.
[2] Khan R, Islam N, Das SK, Muyeen S, Moyeen SI, Ali MF, Tasneem Z, Islam MR, Saha DK, Badal MFR, et al. Energy sustainability–survey on technology and control of microgrid, smart grid and virtual power plant. IEEE Access 2021;9:104663–94.
[3] National Academies of Sciences E, Medicine, et al. Analytic research foundations for the next-generation electric grid. National Academies Press; 2016.
[4] Global electricity demand growth is slowing, weighed down by economic weakness and high prices - News - IEA — iea.org. 2022, [Accessed 05-Aug-2022], https://www.iea.org/news/global-electricity-demand-growth-is-slowing-weighed-down-by-economic-weakness-and-high-prices.
[5] Wikipedia. List of major power outages — Wikipedia, the free encyclopedia. 2022, [Online; accessed 05-August-2022], http://en.wikipedia.org/w/index.php?title=List%20of%20major%20power%20outages&oldid=1101821373.
[6] Khan B. Deregulated electricity market. Apple Academic Press; 2022, p. 3–14.
[7] Owusu PA, Asumadu-Sarkodie S. A review of renewable energy sources, sustainability issues and climate change mitigation. Cogent Eng 2016;3(1):1167990.
[8] Liu Y, Dong H, Lohse N, Petrovic S. Reducing environmental impact of production during a rolling blackout policy–a multi-objective schedule optimisation approach. J. Clean. Prod. 2015;102:418–27.
[9] Zhang G, Zhong H, Tan Z, Cheng T, Xia Q, Kang C. Texas electric power crisis of 2021 warns of a new blackout mechanism. CSEE J. Power Energy Syst. 2022;8(1):1–9.
[10] Zhongming Z, Linong L, Xiaona Y, Wangqiang Z, Wei L, et al. Inside China's desperate race to resolve its energy crisis. 2021.
[11] Jiang Z, Lv H, Li Y, Guo Y. A novel application architecture of digital twin in smart grid. J. Ambient Intell. Humaniz. Comput. 2022;13(8):3819–35.
[12] Zhou M, Yan J, Feng D. Digital twin framework and its application to power grid online analysis. CSEE J. Power Energy Syst. 2019;5(3):391–8.
[13] Mourtzis D, Angelopoulos J, Panopoulos N. Development of a PSS for smart grid energy distribution optimization based on digital twin. Procedia CIRP 2022;107:1138–43.
[14] Qian C, Liu X, Ripley C, Qian M, Liang F, Yu W. Digital twin—Cyber replica of physical things: Architecture, applications and future research directions. Future Internet 2022;14(2):64.
[15] Kandasamy NK, Venugopalan S, Wong TK, Nicholas LJ. Epictwin: An electric power digital twin for cyber security testing, research and education. 2021, arXiv preprint arXiv:2105.04260.
[16] Darbali-Zamora R, Johnson J, Summers A, Jones CB, Hansen C, Showalter C. State estimation-based distributed energy resource optimization for distribution voltage regulation in telemetry-sparse environments using a real-time digital twin. Energies 2021;14(3):774.
[17] Saad A, Faddel S, Mohammed O. IoT-based digital twin for energy cyber-physical systems: design and implementation. Energies 2020;13(18):4762.
[18] Andryushkevich SK, Kovalyov SP, Nefedov E. Composition and application of power system digital twins based on ontological modeling. In: 2019 IEEE 17th international conference on industrial informatics (INDIN), vol. 1. IEEE; 2019, p. 1536–42.
[19] Grieves M. Digital twin: manufacturing excellence through virtual factory replication. White Paper 2014;1(2014):1–7.
[20] Tao F, Zhang H, Liu A, Nee AY. Digital twin in industry: State-of-the-art. IEEE Trans. Ind. Inform. 2018;15(4):2405–15.
[21] Eckhart M, Ekelhart A. Towards security-aware virtual environments for digital twins. In: Proceedings of the 4th ACM workshop on cyber-physical system security. 2018, p. 61–72.
[22] Wang Y, Kang X, Chen Z. A survey of digital twin techniques in smart manufacturing and management of energy applications. Green Energy Intell Transp 2022;100014.
[23] Zhang Z, Jiang J, Cheng X. Research on digital twin model of energy equipment. In: 2022 IEEE 2nd international conference on power, electronics and computer applications (ICPECA). IEEE; 2022, p. 264–8.
[24] Danilczyk W, Sun Y, He H. Angel: An intelligent digital twin framework for microgrid security. In: 2019 north american power symposium (NAPS). IEEE; 2019, p. 1–6.
[25] Atalay M, Angin P. A digital twins approach to smart grid security testing and standardization. In: 2020 IEEE international workshop on metrology for industry 4.0 & iot. IEEE; 2020, p. 435–40.
[26] Veselov F, Pankrushina T, Khorshev A. Comparative economic analysis of technological priorities for low-carbon transformation of electric power industry in Russia and the EU. Energy Policy 2021;156:112409.
[27] Panda S, Mohanty S, Rout PK, Sahu BK. A conceptual review on transformation of micro-grid to virtual power plant: Issues, modeling, solutions, and future prospects. Int J Energy Res 2022;46(6):7021–54.
[28] Dhara S, Shrivastav AK, Sadhu PK. Smart grid modernization: Opportunities and challenges. Electr Grid Mod 2022;5.
[29] Ramsebner J, Haas R, Auer H, Ajanovic A, Gawlik W, Maier C, Nemec-Begluk S, Nacht T, Puchegger M. From single to multi-energy and hybrid grids: Historic growth and future vision. Renew. Sustain. Energy Rev. 2021;151:111520.
[30] Smith M, Ton D. Key connections: The us department of energy? s microgrid initiative. IEEE Power Energy Mag. 2013;11(4):22–7.
[31] Hatziargyriou N. Microgrids: Architectures and control. John Wiley & Sons; 2014.
[32] Hossain MA, Pota HR, Hossain MJ, Blaabjerg F. Evolution of microgrids with converter-interfaced generations: Challenges and opportunities. Int. J. Electr. Power Energy Syst. 2019;109:160–86.
[33] Romankiewicz J, Marnay C, Zhou N, Qu M. Lessons from international experience for China's microgrid demonstration program. Energy Policy 2014;67:198–208.
[34] Bellido MH, Rosa LP, Pereira AO, Falcao DM, Ribeiro SK. Barriers, challenges and opportunities for microgrid implementation: The case of Federal University of Rio de Janeiro. J. Clean. Prod. 2018;188:203–16.
[35] Lasseter B. Microgrids [distributed power generation]. In: 2001 IEEE power engineering society winter meeting. Conference proceedings (cat. no. 01ch37194), vol. 1. IEEE; 2001, p. 146–9.
[36] Katiraei F, Iravani MR. Power management strategies for a microgrid with multiple distributed generation units. IEEE Trans. Power Syst. 2006;21(4):1821–31.
[37] Marnay C, Chatzivasileiadis S, Abbey C, Iravani R, Joos G, Lombardi P, Mancarella P, Von Appen J. Microgrid evolution roadmap. In: 2015 International symposium on smart electric distribution systems and technologies (EDST). IEEE; 2015, p. 139–44.
[38] Ton DT, Smith MA. The US department of energy's microgrid initiative. Electr J 2012;25(8):84–94.
[39] Yan Y, Qian Y, Sharif H, Tipper D. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. IEEE Commun. Surv. Tutor. 2012;15(1):5–20.
[40] Benysek G, Kazmierkowski M, Popczyk J, Strzelecki R. Power electronic systems as a crucial part of Smart Grid infrastructure-a survey. Bull. Pol. Acad. Sci. Tech. Sci. 2011;455–73.
[41] Rani S, Talwar R, Malhotra J, Ahmed SH, Sarkar M, Song H. A novel scheme for an energy efficient Internet of Things based on wireless sensor networks. Sensors 2015;15(11):28603–26.
[42] Sanders A, Elangeswaran C, Wulfsberg JP. Industry 4.0 implies lean manufacturing: research activities in industry 4.0 function as enablers for lean manufacturing. J Ind Eng Manag (JIEM) 2016;9(3):811–33.
[43] Liu T, Sun Y, Liu Y, Gui Y, Zhao Y, Wang D, Shen C. Abnormal traffic-indexed state estimation: A cyber–physical fusion approach for smart grid attack detection. Future Gener. Comput. Syst. 2015;49:94–103.
[44] Beniwal RK, Saini MK, Nayyar A, Qureshi B, Aggarwal A. A critical analysis of methodologies for detection and classification of power quality events in smart grid. IEEE Access 2021;9:83507–34.
[45] Faheem M, Shah SBH, Butt RA, Raza B, Anwar M, Ashraf MW, Ngadi MA, Gungor VC. Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. Comp. Sci. Rev. 2018;30:1–30.
[46] Arnold GW. Challenges and opportunities in smart grid: A position article. Proc. IEEE 2011;99(6):922–7.

[47] Bhuiyan EA, Hossain MZ, Muyeen S, Fahim SR, Sarker SK, Das SK. Towards next generation virtual power plant: Technology review and frameworks. Renew. Sustain. Energy Rev. 2021;150:111358.
[48] Wang X, Liu Z, Zhang H, Zhao Y, Shi J, Ding H. A review on virtual power plant concept, application and challenges. In: 2019 IEEE innovative smart grid technologies-Asia (ISGT Asia). IEEE; 2019, p. 4328–33.
[49] Setiawan EA. Concept and controllability of virtual power plant. kassel university press GmbH; 2007.
[50] Arbab-Zavar B, Palacios-Garcia EJ, Vasquez JC, Guerrero JM. Smart inverters for microgrid applications: A review. Energies 2019;12(5):840.
[51] Andoni M, Robu V, Flynn D, Abram S, Geach D, Jenkins D, McCallum P, Peacock A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 2019;100:143–74.
[52] Li Z, Shahidehpour M, Liu X. Cyber-secure decentralized energy management for IoT-enabled active distribution networks. J. Mod. Power Syst. Clean Energy 2018;6(5):900–17.
[53] Pazouki S, Haghifam M-R. The impacts of virtual power plants on multiple carrier energy networks. In: 2014 5th Conference on thermal power plants (CTPP). IEEE; 2014, p. 51–5.
[54] Berl A, Gelenbe E, Di Girolamo M, Giuliani G, De Meer H, Dang MQ, Pentikousis K. Energy-efficient cloud computing. Comput. J. 2010;53(7):1045–51.
[55] Zhou H, Fan S, Wu Q, Dong L, Li Z, He G. Stimulus-response control strategy based on autonomous decentralized system theory for exploitation of flexibility by virtual power plant. Appl. Energy 2021;285:116424.
[56] Zamora R, Srivastava AK. Controls for microgrids with storage: Review, challenges, and research needs. Renew. Sustain. Energy Rev. 2010;14(7):2009–18.
[57] Singh P, Paliwal P, Arya A. A review on challenges and techniques for secondary control of microgrid. In: IOP conference series: Materials science and engineering, vol. 561. (1):IOP Publishing; 2019, 012075.
[58] Hussain MT, Sulaiman NB, Hussain MS, Jabir M. Optimal Management strategies to solve issues of grid having Electric Vehicles (EV): A review. J. Energy Storage 2021;33:102114.
[59] Tariq M, Ali M, Naeem F, Poor HV. Vulnerability assessment of 6G-enabled smart grid cyber–physical systems. IEEE Internet Things J. 2020;8(7):5468–75.
[60] Salkuti SR. Challenges, issues and opportunities for the development of smart grid. Int J Electr Comput Eng (IJECE) 2020;10(2):1179–86.
[61] Hu J, Vasilakos AV. Energy big data analytics and security: challenges and opportunities. IEEE Trans. Smart Grid 2016;7(5):2423–36.
[62] Yoldaş Y, Önen A, Muyeen S, Vasilakos AV, Alan I. Enhancing smart grid with microgrids: Challenges and opportunities. Renew. Sustain. Energy Rev. 2017;72:205–14.
[63] Stellios I, Kotzanikolaou P, Psarakis M, Alcaraz C, Lopez J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Commun. Surv. Tutor. 2018;20(4):3453–95.
[64] Sanjab A, Saad W, Guvenc I, Sarwat A, Biswas S. Smart grid security: Threats, challenges, and solutions. 2016, arXiv preprint arXiv:1606.06992.
[65] Aloul F, Al-Ali A, Al-Dalky R, Al-Mardini M, El-Hajj W. Smart grid security: Threats, vulnerabilities and solutions. Int J Smart Grid Clean Energy 2012;1(1):1–6.
[66] Alonso M, Amaris H, Alcala D, Florez R DM. Smart sensors for smart grid reliability. Sensors 2020;20(8):2187.
[67] Clements S, Kirkham H. Cyber-security considerations for the smart grid. In: IEEE PES general meeting. IEEE; 2010, p. 1–5.
[68] Haq EU, Xu H, Pan L, Khattak MI. Smart grid security: threats and solutions. In: 2017 13th International conference on semantics, knowledge and grids (SKG). IEEE; 2017, p. 188–93.
[69] Lázaro J, Astarloa A, Rodríguez M, Bidarte U, Jiménez J. A survey on vulnerabilities and countermeasures in the communications of the smart grid. Electronics 2021;10(16):1881.
[70] Gaviano A, Weber K, Dirmeier C. Challenges and integration of PV and wind energy facilities from a smart grid point of view. Energy Procedia 2012;25:118–25.
[71] Mengidis N, Tsikrika T, Vrochidis S, Kompatsiaris I. Blockchain and AI for the next generation energy grids: cybersecurity challenges and opportunities. Inf Secur 2019;43(1):21–33.
[72] Ourahou M, Ayrir W, Hassouni BE, Haddi A. Review on smart grid control and reliability in presence of renewable energies: Challenges and prospects. Math. Comput. Simulation 2020;167:19–31.
[73] Ericsson GN. Cyber security and power system communication—essential parts of a smart grid infrastructure. IEEE Trans. Power Deliv. 2010;25(3):1501–7.
[74] Das AK, Zeadally S. Data security in the smart grid environment. In: Pathways to a smarter power system. Elsevier; 2019, p. 371–95.
[75] Goel S, Hong Y. Security challenges in smart grid implementation. In: Smart grid security. Springer; 2015, p. 1–39.
[76] Kotut L, Wahsheh LA. Survey of cyber security challenges and solutions in smart grids. In: 2016 Cybersecurity symposium (CYBERSEC). IEEE; 2016, p. 32–7.
[77] Gunduz MZ, Das R. Analysis of cyber-attacks on smart grid applications. In: 2018 International conference on artificial intelligence and data processing (IDAP). IEEE; 2018, p. 1–5.
[78] Sullivan JE, Kamensky D. How cyber-attacks in Ukraine show the vulnerability of the US power grid. Electr J 2017;30(3):30–5.
[79] Case DU. Analysis of the cyber attack on the ukrainian power grid, vol. 388. Electricity Information Sharing and Analysis Center (E-ISAC); 2016, p. 1–29.
[80] Mekdad Y, Bernieri G, Conti M, El Fergougui A. The rise of ICS malware: A comparative analysis. In: European symposium on research in computer security. Springer; 2021, p. 496–511.
[81] Li X, Liang X, Lu R, Shen X, Lin X, Zhu H. Securing smart grid: cyber attacks, countermeasures, and challenges. IEEE Commun. Mag. 2012;50(8):38–45.
[82] Eckhart M, Ekelhart A. Digital twins for cyber-physical systems security: State of the art and outlook. In: Security and quality in cyber-physical systems engineering. Springer; 2019, p. 383–412.
[83] Chen G, Tang W, Chen S, Wang S, Cui H. Prediction of self-healing of engineered cementitious composite using machine learning approaches. Appl. Sci. 2022;12(7):3605.
[84] Shyama M, Pillai AS, Anpalagan A. Self-healing and optimal fault tolerant routing in wireless sensor networks using genetical swarm optimization. Comput. Netw. 2022;217:109359.
[85] Begum BA, Nandury SV. Component based self-healing approach for fault-tolerant data aggregation in WSN. IEEE Access 2022;10:73503–20.
[86] Zhang T, Zhu K, Hossain E. Data-driven machine learning techniques for self-healing in cellular wireless networks: Challenges and solutions. Intell Comput 2022;2022.
[87] Malathy V. Turbo coding for avoiding network failure in wireless sensor network. In: AIP conference proceedings, vol. 2418. (1):AIP Publishing LLC; 2022, 030051.
[88] Cheena K, Amgoth T, Shankar G. Proportional-integral-derivative controller-based self-healing of distribution system using wireless sensor networks in smart grid. Int. J. Commun. Syst. 2022;35(7):e5095.
[89] Golshani A, Sun W, Sun K. Advanced power system partitioning method for fast and reliable restoration: toward a self-healing power grid. IET Gener, Transm Distrib 2018;12(1):42–52.
[90] Bitton R, Gluck T, Stan O, Inokuchi M, Ohta Y, Yamada Y, Yagyu T, Elovici Y, Shabtai A. Deriving a cost-effective digital twin of an ICS to facilitate security evaluation. In: European symposium on research in computer security. Springer; 2018, p. 533–54.
[91] Kritzinger W, Karner M, Traar G, Henjes J, Sihn W. Digital Twin in manufacturing: A categorical literature review and classification. IFAC-PapersOnLine 2018;51(11):1016–22.
[92] Jia G, Ni W, Wu J. Research and applications of key technologies of quantum secure communication in energy internet. In: 2019 4th International conference on intelligent green building and smart grid (IGBSG). IEEE; 2019, p. 54–60.
[93] Strasser T, Andrén F, Kathan J, Cecati C, Buccella C, Siano P, Leitao P, Zhabelova G, Vyatkin V, Vrba P, et al. A review of architectures and concepts for intelligence in future electric energy systems. IEEE Trans. Ind. Electron. 2014;62(4):2424–38.
[94] Azzuni A, Breyer C. Energy security and energy storage technologies. Energy Procedia 2018;155:237–58.
[95] Mirsaeidi S, Said DM, Mustafa MW, Habibuddin MH, Ghaffari K. Progress and problems in micro-grid protection schemes. Renew. Sustain. Energy Rev. 2014;37:834–9.
[96] Ashok A, Krishnaswamy S, Govindarasu M. PowerCyber: A remotely accessible testbed for Cyber Physical security of the Smart Grid. In: 2016 IEEE power & energy society innovative smart grid technologies conference (ISGT). IEEE; 2016, p. 1–5.
[97] Almalaq A, Albadran S, Mohamed MA. Deep machine learning model-based cyber-attacks detection in smart power systems. Mathematics 2022;10(15):2574.
[98] Sahu A, Mao Z, Wlazlo P, Huang H, Davis K, Goulart A, Zonouz S. Multi-source multi-domain data fusion for cyberattack detection in power systems. IEEE Access 2021;9:119118–38.
[99] Faisal M, Hannan MA, Ker PJ, Hussain A, Mansor MB, Blaabjerg F. Review of energy storage system technologies in microgrid applications: Issues and challenges. IEEE Access 2018;6:35143–64.
[100] Rosas-Casals M. Power grids as complex networks: topology and fragility. In: 2010 Complexity in engineering. IEEE; 2010, p. 21–6.
[101] Saeed MH, Fangzong W, Kalwar BA, Iqbal S. A review on microgrids' challenges & perspectives. IEEE Access 2021;9:166502–17.
[102] Shaukat N, Ali S, Mehmood C, Khan B, Jawad M, Farid U, Ullah Z, Anwar S, Majid M. A survey on consumers empowerment, communication technologies, and renewable generation penetration within Smart Grid. Renew. Sustain. Energy Rev. 2018;81:1453–75.
[103] Schülke A, Bauknecht J, Häussler J. Power demand shifting with smart consumers: A platform for power grid friendly consumption control strategies. In: 2010 First IEEE international conference on smart grid communications. IEEE; 2010, p. 437–42.
[104] Boork M, Thomtén M, Brolin M, Uyterlinde M, Straver K, Kraan C, Kleine-Hegermann K, Laes E, Valkering P, Maggiore S. Key success factors and barriers to end user engagement in smart grid projects. In: Proceedings of the behave 2014 behaviour and energy efficiency conference, Oxford, UK. 2014, p. 3–4.

[105] De Dutta S, Prasad R. Security for smart grid in 5G and beyond networks. Wirel. Pers. Commun. 2019;106(1):261–73.
[106] dos Santos CH, Montevechi JAB, de Queiroz JA, de Carvalho Miranda R, Leal F. Decision support in productive processes through DES and ABS in the Digital Twin era: a systematic literature review. Int. J. Prod. Res. 2022;60(8):2662–81.
[107] Karanjkar N, Joglekar A, Mohanty S, Prabhu V, Raghunath D, Sundaresan R. Digital twin for energy optimization in an SMT-PCB assembly line. In: 2018 IEEE international conference on internet of things and intelligence system (IOTAIS). IEEE; 2018, p. 85–9.
[108] Aydemir H, Zengin U, Durak U. The digital twin paradigm for aircraft review and outlook. In: AIAA scitech 2020 forum. 2020, p. 0553.
[109] Mashaly M. Connecting the twins: A review on Digital Twin technology & its networking requirements. Procedia Comput. Sci. 2021;184:299–305.
[110] Singh M, Fuenmayor E, Hinchy EP, Qiao Y, Murray N, Devine D. Digital twin: Origin to future. Appl Syst Innov 2021;4(2):36.
[111] Camposano JC, Smolander K, Ruippo T. Seven metaphors to understand digital twins of built assets. IEEE Access 2021;9:27167–81.
[112] Grieves MW. Product lifecycle management: the new paradigm for enterprises. Int J Product Dev 2005;2(1–2):71–84.
[113] Zhou M, Yan J. A new solution architecture for online power system analysis. CSEE J. Power Energy Syst. 2018;4(2):250–6.
[114] Mehonic A, Sebastian A, Rajendran B, Simeone O, Vasilaki E, Kenyon AJ. Memristors—From in-memory computing, deep learning acceleration, and spiking neural networks to the future of neuromorphic and bio-inspired computing. Adv Intell Syst 2020;2(11):2000085.
[115] Uhlemann TH-J, Lehmann C, Steinhilper R. The digital twin: Realizing the cyber-physical production system for industry 4.0. Procedia Cirp 2017;61:335–40.
[116] Khajavi SH, Motlagh NH, Jaribion A, Werner LC, Holmström J. Digital twin: vision, benefits, boundaries, and creation for buildings. IEEE Access 2019;7:147406–19.
[117] Kumar S, Singh AK, Kalam MA. Fault prediction in transmission line using GOOSE protocol and Artificial Neural Network. In: 2021 Fourth international conference on electrical, computer and communication technologies (ICECCT). IEEE; 2021, p. 1–7.
[118] Reshikeshan SSM, Koh MB, Illindala MS. Rainbow signature scheme to secure GOOSE communications from quantum computer attacks. IEEE Trans. Ind. Appl. 2021;57(5):4579–86.
[119] Stusek M, Zeman K, Masek P, Sedova J, Hosek J. IoT protocols for low-power massive IoT: a communication perspective. In: 2019 11th International congress on ultra modern telecommunications and control systems and workshops (ICUMT). IEEE; 2019, p. 1–7.
[120] Conde J, Munoz-Arcentales A, Alonso A, Lopez-Pernas S, Salvachua J. Modeling digital twin data and architecture: A building guide with fiware as enabling technology. IEEE Internet Comput. 2021.
[121] Ala-Laurinaho R, Autiosalo J, Nikander A, Mattila J, Tammi K. Data link for the creation of digital twins. IEEE Access 2020;8:228675–84.
[122] Autiosalo J, Vepsäläinen J, Viitala R, Tammi K. A feature-based framework for structuring industrial digital twins. IEEE Access 2019;8:1193–208.
[123] Kome ML, Cuppens F, Cuppens-Boulahia N, Frey V. CoAP enhancement for a better IoT centric protocol: CoAP 2.0. In: 2018 Fifth international conference on internet of things: systems, management and security. IEEE; 2018, p. 139–46.
[124] Galketiya T, Kahahena J, Chandran J, Kavalchuk I. Novel communication system for scada tied smart inverter for vietnam. In: 2019 25th Asia-pacific conference on communications (APCC). IEEE; 2019, p. 331–5.
[125] Tan J, Sha X, Dai B, Lu T. Wireless technology and protocol for iIoT and digital twins. In: 2020 ITU kaleidoscope: Industry-driven digital transformation (ITU K). IEEE; 2020, p. 1–8.
[126] Silva D, Carvalho LI, Soares J, Sofia RC. A performance analysis of internet of things networking protocols: Evaluating MQTT, CoAP, OPC UA. Appl. Sci. 2021;11(11):4879.
[127] Yang K, Zhang B, Zhang J, Zhu J. Design of remote control inverter based on MQTT communication protocol. In: 2021 IEEE international conference on mechatronics and automation (ICMA). IEEE; 2021, p. 1374–8.
[128] Liu Q, Li Y. Modbus/tcp based network control system for water process in the firepower plant. In: 2006 6th World congress on intelligent control and automation, vol. 1. IEEE; 2006, p. 432–5.
[129] Sharma A, Airan S, Shah D. Designing c library for modbus-rtu to canbus and modbus-tcp iot converters. In: 2021 Second international conference on electronics and sustainable communication systems (ICESC). IEEE; 2021, p. 731–7.
[130] Dayal A, Deng Y, Tbaileh A, Shukla S. VSCADA: A reconfigurable virtual SCADA test-bed for simulating power utility control center operations. In: 2015 IEEE power & energy society general meeting. IEEE; 2015, p. 1–5.
[131] Danilczyk W, Sun YL, He H. Smart grid anomaly detection using a deep learning digital twin. In: 2020 52nd north american power symposium (NAPS). IEEE; 2021, p. 1–6.
[132] Zheng Y, Yang S, Cheng H. An application framework of digital twin and its case study. J. Ambient Intell. Humaniz. Comput. 2019;10(3):1141–53.
[133] Alam KM, El Saddik A. C2PS: A digital twin architecture reference model for the cloud-based cyber-physical systems. IEEE Access 2017;5:2050–62.
[134] Alam KM, Sopena A, El Saddik A. Design and development of a cloud based cyber-physical architecture for the Internet-of-Things. In: 2015 IEEE international symposium on multimedia (ISM). IEEE; 2015, p. 459–64.
[135] Guo Z, Zhang Y, Zhao X, Song X. CPS-based self-adaptive collaborative control for smart production-logistics systems. IEEE Trans. Cybern. 2020;51(1):188–98.
[136] Pan Y, Zhang L. A BIM-data mining integrated digital twin framework for advanced project management. Autom. Constr. 2021;124:103564.
[137] Pan Y, Zhang L, Skibniewski MJ. Clustering of designers based on building information modeling event logs. Comput.-Aided Civ. Infrastruct. Eng. 2020;35(7):701–18.
[138] Karnouskos S. Stuxnet worm impact on industrial cyber-physical system security. In: IECON 2011-37th annual conference of the IEEE industrial electronics society. IEEE; 2011, p. 4490–4.
[139] Fuller A, Fan Z, Day C, Barlow C. Digital twin: Enabling technologies, challenges and open research. IEEE Access 2020;8:108952–71.
[140] He Y, Guo J, Zheng X. From surveillance to digital twin: Challenges and recent advances of signal processing for industrial internet of things. IEEE Signal Process. Mag. 2018;35(5):120–9.
[141] Dafflon B, Moalla N, Ouzrout Y. The challenges, approaches, and used techniques of CPS for manufacturing in Industry 4.0: a literature review. Int. J. Adv. Manuf. Technol. 2021;113(7):2395–412.
[142] Wan K, Man K, Hughes D. Specification, analyzing challenges and approaches for cyber-physical systems (CPS). Eng Lett 2010;18(3).
[143] Gunes V, Peter S, Givargis T, Vahid F. A survey on concepts, applications, and challenges in cyber-physical systems. KSII Trans Internet Inf Sys (TIIS) 2014;8(12):4242–68.
[144] Afsari K, Eastman CM, Shelden DR. Cloud-based BIM data transmission: current status and challenges. In: ISARC. Proceedings of the international symposium on automation and robotics in construction, vol. 33. IAARC Publications; 2016, p. 1.
[145] Ansari S, Ayob A, Lipu MSH, Saad MHM, Hussain A. A review of monitoring technologies for solar PV systems using data processing modules and transmission protocols: Progress, challenges and prospects. Sustainability 2021;13(15):8120.
[146] Bhadani AK, Jothimani D. Big data: challenges, opportunities, and realities. In: Effective big data management and opportunities for implementation. IGI Global; 2016, p. 1–24.
[147] Harper KE, Ganz C, Malakuti S. Digital twin architecture and standards. IIC J Innov 2019;12:72–83.
[148] Zheng X, Lu J, Kiritsis D. The emergence of cognitive digital twin: vision, challenges and opportunities. Int. J. Prod. Res. 2021;1–23.
[149] Huh J-H, Otgonchimeg S, Seo K. Advanced metering infrastructure design and test bed experiment using intelligent agents: focusing on the PLC network base technology for Smart Grid system. J. Supercomput. 2016;72(5):1862–77.
[150] Kim S-K, Huh J-H. A study on the improvement of smart grid security performance and blockchain smart grid perspective. Energies 2018;11(8):1973.
[151] Qin Y, Xu Z, Wang X, Škare M. Green energy adoption and its determinants: A bibliometric analysis. Renew. Sustain. Energy Rev. 2022;153:111780.
[152] Bagdadee AH, Zhang L. A review of the smart grid concept for electrical power system. In: Research anthology on smart grid and microgrid development. IGI Global; 2022, p. 1361–85.
[153] Mahmud K, Khan B, Ravishankar J, Ahmadi A, Siano P. An internet of energy framework with distributed energy resources, prosumers and small-scale virtual power plants: An overview. Renew. Sustain. Energy Rev. 2020;127:109840.
[154] Al-Turjman F, Abujubbeh M. IoT-enabled smart grid via SM: An overview. Future Gener. Comput. Syst. 2019;96:579–90.
[155] Mollah MB, Zhao J, Niyato D, Lam K-Y, Zhang X, Ghias AM, Koh LH, Yang L. Blockchain for future smart grid: A comprehensive survey. IEEE Internet Things J. 2020;8(1):18–43.
[156] Kandasamy NK, Venugopalan S, Wong TK, Leu NJ. An electric power digital twin for cyber security testing, research and education. Comput Electr Eng 2022;101:108061.
[157] Qi Q, Tao F. Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison. IEEE Access 2018;6:3585–93.
[158] Al Noman A, Tasneem Z, Sahed MF, Muyeen S, Das SK, Alam F. Towards next generation Savonius wind turbine: Artificial intelligence in blade design trends and framework. Renew. Sustain. Energy Rev. 2022;168:112531.
[159] Hewitt S, Margetts L, Revell A. Building a digital wind farm. Arch. Comput. Methods Eng. 2018;25(4):879–99.