Challenges and opportunities for the energy management of sustainable data centers in smart grids

Hongliang Wang¹,² and Daogui Tang¹,²,³
¹ Inspur Electronic Information Industry Co., Ltd., Jinan, 250101 China;
² State key laboratory of high-end server and storage technology, Jinan, 250101 China;
³ Corresponding author’s e-mail: tangdaogui@gmail.com

Abstract. With the increase of cloud computing and internet services, data centers are emerging to satisfy the requirement, leading to incremental energy consumption demand and emissions of green house gases. Thus, integration of renewable energies with the traditional power grid is preferred to reduce the environmental impact and increase energy efficiency, which lead to a demand of energy management strategies to coordinate the energy demand and generation. In this paper, we review the challenges for the sustainable data centers in smart grids with regards to energy management strategies, integration with renewable energies and cyber-attacks and propose possible solutions. Through the analysis of the data centers from the perspective of both smart grids level and micro-grid level, the research challenges and potential research directions in the energy management of sustainable data centers have been discussed.

1. Introduction
In the modern society, Internet data centers (IDC) are emerging to supply services for data-intensive and digital technologies, e.g., artificial intelligence and autonomous vehicles [1], which lead to the significant increasing power demand of IDC. IDC is composed of four parts, i.e., power equipment, cooling equipment, IT equipment, and miscellaneous components, among which, IT and cooling equipment consume about 90% of the energy of an IDC [2]. It is estimated that the energy consumption of IDC accounts for 1.3% - 1.5% of total energy usage in the world [3]. Besides, the energy consumption causes a great amount of CO₂ emissions to the environment. It is reported that information and communication technologies (ICT) contribute to about 2% of the total CO₂ emissions around the globe [4] and emitted 116 million metric tons of CO₂ in 2007 [5]. Thus, new technologies and methods are expected to reduce the energy consumption, energy cost and CO₂ emissions.

One promising way to reach the goals is to integrate renewable energies with traditional power systems. In recent studies, renewable energies such as photovoltaic (PV), wind energies and hydrogen-based fuel cell systems (FCS) have attracted much research and application attention [6–8]. Besides the ecological efficiency of the renewable energies, they also bring many challenges, such as forecast of PV and wind energy, energy management of IDC and so on. The energy management of the IDC should take into consideration not only the coordination of various energy sources and the power demand of the IDC, but also the connection of the
distributed energy resources with the bulk power system.

Besides, to reduce energy cost, the IDC can be designed from the smart grids level. From the perspective of smart grids, IDC energy consumption, residential demand and industrial load compose the main energy demand in power distribution systems. Two-way information communication between customers (e.g., IDC) and utility companies, which facilitates demand-response and demand-side management of customers. Various kinds of demand-response programs, such as price-based and utility-based programs, have been proposed to reduce the monetary cost of customers and improve energy efficiency.

When considering IDC as part of future smart grids, which is a cyber-physical system, another side should be taken into consideration, i.e., the cyber security problem in smart grids [9–11]. The integration of information and communication technologies gives malicious attackers opportunities to disturb energy services by cyber attacks. In recent research works, cyber attacks to smart grids have attracted much attention. But most of them are focusing on power transmission networks, only few works have studied the cyber attacks to power distribution networks. Besides, the integration with renewable energies can also be targets of cyber attacks [12, 13].

Recent studies of sustainable IDC mainly focus on two tracks, i.e., reducing the load of the IDC and using renewable energies to supply power for IDC. The former track puts emphasis on reducing the energy consumption of cooling systems since it is one of the major load burden in IDC [3, 14]. Many review papers have summarized recent works and trends of the former track [15–17]. Thus, in this paper, we stress the later track by considering the opportunities and challenges in integration of renewable energies in smart grids.

![Figure 1](https://via.placeholder.com/150)

**Figure 1.** Research framework of the present work.

Figure 1 presents the research framework of the work. The sustainable data centers receive electricity energy from the smart grids and communicate with smart grids through the two-way information exchange. Enabled by the two-way information communication between the IDC and smart grids, demand response programs can be employed to save monetary cost of the IDC. On the other hand, the two-way information exchange gives malicious attackers opportunity to disturb electricity utility service through cyber attacks. The reduction of green house emission and energy consumption of the IDC can be achieved from two aspects, i.e., integration of renewable energy to supply clean energy and development of energy saving technologies to reduce load. In the present study, we focus on the integration of renewable energy given the top of this paper. To leverage renewable energy generation and energy consumption of the IDC, proper energy management strategies need to be designed.

The rest of the paper is organized as follows. Section 2 analyzes challenges of the integration with renewable energies and the demand-side management is introduced in Section 3. In Section
4. we introduce the cyber security problem of IDC and finally the paper is concluded in Section 5.

2. Integration with renewable energies
To reduce the greenhouse gas emissions, renewable energies, such as solar energy, wind energy and hydrogen energy, are a promising solution [18]. However, these renewable energy, as primary energy, cannot be used directly to supply electricity for electrical appliances [19], thus, requires devices to convert them to electricity, for instance, PV panels, wind turbines and fuel cells.

The main advantages of the renewable energy are their zero green gas emissions and low cost. For instance, wind turbines and PV panels transfer wind and solar energy to electricity and produce no other emissions; fuel cells take hydrogen and oxygen as reactant and produce electricity and water [20]. Besides, the energy efficiency of FCS is higher than traditional diesel engines [21, 22].

However, due to the characteristics of these renewable energies, there are inherent disadvantages of each renewable energy, such as incapability of energy storage and intermittent behavior due to atmospheric conditions. Thus, IDC can also be equipped with energy storage systems to remedy those shortcomings. Such energy storage unit includes batteries, ultra-capacitor and hydrogen storage tanks.

The integration with renewable energies can be classified into three steps: supplementary, stand-alone and prosumer. In the first step, renewable energies work as supplementary energies of the IDC and the main energy consumption is satisfied by energy drawn from the bulk power system. With the increasing penetration of renewable energies in IDC, the generation of renewable energy can satisfy the self use of IDC and no energy is required from the bulk power system. Thus, the IDC can work as stand-alone modes [23].

If the renewable energy generation exceeds the energy requirement of an IDC, extra energy can be sold back to the bulk power system, thus, the IDC plays a role of not only an energy consumer but also a producer, thus, is called producer. It should be noticed that the third step is not exclusive of the first step [24]. When the power demand of IDC is very low and renewable energy generation exceeds the power requirement, extra electricity can be sold to other customers or utility companies; besides, the recovery heat of IDC can also be supplied to residential households.

One typical research of the renewable energy integration in IDC can be seen in References [23, 25], where a hybrid power system contains PV panels, wind turbines, fuel cells and batteries are proposed to enable stand-alone operation of the IDC.

3. Demand-side management
The integration of renewable energy brings much flexibility and complexity to the demand-side management of IDC. The demand-side management can be classified into two layers: the micro-grid level and the smart grids level. In the micro-grid level, an energy management system is proposed to coordinate different energy sources, energy storage systems and load whereas in the level of smart grids, various demand-response programs are proposed to reduce monetary cost.

3.1. Energy management systems and strategies
3.1.1. Energy management systems. The hybrid power system is coordinated and managed by an energy management system. Figure 2 shows the energy management system of IDC, which takes into consideration the integration of renewable energies with the bulk power system. For the standalone and prosumer modes of IDC, the bulk power system is out of consideration of the energy management system. The load is composed of main load that is used for information technology (IT) and service load that is used to guarantee the normal operation of IT. The load demand is collected by the energy management system, and
energy sources based on pre-determined energy management strategies. On the other hand, the available energy information is transmitted to the energy management system, and then, control the load to make sure that the important load is fully supplied.

![Energy management system diagram](image)

**Figure 2.** Energy management systems of IDC.

### 3.1.2. Energy management strategies
Energy management strategies are key to the energy management system. The goal of the energy management strategies is to minimize or maximize a goal metric, for instance, the Power Usage Effectiveness (PUE) which represents the total energy consumed by the IDC per unit of energy consumed by the main load, as well as the Carbon Usage Effectiveness (CUE), the Energy Reuse Factor (ERF) and the Green Energy Coefficient (GEC) which takes into consideration of the integration of renewable energies.

Different kinds of energy management strategies for hybrid power systems have been developed given different goals. These strategies are mainly rules-based and optimization based. For instance, a rule-based energy management strategy is proposed for a fuel cell hybrid power system in [20] and fuzzy logic based energy management strategy is developed for a PV hybrid power system [19]. The rule-based energy management strategies rely on the past experience and skills of experts to make rules for the regulation of energy allocation. Optimization-based energy management strategies can be classified into global optimization, e.g., dynamic programming [26], and real-time optimization, e.g., model predictive control [27, 28].

### 3.2. Demand response
IDC is a kind of important load in power distribution systems, as shown in Figure 3. Electricity power is generated by various kinds of generators, such as PV panels, wind turbines, diesel engines etc., and, then, transmitted to substations and, finally, distributed to customers like residential buildings, industry and IDC by power distribution networks. On the other hand, the electricity generated by distributed renewable energy of IDC can be fed back to the bulk power system, which forms the two-way energy flow between smart grids and IDC. Besides, two-way information flow exists between utility companies and customers. The utility companies send energy usage and electricity pricing information to customers, who then schedule their demand according to demand-response programs. At the end of each time slot, energy consumption
information is collected via smart meters and sent to the utility company for adjusting electricity generation and electricity prices via advanced metering infrastructures (AMI) [29].

The main aim of demand-side management in smart grids level is to encourage customers to consume less power in peak time or to shift their energy consumption to off-peak hours [30]. Among various kinds of techniques of demand-side management, demand-response is a specific short-term tariff or program [30]. In order to engage customers in smart grids, various demand-response programs have been developed [31, 32]. These demand-response programs guide customers to schedule or reschedule their consumption by dynamic prices [32]. For instance, time-of-use (TOU) and real-time pricing (RTP) programs are the most common used programs [33]. In TOU, utility companies publish day-ahead electricity prices based on prediction and then customers schedule their energy consumption at each time slot to minimize their energy cost. In RTP, the electricity is updated hourly or even every five minutes.

In order to reduce monetary cost of energy, recent research works focus on methods of demand-response at demand side. Four kinds of price-driven programs with different goals are summarized in Ref. [34], which are reducing the peak-to-average load ratio [35, 36], minimizing economic cost [37, 38], maximizing utility welfare of customers [39, 40] and the improvement of economic cost [41, 42]. However, those research directions are mainly specified for residential customers, the optimization goals of IDC should be re-defined and reformulated. Beside these four research directions, the collaboration of multiple data centers in located different geographical areas by proper resource allocation and load assignment methods can also reduce the operational cost of IDC [43].
| Site                | Time  | Systems               | Cyber attacks       | Impact                                      |
|---------------------|-------|-----------------------|---------------------|---------------------------------------------|
| Soviet Union (Russia)| 1982  | gas pipeline          | code manipulation   | 3 kilotons TNT equivalent explosion         |
| USA                 | 1999  | gasoline pipeline     | code manipulation   | three people killed and many others injured |
| USA                 | 2003  | nuclear plant         | malware injection   | unable to observe parameter for 5 hours     |
| USA                 | 2007  | a diesel engine       | false data injection| generator exploded                         |
| Turkey              | 2008  | oil pipeline          | false data injection| oil explosion and leakage                   |
| Saudi Arabia and Qatar | 2012 | oil and gas           | malware injection   | affect energy generation and delivery       |
| Ukraine             | 2015  | power system          | false data injection| more than 225k customers losing power for 6-12 hours |
| USA                 | 2021  | oil company           | ransomware attack    | 5,500 miles of pipelines shut down          |

4. Cyber security

As discussed in Subsection 3.2, the two-way information communication between utility companies and IDC enables the active engagement of IDC in smart grids. However, the associated cyber security problems through cyber networks are non-negligible. The cyber security goals of smart grids include integrity, confidentiality and availability [44]. Various cyber attacks can target one or more goals of the smart grids [31], for instance, fault injection attacks can be adopted to corrupt data and break the confidentiality in cyber-physical systems [45] whereas data injection attacks can interrupt integrity of smart grids [46–48] and the availability goal can be unsatisfied by denial-of-service attacks [49].

In Table 1, we have summarized the cyber attacks to energy systems in last decades [7, 50]. We can observe from the Table that there is increasing number of cyber attacks targeting the energy systems in recent decades and have caused severe impact. In smart grids, cyber attacks can target the power transmission systems and power distribution systems [44]. For the false data injection to power transmission networks, malicious attackers can inject false measurement data to confuse the state estimation of power system and pass the detection [51]. This kind of cyber attacks can disturb the utility services of substations in smart grids and cause severe impact. Cyber attacks that target power distribution networks mainly focus on disturbing demand-response by injecting false electricity prices [52–55]. Victims who receive the false electricity prices will schedule their consumption according, and this might lead to economic loss and even overload of the power system [52]. Furthermore, false renewable energy generation information can be injected to smart meters to misconduct the energy management behavior of customers [56]. Thus, the cyber attacks to IDC in both smart grids level, i.e., cyber attacks to power transmission networks and price-based demand-response programs, and micro-grid level, i.e., cyber attacks to renewable energy generation, should be taken into consideration to develop resilient and robust IDC.

To mitigate the impact of cyber attacks, timely detection and defending against cyber attacks are very important [31]. Recent works have addressed the cyber attacks detection and defense problems using various methods. Real-time state estimation is performed to detect bad data in power systems [57]. However, intelligent cyber attacks can easily pass the present state estimator [51], thus, many new methods have been developed, in which machine learning approaches have attracted much attention. Ref. [58] proposes an unsupervised cyber attacks detection
method which is based on statistical correlation between measurements. A distributed data-driven approach is proposed to detect stealthy cyber attacks on large scale power systems [59]. For the false data injection attacks to renewable energy, machine learning methods such as long short-term memory networks (LSTM), vector autoregressive models, deep neural networks [12] and convolutional neural networks [13] have been studied.

Another research direction to mitigate the impact of cyber attacks is development of defense methods [60]. Many research works based on Markov decision process and game theory have been proposed to protect power system from cyber attacks [55, 60–62]. The former methods can model the decision process of cyber attackers or defenders, but fail to capture the dynamic interaction between them, whereas the game theoretic approaches can model the dynamics of the cyber attacks. In the design and operation of IDC, cyber attacks need to be taken into consideration to improve the resilience of IDC.

5. Conclusions and future work
In this paper, we review the recent researches of sustainable IDC as part of smart grids. Specifically, due to the rising concern of environmental problems and increasing demand of power consumption, the integration of renewable energy into the development of IDC is proposed as a promising solution. We review the challenges on the commonly used renewable energies such as solar and wind energy and highlight the necessity of hybrid power system. Together with the hybrid power system, the challenges of energy management in both micro-grid level and smart grids level have been studied. Finally, as part of smart grids, the increasing of interaction between the distributed energy generation systems of IDC and the bulk power system is vulnerable to the emerging cyber security problems in smart grids. We review the cyber attacks at power transmission and distribution levels and studied the possible methods to mitigate the impact of such cyber attacks.

In future work, several research directions can be done to reduce energy consumption and green house gases emissions of IDC, and improve the resilience of IDC to cyber attacks. Firstly, different kinds of renewable energies can be employed in the design and operation of IDC. Thus, the optimal installation strategy of renewable energies in the design of IDC, and proper energy management strategies during the operation of IDC should be developed. Then, the coordination of demand-response programs and energy management strategy to reduce monetary cost and energy consumption should be optimized. To provide long-term reliable operation of IDC, intelligent operation systems and fault diagnosis systems can be taken into consideration; and finally, the resilience of IDC can be defined and methods to improve the resilience of IDC should be studied.

Acknowledgement
This work was supported by the Natural Science Foundation of Shandong Province (No. ZR2019LZH006). The authors would like to thank all the reviewers for their questions and suggestion that have helped improve the quality of the work.

References
[1] Tradat M I, Sammakia B G, Hoang C H, Alissa H A et al. 2021 Applied Energy 289 116663
[2] Jin C, Bai X, Yang C, Mao W and Xu X 2020 applied energy 265 114806
[3] Deymi-Dashtebayaz M, Namamo S V and Arabkooohsar A 2019 Applied Thermal Engineering 161 114133
[4] Whitehead B, Andrews D, Shah A and Maidment G 2014 Building and Environment 82 151–159
[5] Guitart J 2017 Computing 99 597–615
[6] Tang D and Wang H 2021 IEEE Access 9 158796–158807
[7] Abdouleah Z, Alammar E and Gastli A 2015 Renewable and Sustainable Energy Reviews 45 249–262
[8] Oré E, Depoorter V, Garcia A and Salom J 2015 Renewable and Sustainable Energy Reviews 42 429–445
[9] Ding D, Han Q L, Wang Z and Ge X 2020 IEEE Transactions on Systems, Man, and Cybernetics:
[10] Yu L, Sun X M and Sui T 2019 IEEE Transactions on Systems, Man, and Cybernetics: Systems 49 1712–1719
[11] Peng C, Sun H, Yang M and Wang Y L 2019 IEEE Transactions on Systems, Man, and Cybernetics: Systems 49 1554–1569
[12] Lore K G, Shila D M and Ren L 2018 Detecting data integrity attacks on correlated solar farms using multilayer data driven algorithm 2018 IEEE Conference on Communications and Network Security (CNS) (IEEE) pp 1–9
[13] Ismail M, Shaaban M F, Naidu M and Serpedin E 2020 IEEE Transactions on Smart Grid
[14] Zhou F, Li C, Zhu W, Zhou J, Ma G and Liu Z 2018 Energy and Buildings 169 295–304
[15] Khalaj A H and Halgamuge S K 2017 Applied energy 205 1165–1188
[16] Darraghmeh H M and Wang C C 2017 Applied Thermal Engineering 114 1224–1239
[17] Ni J and Bai X 2017 Renewable and sustainable energy reviews 67 625–640
[18] Tang D, Yan X, Yuan Y, Wang K and Qiu L 2015 Multi-agent based power and energy management system for hybrid ships 2015 International Conference on Renewable Energy Research and Applications (ICRERA) (IEEE) pp 383–387
[19] Yuan Y, Zhang T, Shen B, Yan X and Long T 2018 Energies 11 2211
[20] Tang D, Zuo E, Yuan Y, Zhao J and Yan X 2017 The energy management and optimization strategy for fuel cell hybrid ships 2017 2nd International Conference on System Reliability and Safety (ICSRS) (IEEE) pp 277–281
[21] Ou K, Yuan W W and Kim Y B 2021 Energy 219 119499
[22] Ettihl H, Boulon L and Agbossou K 2016 Applied Energy 163 142–153
[23] Haddad M, Nicrod J M, Péra M C and Varnier C 2021 Journal of Scheduling 1–19
[24] Huang P, Copertaro B, Zhang X, Shen J, Lőfgren I, Rønnelid M, Fahlen J, Andersson D and Svanfeldt M 2020 Applied Energy 258 201140
[25] Haddad M, Nicod J M, Varnier C and Peéra M C 2019 Mixed integer linear programming approach to optimize the hybrid energy system management for supplying a stand-alone data center 2019 Tenth International Green and Sustainable Computing Conference (IGSC) (IEEE) pp 1–8
[26] Mallon K R and Assadian F 2021 Journal of Dynamic Systems, Measurement, and Control 143 091001
[27] Mariano-Hernández D, Hernández-Caldejo L, Zorita-Lamadrid A, Duque-Pérez O and García F S 2021 Journal of Building Engineering 33 101692
[28] Xie P, Guerrero J M, Tan S, Bazmohammad N, Vasquez J C, Mehrzadi M and Al-Turki Y 2021 IEEE Systems Journal
[29] Mohassel R R, Fung A, Mohammadi F and Raahemifar K 2014 International Journal of Electrical Power & Energy Systems 63 473–484
[30] Waseem M, Sajid I A, Haroon S S, Amin S, Farooq H, Martirano L and Napoli R 2020 Electric Power Components and Systems 48 1339–1361
[31] Tang D 2021 A simulation-based modeling framework for the analysis and protection of smart grids against false pricing attacks Ph.D. thesis université Paris-Saclay
[32] Deng R, Yang Z, Chow M Y and Chen J 2015 IEEE Transactions on Industrial Informatics 11 570–582
[33] Yan X, Ozturk Y, Hu Z and Song Y 2018 Renewable and Sustainable Energy Reviews 96 411–419
[34] Zhang X, Yang X, Lin J, Xu G and Yu W 2016 IEEE Transactions on Parallel and Distributed Systems 28 170–187
[35] Ma K, Hu G and Spence C J 2014 IEEE Transactions on Control Systems Technology 22 1907–1914
[36] Vlahos A G and Biskas P N 2013 IEEE Transactions on Smart Grid 4 1966–1975
[37] Yi P, Dong X, Iwayemi A, Zhou C and Li S 2013 IEEE Transactions on smart grid 4 227–234
[38] Guo Y, Pan M and Fang Y 2012 IEEE Transactions on Parallel and Distributed Systems 23 1593–1606
[39] Yu R, Yang W and Rahardja S 2012 IEEE Transactions on Smart Grid 3 1734–1742
[40] Namerrkawa T, Okuno N, Sato R, Okawa Y and Ono M 2015 IEEE Transactions on Smart Grid 6 2714–2724
[41] Jiang B and Fei Y 2014 IEEE Transactions on Smart Grid 6 3–13
[42] Ma J, Chen H H, Song L and Li Y 2015 IEEE transactions on smart grid 7 771–784
[43] Laganà D, Mastroiacchini C, Mee M and Renga D 2018 Algorithms 11 145
[44] Gunduz M Z and Das R 2020 Computer networks 169 107094
[45] Jiang W, Wen L, Zhan J and Jiang K 2020 Journal of Systems Architecture 107 101739
[46] Esmailifalak M, Liu L, Nguyen N, Zheng R and Han Z 2014 IEEE Systems Journal 11 1644–1652
[47] Kurt M N, Ogundijo O, Li C and Wang X 2018 IEEE Transactions on Smart Grid 10 5174–5185
[48] Cao J, Wang D, Qu Z, Cui M, Xu P, Xue K and Hu K 2020 IEEE Access 8 95109–95125
[49] Wang K, Du M, Maharjan S and Sun Y 2017 IEEE Transactions on Smart Grid 8 2474–2482
[50] Musleh A S, Chen G and Dong Z Y 2019 IEEE Transactions on Smart Grid 11 2218–2234
[51] Khazaei J 2020 IEEE Transactions on Smart Grid 12 2518–2528
[52] Tang D, Fang Y P, Zio E and Ramirez-Marquez J E 2019 IEEE Access 7 80491–80505

8
[53] Tang D, Fang Y, Zio E and Ramirez-Marquez J E 2018 Analysis of the vulnerability of smart grids to social network-based attacks 2018 3rd International Conference on System Reliability and Safety (ICSRS) (IEEE) pp 130–134
[54] Tan R, Badrinath Krishna V, Yau D K and Kalbarczyk Z 2013 Impact of integrity attacks on real-time pricing in smart grids Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security pp 439–450
[55] Liu Y, Hu S and Ho T Y 2015 IEEE Transactions on Dependable and Secure Computing 13 220–235
[56] Krishna V B, Gunter C A and Sanders W H 2018 IEEE Journal of Selected Topics in Signal Processing 12 790–805
[57] Aljohani N and Bretas A 2021 Applied Sciences 11 6540
[58] Karimipour H, Dehghantanha A, Parizi R M, Choo K K R and Leung H 2019 IEEE Access 7 80778–80788
[59] Shi J, Liu S, Chen B and Yu L 2020 IEEE Transactions on Circuits and Systems II: Express Briefs 68 993–997
[60] Tang D, Fang Y and Zio E 2019 A zero-sum markov defender-attacker game for modeling false pricing in smart grids and its solution by multi-agent reinforcement learning 29th European Safety and Reliability Conference (ESREL2019) pp 3285–3291
[61] Liu Y, Hu S and Zomaya A Y 2016 IEEE Transactions on Industrial Informatics 12 1973–1983
[62] Hao Y, Wang M and Chow J H 2016 IEEE Transactions on Smart Grid 9 3191–3202