Received: 25 March 2022 | Revised: 19 May 2022 | Accepted: 22 June 2022

DOI: 10.1049/rpg2.12541

IET Renewable Power Generation

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Analytical reliability evaluation method of smart micro-grids considering the cyber failures and information transmission system faults

Mehrdad Aslani[1] | Hamed Hashemi-Dezaki[1,2] | Abbas Ketabi[1]

[1]Department of Electrical and Computer Engineering, University of Kashan, Kashan, Iran

[2]Research and Innovation Center for Electrical Engineering (RICE), Faculty of Electrical Engineering, University of West Bohemia (UWB), Pilsen, Czech Republic

Correspondence
Hamed Hashemi-Dezaki, Department of Electrical and Computer Engineering, University of Kashan, 8731753153, Kashan, Iran
Email: hamed.hashemi@kashanu.ac.ir; hhashemi@fel.zcu.cz

Abstract

The reliability of smart micro-grids (SMGs), as a cyber-physical system (CPS), might be influenced by cyber failures and information transmission faults. Several Monte Carlo simulation (MCS)-based approaches have been reported to assess the reliability of SMGs and smart grids. On the other hand, analytical reliability assessment methods have been presented in some research works, while the cyber system has not been concerned. However, the literature shows a research gap in developing an accurate and fast reliability evaluation method for SMGs based on the unavailability of cyber elements and information transmission faults. This article tries to fill the discussed gap by adding the analytical modelling of cyber-physical interdependencies and information transmission faults to available analytical methods, focusing on physical uncertainties. Comparing the proposed model with existing MCS-based and analytical reliability evaluation methods illustrates the advantages of this research. Test results show that less than 5.7% expected energy not supplied (EENS) error occurs by the proposed method, which would be much faster than MCS-based ones. Moreover, the sensitivity analyses highlight the impacts of the cyber network topologies on the cyber-physical interdependencies.

1 | INTRODUCTION

The deployment of distributed energy resources (DERs) has been steadily increasing in recent years [1, 2]. On the other hand, the electrical energy systems have been evolving toward the smart microgrids (SMGs) and smart grids' frameworks [3, 4]. The SMG and smart grid concepts could effectively improve the energy systems' resiliency and reliability [5–7]. By integrating the physical power networks and the cyber ones, the SMGs and modernized electrical energy systems become cyber-physical systems (CPSs) [8, 9]. The smart grids and SMGs will exhibit effective bidirectional data flow, smart monitoring, intelligent control, and other supplementary features, such as self-healing, by the cyber system and information and communication technologies (ICTs). However, asides from the advantages of ICTs and cyber systems, their integration into the physical layer comes with some drawbacks, for example, failures of sub-systems, interdependencies, and vulnerabilities to cyber-attacks [10]. Hence, the ICTs and mal-operation of the cyber system might influence the reliable operation of SMGs [11, 12]. The impacts of cyber-physical interdependencies (CPIs) should also be considered, besides the stochastic behaviours of physical networks, in evaluating the SMG reliability [13–15].

Moreover, new technologies and frameworks have been introduced for ICT-based power systems and smart grids, such as dynamic thermal rating (DTR) systems [16]. Although these frameworks and technologies allow available power/physical sub-systems and transmission lines to be operated much closer to their limits, the eventually intensified outages might threaten system reliability [17, 18]. The steadily growing discussed frameworks and technologies highlight the motivations for studying the ICTs, cyber systems, and their interactive effects on the SMG's reliability.

Different studies have focused on the SMGs' reliability evaluation considering the impacts of cyber-physical systems and the integration of ICTs on physical/power systems [10, 19]. The

Monte Carlo simulation (MCS) is a powerful method for evaluating the SMGs' cyber and physical uncertainties [20, 21]. The direct CPIs have been studied by MCS in [22], while the probabilistic output power of DERs under various scenarios was concerned. Hashemi-Dezaki et al. [23] reported a method based on MCS to assess stochastic behaviours of electric vehicles, DERs, and cyber elements. A sequential MCS-based technique was reported in [16] to evaluate the system reliability in the presence of DTR technologies, considering the communication network availability. In some references, such as [15] and [21], the SMG's reliability has been evaluated by MCS considering the data transmission errors besides the outage of cyber and power elements. Sun et al. [25] reported a fault tree-based reliability assessment model considering the interferences of the cyber network by the MCS. In [26], the MCS has been utilized to evaluate the system reliability, while the uncertainties of DERs and cyber networks have been considered. However, Barani et al. [26] have not taken into account data transmission errors and delays. In [27], the reliability evaluation of multi-microgrids based on the information transmission errors (ITEs) and interdependencies by the MCS has been reported. Although various aspects of the information transmission systems (ITSs) have been considered by Barani et al. [27], the uncertainties of the physical layer, e.g., stochastic behaviours of DERs, have not been studied.

Although the literature shows that much attention has been paid to MCS for assessing the SMGs' reliability, the execution time challenges of MCS-based studies limit their applications [28]. Accordingly, several research works have tried to develop fast and accurate non-MCS approaches. The scenario reduction algorithms have been used to raise the speed of reliability calculations in [29]. Physical uncertainties have been examined by Memari et al. [29] with various clustering algorithms, while the CPIs were not concerned. Hariri et al. [30] presented an analytical method for evaluating the smart grids' reliability considering DERs' probabilistic behaviours. However, the cyber impacts have not been evaluated in [30]. Zhu et al. [31] used complex network theory (CNT) to study the impacts of information interference transfer delays on system reliability. Although the cyber impacts have been examined in the introduced non-MCS reliability evaluation method of [31], the physical uncertainties have not been studied. Non-MCS reliability assessment methods considering direct and indirect CPIs have been introduced in [32, 33], but the physical uncertainties were not modelled.

In Table 1, the comparative review of the available research works in the area of reliability evaluation of SMGs and smart grids has been presented. As revealed by the literature overview, there is a research gap in developing an analytical reliability assessment method considering the CPIs.

One of the essential contributions of this research is to fill a discussed gap. The mathematical modelling of the introduced analytical methods in [30, 48] would be modified and extended to concern the CPIs. The investigation of data transmission impacts on the SMGs' operational reliability in addition to other cyber/physical uncertainties by the proposed analytical method is another contribution. The proposed method is studied under various cyber network topologies based on the redundancy of the MG control centre (MGCC), microcontrollers (MCs), and switches. The accuracy and validation of the proposed method are examined by comparing the obtained test results and the MCS one. The obtained results also compared to available analytical methods, like [30, 48] neglecting the CPIs, to highlight the necessities of CPIs. The comparative test results illustrate the advantages of the proposed analytical method from the viewpoint of accuracy and execution time.

As seen in the summary of the literature review of SMGs' reliability assessment, a gap exists in developing an analytical reliability assessment method that could concern the cyber failures and ITEs. This paper tries to fill such a research gap by proposing a new analytical reliability evaluation method, that comprehensively considers the cyber failures and ITEs, like the MCS-based ones (e.g. [15] and [24]).

The main contributions of this article could be listed as follows:

- Developing a new fast and accurate analytical reliability evaluation method for SMGs, considering the cyber failures and ITEs;
- Mathematical modelling of ITEs, besides the cyber failures, in the proposed analytical reliability evaluation method;
- Considering the MGCC's failures impacts on the SMGs' reliability, which has been received less attention in the literature;
- Comprehensive stochastic modelling of SMGs, including the uncertainties of DERs, failures in physical and cyber elements, and ITEs.

The other technical aspects of the introduced method could be listed as follows to emphasize this research work's advantages in comparison with existing references:

- Validating the obtained results from the introduced analytical reliability method and MCS-ones;
- Comparing the computation time and precision of the proposed method with MCS-based ones to highlight the advantages of the proposed method;
- Developing the new reliability method, using the graph theory to model the SMG's states based on physical/cyber failures and ITEs;
- Modelling the uncertainties of hybrid DERs;
- Studying the impacts of cyber network topologies on the SMGs' reliability;
- Sensitivity analyses to investigate how the changes in crucial parameters could affect the SMGs' reliability.

The remainder of this article is organized as follows. Section 2 presents the mathematical modelling of the proposed analytical reliability evaluation method. Test results and discussions are given in Section 3, and the last section draws conclusions.

2 | MODELLING

The SMGs, which are studied in this research, consist of cyber and physical networks, as shown in Figure 1. The sub-systems

TABLE 1 Comparative literature review of SMG's reliability assessment

		Method			Physical uncertainties			Cyber uncertainties				
Reference	Year	MCS	Clustering	Analytical	PV	WT	Load	Cyber Component Failures	MGCCs Faults	Information Transmission Delay	Information Transmission Error	Routing Error
[15]	2021	✓			✓	✓	✓	✓	✓	✓	✓	✓
[24]	2019	✓				✓		✓		✓	✓	✓
[23]	2017	✓				✓		✓				
[20]	2016	✓			✓	✓		✓				
[32]	2012			✓				✓				
[33]	2014			✓				✓				
[26]	2020	✓			✓	✓		✓	✓			
[29]	2021		✓		✓	✓	✓					
[30]	2019			✓	✓	✓						
[34]	2020	✓										
[35]	2019	✓										
[36]	2011	✓		✓	✓	✓						
[37]	2015	✓			✓	✓						
[38]	2019	✓						✓				
[39]	2021	✓	✓		✓	✓						
[22]	2016	✓			✓	✓		✓	✓			
[40]	2017	✓	✓									
[41]	2020		✓	✓	✓	✓	✓					
[42]	2019			✓	✓	✓	✓					
[43]	2018		✓		✓	✓						
[44]	2021	✓	✓	✓	✓	✓						
[45]	2020	✓						✓	✓	✓	✓	✓
[46]	2019	✓						✓	✓			
[47]	2021	✓						✓	✓			✓
[27]	2022	✓						✓	✓			✓
Proposed method		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓

of the physical layer of the understudy SMG could be listed as follows:

- WTs;
- PVs;
- Microturbines (MTs);
- Energy storage systems (ESSs); and
- Loads.

The renewable and non-renewable DERs are essential parts of SMGs, which enable the energy system to operate in grid-connected, islanded, and stand-alone modes [49, 50]. Depending on the SMG's scale and its capacities, different types of DERs could be interconnected to the SMG [51, 52]. Here, the customer-owned privately-owned DERs, for example, WTs, PVs, and MTs, are considered. In addition, much attention has been paid to ESSs in smart grids and SMGs, while different types and technologies for ESSs have been introduced. This paper considers the battery energy storage systems (BESSs) [53, 54]. However, other ESSs' types and technologies could be studied using the proposed model. It should be highlighted that the failure rate and other reliability specifications of ESS depend on the BESS' technology, which might affect the SMG' reliability.

Electric vehicles and non-fossil fuel-based vehicles, like hydrogen vehicles, are increasingly penetrating [55, 56]. The daily operations of SMG would be affected due to their mobile and highly stochastic charging demands. Vehicle owners' stochastic and uncertain behaviours, such as arrival time, departure time, and driving distance, should be concerned with models considering electric vehicles. The proposed model is adequately flexible to add electric vehicles' charging load

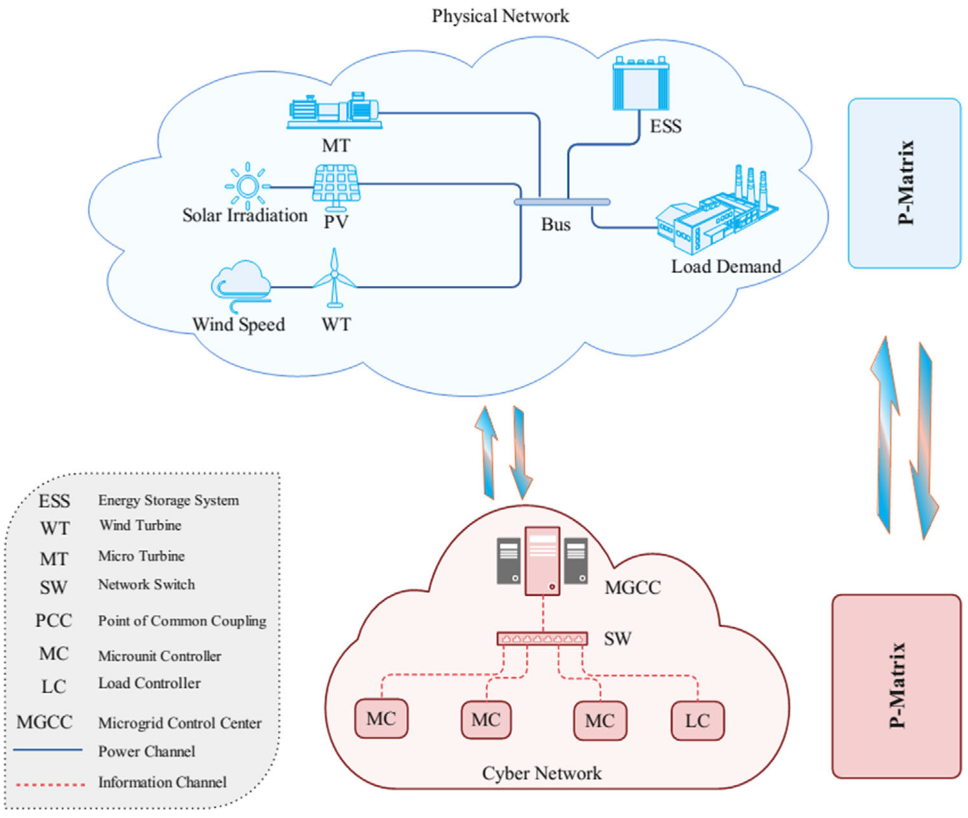


FIGURE 1 Structure of the understudy SMG, as a CPS

because conventional loads' stochastic behaviours and uncertainties have been studied. However, here, electric vehicles and their stochastic nature have not been concerned. Furthermore, extending the proposed model to examine the SMGs' operation and system reliability in the presence of electric vehicles would be an interesting subject for further research works.

Also, the cyber layer of the understudy SMG includes the following elements:

- Micro controllers (MCs);
- Load controllers (LCs);
- Information terminals;
- Information channels;
- Switches; and
- MG control centre (MGCC).

The SMG could be controlled in centralized, decentralized, and distributed control modes [57–59]. This paper has focused on the centralized control mode. The LCs, MCs, information terminals/channels, and switches should be deployed in both control modes of SMGs, while the MGCC is used only in the centralized control mode. In this research, the electrical loads have been concerned. However, if other demands, such as heat and cooling loads, are considered in an integrated multi-carrier energy hub, the proposed study could be extended in the future. Different load controls could be implemented by various LCs depending on the selected energy management paradigms and concerns [60]. The failures and other reliability specifications in the cyber layer's components and elements should be determined according to the hardware and software platforms used in LCs, MCs, MGCC, and ITSs.

In this research, the cyber failures, besides other probabilistic parameters of the physical layer, have been concerned. The unavailability of physical elements [61, 62], the uncertain output power of DERs [63, 64], and stochastic behaviours for load demands [65, 66] are concerned in the proposed analytical reliability assessment method.

It is helpful to illustrate the application ability of the proposed method in the actual smart grid and SMGs. As discussed, evaluating the reliability of smart grids and SMGs is essential. Also, the stochastic behaviours of both cyber and physical subsystems and ITEs might adversely affect the system's reliability. Hence, it is inevitable to evaluate the SMGs' reliability, considering the uncertainties of the physical and cyber layers, besides the ITEs. On the other hand, the MCS-based methods are time-consuming, and they cannot be applicable for large-scale smart grids, reliability-based optimization problems, particularly by the metaheuristic algorithms, and real-time operational decisions. The proposed analytical reliability assessment method is adequately fast and accurate. Accordingly, it can be applied to actual smart grids and SMGs.

The probability matrix (P-Matrix) is created for cyber and physical layers. In addition, the cyber failures are mapped to the

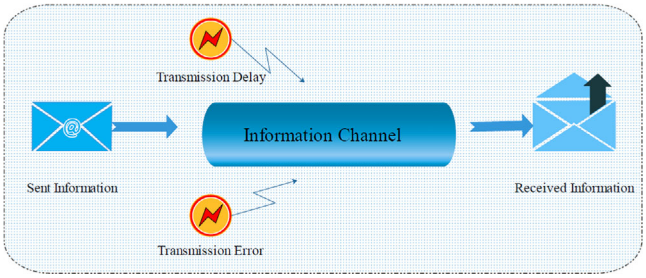


FIGURE 2 Conceptual diagram of information channels and their malfunctions [24]

physical layer, and the probability matrix of the physical layer should be updated. Also, as depicted in Figure 2, the malfunction of the information channel, for example., routing errors, transmission delays, and ITEs [24, 67], are considered in this research.

Finally, the proposed model determines the microgrid state matrix (MGSM) based on the physical/cyber failures and ITEs using the probability matrix of cyber and physical layers.

The MG's state should be distinguished to assess the reliability indices. In addition, determining the states of MG's elements to create the MG's state is essential [44]. In the proposed analytical model based on the state matrix, the element state matrix (ESM) could be defined using (1) [48]. The states of each element are assigned to the first column arrays, and the second column arrays represent the probability of states. Considering the states of cyber elements besides the physical ones is one of this research contributions. Furthermore, the states corresponding to delay, routing, and data errors are defined for each information line connecting two cyber elements.

$$ESM_i = \begin{bmatrix} ES_{i,1} & \mathrm{Pr}_{i,1}^{ES} \\ \vdots & \vdots \\ ES_{i,j} & \mathrm{Pr}_{i,j}^{ES} \\ \vdots & \vdots \\ ES_{i,N_{ES}^i} & \mathrm{Pr}_{i,N_{ES}^i}^{ES} \end{bmatrix}_{N_{ES}^i \times 2} \quad i = 1 : N_C + N_P \tag{1}$$

The number of states for cyber elements and physical ones without stochastic behaviours, such as MTs, would be two because of their availability and unavailability, as mathematically expressed in (2). Otherwise, the states for stochastic elements like WTs and PVs should be determined according to discretized states and corresponding probabilities.

$$ESM_k = \begin{bmatrix} ES_{k,1} = 1 & \mathrm{Pr}_{k,1}^{ES} = A_k \\ ES_{k,2} = 0 & \mathrm{Pr}_{k,2}^{ES} = U_k \end{bmatrix}_{N_{ES}^i \times 2 = 2 \times 2} \quad k = 1 : K \tag{2}$$

As expressed in (3), the packet includes payload and header information [24]. As the first part of the packet's information, the payload would be the information that should be transmitted within the information channel. The voltage, power, current, status of switches, and interconnections of DGs could be the payload information, which is transmitted within the information channel. The header information is the second part of the packet's information. The address of the information that should be sent is assigned in the header information. For instance, in the understudy centralized SMG, the qth element (one of LCs or MCs) sends the information, including the voltage, current, or power, to the MGCC. The destination of the information (header) is the MGCC, and the payload would be the electrical information that should be sent to the MGCC from the LCs/MCs.

In (3), the ideal ITS has been presented, where the received signal would be the same as the sent data. Also, the header at the destination of the information line is not different from the header at the initial terminal. However, as shown in (4), the delay and payload error might appear in the information transmission procedure. Moreover, the header errors might influence the packet data at the destination terminal, as mathematically expressed in (5). The information transmission sent packet data and received packet data considering the ITEs could be expressed using (3)–(5).

$$PD_{Destination}^{T_q,T_{q'}} \left[S_{Destination}^{T_q,T_{q'}}(t), Header_{Destination}^{T_q,T_{q'}} \right] = PD_{Origin}^{T_q,T_{q'}} \left[S_{Origin}^{T_q,T_{q'}}(t), Header_{Origin}^{T_q,T_{q'}} \right] \tag{3}$$

$$S_{Destination}^{T_q,T_{q'}}(t) = S_{Origin}^{T_q,T_{q'}}(t + D) + SE \tag{4}$$

$$Header_{Destination}^{T_q,T_{q'}} = Header_{Origin}^{T_q,T_{q'}} + HE \neq Header_{Origin}^{T_q,T_{q'}} \tag{5}$$

To concern the information transmission interruptions in the proposed analytical model, an element state is assigned to each cyber link connecting two cyber elements. The discussed element is defined based on corresponding states for the delay and header error, as described in (6). The cyber link (CL) state will be considered 1 if the information transmission has not been adversely affected due to delay and header errors. The state of CL is modelled using (7) based on Boolean variables regarding the delay, payload, and header errors.

$$ESM_c = \begin{bmatrix} ES_{c,1} = CL_c = 1 & \mathrm{Pr}_{c,1}^{ES} \\ ES_{c,2} = CL_c = 0 & \mathrm{Pr}_{c,2}^{ES} \end{bmatrix}_{2 \times 2} \quad c = 1 : C \tag{6}$$

$$CL_c = BV_c^{Delay} \times BV_c^{Header} \tag{7}$$

As given in (8), the one value is assigned to the corresponding Boolean variable if the appeared delay is less than the maximum allowed delay for the information transmission links and channels.

Different probability distributions have been extracted according to the statistical nature of delays in ITSs. The uniform, exponential, and normal distributions have been studied in [68]. The exponential probability distribution could be a well-known alternative for modelling the statistical behaviour of information transmission delays in MGs [69, 70]. Also, practical experiments in [64] and [65] have been presented to verify the distribution of delays in ITSs. It has been reported in [15, 20], the references in the field of SMGs' information systems, that the delay in ITSs of SMGs usually follows the exponential distribution. Hence, the selected probability distribution for delays in the ITS of SMGs could be adequately trustable. However, [64] and [65] are only referring to generic networked control systems. On the other hand, different probability distributions have been reported for delays in ITSs, such as those of SMGs and smart grids. It should be noted that the proposed model is adaptable to use various probability distributions for delays in information channels. The delay state matrix for each cyber link could be presented by (9)–(11).

$$BV_c^{Delay} = \begin{cases} 1 & D_c \leq D^{\max} \\ 0 & Otherwise. \end{cases} \tag{8}$$

$$DSM_c = \begin{bmatrix} BV_c^{Delay} = 1 & \Pr\left(D_c \leq D^{\max}\right) \\ BV_c^{Delay} = 0 & \Pr\left(D_c > D^{\max}\right) \end{bmatrix} \tag{9}$$

$$\Pr\left(D_c \leq D^{\max}\right) = 1 - e^{-D^{\max}\mu_{Delay}} \tag{10}$$

$$\Pr\left(D_c > D^{\max}\right) = 1 - \Pr\left(D_c \leq D^{\max}\right) \tag{11}$$

It should be noted that the end-to-end delay in information channels depends on several parameters, for example, the computational capability of cyber elements and information terminals based on their hardware, the real-time operating systems, the application execution times, communication links' speed, the transmission distance, the cyber network topology, and congestion status [71]. The transmission distance effectively affects the delay in the ITS. If the transmission distance increases, the delay and its eventual impacts on the system reliability might be highlighted.

The header errors (HEs) are considered in the states of cyber links, focusing on ITEs, as demonstrated in (12)–(15). The modelling of the HEs is similar to that of delays, and the states of cyber links considering the HEs could be defined by (12)–(15).

$$BV_c^{Header} = \begin{cases} 1 & There\ is\ no\ header\ error. \\ 0 & Otherwise. \end{cases} \tag{12}$$

$$HSM_c = \begin{bmatrix} BV_c^{Header} = 1 & U_c^{HE} + A_c^{HE} \times \Pr\left(\left|HE_c\right| \leq HE^{\max}\right) \\ BV_c^{Header} = 0 & A_c^{HE} \times \Pr\left(\left|HE_c\right| > HE^{\max}\right) \end{bmatrix} \tag{13}$$

$$\Pr\left(HE_c \leq HE^{\max}\right) = CDF\left(HE^{\max}\right) \tag{14}$$

$$\Pr\left(HE_c > HE^{\max}\right) = 1 - \Pr\left(HE_c \leq HE^{\max}\right) \tag{15}$$

In the proposed method, the payload errors in the information transmission of SMGs are considered. The proposed state matrix's definition and mathematical modelling of the payload errors have been shown in (16)–(18). As shown, the payload state matrix (PLSM) is generated by discretizing the payload errors based on an appropriate probability distribution like Gaussian white noise. Since the noise interference is time-varying, the error values in the payload usually follow the Gaussian white noise distribution [24, 72]. The appropriate CDF is used to determine the discretized payload errors and corresponding probability. In addition to the value of the payload errors, the probability of payload error should be concerned in the PLSM. If the payload error does not appear, the payload state of the understudy information channel would be zero. Otherwise, the payload error should be determined, and the payload error probability and the probability of each interval for the payload error values are multiplied together. The payload errors based on PLSM should be used to update the transmitted data of information channels.

$$PLSM_c = \begin{bmatrix} PLS_{c,1}^{Payload} & \Pr_{c,1}^{Payload} \\ \vdots & \vdots \\ PLS_{c,e}^{Payload} & \Pr_{c,e}^{Payload} \\ \vdots & \vdots \\ PLS_{c,N_c^{PLS}}^{Payload} & \Pr_{c,N_c^{PLS}}^{Payload} \end{bmatrix} \tag{16}$$

$$PLS_{c,e}^{Payload} = \begin{cases} 0 & e = 1 \\ SE_c^{\min} + \frac{2(e-1)-1}{2} \times \left(\frac{SE_c^{\max} - SE_c^{\min}}{N_c^{PLS} - 1}\right) & e = 2 : N_c^{PLS} \end{cases} \tag{17}$$

$$\Pr_{c,e}^{Payload} = \begin{cases} \left[\left(1 - A_c^{SE}\right) + \left(A_c^{SE} \times \left[\begin{array}{l} CDF\left(\frac{1}{2} \times \left(\frac{SE_c^{\max} - SE_c^{\min}}{N_c^{PLS} - 1}\right)\right) \\ -CDF\left(-\frac{1}{2} \times \left(\frac{SE_c^{\max} - SE_c^{\min}}{N_c^{PLS} - 1}\right)\right) \end{array}\right]\right)\right] & e = 1 \\ A_c^{SE} \times CDF\left(SE_c^{\min} + \frac{1}{2} \times \left(\frac{SE_c^{\max} - SE_c^{\min}}{N_c^{PLS} - 1}\right)\right) & e = 2 \\ A_c^{SE} \times \left[\begin{array}{l} CDF\left(SE_c^{\min} + \frac{2(e-1)-1}{2} \times \left(\frac{SE_c^{\max} - SE_c^{\min}}{N_c^{PLS} - 1}\right)\right) \\ -CDF\left(SE_c^{\min} + \frac{2(e-2)-1}{2} \times \left(\frac{SE_c^{\max} - SE_c^{\min}}{N_c^{PLS} - 1}\right)\right) \end{array}\right] & e = 3 : N_c^{PLS} \end{cases} \tag{18}$$

Accordingly, the MG's state matrix (MGSM) could be defined as corresponding to states of sub-systems and elements, as presented in (19). The states of physical and cyber elements are considered to generate the system state. Also, the states for cyber links and corresponding payload errors are concerned.

The probability of each state for the MG, depending on its sub-system's states, is determined by (20).

$$MGSM_l = \begin{bmatrix} ES_{1,j} & \Pr^{ES}_{1,j} \\ \vdots & \vdots \\ ES_{i,j'} & \Pr^{ES}_{i,j'} \\ \vdots & \vdots \\ ES_{N_C+N_P+2C,j''} & \Pr^{ES}_{N_C+N_P+2C,j''} \end{bmatrix}_{(N_C+N_P+2C)\times 2} \quad \begin{matrix} l = 1 : N_{MGS} \\ \forall j \in 1 : N^1_{ES} \\ \forall j' \in 1 : N^i_{ES} \\ \forall j'' \in 1 : N^{N_C+N_P+2C}_{ES} \end{matrix} \tag{19}$$

$$\underset{l}{\overset{MGS}{\Pr}} = \prod_{i=1}^{N_C+N_P+2C} \left(\underset{i,j'}{\overset{ES}{\Pr}} \right) \quad \forall j' \in 1 : N^i_{ES} \tag{20}$$

To assess the adequacy and reliability, it is necessary to distinguish that a power channel and an information channel exist for transmitting the power from the supply side to the demand side. Hence, the graph matrix (GM) and graph of the understudy MG should be defined. In (21), the cyber-cyber link matrix (CCLM) to generate the graph of the cyber network based on cyber-cyber links (CC) and their states is defined.

The links connecting cyber elements/terminals should be identified to investigate the graph of the cyber network and the system graph. The state of cyber links between two cyber elements is represented by ($CL_{j',i'}$) in (21). Moreover, cyber-cyber links/indicators ($CC_{j',i'}$)should be defined. The cyber links are considered according to cyber network topology and the communication lines. There is an information channel between two cyber elements; if there is a cyber link, its state would be up. Otherwise, the discussed two cyber elements are not directly interconnected.

$$CCLM_l = \begin{bmatrix} ES_1 & \cdots & (CL_{1,i'} \times CC_{1,i'}) & \cdots & (CL_{1,N_C} \times CC_{1,N_C}) \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ (CL_{i',1} \times CC_{i',1}) & & ES_{i'} & & (CL_{i',N_C} \times CC_{i',N_C}) \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ (CL_{N_C,1} \times CC_{N_C,1}) & \cdots & (CL_{N_C,i'} \times CC_{N_C,i'}) & \cdots & ES_{N_C} \end{bmatrix} \tag{21}$$

The cyber network graph (CNG) is generated using the graph function and the CCLM at each state of the MG, as shown in (22). The input of the graph function has determined the elements/nodes of the system graphs, and the cyber and physical links determine the graph's lines. Afterward, the information channel (IC) between two cyber elements (terminals) through different paths should be determined using (23). The short path function (SPF) has been used to determine the information channels between two cyber terminals.

$$CNG_l = \text{graph}\,(CCLM_l) \tag{22}$$

$$IC^l_{i',i''} = \begin{cases} 1 & If \sum SPF\left(CNG_l, CE_{i'}, CE_{i''}\right) \geq 1 \\ 0 & If \sum SPF\left(CNG_l, CE_{i'}, CE_{i''}\right) = 0 \end{cases} \tag{23}$$

The physical–physical links are used to generate the graph matrix for the physical layer of the MG, as given in (24). The graph of the physical layer of the MG should be generated to evaluate the system's reliability.

$$PPLM_l = \begin{bmatrix} ES_{N_C+1} & \cdots & PP_{1,r} & \cdots & PP_{1,N_C} \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ PP_{r,1} & & ES_{N_C+r} & & PP_{r,N_C} \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ PP_{N_C,1} & \cdots & PP_{N_C,r} & \cdots & ES_{N_C+N_P} \end{bmatrix} \tag{24}$$

Also, the impacts of cyber failures and ITEs (delay and header error) on the MG reliability are mapped to the physical layer using the information channel status, as explained in (23). Hence, the graph matrix of the physical layer should be updated due to eventual interruptions for the corresponding information channel, as mathematically expressed in (25). The graph of the physical layer is generated by the upgraded physical network matrix by (26). Thus, the power channel between physical points and terminals, considering the cyber failures and information errors, is distinguished (27).

$$PPLM_l \rightarrow PPLM'_l : ES'_{N_C+r} = ES_{N_C+r} \times \prod_{c=1}^{L_r} \left(IC_{i',i''}^{l,c} \Big|_{(CP_{i',r} + CP_{i'',r}) \geq 1} \right) \tag{25}$$

$$PNG_l = \text{graph}\left(PPLM'_l\right) \tag{26}$$

$$PC_{r',r''}^{l} = \begin{cases} 1 & If \sum SPF\left(PNG'_l, PE_{r'}, PE_{r''}\right) \geq 1 \\ 0 & If \sum SPF\left(PNG'_l, PE_{r'}, PE_{r''}\right) = 1 \end{cases} \tag{27}$$

Moreover, the payload error states are used to update the states of physical elements according to (28) using the corresponding payload states.

$$PPLM'_l \rightarrow PPLM''_l : ES''_{N_C+r'} = ES'_{N_C+r'} + SE_{N_C+r'} \tag{28}$$

The state matrix for WT based on its stochastic behaviour as a function of metrological factors like the wind speed could be defined by (29)–(30) [30]. Technical specifications and statistical parameters for the wind speed are used to generate the state matrix of the WT [73, 74]. Different probability distributions have been reported for the statistical modelling of wind speed and WTs [75, 76]. The Weibull distribution is one of the most popular ones. The Weibull or other probability distributions could be used to determine the probability of WT output power states [77]. More details about the reliability modelling of the WT using the state matrix/probability table could be found in [30].

A similar state matrix should be generated for the PV unit based on statistical records of metrological factors and technical specifications of PV modules [78]. In (31), the mathematical modelling of the PV unit's output power has been demonstrated. The probability of each state could be determined using the appropriate CDF based on recorded statistical data [79, 80].

$$ESM_{PV}(s,1) = \begin{cases} 0 & s = 1:6\tau \ or \ s = 18\tau : 24\tau \\ P_{rated}^{PV} \times \left[\left(\dfrac{\mathrm{mod}(s,\tau)}{(\tau)} \times \left(SCI_s^{\max} - SCI_s^{\min}\right) \right) + \left(\dfrac{[\mathrm{mod}(s,\tau) - 1]}{(\tau)} \times \left(SCI_s^{\max} - SCI_s^{\min}\right) \right) \right] & s = 6\tau + 1 : 18\tau \end{cases} \tag{31}$$

The states of ESS's available energy and power at each time step depend on PV and WT output power and load demands during previous time steps. Hence, it is necessary to record the historical data for the ESS's SOC and available output power. Also, if the historical data for ESS does not exist, it is necessary to simulate the behaviours of ESS using the MCS. Afterward, the ESS states are determined by (32).

$$ESM_{ESS} = \begin{bmatrix} 0 & U_{ESS} + CDF\left(SOC^{\min}\right) \\ P_{rated}^{ESS} & A_{ESS} \times \left(1 - CDF\left(SOC^{\min}\right)\right) \end{bmatrix} \tag{32}$$

As explained, the stochastic behaviours on the supply and demand sides of the physical layer of the SMG and the uncertainties of the cyber layer and ITS are studied in the introduced model. Some of these stochastic parameters and sub-systems, particularly in the physical layer, are chronologically dependent, and interactive correlations exist [81, 82]. The time-sequence, auto-correlation, and cross-correlation of DERs and loads in the physical layer of the SMG might affect the

$$ESM_{WT}(w,1) = \begin{cases} 0 & w = 1 \\ \dfrac{\left[P_{rated}^{WT} \times \left(\dfrac{(2w+1)}{\left(N_{WT}^{ESM} - 2\right)} \times v_{rated} \right) \right]}{2} & w = 2 : N_{WT}^{ESM} - 1 \\ P_{rated}^{WT} & w = N_{WT}^{ESM} \end{cases} \tag{29}$$

$$ESM_{WT}(w,1) = \begin{cases} CDF(v_{ci}) + \left[1 - CDF(v_{co})\right] + U_{WT} & w = 1 \\ \dfrac{\left[CDF\left(\dfrac{(w+1)}{\left(N_{WT}^{ESM} - 2\right)} \times v_{rated} \right) + CDF\left(\dfrac{(w)}{\left(N_{WT}^{ESM} - 2\right)} \times v_{rated} \right) \right] \times A_{WT}}{2} & w = 2 : N_{WT}^{ESM} - 1 \\ \left[CDF(v_{co}) - CDF(v_{rated})\right] \times A_{WT} & w = N_{WT}^{ESM} \end{cases} \tag{30}$$

developed analytical reliability evaluation model, considering various uncertainties [83, 84].

The recorded and measured data for stochastic parameters, considering their time-sequence correlation, should be used to generate the state matrices [85]. According to the time-sequence correlations, the multi-dimension state matrices will effectively mitigate the challenges corresponding to the correlations between stochastic sub-systems and their parameters. The time-dependency attributes and the correlations between stochastic parameters are considered in the proposed model because all state matrices are generated based on certain time steps, and the reliability evaluation is done at each time step separately [86]. However, supplementary studies using advanced techniques to investigate the correlations between uncertain parameters are interesting in future works.

The state matrix for MT would be created based on its availability and unavailability. If the MT unit is available, its rated power is achievable because it is not stochastic. Furthermore, the load states should be considered based on discretized values of historical data or simulated ones by MCS [30, 42].

Finally, the loss of energy (LOE) and reliability indices, such as expected energy not supplied (EENS) and system average interruption duration index (SAIDI), could be evaluated using (33)–(36) by the proposed analytical method. Furthermore, it is necessary to be concerned about other technical constraints besides the power balance condition [87].

$$\Delta LG_l = ES_l^{load} - \sum_{g=1}^{G}\left(ES_{g,l}^{DG} \times PC_{g,l}^{DG}\right) - ES_l^{ESS} \tag{33}$$

$$LOE_l = Max\{0, \Delta LG_l\} \tag{34}$$

$$EENS = \sum_{l=1}^{N_{MGS}}\left(LOE_l \times \Pr_l^{MGS}\right) \tag{35}$$

$$SAIDI = \frac{EENS}{\bar{P}_{load}} \tag{36}$$

In Figure 3, the flowchart of the proposed reliability evaluation method for SMGs considering the failures in the cyber layer and ITEs is shown.

3 | TEST RESULTS

The proposed method is applied to an SMG, and its physical architecture is shown in Figure 1 [24]. Also, different cyber topologies are studied for selected SMG, as shown in Figure 4 [15].

Applying the proposed method to a test system, which has been reported in available references, is useful to compare the obtained results and highlight the declared advantages. On the other hand, the test system introduced in [15] has been modified to be practical using the actual specifications. However, future works would be useful to apply the proposed method to

TABLE 2 MTTF and MTTR data of SMG's elements [15, 21, 35]

Element	MTTR (h)	MTTF (h)
MT	100	7500
ESS	7.8	50,700
PV	40	17,500
WT	279	11,380
Information terminal	24	13,300
MGCC	48	35,040
Optical fibre	4	500,000
Network switch	48	43,800

TABLE 3 ITEs and information transmission interruptions [15, 24, 38]

Parameters	Values
Average payload error (f/year)	0.0001
Deviation of payload error (f/year)	0.01
Average of the routing error (f/year)	0.0001
Deviation of routing error (f/year)	0.01
Mean value of delay in information transmission links (s)	1.0
Upper bound for the tolerable delay in information transmission links (s)	6.0

SMGs in various climates, different sectors (residential, industrial, commercial), and special consumptions, like SMGs for the hospital and critical infrastructure systems.

There is no redundancy for cyber elements in the first cyber network topology, as shown in Figure 4a. This cyber network topology is economical and easy to install. However, the required information channels for energy terminals might be threatened due to any failure. The redundancies for switches, controllers/observers, and the MGCC have been considered in other cyber network topologies. As seen in Figure 4b, two switches have been considered for the second cyber network topology. The redundancy for the LCs and MCs has been added to the cyber network topology in the third topology, as given in Figure 4c, while the fourth topology in Figure 4d has the MGCC redundancy besides the redundant switches and information terminals.

As shown, an MT has been installed in the studied SMG. The rated capacity of this MT has been assumed to be 100 kW. Also, 0.1 p.u has been considered for the minimum permitted operating power of MT. The capacity of ESS has been assumed to be 500 kWh/10 kW. The actual recorded 15-min load values for a portion of Kashan Electrical Power Distribution Company have been used for this study. The metrological data of the centre area of Iran based on measured/reported data of the Renewable Energy and Energy Efficiency Organization (SATBA) have been utilized to generate the state matrices of WT and PV units [88].

In Table 2, the mean-time to failure (MTTF) and mean time to repair (MTTR) parameters for SMG's elements have been

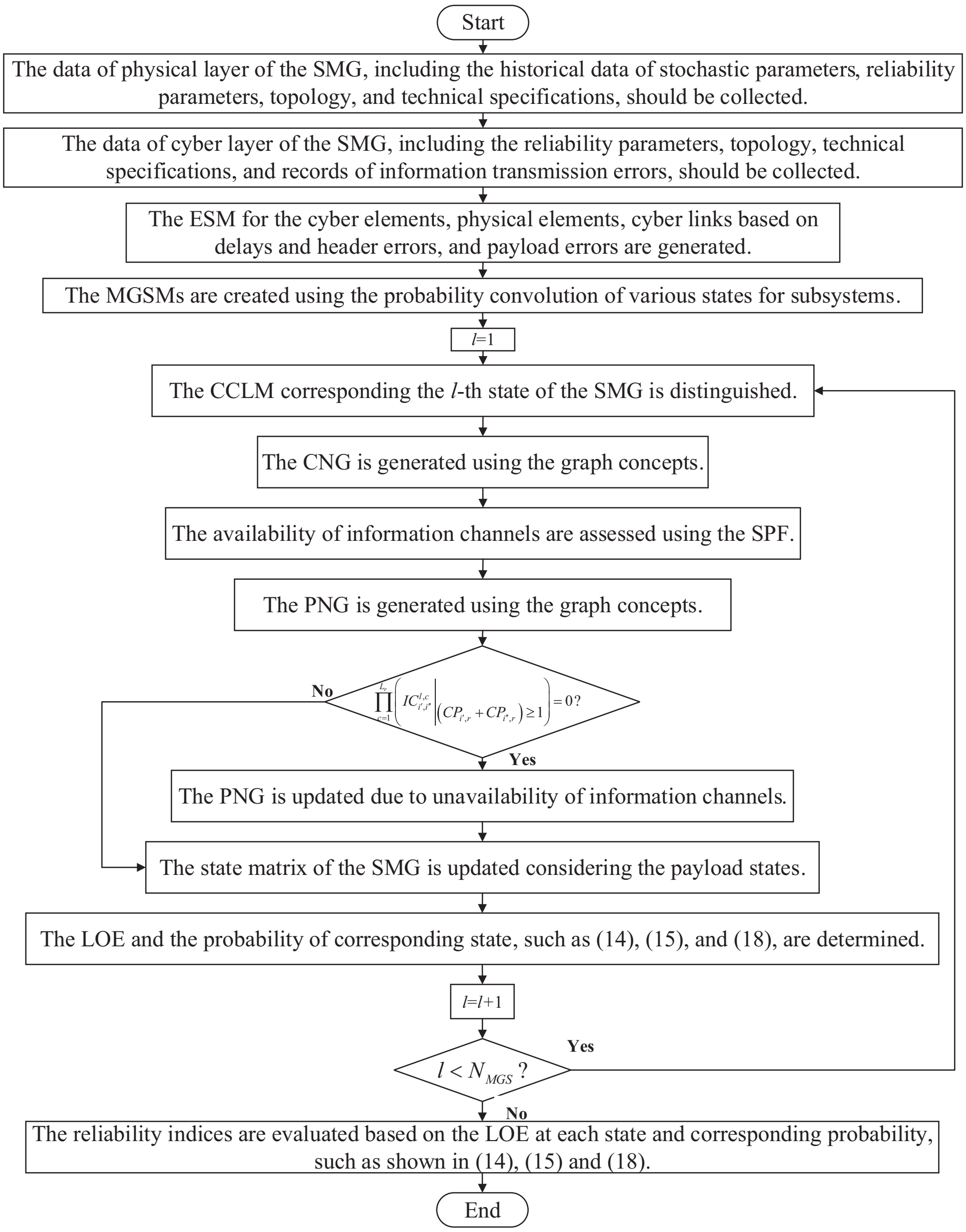


FIGURE 3 Flowchart of the proposed analytical reliability assessment method for SMGs considering the cyber layer and ITEs

reported. The data for ITEs also is given in Table 3 [15, 21, 35]
.

As discussed, the metric must take into account any potential topological changes in communication networks/cyber systems and the physical layer's elements. The cyber-cyber link matrix (CCLM) should be determined using the system state in the proposed model. Afterward, the theory graph's functions and concepts are used to draw the graph of the cyber network. It is possible to distinguish whether any cyber element's failure has affected the SMG or whether the SMG can operate properly within the discussed cyber element's failure. For instance, the graph of the understudy SMG in the second cyber network topology (Figure 4b), while all cyber elements work properly, is shown in Figure 5a. If the13th element (the optic fibre connecting the MC of the ESS to one of the switches) experiences a failure (as an example), the system graph changes to a new graph and interconnections, as depicted in Figure 5b. However, the SMG is not affected due to any failure in the 13th element because other physical and cyber nodes have remained interconnected. Moreover, if failures simultaneously occur in the 13th and 5th (the switches interconnected with the ESS through the optic fibre) SMG's element, the system graph changes to a new graph, as shown in Figure 5c. As depicted, the interconnections of some nodes (like node 1 (MGCC) and 14 (MC of the ESS)) have been interrupted. Hence, the SMG is affected due to simultaneous failures in the 5th and 13th elements.

The selected test system is studied under various DG technology scenarios:

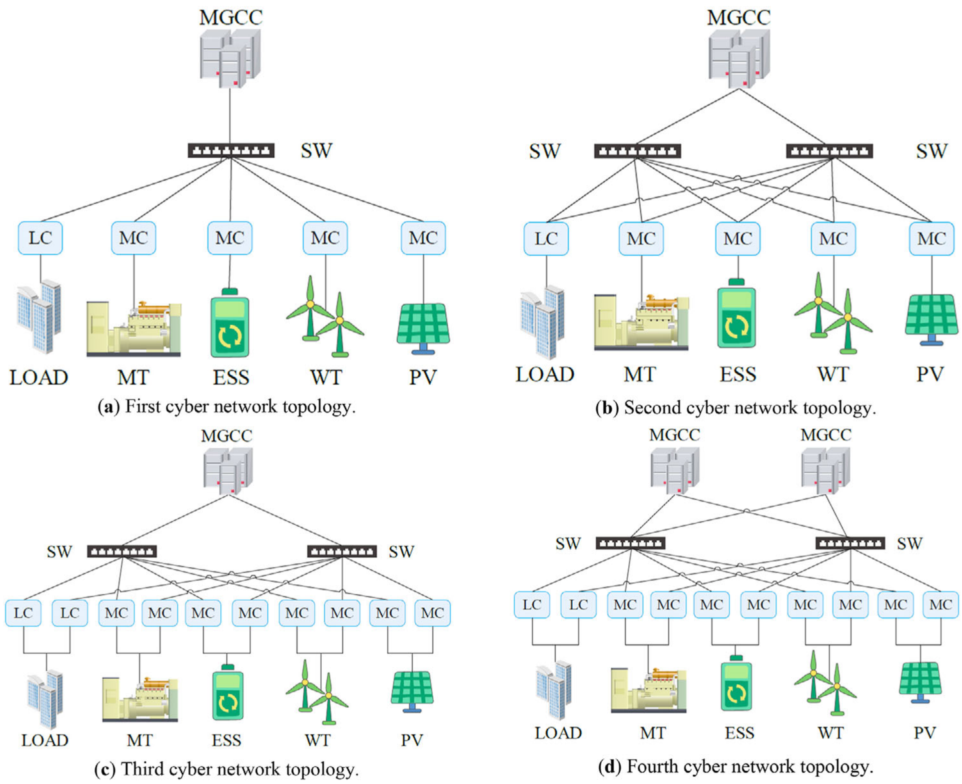


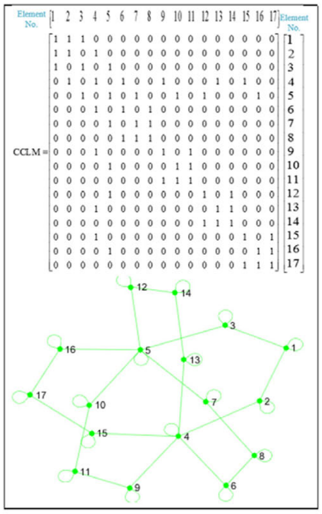
FIGURE 4 Conceptual diagram of information channels and their malfunctions [24]. (a) First cyber network topology. (b) Second cyber network topology. (c) Third cyber network topology. (d) Fourth cyber network topology

TABLE 4 Test results for different cyber network topologies with the ideal MGCC

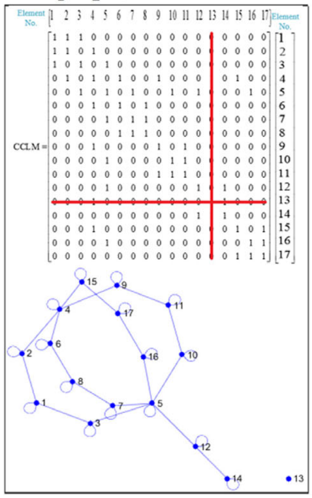
		Proposed analytical method			MCS-based method of [24]	
Scenario no.	Topology no.	EENS error (%)	EENS (kWh/year)	SAIDI (h)	EENS (kWh/year)	SAIDI (h)
1	1	0.3	5260.2	83.0038	5277.8	78.007
	2	0.1	4073.2	64.2734	4075.4	61.581
	3	5.2	3723.9	58.7613	3929.5	57.656
	4	5.2	3723.9	58.7613	3929.5	57.656
2	1	2.6	6466.6	102.0410	6641	98.393
	2	3.1	5263.6	83.0577	5431.3	82.291
	3	5.7	4651.5	73.3998	4933.8	72.63
	4	5.7	4651.5	73.3998	4933.8	72.63
3	1	3.6	5676.5	89.5729	5481.7	84.682
	2	1.9	4555.5	71.8844	4645	70.387
	3	3.8	4018.5	63.4106	4175.5	62.704
	4	3.8	4018.5	63.4106	4175.5	62.704

- Scenario 1: A 50 kW WT unit has been installed for the SMG, and there is no PV unit;
- Scenario 2: A 50 kW PV unit has been installed for the SMG, and there is no WT unit;
- Scenario 3: A hybrid WT-PV system is considered for the SMG, while the capacities of PV and WT units are 25 kW.

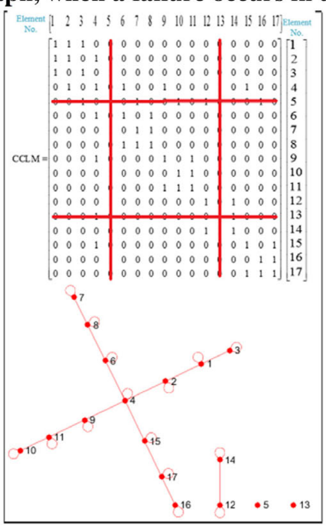
In Table 4, test results using the proposed analytical method under various scenarios for different cyber network topologies, with the ideal MGCC without any failure, have been presented. To validate the proposed analytical model for reliability assessment of SMG considering cyber failures and ITEs, the obtained results are compared with the available MCS-based method of [24].



(a) SMG's graph, when all elements are available.



(b) SMG's graph, when a failure occurs in the 13-th cyber element.



(c) SMG's graph, when the failure occurs in the 13-th and 5-th cyber elements.

FIGURE 5 Understudy SMG's graph for typical conditions

TABLE 5 Comparative analysis of the execution time of the proposed model under various scenarios

Scenario No.	Simulation time (s)	
	MCS-based methods, like [15]	Proposed analytical method
Scenario 1	33,063.615	1.42
Scenario 2	36,382.654	1.74
Scenario 3	42,906.12	2.12

The EENS values obtained by the MCS have been considered as the references, and the differences between test results using the proposed analytical method for the SMG and an ideal MGCC with these reference results have been calculated. The comparative test results infer that the maximum inaccuracy of the proposed analytical method is less than 5.7%. The accuracy level of the proposed method in various cases and different network topologies is satisfying. The studies show that the proposed method accuracy is adequately robust against the changes in cyber network topology and DG technology scenarios.

In Table 6, test results using the proposed analytical method under various scenarios for different cyber network topologies, considering the MGCC failures, have been presented. Also, test results by applying the proposed analytical method have been compared with [15], evaluating the reliability of SMGs based on the MGCC failures, besides other SMG cyber and physical uncertainties.

The computation time of the proposed model compared to MCS-based ones is an essential advantage of this research. As shown in Table 5, the computation times of reliability evaluation of the understudy SMG for the fourth cyber network topology (with the maximum number of cyber elements and corresponding system state) using the MCS, like the method of [15], under Scenarios 1, 2, and 3 are 33,063.615, 36,382.654, and 42,906.12s, respectively. On the contrary, the 1.42, 1.74, and 2.12 s are the computation times of the proposed method under Scenarios 1, 2, and 3 for the fourth cyber network topology, respectively. In this article, the simulations and programming have been implemented in MATLAB 2018b, while an Intel(R)-Core(TM) i7-8550U, CPU @ 1.80 GHz, 1.99 GHz, RAM 12.0 computer has been used. It should be clarified that the MCS-based methods' computation time depends on the number of iterations. However, regardless of the number of MCS iterations, the significant difference between the computation times of the proposed method and available MCS ones is clear.

The obtained test results have approved the declares about the execution time, accuracy, and applicability for actual test systems. Although the test system in this article is not large-scale, the significant decrement in execution times illustrates that the proposed method will be effective for actual test systems. The benefits of the introduced analytical model based on its computation time aspects, especially for actual smart grids, including complicated cyber-physical systems and ITS, are emphasized. This is mainly because the time-consuming MCS-based approaches will not be reasonable for evaluating the system's reliability. Moreover, other technical issues, for example, lack of memory, might appear for actual and large-scale smart grids, which are mitigated by the proposed analytical method. The findings of this study from the viewpoint of speed and precision of the analytical reliability evaluation model for SMGs are highlighted in the discussed issues, while the execution time is emphasized.

The comparative analysis implies that the MGCC failures in cyber network topologies without redundancy of the MGCC might increase the EENS. On the contrary, the EENS increment for the fourth cyber network topology (with the redundancy of the MGCC) is not significant. The comparison

TABLE 6 Test results for different cyber network topologies considering the MGCC failures

		Proposed analytical method			MCS-based method of [15]	
Scenario no.	Topology no.	EENS error (%)	EENS (kWh/year)	SAIDI (h)	EENS (kWh/year)	SAIDI (h)
1	1	0.5	6035.4	95.2370	6004.5	89.71
	2	1.1	4848.4	76.5065	4796.4	73.571
	3	2.9	4494.0	70.9134	4627.4	68.616
	4	4.6	3750.3	59.1792	3929.5	57.656
2	1	1.5	7257.5	114.5218	7368	110.1
	2	1.6	6054.5	95.5384	6152.2	94.281
	3	3.4	5437.6	85.8033	5631.7	83.59
	4	5.7	4653.1	73.4252	4933.8	72.63
3	1	4.0	6448.0	101.7468	6199.7	95.523
	2	1.8	5327.8	84.0707	5425.5	81.748
	3	2.7	4783.6	75.4843	4917.7	74.266
	4	3.8	4017.0	63.3865	4175.5	62.704

TABLE 7 Comparative test results of the proposed analytical method and available ones like [30], neglecting the cyber network failures

		Analytical method of [30] without consideration of cyber failures		
Scenario No.	Topology No.	EENS error due to cyber failures (%)	EENS (kWh/year)	SAIDI (h)
1	1	38.6	3705.6	58.4737
	2	36.56		
	3	17.54		
	4	1.19		
2	1	34.94	4616.8	72.8513
	2	23.74		
	3	15.09		
	4	0.78		
3	1	38.08	3992.2	62.9955
	2	25.07		
	3	16.54		
	4	0.62		

of the proposed method and the MCS-based method of [15] illustrates that the desired accuracy is achievable applying the proposed analytical method considering different failures, including the MGCC failures.

Comparing the test results with other available analytical methods like [30], neglecting the cyber failures and ITEs is another comparative analysis that illustrates the advantages of the proposed method. In Table 7, the obtained test results using the proposed analytical method have been compared to test results based on [30], and the EENS errors due to non-consideration of cyber failures have been calculated.

The significant inaccuracy due to neglecting the cyber failures is the first result that claims attention in the comparative studies of Table 7. Regardless of the DG technology scenarios, the maximum EENS increments due to cyber failures have appeared in the first cyber network topology. This is mainly because of the significant negative impacts of cyber interdependencies, where there is no redundancy for cyber elements. As revealed by test results, the suitable cyber network system with adequate redundancy, the EENS increment due to cyber interdependencies could be limited. However, the comparative test results illustrate the advantages of the proposed analytical model considering the cyber failures and ITEs.

In Figure 6, the sensitivity analysis of EENS against the MGCC failures and information terminal (IT), for example, LC and MC, faults under Scenario 3 for various cyber network topologies have been presented. The failure/fault ratio has been defined based on the considered value regret the base values of the test system. The sensitivity of the reliability indices via the MGCC failures for cyber network topologies 1, 2, and 3 is much more than the IT faults. The importance of the MGCC failures in third cyber network topologies has been highlighted. This result is mainly because of the redundancy of ITs in the

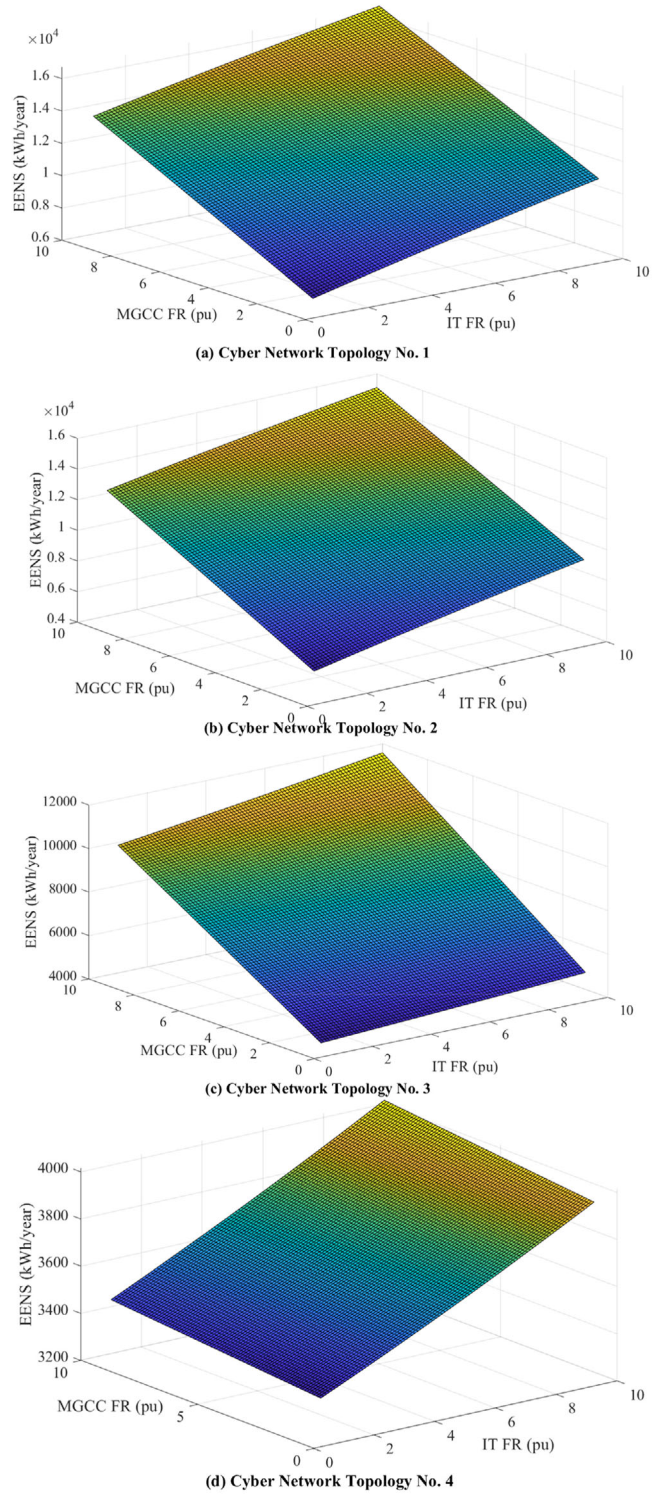


FIGURE 6 Sensitivity analysis of EENS against MGCC failures and ITEs under Scenario 3 for various cyber network topologies

third topology, while the MGCC has no redundant unit. On the contrary, the IT faults would be much more important than the MGCC failures in the fourth cyber network topology because the MGCC redundancy has been considered.

The sensitivity analysis of EENS against the changes in failures of optical fibres and switches, two important types of

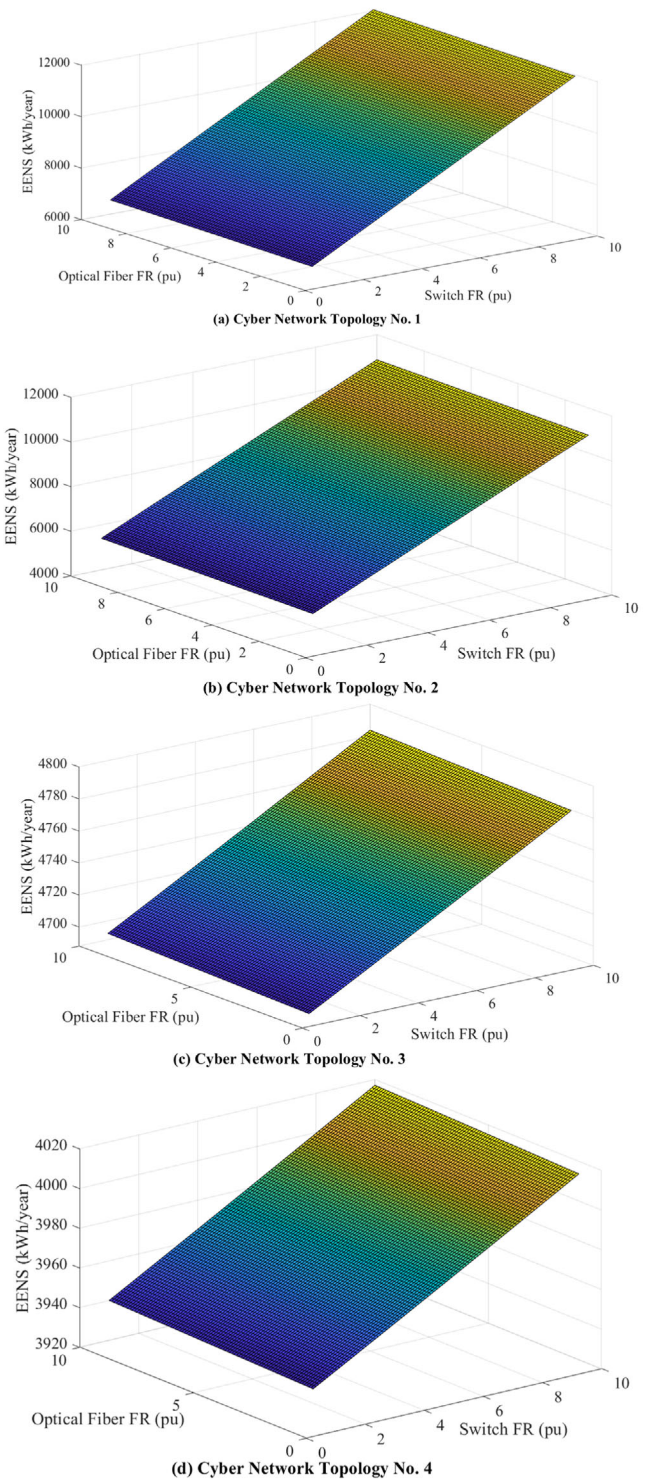


FIGURE 7 Sensitivity analysis of EENS against optical fibre and switches failures under Scenario 3 for various cyber network topologies

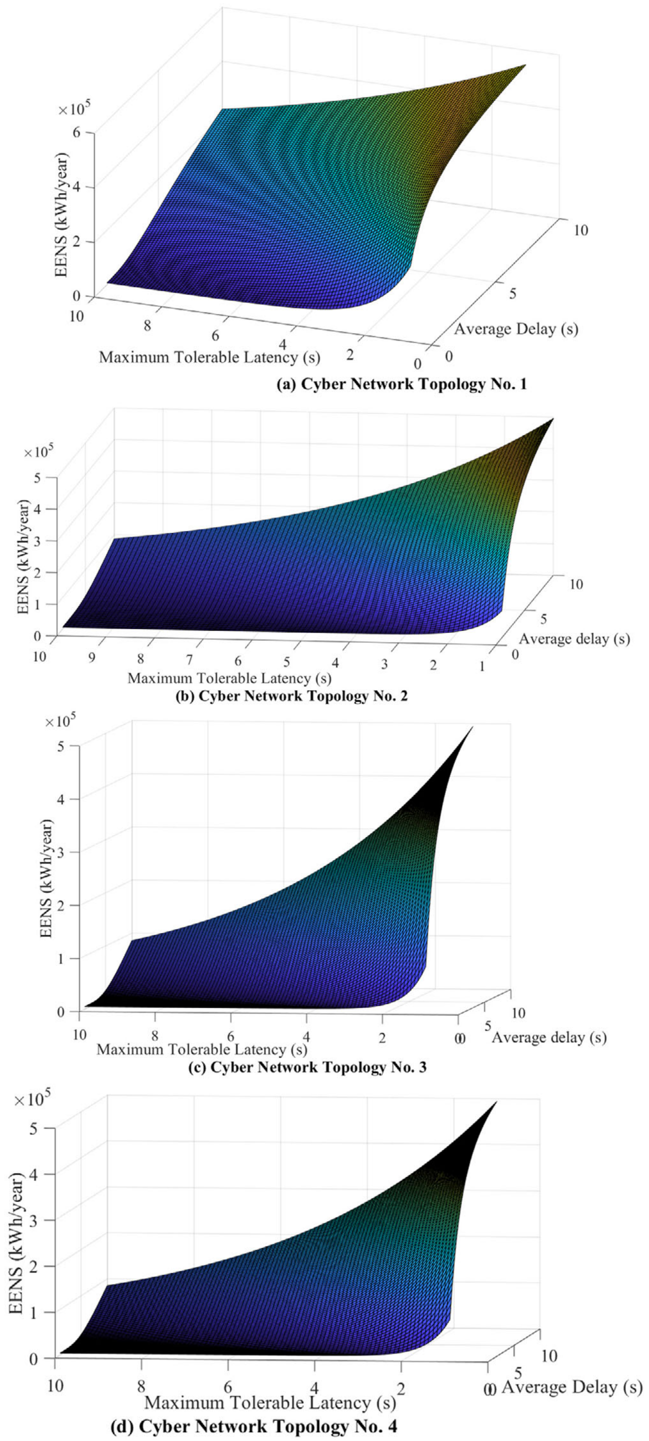


FIGURE 8 Sensitivity analysis of EENS against maximum tolerable latency and the average delay in ITSs under Scenario 3 for various cyber network topologies

communication elements, is shown in Figure 7. Regardless of the cyber network topologies, the sensitivity of the SMG reliability via the failures of switches is much more than optical fibres. The not-significant failure rates of optical fibres in the base condition of the understudy SMG could be one of the most important reasons for this conclusion. The sensitivity analysis highlights the impacts of switches on SMG reliability. Hence, controlling and managing the failures of switches is an effective solution to improve SMG reliability.

Figure 8 shows the sensitivity analysis of EENS via different maximum tolerable latencies and average delays under Scenario 3. As depicted, the EENS might be adversely affected due to an increase in the average of the delays in ITSs. It is concluded that the worst case would occur if the average delay of the information channels is significant and the maximum tolerable latency is not sufficient. Since the transmission distance and other technical specifications of the communication links and information channels affect the delay, the performed sensitivity analyses importance is emphasized. Comparing the test results for the communication system failures with the impacts of delay on the ITS emphasizes that the information transmission interruptions and faults might be much more important than other cyber failures.

In Figure 9, the sensitivity analysis of EENS against the increase in the probability of routing and payload errors has been shown. Test results highlight that the routing errors affect the SMG reliability significantly. Also, the impacts of routing errors would be much more than payload errors. However, the comparative analysis shows that the routing and payload errors' impacts are less than those of delay in the ITS.

The sensitivity analysis implies that the accurate reliability calculations are not obtainable without considering the cyber failures and ITEs.

Studying the interactions of some causes and sub-systems is another interesting issue in this research work. Although some sub-systems might not dramatically affect the system's reliability, other changes intensify their eventual impacts. Test results shown in Figure 9 imply that the threats of delays would be intensified dramatically if the maximum tolerable latency of the information transmission channels decreases. It is concluded that a similar significant interaction between other parameters (except the delay and the maximum tolerable latency of information transmission channels) has not appeared.

It might be challenging that the consideration of all potential sub-system's states and errors, or only selection of some more essential ones, would be more effective. It should be noted that, first of all, it is necessary to study the SMG using the most detailed method and results, as proposed in this research. Because without any precise investigations and studies, it is impossible to judge the important and essential sub-systems and their impacts. After implementing a detailed and precise model, like the proposed method, the essential parts and sub-systems could be determined using sensitivity analyses and supplementary studies. When the critical sub-systems have been ranked, it is possible to simplify the proposed model to speed up the calculations. The reported several sensitivity analyses are useful to get insight into how the changes in sub-systems and their reliability parameters might affect the system reliability.

Moreover, it is helpful to define the appropriate criteria for selecting critical systems and processes in the context of smart MG. In this paper, the sensitivity of the SMG's EENS via changes in failures of sub-systems has been selected as the criterion for determining the critical sub-systems. The critical element criterion of the *m*th element/parameter of the SMG could be defined using (37). As seen, the normalized difference between the EENS for two intervals of the sensitivity analysis corresponding to changes in the *m*th element/parameter has been selected as the criterion to distinguish whether the discussed element/parameter is a critical one or not by (38).

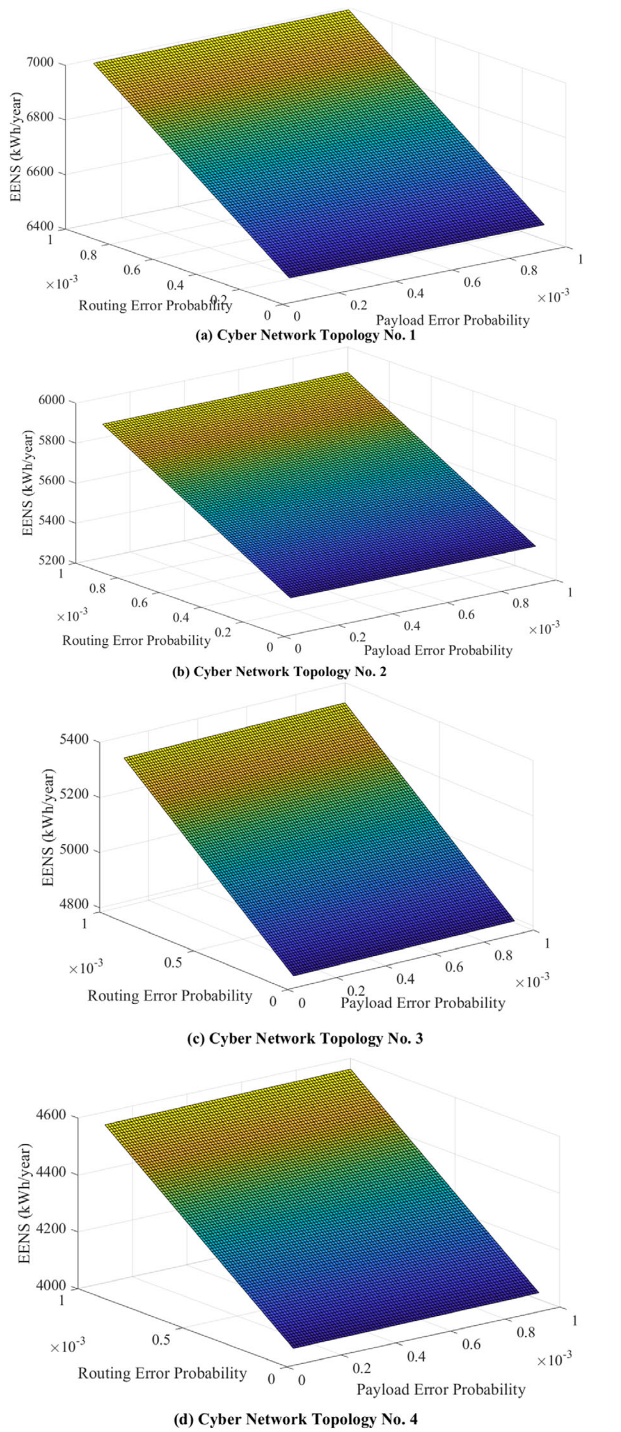


FIGURE 9 Sensitivity analysis of EENS against routing and payload error probabilities under Scenario 3 for various cyber network topologies

$$CEC_m = \frac{EENS^m_{SA,h} - EENS^m_{SA,h'}}{EENS_{Base}} \tag{37}$$

$$CEC_m \geq CEC^{\min} \tag{38}$$

TABLE 8 Sensitivity analysis results of EENS against the changes in the capacity of PVs and WTs

		WTs and PVs' capacity ratio (%) with fixed ESS's capacity							
		50%		75%		125%		150%	
Scenario no.	Topology no.	EENS difference (%)	EENS (kWh/year)	EENS difference (%)	EENS (kWh/year)	EENS difference (%)	EENS (kWh/year)	EENS difference (%)	EENS (kWh/year)
1	1	23.7797	7470.6	13.83338	6870.3	−4.82155	5744.4	−9.96123	5434.2
	2	29.55202	6281.2	17.19124	5681.9	−5.99373	4557.8	−12.3793	4248.2
	3	28.95194	5795.1	17.06943	5261.1	−5.79217	4233.7	−12.5567	3929.7
	4	30.14959	4881.0	16.85998	4382.6	−6.35416	3512.0	−11.3458	3324.8
2	1	10.41681	8013.5	5.82432	7680.2	−2.15915	7100.8	−4.9907	6895.3
	2	12.46511	6809.2	6.968371	6476.4	−2.5832	5898.1	−5.97242	5692.9
	3	12.2223	6102.2	6.84861	5810.0	−2.5526	5298.8	−5.90334	5116.6
	4	13.90686	5300.2	6.535428	4957.2	−4.31755	4452.2	−8.16875	4273.0
3	1	17.1433	7553.4	10.82971	7146.3	−7.13555	5987.9	−12.7667	5624.8
	2	19.85623	6385.7	12.45355	5991.3	−7.90195	4906.8	−14.0546	4579.0
	3	20.30479	5754.9	12.84388	5398.0	−8.52078	4376.0	−15.2605	4053.6
	4	22.95743	4939.2	14.39881	4595.4	−9.13617	3650.0	−16.2509	3364.2

Different criteria and objects, such as EENS, SAIFI, SAIDI, and LOLP%, can be selected to identify the critical sub-systems. The studies have shown that the EENS might be more sensitive via the changes in reliability parameters of sub-systems and model parameters [37]. Hence, the EENS-based critical element criterion (CEC) has been introduced in this study. However, other criteria and reliability indices can be used for the CEC. Studying the multi-criteria CEC will also be interesting as one of further future works.

It should be noted that $CEC^{\min}$ is one of the essential decision-making parameters. The considered $CEC^{\min}$ effectively affects the results for critical and non-critical sub-systems. Depending on the understudy test system, various $CEC^{\min}$ can be used. If the system reliability is not desired and dramatic problems exist, selecting a very low $CEC^{\min}$ is not a reasonable decision because all sub-systems might be critical, and it is not possible to apply effective solutions to improve the system reliability.

After investigating the essential elements and sub-systems on the SMG's reliability (critical ones using (37) and (38)), considering only a subset of SMG's elements and sub-systems might be applicable in the developed model. By applying the zero/insignificant failure rates for elements that might not affect the SMG's reliability, it is possible to neglect their impacts on the system states and studied conditions. Also, the complete re-structure of the system states and their number is another alternative to simplify the model and accelerate the computations. However, it seems the first strategy to neglect the failures of some parts and focus on other sensitive and essential elements without any fundamental changes in the structure of the proposed model would be better.

The capacities of generation units, such as MT, PV, and WT, should be enumerated to validate the reliability metric's robustness in all these operating scenarios. In the base configuration and condition, it has been assumed to exist adequate power to supply the loads and required reserve capacity. It means the system in base condition should operate in healthy mode. The reliability of the SMG due to the outage of each generation unit and changes in the output power of WTs and PVs has been evaluated. However, in addition to the discussed studies, the sensitivity analyses to get insight into how the capacities of different generation units can affect the system reliability, besides the cyber failures and ITEs, would be useful.

In Table 8, the reliability evaluation results of the understudy SMG for different penetrations of PVs and WTs have been presented. The 50, 75, 125, and 150% ratio of PVs and WTs compared to the base condition have been considered. Test results in Table 8 have been obtained with the fixed capacity of the ESSs. As expected, the decrease in the capacity of generation units leads to an increase in the EENS. On the contrary, the increase in the capacity of PVs and WTs improves the system reliability. However, the robustness of the system reliability against the changes in the capacity of generation units could be concluded. The impacts of the capacity of PVs and WTs for various cyber network topologies are different. As revealed by test results, the negative impacts of decrements in the capacity of PVs and WTs on the system reliability for the fourth cyber network topology are more significant. This is mainly because the cyber network has adequate redundancy under the fourth cyber network topology, and the impacts of available generation capacity are highlighted compared to other uncertainties.

To illustrate the impact of the ESS on the SMGs' reliability, supplementary analyses have been done. Table 9 presents the reliability evaluation results of the understudy SMG for different penetrations of PVs and WTs, while the capacity of ESS increases similar to the DERs. The 50, 75, 125, and 150% ratio of PVs, WTs, and ESSs compared to the base condition have

TABLE 9 Sensitivity analysis results of EENS against the changes in the capacity of PVs, WTs, and ESSs

Scenario no.	Topology no	WTs, PVs, and ESSs' capacity ratio (%)							
		50%		75%		125%		150%	
		EENS difference (%)	EENS (kWh/year)	EENS difference (%)	EENS (kWh/year)	EENS difference (%)	EENS (kWh/year)	EENS difference (%)	EENS (kWh/year)
1	1	18.92	7959.0	15.80	7324.8	−21.36	5081.3	−31.87	
	2	23.51	6768.8	19.64	6135.7	−26.55	3895.9	−39.60	3708.2
	3	23.15	6228.1	19.11	5669.1	−26.14	3634.8	−38.58	3453.2
	4	23.63	5290.4	20.43	4751.0	−26.68	2984.0	−41.06	2863.8
2	1	16.45	8350.3	14.21	7999.4	−10.22	6225.7	−15.05	6063.2
	2	19.69	7145.5	17.01	6795.2	−12.23	5024.4	−18.01	4862.2
	3	19.28	6397.3	16.62	6090.4	−12.00	4533.7	−17.64	4388.7
	4	23.75	5586.6	20.71	5235.5	−12.51	3689.2	−20.06	3547.6
3	1	21.82	8131.3	16.76	7724.1	−19.79	5367.1	−26.10	5040.9
	2	24.82	6956.8	19.45	6554.1	−23.01	4291.3	−30.57	4005.0
	3	25.93	6259.6	19.84	5904.0	−23.42	3834.4	−30.85	3543.1
	4	28.70	5437.0	22.49	5085.9	−26.60	3113.4	−35.34	2863.9

been considered. The main difference between the obtained results in Tables 9 and 8 is the changes in the capacity of the ESS, besides the changes in the capacity of PVs and WTs. The comparative test results illustrate the significant impact of the ESS on the system's reliability. It can be concluded that the ESSs intensify the positive impacts of increasing the capacity of PVs and WTs. The ESS can mitigate the challenges regarding the uncertainties of the output power of PVs and WTs. As revealed by the test results shown in Table 9, the positive/negative impacts of increasing/decreasing the capacity of PVs, WTs, and ESSs would be more considerable for the fourth cyber network topology with adequate redundancy level. It means that if the cyber network is reliable, the effects of available generation and storage capacity will be highlighted. Moreover, the advantages of a reliable cyber network with adequate redundancy, besides the ESS, are highlighted

4 | CONCLUSION

Although several kinds of research have been reported for the reliability evaluation of SMGs using the MCS, the literature shows a research gap for an accurate and fast reliability assessment method for SMGs based on the cyber failures and ITEs. This research aimed to fill the discussed gap by introducing an analytical model. The introduced reliability methodology has extended the available analytical reliability evaluation methods by modelling the cyber failures, cyber interdependencies, and ITEs, besides other uncertainties. Test results illustrated that less than 5.7% EENS error occurs by the proposed analytical reliability evaluation method, while its speed would be much more than available MCS-based approaches. The comparative studies showed that significant inaccuracy appears in reliability calculations if the cyber failures and ITEs are neglected. Also, it has been concluded that the EENS error due to non-consideration of cyber failures depends on the cyber network topologies. Moreover, sensitivity analyses have been done to investigate various impacts of the cyber system and ITEs on SMG reliability.

Furthermore, extending the proposed model to examine the smart microgrids' operation and system reliability in the presence of electric vehicles and non-fossil fuel-based vehicles and other new ICT-based technologies and frameworks, such as DTR systems, would be an interesting subject for further research works. Developing a similar model for evaluating the reliability of integrated multi-carrier energy hubs is another suggested future work.

DATA AVAILABILITY STATEMENT

Data available on request from the authors

CONFLICT OF 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.

FUNDING INFORMATION

The author(s) received no specific funding for this work.

NOMENCLATURE

Indices

i	Index of smart microgrid's element ($i = 1 : N_C + N_P$)
j, j', j''	Index of state for smart microgrid's elements ($j = 1 : N_{ES}^i$)
k	Index of physical element without stochastic behaviours ($k = 1 : K$)
c	Index of cyber link ($c = 1 : C$)
c'	Index of the cyber link corresponding to a physical element ($c' = 1 : L_r$)
l	Index of smart microgrid's state (system state) ($l = 1 : N_{MGS}$)
i', i''	Index of cyber element ($i = 1 : N_C$)
w	Index of wind turbine output power's state ($w = 1 : N_{WT}^{ESM}$)
g	Index of the distributed generation unit ($g = 1 : G$)
q	Index of the sending information terminal ($q = 1 : N_C$)
q'	Index of the receiving information terminal ($q' = 1 : N_C$)
e	Index of state for the payload of cyber links ($e = 1 : N_c^{PLS}$)
r, r', r''	Index of physical element ($r = 1 : N_P$)
s	Index of photovoltaic output power's state ($s = 1 : S$)
t	Index of time interval
m	Index of element/parameter of smart microgrids to distinguish the critical ones ($m = 1 : N_C + N_P$)
h, h'	Index of sensitivity analysis's interval ($h = 1 : H$)

Parameters and Variable

ESM_i	Element state matrix of the ith smart microgrid's element
$ES_{i,j}$	The jth element state of the ith smart microgrid's element
$\Pr_{i,j}^{ES}$	Probability of the jth element state of the ith smart microgrid's element
N_{ES}^i	Number of states for the ith smart microgrid's element
N_C	Number of cyber elements
N_P	Number of physical/power elements
A_k	Availability of the kth element
U_k	Unavailability of the kth element
K	Number of physical elements without stochastic behaviours
C	Number of cyber links
$PD_{Destination}^{T_q,T_{q'}}$	Packet data at the destination terminal corresponding to the information channel between

	the qth sending terminal and the q'th receiving terminal
$S_{Destination}^{T_q,T_{q'}}$	Signal/data of the packet data at the destination terminal
$Header_{Destination}^{T_q,T_{q'}}$	Header of the packet data at the destination terminal
$PD_{Origin}^{T_q,T_{q'}}$	Packet data at the origin terminal corresponding to the information channel between the qth sending terminal and the q'th receiving terminal
$S_{Origin}^{T_q,T_{q'}}$	Signal/data of the packet data at the origin terminal
$Header_{Origin}^{T_q,T_{q'}}$	Header of the packet data at the origin terminal
T_q	The qth sending information terminal
$T_{q'}$	The q'th receiving information terminal
D_c	Delay of the cth cyber link
SE	Signal error/payload error
HE	Header error
CL	Cyber link state
BV_c^{Delay}	A Boolean variable for the delay state of the cth cyber link, which it's one value means that the delay is less than the maximum tolerable delay of the information channel, and it's zero value represents that the data transmission has been interrupted due to the delay.
BV_c^{Header}	A Boolean variable for the header error state of the cth cyber link
$D^{\max}$	Maximum tolerable delay of the cyber link/information channel
DSM_c	Delay state matrix of the cth cyber link
erf	Error function
μ_{Delay}	Mean value of the delay for information channels
σ_{Delay}	Standard deviation of the delay for the information channels
HSM_c	Header state matrix of the $c$the cyber link
$HE^{\max}$	Maximum tolerable error for the header of information channels
CDF	Cumulative density function
$PLSM_c$	Payload state matrix of the $c$the cyber link
$PLS_{c,e}^{Payload}$	The eth payload state of the cth cyber link
N_c^{PLS}	Number of payload states of the cth cyber link
$SE_c^{\min}$	Minimum value of the signal error/payload error
$SE_c^{\max}$	Maximum value of the signal error/payload error
A_c^{SE}	Probability of payload error for the cth cyber link
A_c^{HE}	Probability of header error for the cth cyber link
U_c^{HE}	Probability of information transmission without any header error for the cth cyber link
$MGSM_l$	The lth microgrid state matrix
$\Pr_l^{MGS}$	Probability of the lth microgrid state
$CCLM_l$	Cyber-cyber link matrix for the lth microgrid state
CC	Cyber-cyber indicator, which it's one value, represents there is a cyber interconnection between two cyber terminals.
CNG_l	Cyber network graph of the lth microgrid state
graph	Graph function
$IC_{i',i''}^{l}$	Information channel between the i'th and i''th terminals in the lth microgrid state
SPF	Short path function based on graph theory concepts
$CE_{i'}$	The i'th cyber element
$PPLM_l$	Power-power link matrix for the lth microgrid state
PP	Power-power indicator, which it's one value represents there is a power interconnection between two power terminals.
$PPLM_l'$	Updated power-power link matrix for the lth microgrid state based on the states of information channels and corresponding cyber network graph
$PPLM_l''$	Updated power-power link matrix for the lth microgrid state based on the states of payload errors
$ES'_{N_C+r'}$	Updated element state of the r'th physical element considering the states of required information channels
$ES''_{N_C+r'}$	Updated element state of the r'th physical element considering the payload errors
L_r	Number of cyber links corresponding to the rth physical element
CP	Cyber-power link
PNG_l	Power network graph of the lth microgrid state
$PC_{r',r''}^{l}$	Power channel between the r'th and r''th terminals in the lth microgrid state
PE	Power element
$MTTF$	Mean-time to failure
$MTTR$	Mean-time to repair
ESM_{WT}	State matrix of the wind turbine
P_{rated}^{WT}	Rated power of the wind turbine
N_{WT}^{ESM}	Number of states for wind turbine output power
v_{rated}	Rated wind speed
v_{co}	Cut-off wind speed
v_{ci}	Cut-in wind speed
U_{WT}	Unavailability of the wind turbine
A_{WT}	Availability of the wind turbine
ESM_{PV}	State matrix of the photovoltaic unit
τ	Time interval
P_{rated}^{PV}	Rated power of the photovoltaic unit
$SCI_s^{\max}$	Maximum solar clearness index for the sth state of the photovoltaic unit
$SCI_s^{\min}$	Minimum solar clearness index for the sth state of the photovoltaic unit
ESM_{ESS}	State matrix of the energy storage system

P_{rated}^{ESS}	Rated output power of the energy storage system
U_{ESS}	Unavailability of the energy storage system
A_{ESS}	Availability of the energy storage system
$SOC^{\min}$	Minimum state of charge of the energy storage system
ΔLG_l	Difference between the load demand and available generation capacity of the *l*th system state
ES_l^{load}	Load state of the *l*th system state
G	Number of distributed generation units
$ES_{g,l}^{DG}$	Generation state of the *g*th distributed generation unit in the *l*th system state
$PC_{g,l}^{DG}$	Power channel corresponding to the *g*th distributed generation unit in the *l*th system state
ES_l^{ESS}	State of the energy storage system in the *l*th system state
LOE_l	Loss of energy in the *l*th system state
$EENS$	Expected energy not supplied
$SAIDI$	System average interruption duration index
$\bar{P}_{load}$	Average of the load demand of the smart microgrid
$EENS_{SA,h}^{m}$	Expected energy not-supplied of the *h*th interval in the sensitivity analysis to get insight into the impacts of changes in the *m*th element/parameter
$EENS_{Base}$	Base expected energy not-supplied value in the sensitivity analysis, while there is no change in element/parameter of the under-study smart microgrid
$CEC^{\min}$	Minimum value for critical element criterion

Abbreviations

CC	Cyber-cyber interconnection
CCD	Cause consequence diagrams
CCLM	Cyber-cyber link matrix
CDF	Cumulative distribution function
CL	Cyber link
CNG	Cyber network graph
CNT	Complex network theory
CPI	Cyber-physical interdependency
CPMG	Cyber–power microgrid
CPS	Cyber-physical system
DER	Distributed energy resource
DG	Distributed generation
EENS	Expected energy not supplied
ESM	Element state matrix
ESS	Energy storage system
ET	Event trees
FBD	Functional block diagrams
GM	graph matrix
HE	header errors
IC	Information channel
ITE	Information transmission error
ITS	Information transmission system
LC	Load controller
LOE	Loss of energy
LOLP	Loss of load probability
MC	Microunit controller
MCS	Monte Carlo Simulation
MGCC	Microgrid control center
MGSM	Microgrid's state matrix
MT	Microturbine
MTTF	Mean-time to failure
MTTR	Mean-time to repair
PCC	Point of common coupling
PLSM	Payload state matrix
P-Matrix	Probability matrix
PNG	Power network graph
PV	Photovoltaic
SAIDI	System average interruption duration index
SMG	Smart microgrid
SPF	Short path function
SW	Network switch
WT	Wind turbine

ORCID

Hamed Hashemi-Dezaki https://orcid.org/0000-0003-2056-2388
Abbas Ketabi https://orcid.org/0000-0001-9970-2157

REFERENCES

1. Gao, H., Wang, R., Liu, Y., Wang, L., Xiang, Y., Liu, J.: Data-driven distributionally robust joint planning of distributed energy resources in active distribution network. IET Gener. Transm. Distrib. 14(9), 1653–1662 (2020) https://doi.org/10.1049/iet-gtd.2019.1565
2. Paliwal, P., Patidar, N.P., Nema, R.K.: Probabilistic indices for analysing the impact of penetration of distributed energy resources on system reliability. IET Renewable Power Gener. 14(12), 2154–2165 (2020) https://doi.org/10.1049/iet-rpg.2019.1214
3. Yang, J., Guo, W., Ma, K., Tian, Z., Dou, C.: Strategic equilibrium of economic dispatch in smart grid with a bi-level game approach. IET Gener. Transm. Distrib. 14(12), 2227–2236 (2020) https://doi.org/10.1049/iet-gtd.2019.1050
4. Pal, R., et al.: A comprehensive review on IoT-based infrastructure for smart grid applications. IET Renewable Power Gener. 15(16), 3761–3776 (2021) https://doi.org/10.1049/rpg2.12272
5. Ravikumar, K.G., Srivastava, A.K.: Designing centralised and distributed system integrity protection schemes for enhanced electric grid resiliency. IET Gener. Transm. Distrib. 13(8), 1194–1203 (2019) https://doi.org/10.1049/iet-gtd.2018.5381
6. Mongrain, R.S., Ayyanar, R.: Multi-platform real-time microgrid simulation testbed with hierarchical control of distributed energy resources featuring energy storage balancing. IET Renewable Power Gener. 14(5), 834–844 (2020) https://doi.org/10.1049/iet-rpg.2019.0525
7. Faramarzi, F., Niknam, T., Aghaie, J., Rashidi, M.: Resiliency enhancement of power system against intentional attacks. IET Renewable Power Gener. (2022) https://doi.org/10.1049/rpg2.12396
8. Bessani, M., Fanucchi, R.Z., Delbem, A.C.C., Maciel, C.D.: Impact of operators' performance in the reliability of cyber-physical power distribution systems. IET Gener. Transm. Distrib. 10(11), 2640–2646 (2016) https://doi.org/10.1049/iet-gtd.2015.1062
9. Wu, Z., Wang, Q., Cai, X., Dai, J., Liu, X., Tian, Q.: Methods of anomaly state detection for power systems based on bilateral cyber-physical information. IET Gener. Transm. Distrib. 16(7), 1449–1459 (2022) https://doi.org/10.1049/gtd2.12382

10. Jimada-Ojuolape, B., Teh, J.: Impact of the integration of information and communication technology on power system reliability: A review. IEEE Access. 8, 24600–24615 (2020) https://doi.org/10.1109/ACCESS.2020.2970598
11. Tian, J., Wang, B., Li, J., Konstantinou, C.: Adversarial attack and defense methods for neural network based state estimation in smart grid. IET Renewable Power Gener. (2021) https://doi.org/10.1049/rpg2.12334
12. Yang, J., Guo, Y., Guo, C., Chen, Z., Wang, S., Jiang, B.: A robust active distribution network defensive strategy against cyber-attack considering multi-uncertainties. IET Gener. Transm. Distrib. 16(8), 1476–1488 (2022) https://doi.org/10.1049/gtd2.12443
13. Mohebbi, S., et al.: Cyber-physical-social interdependencies and organizational resilience: A review of water, transportation, cyber infrastructure systems and processes. Sustainable Cities Soc. 62, 102327 (2020) https://doi.org/10.1016/j.scs.2020.102327
14. Jimada-Ojuolape, B., Teh, J.: Surveys on the reliability impacts of power system cyber–physical layers. Sustainable Cities Soc. 62, 102384 (2020) https://doi.org/10.1016/j.scs.2020.102384
15. Aslani, M., Hashemi-Dezaki, H., Ketabi, A.: Reliability evaluation of smart microgrids considering cyber failures and disturbances under various cyber network topologies and distributed generation's scenarios. Sustainability 13(10), 5695 (2021) https://doi.org/10.3390/su13105695
16. Jimada-Ojuolape, B., Teh, J.: Impacts of communication network availability on synchrophasor-based DTR and SIPS reliability. in IEEE Syst. J. (2021) https://doi.org/10.1109/JSYST.2021.3122022
17. Jimada-Ojuolape, B., Teh, J.: Composite reliability impacts of synchrophasor-based DTR and SIPS cyber–physical systems. in IEEE Syst. J. (2022) https://doi.org/10.1109/JSYST.2021.3132657
18. Teh, J., Lai, C.-M.: Reliability impacts of the dynamic thermal rating system on smart grids considering wireless communications. IEEE Access. 7, 41625–41635 (2019)
19. Azimian, M., Amir, V., Javadi, S., Mohseni, S., Brent, A.C.: Resilience-oriented planning of multi-carrier microgrids under cyber-attacks. Sustainable Cities Soc. 79, 103709 (2022) https://doi.org/10.1016/j.scs.2022.103709
20. Hashemi-Dezaki, H., Agah, S.M.M., Askarian-Abyaneh, H., Haeri-Khiavi, H.: Sensitivity analysis of smart grids reliability due to indirect cyber-power interdependencies under various DG technologies, DG penetrations, and operation times. Energy Convers. Manag. 108, 377–391 (2016) https://doi.org/10.1016/j.enconman.2015.10.082
21. He, R., Xie, H., Deng, J., Feng, T., Lai, L.L., Shahidehpour, M.: Reliability modeling and assessment of cyber space in cyber-physical power systems. IEEE Trans. Smart Grid. 11(5), 3763–3773 (2020) https://doi.org/10.1109/TSG.2020.2982566
22. Hashemi-Dezaki, H., Askarian-Abyaneh, H., Haeri-Khiavi, H.: Impacts of direct cyber-power interdependencies on smart grid reliability under various penetration levels of microturbine/wind/solar distributed generations. IET Gener. Transm. Distrib. 10(4), 928–937 (2016) https://doi.org/10.1049/iet-gtd.2015.0565
23. Hashemi-Dezaki, H., Askarian-Abyaneh, H., Shams-Ansari, A., DehghaniSanij, M., Hejazi, M.A.: Direct cyber-power interdependencies-based reliability evaluation of smart grids including wind/solar/diesel distributed generations and plug-in hybrid electrical vehicles. Int. J. Electr. Power Energy Syst. 93, 1–14 (2017) https://doi.org/10.1016/j.ijepes.2017.05.018
24. Wang, C., Zhang, T., Luo, F., Li, F., Liu, Y.: Impacts of cyber system on microgrid operational reliability. IEEE Trans. Smart Grid 10(1), 105–115 (2019) https://doi.org/10.1109/TSG.2017.2732484
25. Sun, X., Liu, Y., Deng, L.: Reliability assessment of cyber-physical distribution network based on the fault tree. Renew. Energy 155, 1411–1424 (2020) https://doi.org/10.1016/j.renene.2020.03.188
26. Barani, M., Vadlamudi, V.V., Heegaard, P.E.: Reliability analysis of cyber-physical microgrids: Study of grid-connected microgrids with communication-based control systems. IET Gener. Transm. Distrib. 10, 1–19 (2020) https://doi.org/10.1049/gtd2.12049
27. Barani, M., Vadlamudi, V.V., Farzin, H.: Impact of cyber failures on operation and adequacy of multi-microgrid distribution systems. arXiv Prepr. arXiv2204.08526 (2022)
28. Memari, M., Karimi, A., Hashemi-Dezaki, H.: Reliability evaluation of active distribution networks based on scenario reduction method using PSO algorithm. In: *2020 10th Smart Grid Conference (SGC)*, Kashan, Iran, pp. 1–6 (2020) https://doi.org/10.1109/SGC52076.2020.9335770
29. Memari, M., Karimi, A., Hashemi-Dezaki, H.: Reliability evaluation of smart grid using various classic and metaheuristic clustering algorithms considering system uncertainties. Int. Trans. Electr. Energy Syst. 31(6), e12902 (2021) https://doi.org/10.1002/2050-7038.12902
30. Hariri, A.-M., Hashemi-Dezaki, H., Hejazi, M.A.: A novel generalized analytical reliability assessment method of smart grids including renewable and non-renewable distributed generations and plug-in hybrid electric vehicles. Reliab. Eng. Syst. Saf. 196, 106746 (2020) https://doi.org/10.1016/j.ress.2019.106746
31. Zhu, W., Han, M., Milanovic, J.V., Crossley, P.: Methodology for reliability assessment of smart grid considering risk of failure of communication architecture. IEEE Trans. Smart Grid. 11(5), 4358–4365 (2020) https://doi.org/10.1109/TSG.2020.2982176
32. Falahati, B., Fu, Y., Wu, L.: Reliability assessment of smart grid considering direct cyber-power interdependencies. IEEE Trans. Smart Grid 3(3), 1515–1524 (2012) https://doi.org/10.1109/TSG.2012.2194520
33. Falahati, B., Fu, Y.: Reliability assessment of smart grids considering indirect cyber-power interdependencies. IEEE Trans. Smart Grid 5(4), 1677–1685 (2014) https://doi.org/10.1109/TSG.2014.2310742
34. Wang, Y., Vittal, V., Abdi-Khorsand, M., Singh, C.: Probabilistic reliability evaluation including adequacy and dynamic security assessment. IEEE Trans. Power Syst. 35(1), 551–559 (2020) https://doi.org/10.1109/TPWRS.2019.2923844
35. Nazmul Huda, A.S., Zivanovic, R.: Study effect of components availability on distribution system reliability through multilevel monte carlo method. IEEE Trans. Ind. Inf. 15(6), 3133–3142 (2019) https://doi.org/10.1109/TII.2018.2877822
36. Atwa, Y.M., El-Saadany, E.F., Salama, M.M.A., Seethapathy, R., Assam, M., Conti, S.: Adequacy evaluation of distribution system including wind/solar DG during different modes of operation. IEEE Trans. Power Syst. 26(4), 1945–1952 (2011) https://doi.org/10.1109/TPWRS.2011.2112783
37. Hashemi-Dezaki, H., Hamzeh, M., Askarian-Abyaneh, H., Haeri-Khiavi, H.: Risk management of smart grids based on managed charging of PHEVs and vehicle-to-grid strategy using Monte Carlo simulation. Energy Convers. Manag. 100, 262–276 (2015) https://doi.org/10.1016/j.enconman.2015.05.015
38. Guo, J., Zhao, T., Liu, W., Zhang, J.: Reliability modeling and assessment of isolated microgrid considering influences of frequency control. IEEE Access 7, 50362–50371 (2019) https://doi.org/10.1109/ACCESS.2019.2909153
39. Prajapati, V.K., Mahajan, V.: Reliability assessment and congestion management of power system with energy storage system and uncertain renewable resources. Energy 215, 119134 (2021) https://doi.org/10.1016/j.energy.2020.119134
40. Zhong, S., Yang, T., Wu, Y., Lou, S., Li, T.: The reliability evaluation method of generation system based on the importance sampling method and states clustering. Energy Procedia 118, 128–135 (2017) https://doi.org/10.1016/j.egypro.2017.07.031
41. Liu, Z., et al.: A lagrange multiplier based state enumeration reliability assessment for power systems with multiple types of loads and renewable generations. IEEE Trans. Power Syst. 36(4), 3260–3270 (2020) https://doi.org/10.1109/TPWRS.2020.3045021
42. Hashemi-Dezaki, H., Hariri, A.-M., Hejazi, M.A.: Impacts of load modeling on generalized analytical reliability assessment of smart grid under various penetration levels of wind/solar/non-renewable distributed generations. Sustainable Energy, Grids Networks. 20, 100246 (2019) https://doi.org/10.1016/j.segan.2019.100246
43. Gazijahani, F.S., Salehi, J.: Reliability constrained two-stage optimization of multiple renewable-based microgrids incorporating critical energy peak

pricing demand response program using robust optimization approach. Energy 161, 999–1015 (2018) https://doi.org/10.1016/j.energy.2018.07.191
44. Yaghoubi-Nia, M.-R., Hashemi-Dezaki, H., Halvaei Niasar, A.: Optimal stochastic scenario-based allocation of smart grids' renewable and non-renewable distributed generation units and protective devices. Sustainable Energy Technol. Assessments 44, 101033 (2021) https://doi.org/10.1016/j.seta.2021.101033
45. Cao, G., et al.: Operational risk evaluation of active distribution networks considering cyber contingencies. IEEE Trans. Ind. Inf. 16(6), 3849–3861 (2020) https://doi.org/10.1109/TII.2019.2939346
46. He, Z.: Reliability evaluation of microgrid CPS considering cyber-control-frequency. In: *2019 IEEE 2nd International Conference on Electronics Technology (ICET)*, Chengdu, China, pp. 166–170 (2019)
47. He, R., Yang, S., Deng, J., Feng, T., Lai, L.L., Shahidehpour, M.: Reliability Analyses of Wide-Area Protection System Considering Cyber-Physical System Constraints. IEEE Trans. Smart Grid. 12(4), 3458–3467 (2021)
48. Hariri, A.-M., Hejazi, M.A., Hashemi-Dezaki, H.: Investigation of impacts of plug-in hybrid electric vehicles' stochastic characteristics modeling on smart grid reliability under different charging scenarios. J. Clean. Prod. 287, 125500 (2021) https://doi.org/10.1016/j.jclepro.2020.125500
49. Abolpour, R., Javanmardi, H., Dehghani, M., Hesamzadeh, M.R.: Optimal frequency regulation in an uncertain islanded microgrid: A modified direct search algorithm. IET Renewable Power Gener. 16(4), 726–739 (2022) https://doi.org/10.1049/rpg2.12427
50. Chen, F., Chen, M., Xu, Z., Guerrero, J.M., Wang, L.Y.: Distributed noise-resilient economic dispatch strategy for islanded microgrids. IET Gener. Transm. Distrib. 13(14), 3029–3039 (2019) https://doi.org/10.1049/iet-gtd.2018.5740
51. Karimi, H., Bahmani, R., Jadid, S.: Stochastic multi-objective optimization to design optimal transactive pricing for dynamic demand response programs: A bi-level fuzzy approach. Int. J. Electr. Power Energy Syst. 125, 106487 (2021) https://doi.org/10.1016/j.ijepes.2020.106487
52. Abazari, A., Soleymani, M.M., Babaei, M., Ghafouri, M., Monsef, H., Beheshti, M.T.H.: High penetrated renewable energy sources-based AOMPC for microgrid's frequency regulation during weather changes, time-varying parameters and generation unit collapse. IET Gener. Transm. Distrib. 14(22), 5164–5182 (2020) https://doi.org/10.1049/iet-gtd.2020.0074
53. Seydali Seyf Abad, M., Ma, J., Marzooghi, H., Ahmadyar, A.S.: Probabilistic impact assessment of residential BESSs on the HC of LV distribution systems. Int. J. Electr. Power Energy Syst. 136, 107652 (2022) https://doi.org/10.1016/j.ijepes.2021.107652
54. Hannan, M.A., et al.: Battery energy-storage system: A review of technologies, optimization objectives, constraints, approaches, and outstanding issues. J. Energy Storage. 42, 103023 (2021) https://doi.org/10.1016/j.est.2021.103023
55. Tan, B., Chen, H., Zheng, X., Huang, J.: Two-stage robust optimization dispatch for multiple microgrids with electric vehicle loads based on a novel data-driven uncertainty set. Int. J. Electr. Power Energy Syst. 134, 107359 (2022) https://doi.org/10.1016/j.ijepes.2021.107359
56. Li, L., Han, Y., Li, Q., Pu, Y., Sun, C., Chen, W.: Event-triggered decentralized coordinated control method for economic operation of an islanded electric-hydrogen hybrid DC microgrid. J. Energy Storage. 45, 103704 (2022) https://doi.org/10.1016/j.est.2021.103704
57. Ilic, M.D., Jaddivada, R., Korpas, M.: Interactive protocols for distributed energy resource management systems (DERMS). IET Gener. Transm. Distrib. 14(11), 2065–2081 (2020) https://doi.org/10.1049/iet-gtd.2019.1022
58. Wang, Y., Liang, H., Dinavahi, V.: Decentralized stochastic programming for optimal vehicle-to-grid operation in smart grid with renewable generation. IET Renewable Power Gener. 15(4), 746–757 (2021) https://doi.org/10.1049/rpg2.12064
59. Du, G., Zhao, D., Liu, X., Wu, Z., Li, C.: Decentralized robust dispatch for multi-area AC/DC system considering wind power uncertainty. IET Gener. Transm. Distrib. 15(19), 2710–2721 (2021) https://doi.org/10.1049/gtd2.12209
60. Rashidi, R., Hatami, A., Abedini, M.: Multi-microgrid energy management through tertiary-level control: Structure and case study. Sustainable Energy Technol. Assessments 47, 101395 (2021) https://doi.org/10.1016/j.seta.2021.101395
61. Assis, F.A., Leite da Silva, A.M., Resende, L.C., Moura, R.A.R., Schroeder, M.A.O.: Generation maintenance scheduling with renewable sources based on production and reliability costs. Int. J. Electr. Power Energy Syst. 134, 107370 (2022) https://doi.org/10.1016/j.ijepes.2021.107370
62. Rahimi, K., Davoudi, M.: Electric vehicles for improving resilience of distribution systems. Sustainable Cities Soc. 36, 246–256 (2018) https://doi.org/10.1016/j.scs.2017.10.006
63. Shang, X., Li, Z., Zheng, J., Wu, Q.H.: Equivalent modeling of active distribution network considering the spatial uncertainty of renewable energy resources. Int. J. Electr. Power Energy Syst. 112, 83–91 (2019) https://doi.org/10.1016/j.ijepes.2019.04.029
64. Daneshvar, M., Eskandari, H., Sirous, A.B., Esmaeilzadeh, R.: A novel techno-economic risk-averse strategy for optimal scheduling of renewable-based industrial microgrid. Sustainable Cities Soc. 70, 102879 (2021) https://doi.org/10.1016/j.scs.2021.102879
65. Poorvaezi-Roukerd, S., Abdollahi, A., Peng, W.: Flexibility-constraint integrated resource planning framework considering demand and supply side uncertainties with high dimensional dependencies. Int. J. Electr. Power Energy Syst. 133, 107223 (2021) https://doi.org/10.1016/j.ijepes.2021.107223
66. Vahedipour-Dahraie, M., Rashidizadeh-Kermani, H., Anvari-Moghaddam, A., Siano, P.: Risk-averse probabilistic framework for scheduling of virtual power plants considering demand response and uncertainties. Int. J. Electr. Power Energy Syst. 121, 106126 (2020) https://doi.org/10.1016/j.ijepes.2020.106126
67. Yang, X., Wang, Y., Zhang, Y., Yao, W., Wen, J.: Impact analysis of cyber system in microgrids: Perspective from economy and reliability. Int. J. Electr. Power Energy Syst. 135, 107422 (2022) https://doi.org/10.1016/j.ijepes.2021.107422
68. Baroudi, U., Al-Roubaiey, A., Mekid, S., Bouhraoua, A.: Delay characterization and performance evaluation of cluster-based WSN with different deployment distributions. Futur. Gener. Comput. Syst. 39, 100–110 (2014) https://doi.org/10.1016/j.future.2014.02.011
69. Park, J.W., Lee, J.M.: Transmission modeling and simulation for Internet-based control. In: IECON'01 27th Annual Conference of the IEEE Industrial Electronics Society (Cat. No. 37243), pp. 165–169, Denver, CO (2001)
70. Tipsuwan, Y., Chow, M.Y.: Gain scheduler middleware: A methodology to enable existing controllers for networked control and teleoperation - Part I: Networked control. IEEE Trans. Ind. Electron. 51(6), 1218–1227 (2004) https://doi.org/10.1109/TIE.2004.837866
71. Kounev, V., Tipper, D., Yavuz, A.A., Grainger, B.M., Reed, G.F.: A secure communication architecture for distributed microgrid control. IEEE Trans. Smart Grid. 6(5), 2484–2492 (2015) https://doi.org/10.1109/TSG.2015.2424160
72. Rojas, A.J.: Feedback control over signal-to-noise ratio constrained communication channels with channel input quantisation. In: Proceedings of the 2010 American Control Conference, Baltimore, MD, pp. 265–270 (2010) https://doi.org/10.1109/acc.2010.5530601
73. Rubanenko, O., Miroshnyk, O., Shevchenko, S., Yanovych, V., Danylchenko, D., Rubanenko, O.: Distribution of wind power generation dependently of meteorological factors. In: IEEE KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, pp. 472–477 (2020) https://doi.org/10.1109/KhPIWeek51551.2020.9250114
74. Salehimaleh, M., Akbarimajd, A., Dejamkhooy, A.: A shrinking-horizon optimization framework for energy hub scheduling in the presence of wind turbine and integrated demand response program. Sustainable Cities Soc. 79, 103689 (2022) https://doi.org/10.1016/j.scs.2022.103689
75. Hakimi, S.M., Hasankhani, A., Shafie-khah, M., Catalão, J.P.S.: Stochastic planning of a multi-microgrid considering integration of renewable energy resources and real-time electricity market. Appl. Energy 298, 117215 (2021) https://doi.org/10.1016/j.apenergy.2021.117215
76. Shahrabi, E., Hakimi, S.M., Hasankhani, A., Derakhshan, G., Abdi, B.: Developing optimal energy management of energy hub in the

presence of stochastic renewable energy resources. Sustainable Energy, Grids Networks 26, 100428 (2021) https://doi.org/10.1016/j.segan.2020.100428
77. Galvani, S., Bagheri, A., Farhadi-Kangarlu, M., Nikdel, N.: A multi-objective probabilistic approach for smart voltage control in wind-energy integrated networks considering correlated parameters. Sustainable Cities Soc. 78, 103651 (2022) https://doi.org/10.1016/j.scs.2021.103651
78. Hasankhani, A., Hakimi, S.M.: Stochastic energy management of smart microgrid with intermittent renewable energy resources in electricity market. Energy 219, 119668 (2021) https://doi.org/10.1016/j.energy.2020.119668
79. Sahoo, A., Hota, P.K.: Impact of renewable energy sources on modelling of bidding strategy in a competitive electricity market using improved whale optimization algorithm. IET Renewable Power Gener. 15(4), 839–853 (2021) https://doi.org/10.1049/rpg2.12072
80. Suliman, M.S., Hizam, H., Othman, M.L.: Determining penetration limit of central PVDG topology considering the stochastic behaviour of PV generation and loads to reduce power losses and improve voltage profiles. IET Renewable Power Gener. 14(14), 2629–2638 (2020) https://doi.org/10.1049/iet-rpg.2019.1376
81. Li, Z.-L., Li, P., Yuan, Z.-P., Xia, J., Tian, D.: Optimized utilization of distributed renewable energies for island microgrid clusters considering solar-wind correlation. Electr. Power Syst. Res. 206, 107822 (2022)
82. Yu, D., Ghadimi, N.: Reliability constraint stochastic UC by considering the correlation of random variables with Copula theory. IET Renewable Power Gener. 13(14), 2587–2593 (2019) https://doi.org/10.1049/iet-rpg.2019.0485
83. Yang, K., Tang, Y., Zhang, S., Zhang, Z.: A deep learning approach to state of charge estimation of lithium-ion batteries based on dual-stage attention mechanism. Energy 244(B), 123233 (2022)
84. Murcia, J.P., et al.: Validation of European-scale simulated wind speed and wind generation time series. Appl. Energy 305, 17794 (2022)
85. Tavakoli, A., Karimi, A., Shafie-khah, M.: Optimal probabilistic operation of energy hub with various energy converters and electrical storage based on electricity, heat, natural gas, and biomass by proposing innovative uncertainty modeling methods. J. Energy Storage 51, 104344 (2022)
86. Mosadeghy, M., Yan, R., Saha, T.K.: A time-dependent approach to evaluate capacity value of wind and solar PV generation. IEEE Trans. Sustainable energy. 7(1), 129–138 (2015)
87. Ashrafi, R., Amirahmadi, M., Tolou-Askari, M., Ghods, V.: Multi-objective resilience enhancement program in smart grids during extreme weather conditions. Int. J. Electr. Power Energy Syst. 129, 106824 (2021)
88. Renewable Energy and Energy Efficiency Organization of Iran. Wind Speed and Radiation Data Sheets. http://www.satba.gov.ir/en/regions, http://www.satba.gov.ir/en/regions/esfahan. Accessed 2008

How to cite this article: Aslani, M., Hashemi-Dezaki, H., Ketabi, A.: Analytical reliability evaluation method of smart micro-grids considering the cyber failures and information transmission system faults. IET Renew. Power Gener. 16, 2816–2839 (2022). https://doi.org/10.1049/rpg2.12541