Received: 9 March 2020 | Revised: 7 July 2020 | Accepted: 1 October 2020

DOI: 10.1049/gtd2.12049

ORIGINAL RESEARCH PAPER

The Institution of Engineering and Technology WILEY

Reliability analysis of cyber-physical microgrids: Study of grid-connected microgrids with communication-based control systems

Mostafa Barani[1] | **Vijay V. Vadlamudi**[1] | **Poul E. Heegaard**[2]

[1] Department of Electric Power Engineering, Norwegian University of Science and Technology, Trondheim, Norway
(Email: vijay.vadlamudi@ntnu.no)

[2] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim, Norway
(Email: poul.heegaard@ntnu.no)

Correspondence
M. Barani, Department of Electric Power Engineering, Norwegian University of Science and Technology, Trondheim, Norway.
(Email: mostafa.barani@ntnu.no)

Abstract

Due to the greater penetration of renewable energy resources and the increasing complexity of the distribution system, moving towards a smart distribution system is essential and achievable via advanced information and communication technologies. These technologies come with side effects: not only do they change the structure and functionality of the system, their availability and efficiency alter the operation of the system as a whole. The aim of this paper is to examine the reliability of a cyber-physical microgrid as a part of a smart distribution grid to evaluate the impact of the integration of information and communication technologies into the system and the impact of non-dispatchable renewable energy resources, that is, photovoltaic and wind farms. This paper proposes a framework for developing reliability assessment tools for a grid-connected microgrid with a hierarchical three-level and communication-based control system. Emphasis is laid on incorporating the interdependencies between the cyber system and the microgrid and on detailed models of renewable energy resources.

1 | INTRODUCTION

1.1 | Aim and motivation

Moving towards a smart distribution system is vital due to many concerns and requirements of modern power system; for example, the integration of distributed renewable energy resources (RERs), the growing number of electric vehicles, demand-side management programs, generation-side management, and switching [1–3]. These requirements can be achieved by the deployment of Information and Communication Technologies (ICTs) in the distribution system. These technologies increase the functionality of the distribution system by facilitating system (automated) control, peer to peer communication, monitoring, protection, and data gathering and processing [4]. As such, the effective operation of the modern distribution system without ICTs seems to be impossible. Since the distribution system becomes increasingly dependent on the operation of ICTs, it is essential for ICTs to be reliable.

Firstly, due to the large deployment of ICTs, the smart distribution system is by nature a cyber-physical system [5]. Cyber-physical systems can be defined as *"physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core"* [6]. A cyber-physical power system (CPPS) consists of two interdependent parts—cyber and power infrastructures—whose operation is highly interdependent. These interdependencies between cyber and physical power systems can be divided into three categories: common cause, direct interdependency and indirect interdependency [7]. Components within both systems can fail due to a common cause. The reason could be that the systems are geographically close. In the case of direct interdependency, failure in one infrastructure can directly cause failure(s) in another one. In the case of indirect interdependency, failure in one infrastructure does not directly lead to a failure in the other, but it can intensify an independent failure in the other infrastructure. Consequently, failure in the cyber system causes direct and indirect power system failures. Traditionally, in order to evaluate the power sys-

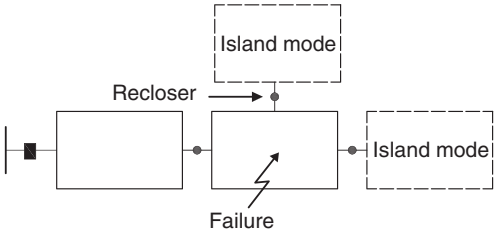

FIGURE 1 Typical multi-microgrid radial distribution system

tem reliability, it was assumed that the cyber system was ideal. However, with higher penetration of ICTs into the power system, their impact needs to be incorporated into the evaluation of the system performance and the assumption of ideality is no longer valid [8]. Accordingly, it is essential to develop methodologies to analyse the reliability of CPPS by incorporating the interdependencies between cyber and distribution systems into the modelling.

Secondly, greater penetration of distributed RERs has changed the operation of the distribution system in recent years [9]. To cope with this, and to promote the secure and efficient operation of the distribution system as well as its controllability, a distribution system can be partitioned into a number of microgrids [10] thanks to the development of ICTs. The implementation of microgrids in the smart distribution system is straightforward and assists the execution of many functions therein, for example, higher integration of RERs, improved reliability, load control, self-healing, and asset utilisation. For instance, self-healing can be carried out by switching to the island mode during outages in the upstream network. By way of illustration, a multi-microgrid smart distribution system is indicated in Figure 1. As can be seen in this figure, outages in the upstream network may result in islanded microgrids, in which available distributed generators (DGs) within can supply all or some of the consumers (with respect to the generation level) without obtaining power from the electric utility. A highly reliable electricity supply is thus provided via available DGs due to the reliability of the microgrid and its ability to operate in island mode. In this regard, the microgrid energy management system is the key element of microgrid operation. It consists of the control functions that enable the microgrid as a unit that can operate both in grid-connected mode and autonomously. Accordingly, it is essential that the impacts of the failure of the control system employed for the operation of a microgrid are studied exclusively during the evaluation of microgrid reliability.

1.2 | Background

The reliability of CPPS is relatively a new topic. However, it has attracted researchers' interest in recent years and is already a major topic among both researchers and engineers [11–33]. Generally, a cyber network may fail because of internal and/or external factors. Internal factors, by which the performance of the cyber network and its configuration can be assessed, consist of random failures and unavailability of cyber components as well as malfunction of the cyber network due to the packet loss, packet delay, and/or errors in data. Cyberattacks (intrusion) are classified as external factors [8]. Analysis of cyberattacks is related to the security of the system which is mainly termed cybersecurity. Due to the distinct origination, modelling frameworks and purposes, the impacts of these two factors on the reliability of CPPS are generally analysed independently [11]. Reference [12] gives a review of cybersecurity in the power grid. The focus of this paper is to evaluate the impact of random failures and the unavailability of cyber components on the reliability of Cyber-Physical MicroGrid (CPMG).

Current research on the reliability of CPPS is focused on the interdependency modelling and reliability assessment methodologies. Furthermore, in the same manner as conventional power systems, due to the differences in structure and complexities of evaluating the system as a whole, the reliability of CPPS is independently evaluated for different parts of the power system, for example, cyber-physical composite system and cyber-physical distribution system (CPDS) which may include CPMG.

The cyber system is dependent on the power system because of its required power supply. The cyber system's elements mostly work with uninterrupted power supply and their failure (because of lack of power supply) has not been studied yet in the literature related to the evaluation of CPPS reliability. However, the power system operation is strongly dependent on the operation of the cyber system. Based on the specific applications, these dependencies have been modelled differently for different functionalities.

As mentioned before, interdependencies between cyber and physical power system are categorised into common cause, direct interdependency and indirect interdependency [7]. Various direct and indirect interdependencies have been introduced in the literature, for example, direct interdependency between a feeder in a distribution system and the related cyber elements, particularly energy management units, the control centre (server) and the elements required for transmitting the data to the control centre [13, 14]; the indirect interdependency between protection and monitoring systems with the related equipment in the power system [15]; the indirect interdependency between the cyber fault and distribution automation system in distribution networks [16], the direct interdependency between DGs and loads in a microgrid with their related microcontrollers [14]; and the indirect interdependency between circuit breaker controller (CBC) and the circuit breaker [17].

Generally, two reliability assessment methodologies for analysis and calculation of CPPS reliability are presented in the literature, namely mathematical analysis (an analytical method) [13, 15, 18–24] and modelling based on simulation [14, 16, 17, 25–28]. A CPPS is an interdependent complex network [29] and thus employing analytical methods needs some simplification assumptions. References [18] and [19] used a reliability block diagram to provide a risk assessment method for cascading failure and to calculate the reliability of a composite system, respectively. Percolation theory was used in [29] to model the cascading failure in a smart grid. Reference [28] used the pseudo Monte Carlo simulation (MCS) to calculate the reliability of a CPDS for a simple case. Both sequential and non-sequential

TABLE 1 Reliability assessment methodologies and the application in the literature

Reference(s)	Methodology	Application
[13]	Analytical	Isolated microgrid
[14, 17]	MCS	Isolated microgrid
[15]	Analytical	High-voltage substation
[16, 23, 24]	MCS	Distribution system
[18, 19]	Reliability block diagram	Composite system
[25–27]	MCS	Composite system
[28]	Pseudo MCS	Distribution system
[29]	Percolation theory	Distribution system
[30]	Both analytical and MCS	Distribution system
[31]	Co-simulation	Distribution system

MCS have been used to calculate the reliability of a cyber-physical composite system [25–27], a CPDS [16, 23, 24] and an isolated CPMG [14, 17]. A combination of both methods has also been used [30]. Co-simulation is another methodology that was used to calculate the reliability of a CPDS; for example, reference [31] proposed a co-simulation platform to incorporate the impact of a cyber system into the reliability assessment of CPDS. Table 1 gives a summary of the methodologies and their application in the literature.

1.3 | Contribution

In light of above review, it is obvious that very few studies in the literature have assessed the reliability of a CPMG [14, 17]. Both of these studies on CPMGs have only evaluated the reliability of isolated microgrids and did not address grid-connected microgrids. Although the isolated microgrid has many applications, microgrids generally operate connected to the grid in smart distribution systems. Since an isolated microgrid is a stand-alone system, it does not require coordination with the other entities outside the microgrid, such as Distribution Management System (DMS). In this case, the microgrid control centre (MGCC) and the local controllers of DG units are entirely responsible for the operation of the microgrid. In isolated microgrids, there is usually a dispatchable DG resource that, in its working state, is able to supply all loads in the microgrid. Due to the green shift in energy and the increasing penetration of non-dispatchable RERs (such as distributed wind and photo-voltaic (PV) farms) in the smart distribution system, this is not the case for a practical CPMG in a distribution system. In this case, the microgrid is connected to the distribution system at a Point of Interconnection (POI), and, therefore, it can sell/purchase energy to/from the grid. Therefore, a coordination between the microgrid and distribution system is necessary. This coordination requires a new control layer and ICTs which are responsible for the operation of the smart distribution system and the coordination between distribution system and microgrid at the POI. The new control layer changes the required cyber system, and new interdependencies between the cyber and power components are brought into the picture. There is a lack of knowledge on what these interdependencies between components of a cyber system and a grid-connected microgrid are. The impact of these interdependencies on the reliability of microgrid affects the design of both cyber system and physical-microgrid. Therefore, determining these interdependencies and studying their impact on the reliability indices are very crucial. This paper seeks to fill this gap by determining the interdependencies between the cyber and power components in a grid-connected CPMG equipped with a hierarchical three-layer control system, and by evaluating the CPMG reliability. In addition to the proposed systematic approach, this paper contributes as follows:

i. A simple method for the evaluation of the cyber links' availability is proposed in the form of a 'structure function'.
ii. The impact of non-ideal cyber components on the load shedding in a CPMG and their impact on the reliability is evaluated. For this purpose, three polices for load shedding are taken into account and compared.
iii. During the study, it was seen that traditional reliability indices could not capture the impact of failure of the local controllers of the wind farm, PV farm, and ESS, and, therefore, an economic index is proposed to capture their impact on the CPMG.
iv. A detailed model of a PV farm is proposed that can be used in alignment with MCS or to directly derive an analytical solution for the PV farm.

1.4 | Paper structure

The rest of the paper is organised as follows: In Section 2, the modelling of the power system components is described. Section 3 gives an explanation of the cyber system infrastructure and modelling. Methodologies for the operation of the system in the grid-connected and the island modes are presented in Section 4. Section 5 applies the proposed methodology to a case and carries out a relevant sensitivity analysis for various critical elements. Finally, Section 6 concludes the paper.

2 | MODELLING OF THE POWER SYSTEM COMPONENT

This study considers two states—working and failed—for the power components other than the wind and PV farms. Failure of the components is a stochastic process, and the times to repair and failure are assumed to follow exponential distribution.

$$f(x) = \zeta e^{-\zeta x}. \tag{1}$$

Therefore, the time to the next event can be sampled using the following random variate:

$$X = -\frac{\ln(U)}{\zeta}, \tag{2}$$

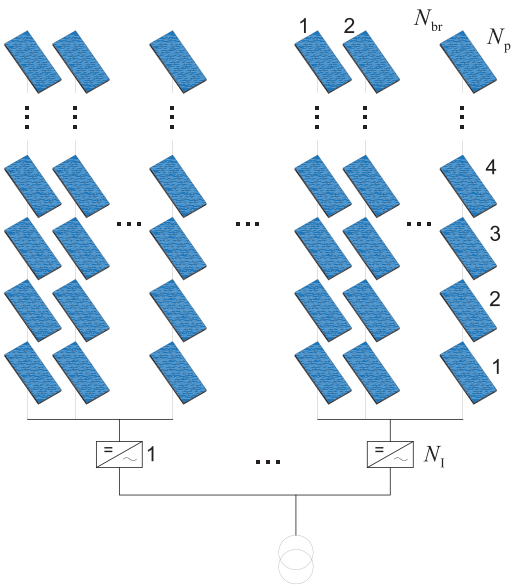

FIGURE 2 Configuration of a multi-string inverter PV farm

where U is a uniformly distributed random variate over [0,1]. In (2), with respect to the state—working and failed—of the component, failure rate λ or repair rate μ is used in place of ζ, respectively. Equation (2) is used repeatedly to sample up and down times (X) for each component during the entire simulation period.

2.1 | Modelling of the PV farm

2.1.1 | Failure and repair process

PV modules and inverters are connected in different configurations, namely, central inverter, micro-inverter, multi-string inverter, and string inverter [32]. This paper considers the multi-string configuration indicated in Figure 2; however, the methodology with slight changes can be implemented for other configurations. The proposed model is the continuation of the work presented in [33]. Reference [33] samples the hourly state of each component in the PV farm using non-sequential MCS, individually. Due to the large number of the PV panels, a large amount of sampling is required for each time period in this method. In addition, this method is only applicable to be used with MCS. To overcome these limitations, a combination of the analytical and simulation-based methods is proposed in this study to model the PV farm. Note that this model can be used to derive an analytical solution for the reliability of a detailed PV farm directly, or it can be used in alignment with MCS as explained in the following:

Modelling each branch: It is assumed that failure in any of the PV panels in one branch will cause the separation of that branch from the unit since they are connected in series. Moreover, since the failure rate of individual panels is much smaller than their repair rate ($\lambda_p \ll \mu_p$), it is assumed that the failure and repair of panels are statistically independent in one branch.

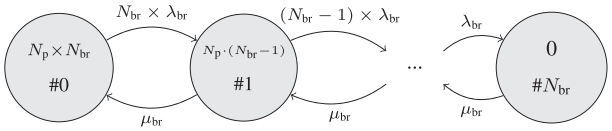

FIGURE 3 State diagram for multiple branches connected to one inverter

Thus, the panels in one branch can be considered as a series system, and consequently the failure rate of each branch is equal to the number of PV panels in that branch N_p times the individual failure rate λ_p of each panel.

$$\lambda_{br} = N_p \times \lambda_p. \tag{3}$$

The availability A_{br} and unavailability U_{br} of a branch with N_p identical PV panels can be calculated as follows:

$$A_{br} = \prod_{1}^{N_p} \left(\frac{\mu_p}{\mu_p + \lambda_p} \right) = \left(\frac{\mu_p}{\mu_p + \lambda_p} \right)^{N_p}, \tag{4}$$

$$U_{br} = 1 - A_{br} = 1 - \left(\frac{\mu_p}{\mu_p + \lambda_p} \right)^{N_p}. \tag{5}$$

The overall system balance equation for each branch is as follows:

$$\frac{A_{br}}{U_{br}} = \frac{\mu_{br}}{\lambda_{br}}. \tag{6}$$

Using Equations (3)–(6), the repair rate of a branch is calculated as follows:

$$\mu_{br} = \lambda_{br} \cdot \frac{A_{br}}{U_{br}} \approx \mu_p, \tag{7}$$

where the approximation $\mu_{br} \approx \mu_p$ is made because $\lambda_p \ll \mu_p$. However, the exat amount is used in this study.

Modelling multiple branches connected to one inverter: The power production of the branches connected to one inverter can be modelled using the state diagram shown in Figure 3. The first row in each circle indicates the generation capacity of PV panels connected to one inverter, where N_b is the number of working branches connected to one inverter and N_p is the number of panels in each branch. The number assigned to each state (second row in each circle) is equal to the number of failed branches. Note that only one technical repair team is considered for repairing the branches connected to one inverter. If there is more than one repair team, the repair rate in each state is *minimum* {number of the failed branches, number of repair teams} $\times \mu_{br}$.

Sequential MCS is employed to sample the state of the number of failed branches connected to one inverter, as per Figure 3. To this end, q random numbers equal to the number of possible transitions from the current state are generated from the uniform distribution. Then the possible transition times out of the current state for each generated uniform random number

are calculated using Equation (2), where ζ is the possible transition rates out of the current state (e.g. if current state of system is #1 then the possible transition rates are $(N_{br}-1)\times\lambda_{br}$ and μ_{br}). The smallest of the calculated transition times is the time to the next state and the corresponding state is the next state. The state of the inverter is sampled by a two-state Markov model to determine it as working or not working using MCS. In a sampled state, the overall capacity of PV panels connected to the inverter i (C_i) is as follows:

$$C_i = \begin{cases} P^{p,rated}\left(N_p \times (N_{br} - j_i)\right) & : \text{Inverter } i \text{ is working,} \\ 0 & : \text{Inverter } i \text{ is not working,} \end{cases} \tag{8}$$

where $P^{p,rated}$ is the rated power of a PV panel and j_i is the number of failed branches connected to the inverter i.

Modelling the whole PV farm: Failure of the transformer between the PV farm and the grid results in the failure of the unit. The state of the transformer, either as working or not working, is sampled using sequential MCS. Therefore, the overall capacity of the PV farm (C^{pv}) with N_I inverters, shown in Figure 2, in a sampled state is as follows:

$$C^{pv} = \begin{cases} \sum_{i=1}^{N_I} C_i & : \text{Transformer is working,} \\ 0 & : \text{Transformer is not working.} \end{cases} \tag{9}$$

2.1.2 | Output power of a PV farm regardless of failure

Solar radiation is uncertain and can be modelled as a stochastic process in which the random variable is solar radiation and the index is time. The uncertainty of solar radiation is modelled using beta Probability Density Functions (PDFs) [10], as shown in the following equation, given that $0 \le S \le 1$, $\alpha \ge 0$ and $\beta \ge 0$:

$$f(S;\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} S^{\alpha-1}(1-S)^{\beta-1}, \tag{10}$$

where α and β are the parameters of the beta distribution function and S is solar radiation.

In order to model the PV production, each year is split into four seasons. Then 24 hourly PDFs are considered for each season, and each is assigned to a specific hourly time period for the entire season. Five years of historical data are used to estimate the PDFs. Presuming a month to be 30 days, the number of irradiance samples for each PDF is then 450 (5 years × 30 days per month × 3 month per season). It should be noted that 12 hourly PDFs (from 6:00 AM to 6:00 PM) are estimated for the solar irradiance. For the remaining hours of a day, the amount of solar irradiance is zero based on historical data used in this study. These hourly PDFs are then used to sample the solar radiation. The output power of the PV farm is dependent on the solar radiation, ambient temperature, and the characteristic of the PV modules. In this study, simple algebraic equations based on [34] are used to estimate the output power of PV farm P^{PV} for each time period using the sampled solar radiation.

Finally, the following equation gives the overall hourly output power of the PV farm by considering its random nature and failure.

$$P^{PV,avail} = P^{PV} \cdot \left(\frac{C^{pv}}{C^{pv,nom}}\right), \tag{11}$$

where $C^{pv,nom}$ is the nominal capacity of the PV farm.

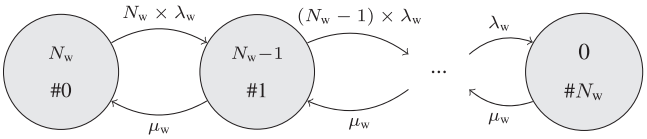

FIGURE 4 State diagram for a wind farm with N_w WTs

2.2 | Modelling of a wind farm

2.2.1 | Failure and repair process

A two-state Markov model is employed to model each individual wind turbine (WT). Generally, the failure of a WT has no impact on the probability of the failure of a second WT. Therefore, WTs can be assumed to be statistically independent of each other [35]. Consequently, there are 2^{N_w} possible states for a wind farm with N_w WTs. However, if all WTs in a wind farm are identical, which is the case in most wind farms, the number of states can be reduced to $N_w + 1$. Figure 4 is the state transition diagram for a wind farm with N_w WTs. The number of each state is equal to the number of failed WTs in that state. Sequential MCS is used to sample the number of failed WTs using the state diagram in Figure 4. To build this model, the following assumptions have been made:

i. The failure rates λ_w of WTs are constant and not dependent on the wind speed.
ii. There is only one technical repair team on the farm, and WTs cannot be repaired simultaneously. If there is more than one repair team, the repair rate of each state is equal to *minimum* {number of repair teams, number of failed WTs}×μ_{br}.

The manner explained in Section 2.1.1 is utilised to sample from this Markov model. The number of working wind turbines is calculated as follows:

$$N_{\mathbf{w}}^{avail} = (N_w - j_w), \tag{12}$$

where j_w is the number of failed wind turbines at the corresponding state. Note that the available generation capacity of the wind farm is $N_{\mathbf{w}}^{avail}$ times the rated power of one WT. $N_{\mathbf{w}}^{avail}$ is zero if the transformer that connects the wind farm to the grid has failed.

2.2.2 | Output power of a wind farm

The output power of a wind farm is dependent on the wind speed and the characteristic features of the WTs. The behaviour of wind speed is uncertain and can be modelled as a stochastic process. Weibull distribution [36] is employed here to model the hourly wind speed given by the following PDF:

$$f(v) = \left(\frac{k}{c}\right) \cdot \left(\frac{2v}{c}\right) \cdot \exp\left[-\left(\frac{v}{c}\right)^{k}\right], \tag{13}$$

where k is the shape factor and c is the scale factor. In the same manner as for solar radiation, wind speed is modelled using 24 hourly Weibull PDFs for each season, estimated using five years of historical data. Then, the hourly wind speeds are sampled using the related PDFs. Based on the hourly sampled wind speed and characteristic features of wind turbines, the hourly output power of the wind farm P^{W} is estimated as follows [36]:

$$P^{W} = \begin{cases} N_{w} \cdot P^{WT,rated} \cdot (A + Bv + Cv^{2}) & : v^{ci} \le v \le v^{r}, \\ N_{w} \cdot P^{WT,rated} & : v^{r} \le v \le v^{co}, \\ 0 & : \text{otherwise}, \end{cases} \tag{14}$$

where $P^{WT,rated}$ is the rated power of one WT. v^{ci}, v^{co}, and v^{r} are the cut in, cut out, and rated speeds of the WT, respectively.

Finally, the overall output power of the wind farm is calculated by considering its random nature and failure as follows:

$$P^{W,avail} = P^{W} \cdot \left(\frac{N_{w}^{avail}}{N_{w}}\right). \tag{15}$$

Note that in Sections 2.1 and 2.2, subscript t was eliminated for the sake of simplicity.

3 | MODELLING OF THE CYBER SYSTEM

3.1 | Cyber system architecture

A Cyber system deployed in a power system can be categorised into three layers [8]: decision layer, communication layer, and interface layer. The schematic configuration of the cyber system considered in this paper is depicted in Figure 5.

In a microgrid, the decision layer, that is, the MGCC, may include hardware, software, and human-machine interfaces. First, the MGCC receives the information from the network and then, by processing the data, proper commands are submitted to the local control panels and actuators for different purposes, for example, frequency and voltage control, maintaining the power balance, and system protection and restoration. In this study, the data are processed to minimise the operation cost and to maintain the power balance in the system. Note that MGCC is also responsible for the exchange of the information with the upper network.

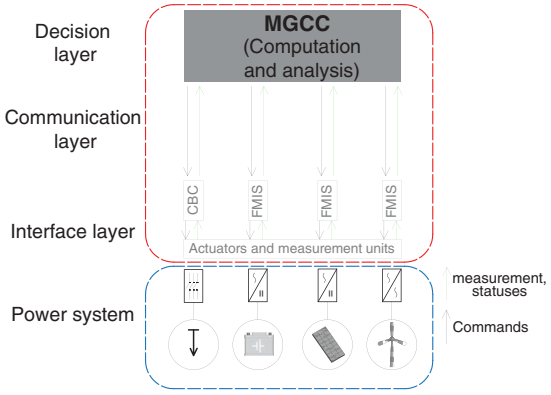

FIGURE 5 Configuration of the three-layer cyber system

The communication layer is a bidirectional bridge between the decision and interface layers, and its function is to transfer data, including statuses, commands, and feedback signals, between the MGCC, local control panels, and the actuators in the interface layer. Different communication media—wireless or wired—can be employed in this layer. In this paper, fibre-optic lines and network switches (SWs) have been considered in the communication layer.

The interface layer includes local control panels, intelligent metering devices and sensors, communication modules, and actuators. Some critical operations, such as those of the protection system, can be performed locally using predetermined settings in the local control panel of the switches. However, the status of switches should be submitted to the control centre by these local controllers.

3.2 | Modelling cyber system components

In the same manner as explained in Section 2, the cyber components are also modelled using a two-state Markov model. However, in regards to the cyber system used in the power system, both the failure of the cyber element(s) and a failure in the links between different elements can affect the system's operation and, consequently, the reliability. For instance, a failure in either the local controller of a DG unit, that is, a field measurement information system (FMIS), or in the cyber link between this element and the MGCC can cause the unavailability of the status and measurement signal from the corresponding unit to the MGCC and the command signal from the MGCC to this unit. Hence, it is necessary to model the availability of cyber links to study the reliability of the system.

3.3 | Availability of the cyber links

The availability of the cyber link between each cyber component in the interface layer and the MGCC is expressed in the form of a structure function based on the state of the individual components. A route table is then developed to determine the availability of the cyber links required for transmitting data. The structure function of a system is defined as a logical

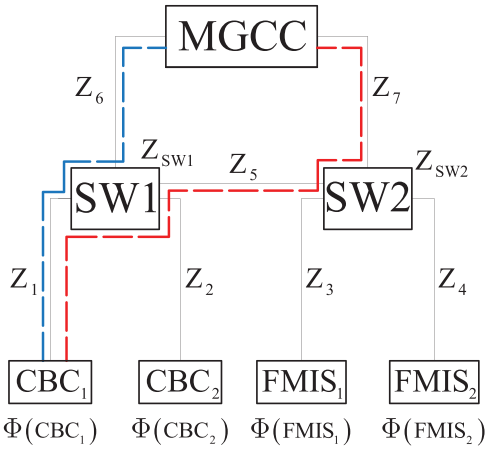

FIGURE 6 Schematic configuration of a simple cyber system

function that indicates whether the system is working or has failed. In this paper, the structure function is expressed in the form of a minimal sum-of-products. A minimal sum-of-products is an irreducible Boolean sum (logical OR) of minterms, where a minterm is a Boolean product (logical OR) that may include a variable only once. Here, each minterm corresponds to a *minimal path set*. For instance, considering the simple cyber system shown in Figure 6, there are two minimal path sets between CBC_1 and MGCC: $\{Z_{CBC_1}, Z_1, Z_{SW_1}, Z_6\}$ and $\{Z_{CBC_1}, Z_1, Z_{SW_1}, Z_5, Z_{SW_2}, Z_7\}$. Therefore, the minimal sum-of-products is expressed as follows:

$$\Phi(CBC_1) = (Z_{CBC_1} \cdot Z_1 \cdot Z_{SW_1} \cdot Z_6) + (Z_{CBC_1} \cdot Z_1 \cdot Z_{SW_1} \cdot Z_5 \cdot Z_{SW_2} \cdot Z_7), \quad (16)$$

where $\Phi(CBC_1)$ is the state of the cyber link between cyber component CBC_1 and the MGCC, and its value is either one (cyber link is available) or zero (cyber link is not available). Z_* is the state of cyber component $*$, and its value is either one (working state) or zero (failed state). Note that the state of a component is sampled using sequential MCS based on its failure and repair rates. The link between CBC_1 and the MGCC is available if and only if $\Phi(CBC_1)$ is one. For instance, if SW1 fails, Z_{SW_1} is zero and then both minterms in Equation (16) are zero; as a result $\Phi(CBC_1)$ is zero and the related cyber link between the CBC_1 and the MGCC is not available. Another example is the failure of the fibre optic cable between SW1 and the MGCC. In this case, Z_6 is zero and, therefore, the first minterm in Equation (16) is equal to zero. However, as the second minterm is one, $\Phi(CBC_1)$ is one, indicating the availability of the cyber link between the CBC_1 and the MGCC.

3.4 | Interdependencies between cyber and power systems

Both the relevant direct interdependency and indirect interdependency between power and cyber components of a CPMG are modelled in this paper. Interdependencies between the different control units and microgrid and the consequences of these controller's failure will be explained in Section 4.1. The interdependencies at the Point of Interconnection (POI) and an assumption that has been made in this study are explained in Section 4.3.

In an automated power system, circuit breakers are used for system protection, restoration, reconfiguration, and load shedding purposes. These circuit breakers are equipped with a CBC and a communication module. Regarding the circuit breaker operation, different strategies, such as centralised, distributed, or local can be taken into account in an automated power system. Availability of CBCs are necessary for actions such as processing the local data, reporting the status of the circuit breaker, generating the execution command, and so on. Accordingly, the CBC's operation is necessary for the operation of the circuit breaker, and its failure results in the mis-operation of the circuit breaker when its action is required, which is an indirect interdependency. For example, in the case of contingencies during the operation of a microgrid, load shedding might be required, for which circuit breakers execute load interruption orders from the MGCC if a centralised control system is employed. In this case, if the relevant CBC or its cyber link fails, the MGCC should interrupt another load point to secure the operation of the microgrid, which might result in more loss of load. This is an indirect interdependency. The impact of the failure of cyber link on a CBC is dependent on the strategy employed for the operation of the circuit breaker. For example, if a circuit breaker is able to carry out its protection function locally, failure of the cyber link between its controller and the MGCC does not affect its protection function, but its status cannot be sent to the MGCC. If a centralised protection system is considered, the availability of the corresponding cyber link is necessary for the operation of the circuit breaker. In this case the cyber link's failure results in mis-operation mode of circuit breaker. In this study, the circuit breakers are employed for the load shedding purposes under a centralised controller.

4 | SYSTEM OPERATION

The operation of the system in a communication-based control system, as its name suggests, is achieved by a continuous communication between the controller of different microgrid components and the resources. This type of control system can be implemented as centralised or partly/fully distributed [37]. This study examines the impact of a centralised communication-based control system on the reliability of a microgrid. In centralised communication-based control, all the data are transmitted to the MGCC from the other controllers. The MGCC then processes the data and calculates the operational set points and then sends the control actions to the local controllers.

4.1 | Structure of the hierarchical control system

Figure 7 illustrates the structure of the three-layer control strategy implemented in this paper. The top layer, level 3, is the

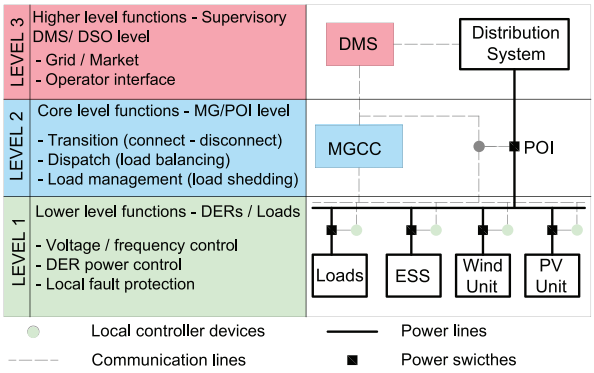

FIGURE 7 Three-layer configuration of a microgrid control strategy. There are more control functions for each level (IEEE 2030.7), but only relevant functions are indicated here

tertiary controller or distribution management system (DMS), and it is typically responsible for coordinating the microgrids to maintain the economy and security of the distribution grid [38]. DMS is usually recognised as a third party or as a part of the utility control centre. Its operation, nevertheless, is required for coordination between the microgrids. Consequently, it can be assumed that when the DMS and/or the cyber link between it and the MGGC have/has failed, the microgrid will be disconnected and operated in island mode, leaving the MGCC to perform the microgrid operations alone. The failure of the DMS does not cause the failure of a specific element in the power system; however, it forces the system to operate in island mode, which may impair the optimal operation of the microgrid and result in loss of load. The failure of this control unit can be regarded as direct interdependency, since its failure immediately results in changes in the operation of the system. Yet, since it might not necessarily influence the reliability, it has an indirect impact on it.

The intermediate layer, which is the centralised secondary control system or MGCC, is responsible for calculating the operation plans based on the predicted amount of power generated by RERs; and the information that is received through communication channel from the DMS (e.g. market prices), the measurement units, and the local control units. The output power of DGs, the consumption of loads, and the schedule of ESS in real-time operation are then adjusted accordingly to ensure the power balance, voltage, and frequency stability. Based on the IEEE std 2030.7, the functionalities to be served by core dispatch function, that is, the MGCC, are as follows: (i) maintaining the power balance between generation and load under normal and island mode operating conditions; (ii) re-dispatching the controllable resources to react to the internal events corresponding to the load and generation profiles; and (iii) responding to external orders (such as interconnection agreement requirements and external events) by re-dispatching resources. Since a centralised controller is considered in this level, its operation is necessary for the operation of the microgrid, and, thus, the microgrid will be shut down if this controller fails. This is a direct interdependency between the cyber and power systems.

The bottom layer consists of CBCs and local controllers of the DGs (FMISs). These perform the primary adjustment of voltage and frequency in DGs and ESS. The output power of DGs and ESS are adjusted via the MGCC based on the dispatch orders. These controllers send the information to the MGCC and execute its dispatch commands. The operation of these control units is in the range of sub-seconds to 5/10 min, based on IEEE 2030.7, and is beyond the scope of this paper. Nonetheless, their operation is essential for the operation of the units under control [14, 16] and, thus, is regarded as a direct interdependency.

4.2 | Modes of operation

A microgrid is connected to the grid at the POI. A microgrid can operate in either grid-connected mode or island mode. In grid-connected mode, the microgrid operates according to IEEE 1547-2003. The transition to island mode can be caused by intentional or unintentional events. In this paper, the microgrid operates in grid-connected mode and changes to island mode only when there is an event that forces it to, and, therefore, there is no intentional islanding.

The core dispatch function, the MGCC, consists of the necessary dispatching logic for different modes of operation. These modes of operation include steady-state grid-connected mode M_1, steady-state island mode M_2, and the transition between these modes. A dispatch rule is required for each dispatch mode. Based on each dispatch rule, the core dispatch function sends a set of commands to the microgrid assets to execute dispatch orders. This paper only deals with steady-state modes; therefore, two sets of dispatch rules are formulated for each mode of operation in Sections 4.2.1 and 4.2.2. The objective in grid-connected mode is the economic operation of the microgrid while maintaining the power balance. In island mode operation, the MGCC regulates the output power of the DGs and load consumption and schedules the ESS to maintain the power balance and to ensure the secure operation of the microgrid. Note that the dispatch function requires information on the microgrid's states to carry out its functions. In this paper, it is assumed that the states of all loads are ideally estimated and, therefore, are known for the calculation of the necessary orders except when all links to the MGCC are interrupted.

Note that the following assumptions have been made to derive the operation functions of the microgrid: (i) this study only considers active power flow. To this end, capacity limits of DERs, capacity limits of ESS and, active power balance within the microgrid are taken into account, (ii) this study assumes that the voltage level of all buses can be properly regulated within allowable limits. Thus, the constraints related to voltage are not taken into account.These assumptions are widely accepted in long-term reliability studies of microgrids and distribution systems [13–19]. If it is nevertheless required, in particular cases, an AC power flow can be employed instead, at the cost of increasing computational burden.

4.2.1 | Grid-connected operation

As mentioned earlier, economic operation is the objective in grid-connected mode. In this mode, an individual microgrid unit can purchase deficit energy from the grid or sell the excess energy to the grid. The MGCC receives the market signals from the DMS and then calculates the optimal operation of the microgrid. To this end, the following optimisation problem is employed to minimise the cost of the purchased energy:

$$\underset{P_t^{\mathrm{POI}},P_t^{\mathrm{dch}},P_t^{\mathrm{ch}}}{\text{Minimise}} \{\mathrm{COST}\} = \sum_{t\in T} P_t^{\mathrm{POI}} \cdot \rho_t \cdot d_t, \tag{17}$$

where P_t^{POI} and ρ_t are the transmitted power between the microgrid and the upstream grid (at POI) and the energy price at time period t, respectively. d_t is the duration of time period t which is one hour. A negative amount of P_t^{POI} means that the microgrid sells the power to the grid. The operational constraints of the system are the power balance and the operation of the ESS, as follows:

$$P_t^{\mathrm{POI}} + P_t^{\mathrm{PV,avail}} + P_t^{\mathrm{W,avail}} + P_t^{\mathrm{bat}} = L_t^{\mathrm{tot}} \quad \forall t \in T, \tag{18}$$

$$P_t^{\mathrm{bat}} = \eta^{\mathrm{dch}} P_t^{\mathrm{dch}} - P_t^{\mathrm{ch}} \quad \forall t \in T, \tag{19}$$

$$SOC_t = SOC_{t-1} - P_t^{\mathrm{dch}} \cdot d_t + \eta^{\mathrm{ch}} P_t^{\mathrm{ch}} \cdot d_t \quad \forall t \in T, \tag{20}$$

$$SOC_0 = C_0, \tag{21}$$

$$SOC^{\min} \le SOC_t \le SOC^{\max} \quad \forall t \in T, \tag{22}$$

$$0 \le P_t^{\mathrm{dch}} \le P^{\mathrm{dch,max}} \quad \forall t \in T, \tag{23}$$

$$0 \le P_t^{\mathrm{ch}} \le P^{\mathrm{ch,max}} \quad \forall t \in T. \tag{24}$$

Equation (18) maintains the power balance of the microgrid, where $P_t^{\mathrm{PV,avail}}$ and $P_t^{\mathrm{W,avail}}$ are the available output powers of the PV and wind farms in time period t, respectively. The output powers of wind and PV farms are considered as parameters, which means these units inject their maximum available generation to the microgrid in the corresponding time period. L_t^{tot} is the aggregated load in the time period t. Equation (19) calculates the ESS power in the grid side, where P_t^{bat} is the amount of charging or discharging power of ESS in the grid side. $\eta^{\mathrm{dch}} P_t^{\mathrm{dch}}$ is the amount of injected power of the ESS to the grid in the grid side, and P_t^{ch} is the injected power to the ESS in the grid side. Obviously, a positive value of P_t^{bat} indicates the discharging state and a negative value indicates the charging state of ESS. Equation (20) yields the State of Charge (SOC) of the ESS in time period t with respect to its amount in the previous time period and the current charging/discharging value. Equation (22) limits the SOC of the ESS to the minimum allowable amount $SOC^{\min}$ and the maximum energy capacity of ESS $SOC^{\max}$. Equations (23) and (24) limit the charging and discharging power of ESS where $P_t^{\mathrm{ch,max}}$ and $P_t^{\mathrm{dch,max}}$ are the maximum charging and discharging power in each time period, respectively.

The failure of the ESS unit, its FMIS, and/or the cyber link between its FMIS and the MGCC result in the separation of this unit from the microgrid. In this case, the aforementioned optimisation problem is not required, and the difference between the generation and the load is traded between the grid and the microgrid; the SOC of the ESS is assumed to remain the same as its previous amount.

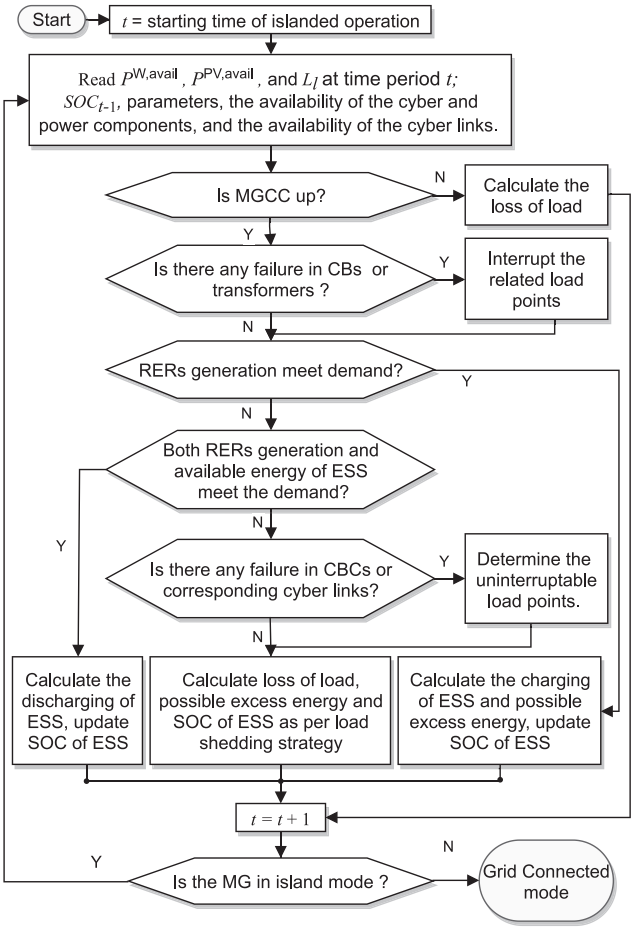

FIGURE 8 Flowchart for the operation of the microgrid during island mode

4.2.2 | Island mode operation

Island mode operation can be further divided into healthy M_{20}, emergency M_{21}, and shutdown M_{22} modes based on the amount of interrupted load. In the healthy operation M_{20}, all the loads in the microgrid are supplied using the generation resources and ESS (if required) in the microgrid. In this situation, the ESS might be charged or discharged, and there may be excess energy which is dumped. When no load in microgrid is supplied, the microgrid is recognised as being in shutdown mode M_{22}. This can occur when there is no power generation in the microgrid, when the MGCC is down, and when the power balance cannot be met because of the failure of the cyber elements required for this purpose. For further analysis, some of the loads can be assumed to be critical based on their importance, but this goes beyond the scope of this paper. The operation of the system in island mode is illustrated in Figure 8. Based on the level of cyber equipment deployed in the microgrid, the MGCC may

have control over the smaller loads or a bulk load at a bus. Here, three different policies for load curtailment in emergency mode are presented and compared to study the impact of the cyber system on load curtailment.

1. **Policy #1, based on predetermined load shedding priority (using a look-up table)**: First, the operator ranks the loads to be curtailed sequentially. Then, in the case of a deficit in the power generation, the loads are curtailed sequentially based on the predetermined list until the load is equal to or less than the generation.
2. **Policy #2, minimising load curtailment using an optimisation function as follows**:

$$\underset{P_t^{\mathrm{dch}},P_t^{\mathrm{ch}},P_t^{\mathrm{ex}},y_t,x_{l,t};l\in 1:N_l}{\text{Minimise}} \quad OF(t)=\overbrace{\sum_{l=1}^{N_l}\alpha_l\cdot x_{l,t}\cdot L_{l,t}}^{\text{Load curtailment}}+\overbrace{P_t^{\mathrm{ex}}}^{\text{Excess power}}, \tag{25}$$

S.t.

$$P_t^{\mathrm{PV,avail}}+P_t^{\mathrm{W,avail}}+P_t^{\mathrm{bat}}-P_t^{\mathrm{ex}}=L_t-\sum_{l=1}^{N_l}x_{l,t}\cdot L_{l,t}, \tag{26}$$

$$P_t^{\mathrm{bat}}=\eta^{\mathrm{dch}}P_t^{\mathrm{dch}}-P_t^{\mathrm{ch}}, \tag{27}$$

$$x_{l,t}=\{0,1\}\qquad \forall l\in 1:8\ \ \&\ \Phi(\mathrm{CBC}_{l,t})=1, \tag{28}$$

$$x_{l,t}=x_{l,t-1}\qquad \forall l\in 1:8\ \ \&\ \Phi(\mathrm{CBC}_{l,t})=0, \tag{29}$$

$$0\le P_t^{\mathrm{dch}}\le \min(P^{\mathrm{dch,max}},(SOC_{t-1}-SOC^{\min})/dt)\cdot y \tag{30}$$

$$0\le P_t^{\mathrm{ch}}\le \min(P^{\mathrm{ch,max}},(SOC^{\max}-SOC_{t-1})/\eta^{\mathrm{ch}}dt)\cdot(1-y) \tag{31}$$

$$P_t^{\mathrm{ex}}\ge 0. \tag{32}$$

The first term in the objective function minimises the curtailed load, where $x_{l,t}$ is a decision binary variable that determines if the load point l is to be curtailed or not in time period t. $x_{l,t}=1$ indicates that the pertinent load point is curtailed. α_l denotes the importance factor of each load point. If the importance factors of different load points are determined only by their Interruption Cost (IC), then α_l can be calculated using the following equation:

$$\alpha_l=\frac{IC_l}{\sum_{l=1}^{N_l}IC_l}. \tag{33}$$

The second term minimises the dumped energy by forcing the ESS to be charged. Since the loads are discrete, load curtailment and excess energy may occur simultaneously. For example, if there are two load points 0.5 MW and 1 MW and the generation in the microgrid is 1.2 MW and the ESS is not working, then the load 0.5 MW is curtailed and 0.2 MW generation remains, which should be dumped to maintain the power balance. When the ESS is available, the second term in the objective function forces the ESS to be charged to decrease the amount of dumped energy if any. Excess power P_t^{ex} is limited by Equation (32), whose value is zero when there is no excess power in the system. Constraint (26) maintains the power balance, and P_t^{bat} in (27) is the injected/received power to/from the microgrid. $\Phi(\mathrm{CBC}_{l,t})$ in Equations (28) and (29) shows the availability of the cyber link between the MGCC and the CBC for load point l at time period t. If the link is not available, $\Phi(\mathrm{CBC}_{l,t})=0$, the pertinent load point cannot be curtailed or re-supplied, and, therefore, $x_{l,t}$ maintains its previous state, according to Equation (29); otherwise, load point l can change its state if needed as per Equation (28). Equations (30) and (31) limit the charging and discharging power of ESS with respect to the maximum charging and discharging rates and the available energy capacity. Unlike the optimisation problem in Section 4.2.1, due to the structure of the optimisation problem in the present section, the optimum value of decision variables may result in simultaneous charging and discharging of ESS, and, therefore, a binary variable y is required to guarantee that the charging and discharging of ESS do not occur at the same time. The policy #2 of load shedding results in a mixed integer linear problem (MILP). When the problem is solved, the SOC of ESS is updated using Equation (20), giving the initial SOC for the next hour. It should be noted that when the ESS in not available due to any reason, the upper bounds of both Equations (30) and (31) are zero.
3. **Policy #3, minimising load curtailment assuming that individual loads are controllable**: This policy needs a higher penetration of cyber elements such as load controller for each bulk load point and each smaller load point. In this case, the load controller is assumed to be ideal, and, therefore, the load can be curtailed almost continuously. In this respect, the difference between the generation and the load gives the loss of load.

4.3 | Causal analysis of the operation mode at a POI

Unintentional islanding might occur due to the failure of both cyber and power components, based on the structure and design of the CPMG. In the case of the power system, a failure of the upstream network may result in islanding, and failure inside microgrid may result in the shutdown of the microgrid. In the case of cyber system, the failure of some components might lead to the islanding or shutdown of the microgrid, as illustrated in Figure 9, for a sample cyber system. As mentioned before, since a centralised controller is considered in this study, failure of the MGCC and its network switch result in shutdown mode of the microgrid. Second condition in Figure 9 checks the availability of the DMS, its network switch, and the cyber link between the MGCC and DMS. The unavailability of each of them disconnects the MGCC from the DMS and results in island mode

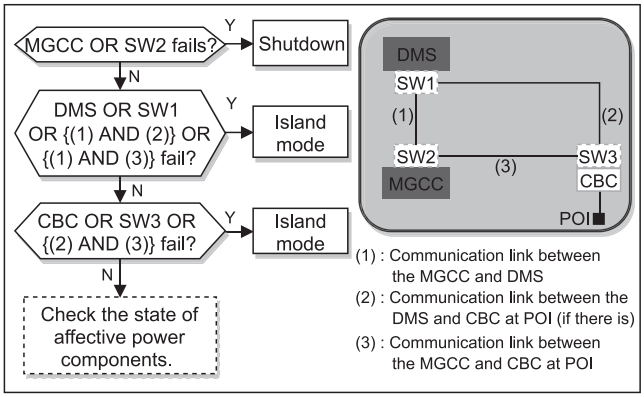

FIGURE 9 Impact of the failure of different elements of a cyber system on the mode of operation

operation. Here, it is assumed that availability of the local controller of the power switch at POI (SW3), and at least one of the cyber links between this controller and MGCC/DMS are necessary for the fail-safe operation of the system, and the unavailability of each will shift the system to island mode, as shown in third condition in Figure 9.

4.4 | Steps of the simulation

With respect to the generation of states for power elements proposed in Section 2 and for cyber elements presented in Section 3, the overall proposed algorithm according to the sequential MCS to calculate the reliability indices of CPMG is as follows:

Step 1 : Set the criteria for stopping the simulation. In this regard, the maximum number of simulation years and the precision e are considered.

Step 2 : Read the data, which includes the failure and repair rates of the cyber and power components, the historical data of wind speed and solar radiation, and the characteristics of the RER farms and ESS, to initialise the simulation process. Set the initial state of all components as working, and set the simulation time to 0.

Step 3 : Draw a uniformly distributed random variate over [0,1] for each element, and calculate the time to the next event using Equation (2). Note that for wind and PV farms, more than one random variate may be required using the method proposed in Section 2. Generate the states of the system's components—working or failed—and relevant times using sequential MCS for one year. For more details on sequential MCS, the reader is referred to [39]. Save the residual time for the next year. This step yields the system's yearly states, in which each state includes the availability of the equipment and its duration.

Step 4 : Select a system state chronologically.

Step 5 : Determine the availability of the cyber links as per the method explained in Section 3.3.

Step 6 : In each state of the system based on the state of individual components, ascertain the mode of operation of the microgrid. Based on the assumption in this paper, the system will shift to island mode due to the following events: failure of the DMS, the unavailability of the cyber link between the DMS and the MGCC, failure of the upstream grid, failure of the switch at the POI, failure of the CBC at the POI, and failure of all cyber links to the CBC at the POI. The MGCC will be in shutdown mode due to the following: failure inside the microgrid, failure of the MGCC, and failure of all cyber links to the MGCC. Otherwise, the system is in grid-connected mode.

Step 7 : Analyse the system according to the mode of operation. If the CPMG is in shutdown mode, the ESS remains unaltered and all load points are interrupted. In grid-connected mode, the power at the POI in each time period P_t^{POI} is calculated, and the state of the charge of ESS is updated based on the method proposed in Section 4.2.1. In island mode, the loss of load is calculated according to the flowchart illustrated in Figure 8. Note that loss of load due to the failure of various components, such as transformers and circuit breakers, needs to be calculated in both modes.

Step 8 : If there are more states in the year under consideration, go to step 4. Otherwise, save the computational time for the corresponding year and go to step 9.

Step 9 : Calculate coefficient of variation (COV) using Equation (34). This measure, as a dimensionless quantity, is defined as the ratio of the standard deviation of the sample mean to the sample mean.

$$COV = \sqrt{\frac{\mathrm{Var}(X)}{N \cdot \mathrm{E}^2(X)}}. \tag{34}$$

When the convergence criterion $COV < e$ is satisfied, reliability indices can be computed. If the accuracy of the estimate is acceptable, stop; otherwise, continue the simulation for the next year. A minimum number of simulation years is considered to avoid any local minimum that may be obtained during the first years when the algorithm is still far from convergence.

5 | RESULTS AND DISCUSSION

5.1 | Test case

Figure 10 illustrates the configuration of the AC microgrid under study in this paper. It is a part of feeder 4 at bus 6 of the Roy Billinton Test System (RBTS) distribution network presented in [40]. The microgrid has 11 load points consisting of agricultural and residential customers. It has a total peak load of 4.65 MW. The data related to the size and type of each load point and the length of the distribution lines can be found in [40]. The length of fibre optic cables are shown in Table 2. The following are added to form a microgrid: a 2.4 MW PV farm integrated into the microgrid through DC/AC inverters and a transformer (the rated power of each PV panel is 300 W, and 16 branches and 4 inverters are considered in the PV farm according to the configuration depicted in Figure 2); a 6 MW wind farm including four WTs (each turbine characteristic, rated power:

TABLE 2 Length of fibre optic cables. The length of fibre optic cables that are not listed here are 10 m

From	To	Length (km)	From	To	Length (km)	From	To	Length (km)
SW1	SW2	3.7	SW2	CBC_2	3.4	SW5	CBC_6	5.7
SW1	SW3	14.4	SW2	CBC_3	6.3	SW6	$FMIS_1$	0.1
SW1	SW4	16.9	SW3	CBC_8	0.75	SW6	$FMIS_2$	2
SW1	SW5	14.4	SW3	CBC_9	1.6	SW6	$FMIS_3$	4
SW1	SW6	3	SW3	CBC_{10}	4.8	FMIS	CBC	0.1
SW1	SW7	1	SW3	CBC_{11}	7.6			
SW1	SW8	8	SW5	CBC_5	3.2			

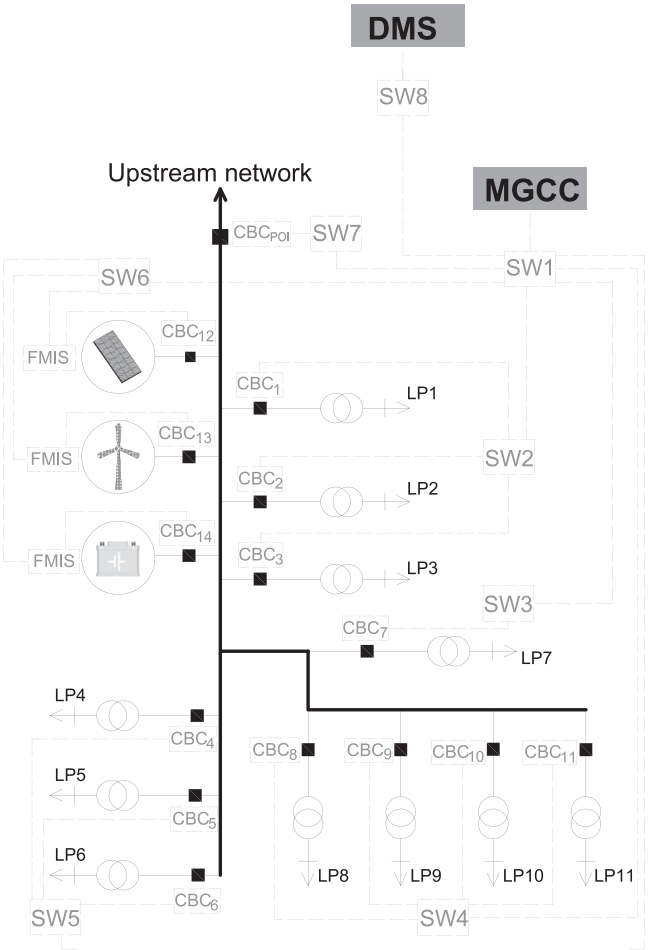

FIGURE 10 Configuration of the microgrid under study

1.5 MW; rated speed, cut-in and cut-out speeds: 10.5 m/s, 3.5 m/s, and 25 m/s, respectively); and a 3 MWh ESS connected to the microgrid through a bidirectional DC/AC inverter with a maximum hourly charging and discharging power of 0.5 MW. The charging and discharging efficiency of ESS is considered to 0.95. These values are related to the base case; however, different values of the capacity of RERs and ESS are implemented in this paper to study their impacts on the reliability of a CPMG. Note that the indices shown are expected values.

5.2 | Reliability parameters and simulation data

The failure rates and repair times of both the cyber and power components used in this study are shown in Table 3 ([17, 33 41]). The mean time to failure (MTTF) and the mean time to repair (MTTR) of the upstream grid are assumed to be 5200 and 55 h, respectively. IEEE-RTS load profile is used as the hourly chronological load profile. Historical data on the wind speed and solar radiation over five years in Spain at latitude 36.8573 and longitude −2.5147 [42] were used to estimate the output power of the corresponding units using the method explained in Section 2. Market prices are assumed to be deterministic. In this regard, Spanish electricity market prices of year 2019 [43] were used in this study. Figure 11 depicts the average, upper boundary, and lower boundary of the market prices.

5.3 | Impact of cyber system failure

In order to examine the impact of cyber system failure on CPMG reliability, the reliability indices expected energy not supplied (EENS) and loss of load probability (LOLP) are calculated for ideal and non-ideal power and cyber systems. It is assumed that the cyber and power systems are ideal in Cases 1 and 2, respectively. Case 3 illustrates the result when both systems can fail. Table 4 provides the EENS indices for different load points. The last column in this table is the percentage increase of EENS due to the failure of the cyber system as a result of both direct interdependency and indirect interdependency. Table 5 gives the percentage increase of the reliability indices of the whole microgrid owing to failures in the cyber system. As can be seen in this table, EENS and LOLP increase 12.2% and 11.5%, respectively, due to the failure of the cyber system.

5.4 | Analysis of the operation modes of the microgrid

The period of operation in each mode and the related probabilities are shown in Table 6. As expected, the CPMG operates in grid-connected mode most often. The probability, in this case, that the CPMG will operate in grid-connected mode is 0.984.

TABLE 3 Failure rates and repair times for both power and cyber components

Power Elements	Failure Rate (1/year)	Repair Time (h)	Cyber Elements	Failure Rate (1/year)	Repair Time (h)
Power line	0.091	9.5	Tertiary controller	0.07008	48
Transformer	0.002	75	Secondary controller	0.07008	48
Circuit breaker	0.0033	120.9	Primary controller	0.07008	48
PV panel	0.000133	48	Fibre optic	0.004	48
Inverter	0.253	20	Network switch	0.02	48
ESS	5	10	CBC	0.067	48
Wind turbine	1.1	36			

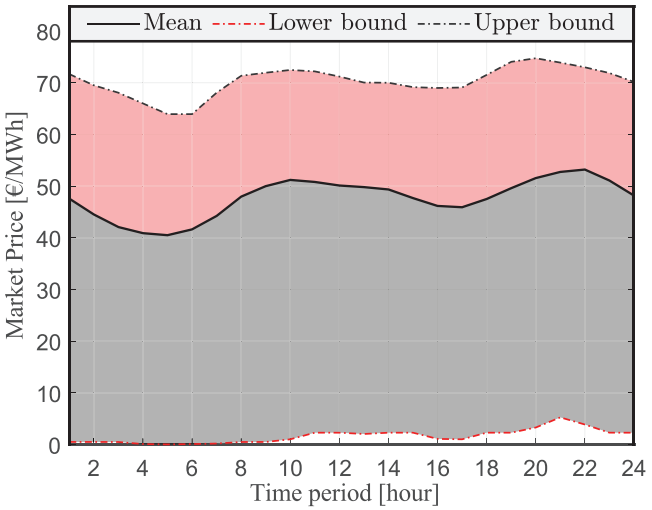

FIGURE 11 Market prices of Spanish electricity market 2019

TABLE 4 Comparison of EENS for all load points caused by failure in the components of the power system, cyber system, and both

	EENS (MWh/year)			
Load Points	Case 1	Case 2	Case 3	Percentage Increase
LP1	17.78	2.19	19.97	12.3%
LP2	47.05	5.78	52.83	12.3%
LP3	13.75	1.75	15.51	12.8%
LP4	20.32	2.46	22.77	12.1%
LP5	17.59	2.17	19.75	12.3%
LP6	43.80	5.37	49.16	12.2%
LP7	22.74	2.74	25.46	12.0%
LP8	34.94	4.26	39.20	12.2%
LP9	58.52	7.04	65.51	11.9%
LP10	20.71	2.50	23.20	12.0%
LP11	51.38	6.31	57.69	12.3%

TABLE 5 Impact of the non-ideal cyber system on the reliability indices

CPMG Characteristic	EENS [MWh/year]	LOLP
CPMG: ideal cyber system	348.57	0.0130
CPMG: non-ideal cyber system	391.04	0.0145
Percentage increase due to the failure of cyber system	**12.2** %	**11.5** %

In grid-connected mode, loss of load may occur in a number of time periods, which, in this case, is 6.17 h, because of the failure of individual components, such as a transformer or circuit breaker. Based on Table 6, the probability of being in island mode is about 0.012 (102.4 h/year), of which 9.9% occurs due to the failure of the cyber system. When the CPMG is in island mode, the number of healthy hours is dependent on the adequacy of generation resources inside the microgrid. The results in this table are based on policy #2, which is proposed for load shedding and the aforementioned capacity of the RERs. The importance factor for all loads is assumed to be 1, and, therefore, there is no critical load point in the system. When the microgrid is in island mode, all loads may be interrupted due to the lack of generation as a result of no generation in the RERs, a lack of stored energy in the ESS, or the failure of their controller. Finally, the probability of being in shutdown mode due to the failure of both cyber and power systems is 0.0038, of which 12.7% occurs due to the failure of the cyber system.

The capability of the CPMG to operate in island mode has a significant impact on the reliability of the system. Note that if the system is not designed to operate in island mode, the healthy and emergency mode in islanded operation will be shutdown mode, which considerably increases the loss of load in the system. Efficient operation of the microgrid is dependent on the design of the generation resources and the capacity of ESS based on the requirement of the microgrid operator and investment and economic analysis of the system, which is beyond the scope of this paper. According to Table 6, the microgrid is in emergency mode when it is grid-connected, for only 6.2 h. This is because during grid-connected mode, there is no deficit in the generation as the CPMG is connected to the upstream grid, and the only factor that can result in loss of load is the failure of a component such as a transformer.

TABLE 6 Results of the microgrid operation modes due to failures in the both power and cyber systems, showing time periods, probability of occurrences, and causes. Shutdown mode, indicated by *, is a result of the lack of generation in the microgrid because of any reason

				Cause [%]		
Mode of Operation	**Sub-Mode**	**Time Period**	**Prob.**	**Power System Failure**	**Cyber System Failure**	**Common**
Grid-connected	Healthy (M_{10})	8611.4	0.983	-	-	-
	Emergency (M_{11})	6.2	0.0007			
Island mode	Healthy (M_{20})	15.1	0.0017	90.0	9.89	0.098
	Emergency (M_{21})	71.3	0.008			
	Shutdown* (M_{22})	16.01	0.0018			
Shutdown (M_3)	-	33.6	0.00380	87.21	12.75	0.038

TABLE 7 Comparison of the impact of different load shedding polices on the reliability indices

	With ESS		**Without ESS**	
Load Shedding Policies	**EENS (MWh/year)**	**LOLP**	**EENS (MWh/year)**	**LOLP**
Policy #1	393.87	0.0144	417.17	0.0146
Policy #2	391.04	0.0145	399.85	0.0146
Policy #3	390.61	0.0145	397.40	0.0146

5.5 | Impact of different load shedding programs

As explained in Section 4.2.2 and based on IEEE std 2030.7, various load shedding programs, that is, in the form of a look-up table or an optimisation function (if applicable), can be adopted by the system operator. In this section, the impact of the different policies identified in Section 4.2.2 on CPMG reliability are investigated; Table 7 shows the corresponding results. As can be seen in this table, when the optimisation problem is applied, the EENS index shows an improvement of 0.72% compared to a look-up table. When the loads are controllable, the amount of interrupted load can be the same as the deficit in the generation. The results show that the optimisation model is near to the minimum amount of load reduction, which is the amount indicated in policy #3. The difference between a look-up table and an optimisation model is obvious when there is no ESS in the microgrid. In this case, the optimisation model improves the EENS index by 4.15% over a look-up table.

5.6 | Impact of cyber system topology

This section evaluates the impact of different cyber network topologies and the inclusion of a backup controller on microgrid reliability. Different topologies can be implemented for both inside the microgrid and between microgrids and DMS. This section considers the topology of six different cyber systems, three of which use a backup controller, as shown in Figure 12, in addition to the cyber network topology in the base case. Note that the power system is assumed to be failure free and that policy #1 is considered for load shedding purposes. Table 8 summarises the results for different cyber network topologies. By using a ring topology between the MGCC and DMS (Topology #3), the cyber link between them is not vulnerable to one-point failure; therefore, the availability of the cyber link between the MGCC and DMS increases, which decreases the islanding time period and improves the reliability of the microgrid. Adding a backup controller to the MGCC results in lower shutdown time and improves the reliability the most. Ring topology inside the microgrid increases the reliability very little. This is due to the following: (i) failure of FMISs assigned to the RERs and ESS does not have a great impact on reliability indices, since the upstream network can supply all the load points when the system is in grid-connected mode, and (ii) the failure of the CBCs and the related cyber links leads the circuit breaker to mis-operation mode, and since the other load points can, in most cases, be interrupted, the failure of the CBCs and related cyber links does not impact the reliability of the microgrid very much. However, by taking into account the impact of failure of lateral branches and monitoring system inside the microgrid, there might be more benefit in using ring topology inside the microgrid. As can be seen from Table 8, considering a backup controller in the MGCC has a significant impact on the reliability indices. The reason is that the centralised control systems are vulnerable to single point failure. Considering a backup controller is thus necessary, if a centralised control system is designed for the CPMG.

5.7 | Sensitivity analysis of the cyber components

To determine the impact of the different cyber components on the reliability of the microgrid, a sensitivity analysis of the components' failure rates was carried out. As can be seen in

TABLE 8 Impact of the cyber network topology on the reliability indices

Cyber Network Topology	Inside Microgrid	Between Microgrid and DMS	Spare MGCC	EENS [MWh/year]	LOLP
Topology #1	Star	Star	-	42.8	0.0015
Topology #2	Star	Ring	-	42.2	0.0014
Topology #3	Ring	Star	-	38.7	0.0013
Topology #4	Ring	Ring	-	38.1	0.0013
Topology #5	Star	Star	✓	29.2	0.0011
Topology #6	Star	Ring	✓	26.8	0.0010
Topology #7	Ring	Ring	✓	**20.6**	**0.0008**

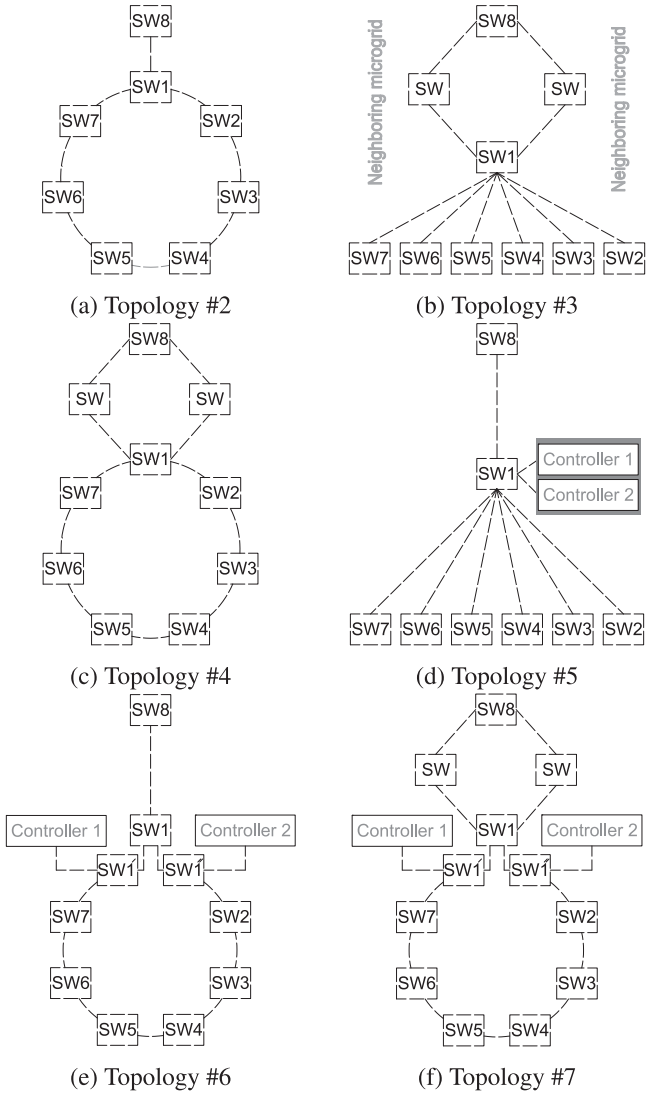

FIGURE 12 Cyber network topologies

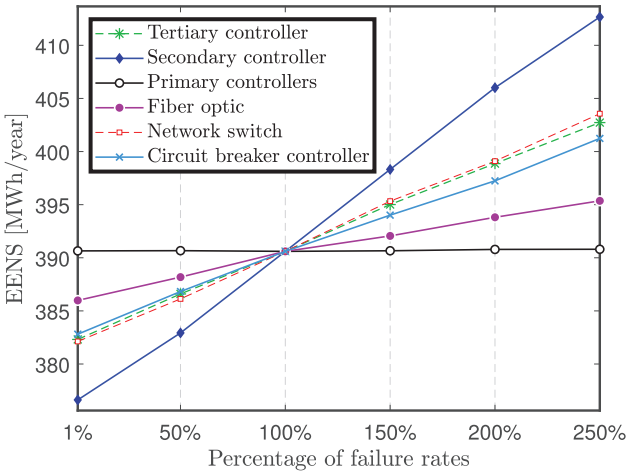

FIGURE 13 Impact of the failure rates of various ICT components on the EENS index

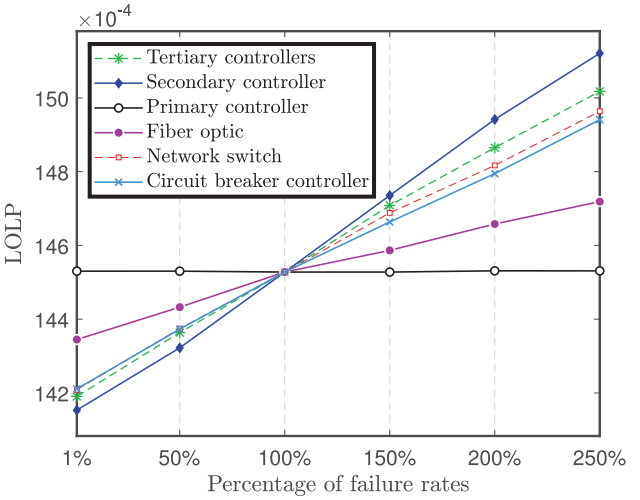

FIGURE 14 Impact of the failure rates of various ICT components on the LOLP index

Figures 13 and 14, failure of the secondary (MGCC) and the tertiary controllers has a significant impact on the reliability of the microgrid. However, the primary controller does not have a significant effect on the reliability indices. This is due to the fact that when the microgrid is in grid-connected mode, the failure of the RERs does not lead to the loss of load and the required power is supplied from upstream. When the microgrid is islanded, failure of these units influences the amount of the loss of load. The probability of coincident failure of these units and the islanded microgrid, nevertheless, is very low. The probability of the islanded microgrid, as per Table 6, is P_1 =

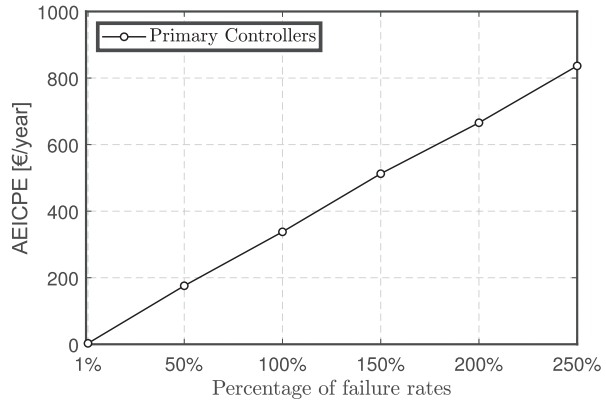

FIGURE 15 Changes in the cost of purchased energy due to the failure of the local controller of the renewable energy resources and energy storage system at the interface layer

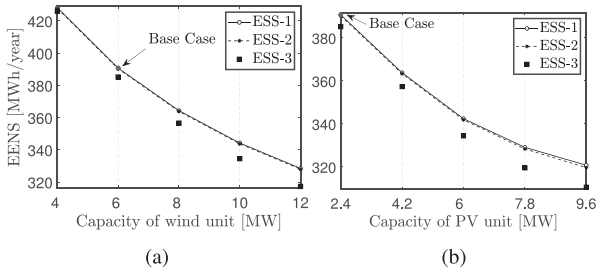

FIGURE 16 Impact of the capacity of RERs on the reliability indices for three different ESSs; (a) wind farm and (b) PV farm

0.012, and the probability of failure of the primary controller of the wind farm, according to Table 3, is approximately $P_2 = 0.0004$. Therefore, the probability of the simultaneous occurrence of these events is 5×10^{-6}, which means that this is a rare occurrence. However, in grid-connected mode, the failure of these units increases the cost of operation due to the need to purchase more energy from upstream. The annual expected increased cost of purchased energy (AEICPE) is defined as Equation (35), where $ACPE_y^{FF}$ is the annual cost of purchased energy in year y of a simulation when the primary controllers, that is, FMISs, are failure free. N is the number of simulation years. This is a good measure to evaluate the impact of the failure of the primary controllers because the EENS and LOLP indices are not sensitive to the failure of these elements. Figure 15 illustrates the AEICPE due to the failure of primary controllers. Note that the results in Figures 13 and 14 might change within a boundary, which have not been shown for the clarity.

$$AEICPE = \frac{1}{N}\sum_{y=1}^{N} ACPE_y^{FF} - ACPE_y. \quad (35)$$

5.8 | Impact of RERs and ESS on reliability

Figures 16a and 16b show the EENS index for various capacities of wind and PV farms, respectively, for three ESSs with different capacities and charging and discharging rates. The respective energy capacity and maximum hourly charging and discharging of ESS-1 is 3 MWh and 0.5 MW, ESS-2 is 4 MWh and 0.5 MW, and ESS-3 is 5 MWh and 1 MW. Increasing the penetration of RERs and ESS improves the reliability of the system. However, to obtain the optimal values of these resources, a cost-benefit analysis is required. As can be seen in Figure 16, the impact of ESS increases when there is more RER generation in the microgrid.

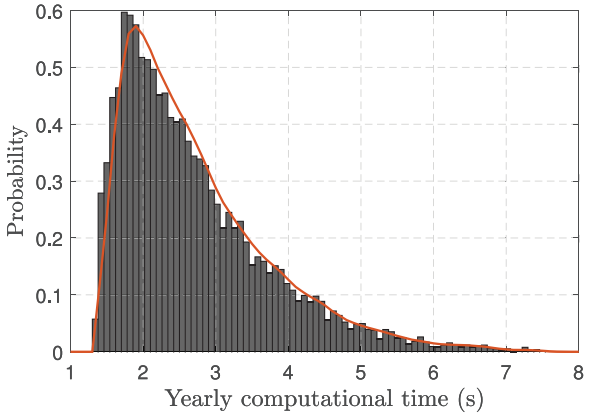

FIGURE 17 Distribution function of yearly computational time for policy #3 load shedding strategy

5.9 | Implementation, computational time, and convergence of the method

All the simulations were conducted in Matlab on a Windows-based personal computer Intel CORE i7 with processors clocking at 2.8 GHz and 32 GB of RAM. The hourly optimisation problem in island mode operation was solved using the '*intlinprog*' solver, and the average computational time for each optimisation was approximately 0.009 s. The optimisation problem in grid-connected mode was solved using the '*linprog*' command. T in Equation (18) was chosen to be 96 (4 days), if applicable, and the average time for this problem was 0.016 s. The yearly computational time of the simulation is dependent on load shedding strategies. The average yearly computational time of polices #1 and #3 was approximately 1.5 s. The yearly computational time for policy #2 was dependent on the number of hours that the microgrid operates in island mode. Figure 17 shows the distribution of the yearly computational times of this case.

Figure 18 shows the EENS and COV with respect to the number of simulation years. A large number of simulation years were taken into account in order to study the sufficient number of simulation years and precision factor e. As can be seen from Figure 18, the precision e under 0.019 can be acceptable; this occurred after 1473 simulation years in this case.

5.10 | Further discussion

As mentioned before, two main approaches can be identified for the control system of a microgrid, that is, centralised and

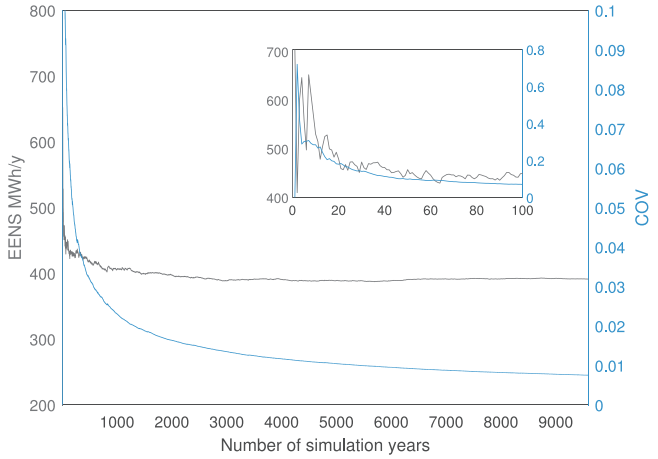

FIGURE 18 COV and EENS with respect to the number of simulation years

decentralised. This study considered a centralised control system, but a microgrid with a decentralised control system can also be examined using this methodology. For instance, if the microgrid is able to switch to a decentralised control system (using primary controllers) during grid-connected mode (even if it is not the optimal operation), then the failure of the MGCC will not result in shutdown mode. In this situation, the amount of shutdown time M_3 in Table 6, which caused by the cyber system, will decrease significantly; Although, the ESS may not be operating optimally, the amount of loss of load is decreased.

6 | CONCLUSION

The purpose of the present research was to provide a methodology for assessing the impact of the failure of various elements in a cyber system on the reliability of a microgrid connected to a distribution system. The microgrid as a solution for the increasing penetration of the RERs into the distribution grid operates under a communication-based and hierarchical three-level control system. Based on the results obtained in this research, the failure of different parts of the control system in a cyber system affects the operation and, consequently, the reliability of a grid-connected CPMG. Therefore, it is vital to take into account the impact of the cyber system on the reliability of a microgrid when designing a microgrid. This research helps to obtain the reliability indices, such as EENS and LOLP, for a grid-connected CPMG. However, these findings are subject to some limitations, and more research is needed to include the impact of the monitoring system and measurement units as well as other internal factors of a cyber system, such as delay, packet loss, and measurement errors, on the reliability. The impact of different load shedding schemes on the various reliability indices of CPMG was also evaluated in study, and the results show that when ESS are available in the microgrid, there is no noticeable difference between an optimisation model and a look-up table. Therefore, in the presence of ESS, a look-up table scheme is superior due to its simple implementation. However, when there is no ESS in the microgrid, an optimisation model can decrease the loss of load and improve the system's reliability. The results also show that the failure of the cyber components that leads to the interruption of the RERs from microgrid does not have a noticeable effect on the reliability indices, such as EENS and LOLP. This is because the upstream network is able to supply all the load points in the microgrid in grid-connected mode; thus, a new index (AEICPE) was proposed to explore these impacts. It must be noted that the capacity of RERs have a profound impact on the system's reliability. Thus, in addition to economic and technical issues, reliability indices should be taken into account during the designing phase of a CPMG.

NOMENCLATURE

Main symbols, notation, and abbreviations are defined and listed alphabetically here for quick reference. Some are described again at their first appearance for the sake of clarity.

List of Acronyms

CBC	Circuit breaker controller
CPDS	Cyber-physical distribution system
CPMG	Cyber-physical microgrid
CPPS	Cyber-physical power system
DG	Distributed generations
DMS	Distribution management system
EENS	Expected energy not supplied
ESS	Energy storage system
FMIS	Field management information system
ICT	Information and communication technology
LOLP	Loss of load probability
MCS	Monte carlo simulation
MGCC	Microgrid control centre
PDF	Probability density function
POI	Point of interconnection
PV	Photo-voltaic
RER	Renewable energy resource
SW	Network switch
WT	Wind turbine

Indices and Numbers

$t(T)$	Index (set) for time period
$p(N_p)$	Index (number) of PV panels
$br(N_{br})$	Index (number) of PV branches connected to one inverter
$w(N_w)$	Index (number) of wind turbines
$l(N_l)$	Index (number) of load points
N	Number of simulation years

Parameters

L_t^{tot}	Total load of microgrid in time period t [MW]
$L_{l,t}$	Amount of the load at load point l in time period t [MW]
ρ_t	Market price at time period t [€ /MWh]
$\eta^{\text{ch}}, \eta^{\text{dch}}$	Efficiency of charging and discharging of the ESS
C_0	Initial state of charge of the ESS [MWh]

$P^{ch,min}$ Minimum hourly charging of ESS [MW]
$P^{ch,max}$ Maximum hourly charging of ESS [MW]
SOC^{min} Minimum allowable state of charge of ESS [MWh]
SOC^{max} Maximum allowable state of charge of ESS [MWh]
α_l Importance factor of load point l
IC_l Interruption cost of load point l

Random Variables

P_t^{PV}, P_t^{W} Output power of PV and wind farms in time period t without units' failure [MW]
$P_t^{PV,avail}$ Available output power of PV farm in time period t considering unit's failure [MW]
$P_t^{W,avail}$ Available output power of wind farm in time period t considering unit's failure [MW]
$\Phi(*)$ State of cyber link between MGCC and cyber component (∗)
Z_* State of the cyber element ∗

Variables

P_t^{POI} Exchange power at the point of interconnection [MW]
P_t^{bat} Exchange power of ESS at grid side [MW]
P_t^{dch}, P_t^{ch} Injected/received power of ESS at the grid side [MW]
SOC_t State of charge of ESS in time period t [MWh]
$x_{l,t}$ Binary variable indicating interrupted load point l in time period t during island mode operation
P_t^{ex} Excess power that cannot be consumed in time period t during island mode operation [MW]

REFERENCES

1. Fang, X., et al.: Smart grid - The new and improved power grid: A survey. IEEE Commun. Surv. Tutor. 14(4), 944–980 (2012)
2. Taylor, J., et al.: Assessing the impact of on the reliability of active distribution systems. In: 22nd International Conference and Exhibition on Electricity Distribution, pp. 1–4. IEEE, Piscataway (2013)
3. Schacht, D., et al.: Modelling of interactions between power system and communication systems for the evaluation of reliability. In: Power Systems Computation Conference (PSCC), pp. 1–7. IEEE, Piscataway (2016)
4. Sha, K., et al.: A secure and efficient framework to read isolated smart grid devices. IEEE Trans. Smart Grid 8(6), 2519–2531 (2017)
5. Gungor, V., et al.: Smart grid technologies: Communication technologies and standards. IEEE Trans. Ind. Inform. 7(4), 529–539 (2011)
6. Rajkumar, R., et al.: Cyber-physical systems: The next computing revolution. In: Design Automation Conference, pp. 731–736. IEEE, Piscataway (2010)
7. T¸ndel, I., et al.: Interdependencies and reliability in the combined and power system: An overview of current research. Appl. Comput. Informatics 14(1), 17–27 (2018)
8. Aravinthan, V., et al.: Reliability modeling considerations for emerging cyber-physical power systems. In: IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), pp. 1–7. IEEE, Piscataway (2018)
9. Mosadeghy, M., et al.: A time-dependent approach to evaluate capacity value of wind and solar PV generation. IEEE Trans. Sustainable Energy 7(1), 129–138 (2016)
10. Barani, M., et al.: Optimal partitioning of smart distribution systems into supply-sufficient microgrids. IEEE Trans. Smart Grid 10(3), 2523–2533 (2019)
11. Lei, H., et al.: Security and reliability perspectives in cyber-physical smart grids. In: IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia), pp. 42–47. IEEE, Piscataway (2018)
12. Sun, C., et al.: Cyber security of a power grid: State-of-the-art. Int. J. Electrical Power Energy Sys. 99, 45–56 (2018)
13. Falahati, B., et al.: Reliability assessment of smart grid considering direct cyber-power interdependencies. IEEE Trans. Smart Grid 3(3), 1515–1524 (2012)
14. Wang, C., et al.: Impacts of cyber system on microgrid operational reliability. IEEE Trans. Smart Grid 10(1), 105–115 (2019)
15. Falahati, B., Fu, Y.: Reliability assessment of smart grids considering indirect cyber-power interdependencies. IEEE Trans. Smart Grid 5(4), 1677–1685 (2014)
16. Liu, W., et al.: Reliability modeling and evaluation of active cyber physical distribution system. IEEE Trans. Power Systems 33(6), 7096–7108 (2018)
17. Guo, J., et al.: Reliability assessment of a cyber physical microgrid system in island mode. CSEE J. Power Energy Syst. 5(1), 46–55 (2019)
18. Zhao, T., et al.: A risk assessment method for cascading failure caused by electric cyber-physical system (ECPS). In: 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT). pp. 787–791. IEEE, Piscataway (2015)
19. Hajian-Hoseinabadi, H., et al.: Quantitative reliability assessment of various automated industrial substations and their impacts on distribution reliability. IEEE Trans. Power Delivery 27(3), 1223–1233 (2012)
20. Yang, Y., et al.: Reliability modeling and evaluation of cyber-physical system (CPS) considering communication failures. J. Franklin Inst. (2018)
21. Marashi, K., et al.: Consideration of cyber-physical interdependencies in reliability modeling of smart grids. IEEE Trans. Sustain. Comput. 3(2), 73–83 (2018)
22. Falahati, B., et al.: Reliability modeling and evaluation of power systems with smart monitoring. IEEE Trans. Smart Grid 4(2), 1087–1095 (2013)
23. Hashemi-Dezaki, H., et al.: 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)
24. Heidari-Kapourchali, M., et al.: Reliability analysis of cyber-enabled power distribution system using sequential monte-carlo. In: North American Power Symposium (NAPS), pp. 1–6. IEEE, Piscataway (2015)
25. Han, Y., et al.: Incorporating cyber layer failures in composite power system reliability evaluations. Energies 8(9), 9064–9086 (2015)
26. Panteli, M., Kirschen, D.: Assessing the effect of failures in the information and communication infrastructure on power system reliability. In: IEEE/PES Power Systems Conference and Exposition, pp. 1–7. IEEE, Piscataway (2011)
27. Bessani, M., et al.: Impact of operators performance in the reliability of cyber-physical power distribution systems. IET Gener. Transm. Distrib. 10(11), 2640–2646 (2016)
28. Celli, G., et al.: Impact of on the reliability of active distribution networks. In: CIRED Workshop: Integration of Renewables into the Distribution Grid, pp. 1–4. IEEE, Piscataway (2012)
29. Huang, Z., et al.: Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory. In: 8th IEEE Conference on Industrial Electronics and Applications (ICIEA), pp. 1023–1028. IEEE, Piscataway (2013)
30. Gunduz, H., Jayaweera, D.: Reliability assessment of a power system with cyber-physical interactive operation of photovoltaic systems. Int. J. Electr. Power Energy Sys. 101, 371–384 (2018)
31. Garau, M., et al.: reliability modelling in co-simulation of smart distribution networks. In: IEEE 1st International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow (RTSI), pp. 365–370. IEEE, Piscataway (2015)
32. Čorba, Z., et al.: In-grid solar-to-electrical energy conversion system modeling and testing. Thermal Sci. 16(1), 159–171 (2012)
33. Su, S., et al.: An assessment procedure of distribution network reliability considering photovoltaic power integration. IEEE Access 7, 60171–60185 (2019)

34. Fuentes, M., et al.: Application and validation of algebraic methods to predict the behaviour of crystalline silicon PV modules in mediterranean climates. Sol. Energy 81(11), 1396–1408 (2007)
35. Giorsetto, P., Utsurogi, K.: Development of a new procedure for reliability modeling of wind turbine generators. IEEE Trans. Power Apparatus Syst. PAS- 102(1), 134–143 (1983)
36. Wen, J., et al.: A review on reliability assessment for wind power. Renew. Sust. Energy Rev. 13(9), 2485–2494 (2009)
37. Saleh, M., et al.: Communication-based control for DC microgrids. IEEE Trans. Smart Grid 10(2), 2180–2195 (2019)
38. Fusheng, L., et al.: Chapter 2 - Composition and classification of the microgrid. In: Fusheng, L., Ruisheng, L., Fengquan, Z., (eds.) Microgrid Technology and Engineering Application, pp. 11–27. Academic Press, Oxford (2016). http://www.sciencedirect.com/science/article/pii/B9780128035986000024
39. Lei, H., et al.: Reliability modeling and analysis of IEC 61850 based substation protection systems. IEEE Trans. Smart Grid 5(5), 2194–2202 (2014)
40. Billinton, R., Jonnavithula, S.: A test system for teaching overall power system reliability assessment. IEEE Trans. Power Syst. 11(4), 1670–1676 (1996)
41. Hernando-Gil, I., et al.: Impact of DG and energy storage on distribution network reliability: A comparative analysis. In: IEEE International Energy Conference and Exhibition (ENERGYCON), pp. 605–611. IEEE, Piscataway (2012)
42. Renewables njnja, https://www.renewables.ninja. Accessed January 2020
43. OMIE, https://www.omie.es. Accessed January 2020

How to cite this article: Barani M, Vadlamudi VV, Heegaard PE. Reliability analysis of cyber-physical microgrids: Study of grid-connected microgrids with communication-based control systems. *IET Gener Transm Distrib*. 2020;1–19.
https://doi.org/10.1049/gtd2.12049