

Article citation info:

Gholami M, Karimi Ghaleh Jough F, Gholami A, Streamlining Smart Grids Reliability Assessment: An Innovative Mapping Approach, *Eksploracja i Niezawodność – Maintenance and Reliability* 2025; 27(2) <http://doi.org/10.17531/ein/195258>

## Streamlining Smart Grids Reliability Assessment: An Innovative Mapping Approach

Indexed by:  
 Web of Science Group

Mohammadreza Gholami<sup>a,\*</sup>, Foad Karimi Ghaleh Jough<sup>b</sup>, Alireza Gholami<sup>c</sup>

<sup>a</sup> Department of Electrical and Electronic Engineering, Final International University, Kyrenia 99320, Turkey

<sup>b</sup> Department of Civil Engineering, Faculty of Engineering, Final International University, Kyrenia 99320, Turkey

<sup>c</sup> Department of maintenance and repairment, Ekbatan Gas Control Co (EGC), Iran

### Highlights


- Proposed streamlining approach reduces system states significantly, enhancing computational efficiency.
- Redundant elements do not guarantee enhanced reliability for the entire cyber-physical power grid.
- Dynamic thermal rating integration boosts reliability indices of a cyber-physical power grid (up to 43.58% in star topology).

### Abstract

Assessing smart grid reliability, considering both cyber and physical components, typically involves a mapping step, escalating complexity and computational overhead. This paper presents a pioneering mapping approach that redefines the fundamental paradigm of smart grid reliability assessment. By leveraging a defined interconnection matrix rooted in cyber network topology, our method optimizes computational efficiency, curtailing the array of potential system states. Evaluation employing key performance metrics - Loss of Load Probability (LOLP) and Expected Energy Not Supplied (EENS) - quantitatively demonstrates the superiority of our approach. Also, we explore the ramifications of integrating a dynamic thermal rating (DTR) in the process of reliability assessment, augmenting component safety through permissible enhancements in their ratings. Results underscore a notable reduction in total system states, from  $2^{21}$  to  $2^{14}$  for the bus topology and from  $2^{22}$  to  $2^{16}$  for the ring topology. Moreover, the analysis reveal substantial enhancements (Up to 43.58% considering star topology) in reliability indices upon consideration of the DTR system.

### Keywords

smart grid reliability, Dynamic Thermal Rating (DTR), cyber physical systems, network topologies, Expected Energy Not Supplied (EENS)

This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>) 

### 1. Introduction

Recently, developments of the communication based technologies within microgrids (MGs) are undoubtedly enhanced the operation of smart grids [1] [2]. However, despite their numerous techno-economic advantages, the malfunctioning of cyber components can result in disruptions to the performance of physical elements [3] [4]. Indeed, studies such as those referenced in [5] and [6] underscore the

pivotal role of cyber network failures in causing power system outages. Consequently, the unavailability of cyber networks emerges as an important factor influencing the performance of contemporary cyber-physical systems (CPS). In contrast to the reliability assessment in traditional power systems, which typically involves searching for possible system states, evaluating these states, and assessing reliability indices,

(\*). Corresponding author.

E-mail addresses:

[mohammadreza.gholami@final.edu.tr](mailto:mohammadreza.gholami@final.edu.tr)

M. Gholami (ORCID:0000-0002-9136-5026) [mohammadreza.gholami@final.edu.tr](mailto:mohammadreza.gholami@final.edu.tr), F. Karimi Ghaleh Jough (ORCID:0000-0003-0697-5167) [fooad.karimi@final.edu.tr](mailto:fooad.karimi@final.edu.tr), A. Gholami (ORCID:0009-0008-8684-3725) [gholami.ali.r@gmail.com](mailto:gholami.ali.r@gmail.com)

evaluating cyber-physical systems introduces significantly greater complexity. Primarily, when considering the cyber network elements, the total number of potential states escalates significantly. Specifically, in a network with  $N_p$  and  $N_c$  physical and cyber elements, the total number of possible states equals  $2^{N_p+N_c}$ . Moreover, an additional mapping step becomes necessary in these processes to account for the intricate interdependencies between networks, thereby substantially increasing computational overhead. While reliability studies of smart grids often acknowledge the conceptual impact of cyber networks [7] [8], their comprehensive integration into reliability assessments remains limited.

While most of the studies investigated the assessment of reliability of a MG without considering the effect of cyber networks [9] [10] [11], a few studies have endeavored to quantitatively evaluate the grid reliability considering the cyber components. Notably, pioneering works such as those discussed in [12] and [13] have provided novel insights by evaluating the reliability of CPS while incorporating both directly and indirectly interdependency of components. These studies introduced an addition step, namely mapping stage, to correlate cyber network's components faults with physical's element failures. Given the impracticality of exhaustively searching and evaluating all possible states for large systems, the authors advocate for considering a maximum order of states in their methodology. In [14], researchers computed composite power system reliability indices by accounting for malfunctions in the protection level. They employed CPS related matrix to capture nonlinear relationship between CPS components. However, their method imposes a high computational burden due to the large number of components in protection level and the intricate technical details of their operations. Efforts to streamline the assessment of CPS's reliability is explored in [15], where a fuzzy c-means clustering-based algorithm was utilized to reduce computation time and the number of uncertain parameters. Nevertheless, this method only considers direct cyber-physical interdependencies, neglecting indirect interconnections such as element-element and network-element interactions. In [16], an innovative CP interdependencies matrix (CPIM) is proposed. However, the necessity to update the network graph

and related interconnections after each failure poses a challenge, potentially increasing the complexity of the mapping step. Addressing this issue warrants further investigation and refinement in future studies. In [17] the authors employed an k-shortest path algorithms to find the most probable CPS states considering the interdependencies between both networks. In their proposed approach, the problem of is converted to a shortest path algorithm by applying a transformation step. However, their approach focus on decreasing the total number of system states, and the lack of simplification in the mapping step results in computational challenges and extended assessment times. The authors in [18] attempt to address the gap by integrating an analytical model for CP interdependencies. While their approach successfully incorporates these cyber elements, it introduces substantial complexity, making the method difficult to apply in practical scenarios, particularly in large-scale smart grids. A study in [19] introduces a Markov chain model that modifies the availability of physical components based on the failures of the cyber layer. This approach leverages a reliability block diagram method to capture the CP layers interdependencies. However, despite its comprehensive framework, this method suffers from the limitation of considering all possible cyber layer failures, which significantly increases computational cost, especially in larger systems. Another study in [20] proposes a CP interface matrix to map the relationship between the failure modes of cyber and physical components in substation protection systems. While this matrix-based approach systematically captures interactions between subsystems, it requires extensive analysis to identify major interaction points, determine probabilities of interface events, and calculate the failure impacts on the physical layer. Although effective in small-scale applications, such methodologies can become computationally intensive as system size grows due to the complexity of failure mode analysis and the large number of interface parameters that need to be considered. A different approach in mapping step can be found in methods based on correlation matrices. The study in [21] presents a correlation characteristic matrix that captures the interactions between power system components and their corresponding cyber layers, including the communication network. This method utilizes multiple sub-

matrices to represent specific layers within the system, as seen in [22], where matrix decomposition techniques are applied to model interdependencies, such as communication routers that do not directly interface with power system components. By employing an upstream and downstream information flow architecture, this approach propagates data between the physical layer and the control center at the top level. However, while this method successfully captures detailed interconnections between layers, the decomposition of matrices and the propagation of information signals across multiple layers adds complexity, particularly when applied to large-scale smart grids.

In contrast to previous studies that have grappled with the exhaustive consideration of all potential states and connections between cyber and power networks, our paper introduces a pioneering and streamlined mapping approach. Our method seeks to mitigate the complexity and extended assessment times associated with reliability evaluations of cyber-physical systems. By leveraging a predefined interconnection matrix rooted in cyber network topology, our approach simplifies computation by reducing the myriad possible system states, ultimately leading to significant cost savings.

The primary novelty of the study lies in the introduction of a novel mapping approach that fundamentally transforms the assessment of smart grid reliability. Our method represents a paradigm shift in the field, promising to revolutionize the assessment process through its innovative simplifications. By offering fresh insights into the challenges posed by complex cyber-physical systems, our groundbreaking approach distinguishes itself from conventional methodologies. Moreover, our method holds the potential to influence the decision-making processes of power system planners and operators by streamlining the assessment process and enhancing reliability evaluations. To quantitatively evaluate the efficacy of our approach, we employ rigorous performance metrics such as expected energy not supplied (EENS) and loss of load probability (LOLP). These metrics provide a robust assessment of our method's contributions to enhancing smart grid reliability assessments, thus underlining its significance in advancing the field.

The architecture and topology of cyber networks play

a crucial role in influencing reliability indices [23]. However, accounting for the configurations of cyber systems poses a computational challenge due to the diverse configurations and their impact on computing time. Different configurations including bus, ring, star, and mesh topologies characterize cyber systems [24]-[25]. The occurrence of cascading failures of the cyber components further complicates reliability assessments. To address these challenges, we propose an improved mapping stage in this paper, remarkably reducing the computational burden. Through the use of a connection matrix and defined parameters, we eliminate unnecessary states and redundant calculations without compromising the problem's generality. Distinct simplification processes are delineated for different cyber network topologies. In our methodology, we employ Monte Carlo Simulation (MCS), a widely utilized method by researchers for system state searching [26] [27]. MCS has demonstrated high efficacy in such problems, particularly regarding CPS with high number of components [28] [29]. Subsequently, we utilize an optimized DC load flow (DCLF) analysis in the process of evaluating the selected system states. This evaluation yields insights into the status of each state and determines the load not supplied amount regarding each state. This combined approach enables comprehensive reliability assessments while mitigating computational complexities associated with cyber-physical system evaluations.

In the preceding studies, system evaluation and modeling predominantly are based on the static thermal rating (STR). While, considering the dynamic thermal rating (DTR) for transmission lines is necessary for an accurate evaluation of CPS reliability. The DTR system harnesses advancements in sensor technologies to dynamically determine transmission line thermal rating, offering a flexible approach to capacity enhancement [30] [31] [32]. Extensive research has explored the reliability of power networks under the influence of the DTR system [33], which introduced two transmission line failure models incorporating factors such as natural aging and loading conditions. Moreover, the effect of the DTR on the CPS's performance has been considered in prior works [34] and [35]. These studies showcased significant enhancements in reliability indices through the adoption of various DTR network topologies [34]. Additionally, the formulation of DTR

system availability was presented in [35]. In this paper, we build upon this research by incorporating the two-state reliability model for DTR components and update the DCLF equations.

The rest of the paper is sectionalized as follows: Section 2 presents explanations of the proposed approach. In Section 3, we present the empirical data from our case study, alongside the results obtained through the application of the simplified approach. Section 4 offers a thorough discussion of the obtained results. Lastly, the conclusion section synthesizes our findings, drawing comprehensive conclusions and delineating potential avenues for future research.

## 2. Methodology and proposed approach

In this section, the proposed approach is detailed and related mathematical formulas are provided. Assessing the reliability of a CPS with the new proposed simplification step involves a structured approach to streamline the process and enhance computational efficiency. The first step is to create a comprehensive state-table that lists all possible system states along with their associated probabilities. This table is initially populated with the probabilities of each component being in either an "up" or "down" state, factoring in the simplified model for parallel components where applicable. Next, the mapping step is applied, focusing on states where at least one cyber element is in the "down" state. This step updates the overall system state based on the cascading effects of these failures, significantly reducing redundant computations by considering the dependencies only once. In the streamlining mapping step, the focus shifts to updating the status and associated probabilities of cyber networks, leveraging the streamlined approach. Here, the updated probabilities reflect the cascading effects of failures in cyber elements, considering the dependencies between interconnected components. By incorporating these updates, the mapping step

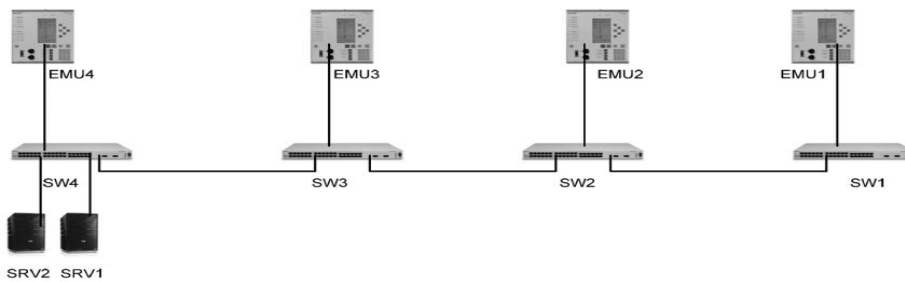


Fig. 1. The cyber network of a CPS: Bus configuration [12].

significantly reduces redundant computations and simplifies the overall reliability assessment process.

Following the mapping step, the evaluation phase determines the system's operational status (failure or success) and calculates the minimum load curtailment using an optimal DC load flow model. This involves solving a series of equations under given constraints to identify how failures impact the system's ability to meet demand. Finally, the reliability indices, such as Loss of Load Probability (LOLP) and Expected Energy Not Supplied (EENS), are computed. Only the failure states identified in the evaluation phase are used for these calculations, ensuring accuracy while minimizing computational overhead. This methodology, enhanced by the proposed simplification step, effectively reduces the number of system states that need to be considered, thereby improving the efficiency and feasibility of reliability assessments for large CPS networks.

Let's delve into the composition of a CPS, comprising total  $(N=N_{power}+N_{cyber})$  components. A two states reliability model can be used for the components to show their status as up or down. The probabilities associated with these states are computed utilizing Eq.1 Eq.2, which leverage the respective failure rate,  $\lambda_i$ , and repair rate,  $\mu_i$ , for each component.

$$P_{UP} = \frac{\mu_i}{\lambda_i + \mu_i} \quad (1)$$

$$P_{DOWN} = \frac{\lambda_i}{\lambda_i + \mu_i} \quad (2)$$

We define a matrix considering the connections between components, specifically tailored for cyber components, as follows:

$$\begin{bmatrix} \alpha_{1,1} & \alpha_{1,j} & \alpha_{1,N_c} \\ \vdots & \ddots & \vdots \\ \alpha_{i,1} & \alpha_{i,j} & \alpha_{i,N_c} \\ \vdots & \vdots & \vdots \\ \alpha_{N_c,1} & \alpha_{N_c,j} & \alpha_{N_c,N_c} \end{bmatrix}$$

Here,  $i$  and  $j$ , ranging from 1 to  $N_c$ , denote the  $i$ th and  $j$ th cyber elements within the network.

The variable  $\alpha_{i,j}$  takes a value of 1 to signify the presence of a connection between cyber components  $i$  and  $j$ , while it assumes a value of 0 to indicate the absence of such a

connection. Fig. 1 and Fig.2 illustrate the cyber network, within a MG, configured by the bus and ring topologies respectively.

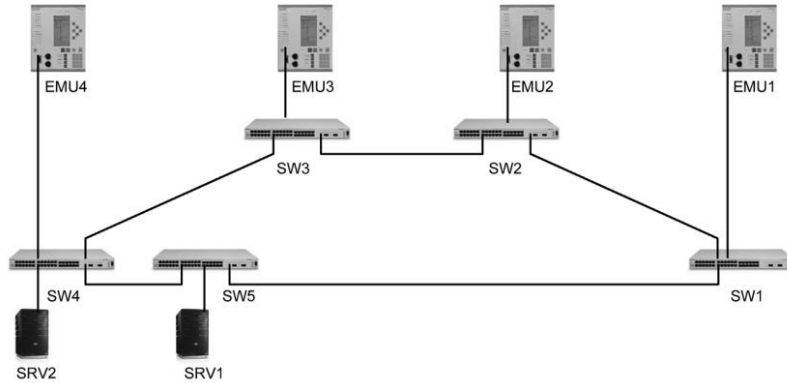


Fig. 2. The cyber network of a CPS: Ring configuration [12]

As it is shown in the figures, the cyber components consist of 2 servers, 4 switches, and 4 energy units (EUs), totally 10 elements. EUs are crucial cyber components used to balance generation and loads [36] [37] and are responsible for controlling the operation of breakers [38]. The cyber component vector for this network is defined as  $C = \{\text{Server}_1,$

Server<sub>2</sub>, S<sub>1</sub>, S<sub>2</sub>, S<sub>3</sub>, S<sub>4</sub>, EU<sub>1</sub>, EU<sub>2</sub>, EU<sub>3</sub>, EU<sub>4</sub>\}. In contrast, an additional switch is added to the network to enhance network connectivity and redundancy.

The cyber element interconnection matrixes for the networks illustrated in both figures are provided below:

Components	Server <sub>1</sub>	Server <sub>2</sub>	S <sub>1</sub>	S <sub>2</sub>	S <sub>3</sub>	S <sub>4</sub>	EU <sub>1</sub>	EU <sub>2</sub>	EU <sub>3</sub>	EU <sub>4</sub>
Server <sub>1</sub>	0	0	0	0	0	1	0	0	0	0
Server <sub>2</sub>	0	0	0	0	0	1	0	0	0	0
S <sub>1</sub>	0	0	0	1	0	0	1	0	0	0
S <sub>2</sub>	0	0	1	0	1	0	0	1	0	0
S <sub>3</sub>	0	0	0	1	0	1	0	0	1	0
S <sub>4</sub>	1	1	0	0	1	0	0	0	0	1
EU <sub>1</sub>	0	0	1	0	0	0	0	0	0	0
EU <sub>2</sub>	0	0	0	1	0	0	0	0	0	0
EU <sub>3</sub>	0	0	0	0	1	0	0	0	0	0
EU <sub>4</sub>	0	0	0	0	0	1	0	0	0	0

Components	Server <sub>1</sub>	Server <sub>2</sub>	S <sub>1</sub>	S <sub>2</sub>	S <sub>3</sub>	S <sub>4</sub>	S <sub>5</sub>	EU <sub>1</sub>	EU <sub>2</sub>	EU <sub>3</sub>	EU <sub>4</sub>
Server <sub>1</sub>	0	0	0	0	0	1	0	0	0	0	0
Server <sub>2</sub>	0	0	0	0	0	0	1	0	0	0	0
S <sub>1</sub>	0	0	0	1	0	0	1	1	0	0	0
S <sub>2</sub>	0	0	1	0	1	0	0	0	1	0	0
S <sub>3</sub>	0	0	0	1	0	1	0	0	0	1	0
S <sub>4</sub>	1	1	0	0	1	0	1	0	0	0	1
S <sub>5</sub>	0	0	0	0	1	1	0	0	0	0	0
EU <sub>1</sub>	0	0	1	0	0	0	0	0	0	0	0
EU <sub>2</sub>	0	0	0	1	0	0	0	0	0	0	0
EU <sub>3</sub>	0	0	0	0	1	0	0	0	0	0	0
EU <sub>4</sub>	0	0	0	0	0	1	0	0	0	0	0

In these matrices, each element ( $\alpha_{i,j}$ ) is set to 1 if there is a connection between the  $i$ th and  $j$ th components, and 0 otherwise. These matrices provide a clear representation of the connectivity within the cyber networks of the bus and ring

topologies, respectively.

At the rest of the section, various steps to simplify the mapping task and related updated probabilities are detailed:

## 2.1. Streamlining of two parallel elements

To ensure the problem's generality, the two parallel elements are modeled as a two-state single component. Applying this stage results to decreasing the system possible states from  $2^{N_{power}+N_{cyber}}$  to  $2^{N_{power}+N_{cyber}-1}$ . For instance, in Figure 1, the two servers are represented with a one two-state component which is in an 'on' status if both elements are 'on'. The Eq.3 and Eq.4 formulate the updated probabilities.

$$P_{UP\_Server} = P_{UP\_Server\_1} \times P_{UP\_Server\_2} \quad (3)$$

$$P_{DOWN\_Server} = 1 - P_{UP\_Server} = 1 - (P_{UP\_Server\_1} \times P_{UP\_Server\_2}) \quad (4)$$

$$\begin{bmatrix} \text{Server}_1 & \text{Server}_2 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} \text{Server}_{1,2} \\ 1 \\ 0 \end{bmatrix}$$

## 2.2. Streamlining of cascade failures

Cascade failures refer to a sequence of failures in a system where the failure of one component triggers the failure of subsequent components, potentially leading to a widespread system failure. This phenomenon is common in interdependent networks such as power grids, communication systems, and transportation networks. This type of failures observed in the cyber system depicted in Fig. 1, where the failure of S4 leads to the failure of all other switches due to the unsuccessful operation of SW4. From a computational perspective, cascade failures involve redundant and repetitive calculations. In this case we can update the probabilities using Eq. 5 and Eq.6.

$$P_{UP\_SW_i} = \prod_{j=i}^{n_{sw}} \alpha_{i,j} \times P_{UP\_SW_i} \times P_{UP\_SW_j} \quad (5)$$

$$P_{DOWN\_SW_i} = 1 - P_{UP\_SW_i} \quad (6)$$

where  $\alpha_{i,j}$  ensures the connectivity of each SW and its preceding SWs.

## 2.3. Streamlining of interconnected components

One of the key benefits of employing ring, star, and mesh topologies lies in their ability to sustain operation even in the event of failure in some connected elements. This characteristic ensures that the reliability calculations

adequately consider the redundancy inherent in these network configurations, thereby bolstering the overall dependability of the system. For example, in Fig. 2, the functionality of S3 persists even if either S4 or S2 experiences a failure, thanks to its ability to establish connections with the servers through alternative pathways. Put simply, S3 only ceases to function if both its own operation and that of S4 and S2 fail simultaneously. As a result, the probabilities associated with such switches are updated accordingly:

$$P_{DOWN\_SW_i} = P_{DOWN\_SW_i} + \prod_{j=i}^{n_{sw}} \alpha_{i,j} \times P_{DOWN\_SW_j} \quad (7)$$

$$P_{UP\_SW_i} = 1 - P_{DOWN\_SW_i} \quad (8)$$

## 2.4. Streamlining of single-connected elements

In the context of networked systems, single connected refers to elements that are connected to the network through only one other element. In a cyber network, a device like a server or a switch that is connected to only one other switch or router is considered single-connected. If the connecting switch or router fails, the device loses its connectivity. Also, in a power system, a substation that is connected to the grid through only one transmission line is single-connected. If the transmission line fails, the substation or transformer loses its power supply. Most components within cyber system are singularly linked to other elements, their functionality directly influenced by the operational status of these connections. For example, EUs and S4 depicted in Fig.1 are tethered to respective switches and the server unit, respectively. Assuming element  $i$  is singularly connected, so its probability undergo updating via Eq.9 and Eq.10. It's worth noting that the probability attributed to element  $j$  is the revised value post the preceding update procedures:

$$P_{UP_i} = P_{UP_i} \times \hat{P}_{UP_j} \quad (9)$$

$$P_{DOWN_i} = 1 - P_{UP_i} = 1 - (P_{UP_i} \times \hat{P}_{UP_j}) \quad (10)$$

where  $\hat{P}_{UP_j}$  signifies the revised value of element  $j$  following the preceding update iterations. Take EU1, for instance, which is solely linked to S1. Implementing the procedure for every singly connected element allows for the exclusion of element  $j$  from the reliability evaluation process.

$$\begin{bmatrix} \text{EU}_1 & \hat{S}_1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} \widehat{\text{EU}}_1 \\ 1 \\ 0 \end{bmatrix}$$

## 2.5. System reliability evaluation

The reliability assessment process comprises four main steps, beginning with the creation of a state-table. To obtain the state-table and probability values, we begin by constructing a comprehensive state-table that enumerates all possible system states for each component within the CPS, modeling them using a two-state reliability framework where each component can be in either an "up" or "down" state. The probabilities of these states are derived from the respective failure rates and repair rates of the components, calculated using equations that reflect their operational status and any updates. By applying a mapping step that focuses on states with one or more cyber elements in a "down" state, we can update the overall system state to account for cascading failures, ensuring computational efficiency by reducing redundancy in calculations. These probabilities are then used

Table. I. A sample state of the system with failure on EU<sub>1</sub>

Physical system components											Cyber components			
GU -1	GU -2	GU -3	GU -4	Line -1	Line -2	Line -3	Bus 1	Bus 2	Bus 3	Bus 4	EU <sub>1</sub>	EU <sub>1</sub>	EU <sub>1</sub>	EU <sub>1</sub>
up	up	up	up	up	up	up	up	up	up	up	Down	Down	up	up

Table. II. Applying the mapping step to the sampled system state.

Power system elements											Cyber network elements			
GU -1	GU -2	GU -3	GU -4	Line -1	Line -2	Line -3	Bus 1	Bus 2	Bus 3	Bus 4	EU 1	EU 2	EU 3	EU 4
Down	Down	p	p	p	p	p	p	p	p	p	own	Down	p	p

In Step 3, the evaluation of states occurs, employing an optimal DCLF methodology to determine the system's status (success or failure) and calculate the minimum load curtailment required. This evaluation is facilitated by Equations 11 through 16, guiding the process. Notably, Equation 17 stipulates the maximum transmission line capacity, contingent upon the ratings provided by either the DTR or the STR ratings.

Moving to Step 4, the calculation of reliability indices takes place. Specifically, the LOLP and EENS are computed using Equations 18 and 19, respectively. It should be noted that only the failure states, as determined through the evaluation step, are utilized in the computation of reliability indices. The single line diagram related to the power network is shown in Fig.3. The power grid components include four

to calculate the overall reliability metrics of the system.

In Step 1, the various possible system states are enumerated, and the probability of occurrence for each state is recorded in a dedicated table.

Moving to second stage, the mapping step is employed, focusing on states where one or more cyber elements have failed ("down" state). During this mapping process, the totals states undergoes updates using the cascading effects of cyber element failures. For instance, the failure of EU 1 and EU2 results in the disruption operation of generation units 1 and 2, as depicted in Table I and mapped in Table II. Notably, the computational complexity associated with the mapping step, typically the most intricate phase in CPS reliability evaluation, is notably decreased following the implementation of the prescribed simplification procedures.

generation units (GU), three transmission lines (TL), and four buses.

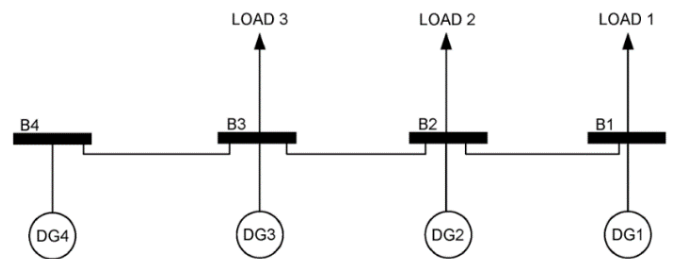


Fig. 3. The power network diagram of the case study

$$\min \sum_{i=1}^{nb} LC_i \quad (11)$$

$$\sum_{i=1}^{nd} PD_i - \sum_{i=1}^{nd} LC_i = \sum_{g=1}^{ng} PG_g - \sum_{l=1}^{nl} PL_l \quad (12)$$

$$PL_i = \frac{\theta_m - \theta_n}{x_{mn}} \quad (13)$$

$$PG_g^{min_g^{max}} \quad (14)$$

$$PL_l^{min_l^{max}} \quad (15)$$

$$0 < LC_d < PD_d \quad (16)$$

$$PL \begin{cases} p_{Max}^{DTR} \\ p_{Max}^{STR} \end{cases} \quad (17)$$

Here, in Equation 13,  $\theta_m$  and  $\theta_n$  denote the angle of phases at buses  $m$  and  $n$ . Also,  $LC_i$  represents the load curtailment in the bus  $i$ . Moreover,  $PD_i$ ,  $PG_i$ , and  $PL_i$  symbolize the demand, generation, and line power at bus  $i$ , respectively. Eq.14 and Eq.15 show the restrictions of GU and TL capacities. These equations play crucial roles in ensuring the feasibility and reliability of the system under evaluation.

$$LOLP = \sum_{i=1}^{n_f} p_i \quad (18)$$

$$EENS = \sum_{i=1}^{n_f} p_i \times LC_i \times 8760 \quad (19)$$

Here,  $n_f$  is the number of failure states in which we have load curtailment.  $p_i$  is the related probability of selected failure state. Also, 8760 is used for total hours in a year.

## 2.6. Unified Framework for Streamlining Reliability Assessment

Here, we propose a unified framework that consolidates various streamlining methodologies into a cohesive approach. This framework employs a binary connectivity indicator  $\alpha_{i,j}$  which signifies the presence (1) or absence (0) of connections between components  $i$  and  $j$ . By extending this indicator to encompass different scenarios, including parallel elements, cascading failures, and single connections, we can effectively model and update the probabilities associated with each component's operational state. This unified approach simplifies the reliability evaluation process. In this subsection, we detail the steps involved in implementing the unified framework, including the initialization of state tables, the update of probabilities based on connectivity, and the assessment of cascading failures:

- **Generalized State Representation:** Each component within the CPS is represented in a two-state reliability model, defined as either "up" (operational) or "down" (failed). This

state representation applies uniformly across all component types, including servers, switches, and energy units.

- **Common Probability Update Equation:** The probabilities associated with the states of all components can be updated using a unified equation format. The general form is expressed as:

$$P_{UP,i} = f(P_{UP,j}, \alpha_{i,j}) \quad (20)$$

where:  $P_{UP,i}$  is the updated probability of component  $i$  being operational.  $P_{UP,j}$  represents the operational probabilities of connected components.

Also,  $\alpha_{i,j}$  is a connectivity indicator between components  $i$  and  $j$ , with a value of 1 indicating a direct connection and 0 indicating no connection. This can be further extended to capture different types of interdependencies: For parallel elements, if components  $i$  and  $j$  are parallel,  $\alpha_{i,j}$  can be modified to reflect their combined reliability, where both must be operational for the system to function effectively. For cascading failures, in scenarios where the failure of one component influences others,  $\alpha_{i,j}$  should account for the direction and nature of dependencies. If component  $i$  can cause the failure of  $j$ , the connectivity indicator may carry a weight reflecting the likelihood of cascading failure. In addition, for single connections, where component  $i$  relies solely on  $j$  for functionality,  $\alpha_{i,j}$  will again be set to 1, emphasizing the critical dependency.

- **Cascading Failure Propagation:** For components that exhibit cascading failures, the unified framework dictates that the failure of one component can trigger updates in the states of connected components through a recursive application of the common probability update equation. Specifically, if component  $i$  fails, all dependent components  $j$  will have their probabilities updated as follows:

$$P_{DOWN,j} = P_{DOWN,j} + \prod_{k \in \text{connections}(j)} \alpha_{j,k} \cdot P_{UP,k} \quad (21)$$

This ensures that all relevant states are considered without redundancy. Also, the specific procedures and pseudo code that embody this approach is outlined, enabling a comprehensive understanding of how interconnected components within a CPS can be evaluated for reliability under various operational conditions.



```

// Define the number of components and initialize states and probabilities
N = total number of components
state_table = initialize state table (2^N)
probabilities = initialize probabilities array of size N
// Define the connectivity matrix  $\alpha$ 
 $\alpha$  = initialize connectivity matrix (N x N)
// Initialize probabilities based on failure rates and repair rates
for i from 1 to N do
    P_UP[i] =  $\mu_i / (\lambda_i + \mu_i)$  // Probability of component i being operational
    P_DOWN[i] =  $\lambda_i / (\lambda_i + \mu_i)$  // Probability of component i being down
end for
// Unified probability update function
function update_probability(i):
    P_UP[i] = 1
    for j from 1 to N do
        if  $\alpha[i,j] == 1$  then
            // Update the probability based on the connected component j
            P_UP[i] = P_UP[i] * P_UP[j]
        end if
    end for
    P_DOWN[i] = 1 - P_UP[i] // Update the down probability
function evaluate_cascading_failures():
    for i from 1 to N do
        if P_DOWN[i] > threshold then // If component i is down
            for j from 1 to N do
                if  $\alpha[i,j] == 1$  then
                    update_probability(j) // Update connected components
                end if
            end for
        end if
    end for
end function
// Main assessment process
function assess_reliability():
    // Step 1: Populate initial states and probabilities
    populate_state_table()
    // Step 2: Update probabilities based on connectivity
    for i from 1 to N do
        update_probability(i)
    end for
    // Step 3: Evaluate cascading failures
    evaluate_cascading_failures()
    // Step 4: Calculate reliability metrics
    LOLP = calculate_LOLP()
    EENS = calculate_EENS()
    return (LOLP, EENS) // Return reliability metrics
end function
// Execute the reliability assessment
(LOLP, EENS) = assess_reliability()

```

Fig. 4. The pseudo code of the proposed approach

### 3. Case study and results

In the following section, we delve into the outcomes of our study. Initially, we showcase the probabilities derived from

the proposed procedures. Subsequently, the reliability indices are computed across various scenarios and configurations. Furthermore, we delve into the evaluation of reliability indices for a star topology to discern the influence of topology

on the MG reliability. Tables III and IV furnish comprehensive reliability data pertaining to both the CPS components of the MG, as depicted in Figures 1 to 3. It's important to note that we assume a transmission line capacity of 1.2 per unit. Additionally, while previous research assumed a perfect availability of distributed generators and transmission lines [12], our study adopts standard values for these physical components. Moreover, in our examination of the DTR system, we presume a failure and repair rate of (3/per year) and (364/per year) respectively.

Table. III. The input data for power network elements [12].

Physical Components	Distribution Sources				Load demands		
	1th DG	2th DG	3th DG	4th DG	L1	L2	L3
magnitude	0.3	1	1	1	1.2	1	0.7

Table IV. Input data for CPS component's reliability.

Components	Mean time to failure (MTTF) / yr	Mean time to repair (MTTR) / hour
<b>Physical system</b>		
Distributed Generators	0.1666	45
Transmission lines	0.6666	10
Power buses	1.6666	24
<b>Cyber system</b>		
Energy management units	10	120
Servers		
Switches	3.3333	

Table V. The results of applying the proposed approach in new probabilities.

Components	Probability of Down state	Bus configuration	Ring configuration
		$P'_{down}$	$P'_{down}$
Server <sub>1</sub>	$1.367989 \times 10^{-3}$	$2.734107 \times 10^{-3}$	...
Server <sub>2</sub>			...
S <sub>1</sub>	$4.092769 \times 10^{-3}$	$1.8960468 \times 10^{-2}$	$4.10952 \times 10^{-3}$
S <sub>2</sub>		$1.4928798 \times 10^{-2}$	$4.10952 \times 10^{-3}$
S <sub>3</sub>		$1.088056 \times 10^{-2}$	$4.10952 \times 10^{-3}$
S <sub>4</sub>		$6.81569 \times 10^{-3}$	$5.477509 \times 10^{-3}$
S <sub>5</sub>		...	$5.477509 \times 10^{-3}$
EU <sub>1</sub>	$1.367989 \times 10^{-3}$	$2.0302519 \times 10^{-2}$	$5.471887 \times 10^{-3}$
EU <sub>2</sub>		$1.6276365 \times 10^{-2}$	$5.471887 \times 10^{-3}$
EU <sub>3</sub>		$1.2233665 \times 10^{-2}$	$5.471887 \times 10^{-3}$
EU <sub>4</sub>		$8.174351 \times 10^{-3}$	$6.838005 \times 10^{-3}$

In the initial assessment of the CPS, a total of 11 power and 10 cyber elements were considered, resulting in  $2^{11+10}$  and  $2^{11+11}$  states for the first and second configurations. However, after employing the simplifying task, the focus shifts to only

The probabilities of the cyber elements' updated two-state model are outlined in Table V, reflecting the outcomes of implementing the simplification step on these elements. Let's delve into the specifics of calculating a few of the updated values presented in Table V: First, we treat the two servers as a unified entity, denoting their state as "up" only when both servers are operational (Eq. 3). Moreover, S4's status is contingent on the operational status of servers connected to that, resulting in an "ON" state. Utilizing Eq. 5, we update the probabilities of other switches, factoring in the cascading failure between their operations. When updating S3, it's crucial to incorporate the updated value of S4.

Also, we approach the updating of S4 and S5 in two distinct phases due to their classification into separate categories. Initially, they are treated as singularly connected elements linked to Server1 and Server2. Subsequently, these elements are interconnected elements. Moreover, S4 is deemed "Off" if either S4 or both S3 and S5 be non-operational. The probabilities of other switches are then calculated using Eq. 7. Finally, we determine the state probabilities of all EUs mirroring the process in the first topology using Eq. 9.

4 EUs and 6 components (4 EUs and two Servers) for the first and second configurations, respectively, thereby reducing the total system states to  $2^{10+4}$  and  $2^{10+6}$ . To handle the creation of the state-table for large systems with numerous possible states,

methods such as Monte Carlo simulation or meta-heuristic-based approaches can be employed to identify the most probable states. In this study, we generated all conceivable system states and applied a threshold value of  $10^{-8}$  to filter out states with extremely low probabilities, thus ensuring accuracy. Despite this, the mapping step remains necessary. It's worth noting that alongside the decrease in the number of possible system states, the computational burden associated with the mapping step is significantly alleviated. This reduction is attributed to the fact that only states featuring at least one cyber element in the 'down' state necessitate mapping to another state. Furthermore, we extended the application of the method to the cyber network with a star topology, as depicted in Fig. 5, with two additional switches incorporated as part of a redundant star topology. The reliability indices obtained are compared with those from [9] in Table VI.

Table VI provides a comprehensive comparison of reliability indices obtained from different scenarios, showcasing the efficiency of the introduced approach alongside traditional approaches. For instance, when examining the case of cyber element failure combined with bus bar failure in Topology 1, a nuanced reduction in both LOLP and EENS is observed with the introduced approach compared to the reference method. Using the method referenced in [9], the LOLP is calculated as 0.0534 and the EENS is 0.1254. With our proposed method, these values

slightly decrease to 0.0529 and 0.1236, respectively. Notably, the incorporation of a threshold value in the proposed method leads to further improvements, underlining the method's adaptability to different scenarios.

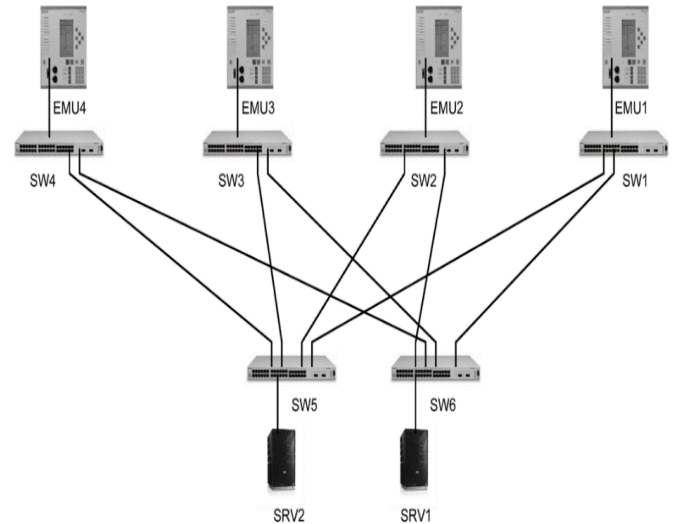


Fig. 5. The cyber network of a CPS: Star configuration [12]

Similarly, in scenarios where cyber element failure occurs while the power network remains operational, the proposed method demonstrates its reliability by maintaining lower LOLP and EENS values compared to the reference method, with additional enhancements when employing the threshold value approach.

Table. VI. The achieved reliability metrics compared to references for different topologies.

Case study	Configuration	Values in [9]		Introduced approach		Proposed method using threshold value	
		LOLP	EENS (p.u)	LOLP	EENS (p.u)	LOLP	EENS (p.u)
<b>Cyber components failures - Failure just in bus bars</b>	Bus topology	0.0534	0.1254	0.0529	0.1236	0.0513	0.1208
<b>Cyber components failures - No failure in Power elements</b>	Bus topology	0.03584	0.08367	0.03583	0.08367	0.03516	0.08294
<b>Cyber components failures - No failure in Power elements</b>	Ring Topology	0.021643	0.01924	0.021644	0.01924	0.021582	0.01918
<b>Cyber components failures - No failure in Power elements</b>	Star	0.021659	0.019132	0.02166	0.01913	0.021614	0.01901

Table. VII. LOLE and EENS: all system components can be failed.

Topology	Introduced approach: Without threshold		Introduced approach: With threshold	
	LOLP	EENS (p.u)	LOLP	EENS (p.u)
<b>Bus</b>	0.1268	0.8117	0.1225	0.8063
<b>Ring</b>	0.08467	0.47853	0.08413	0.47809
<b>Star</b>	0.08494	0.47885	0.08403	0.47885

Table. VIII. The reliability enhancement: DTR system instead of STR

Topology	EENS		
	STR system	DTR system	Improvement (%)
Bus	0.8063	0.5453	32.37
Ring	0.47809	0.34121	28.63
Star	0.47885	0.27016	43.58

Transitioning to Table VII, which presents the reliability metrics for both configurations, taking into account failures in all physical and cyber components, a consistent performance of the proposed method is observed. Despite the complexity of including failures across all components, the proposed method maintains reliability indices comparable to those obtained from the reference method, reinforcing its robustness and accuracy in assessing system reliability. The slight variations in LOLP and EENS between the proposed method and the method using a threshold value emphasize the method's adaptability to different modeling approaches, ensuring consistent reliability assessments across various scenarios.

Furthermore, Table VIII highlights the significant improvements in EENS resulting from the adoption of the DTR ratings across various topologies yields significant improvements in reliability. This shift from the STR ratings to the DTR system results in substantial reductions in EENS, signifying an enhanced level of reliability under dynamic operational scenarios. For example, in Topology 1, the adoption of the DTR system results in a remarkable 32.37% reduction in EENS, demonstrating the transformative impact of advanced technologies on system reliability. In summary, the results underscore the effectiveness and versatility of the proposed method in evaluating smart MG reliability.

#### 4. Discussion

In this section, the highlight achievements are explained and discussed, also, the limitations related to the proposed approach is provided.

##### 4.1. Achievements

First, the results highlights the effectiveness of introduced approach, showing that the metrics are computed with high precision by evaluating only  $2^{14}$  and  $2^{16}$  states for topology-1 (bus topology) and topology-2 (ring topology), respectively, compared to the original  $2^{21}$  and  $2^{22}$  states. This significant

decrease in the quantity of system configurations not only simplifies the computing process but also underscores the practicality of our approach, especially in evaluating the reliability of larger systems with an increased quantity of CPS elements. Furthermore, the findings indicate that several potential fault scenarios possess a likelihood of occurrence that is lower than a specified threshold value. These low-probability failure states can be excluded from the reliability assessment without significantly impacting the overall accuracy, thereby streamlining the process and focusing computational resources on more probable states. This selective inclusion based on probability thresholds highlights the robustness and scalability of our method in efficiently handling complex cyber-physical systems.

Moreover, the configuration of cyber networks plays a crucial role in evaluating the CPS reliability. In the case of a ring-type topology, such as in the second scenario analyzed, both the LOLE and the EENS significantly decrease from 33.22 % and 41.04%, respectively. Regarding the star configuration, these enhancements are 33.01% and 41% respectively. These enhancements represent a notable 36% and 41% improvement, respectively, emphasizing the critical role of cyber network topology in influencing reliability metrics. Notably, the impact on EENS is more pronounced, highlighting the importance of selecting an optimal topology to bolster the overall reliability of smart grids. Additionally, it's essential to recognize that simply augmenting the number of cyber components or implementing redundant elements in a star topology doesn't automatically guarantee enhanced reliability for the entire smart MG. Determining the most suitable topology, as well as the optimal number and placement of cyber components, might necessitate employing an optimization-based approach. However, this falls outside the scope of the present study and could be a valuable avenue for future research.

Furthermore, the results in Table VIII show notable improvements in the EENS with reductions of 32.37%, 28.63%, and 43.58% for the first, second, and third topology, respectively, due to the integration of the DTR system. This improvement is primarily attributed to the fact that in numerous system configurations, load curtailment at specific buses results from failures in other components and the

restricted capacity of interconnected transmission lines. With the implementation of the DTR system, transmission lines are able to operate closer to their capacity limits, transforming many system configurations previously considered as failure states into successful states. As a result, these configurations are no longer included in the calculation of reliability indices, leading to the observed improvements in EENS. A comparative analysis is conducted between our proposed method and other widely recognized reliability assessment methods. The comparison focuses on accuracy of reliability metrics, provided in Table IX.

Table. IX. Comparison between proposed method and other methods – Case study: RBTS.

Reference	Method	LOLP	EENS (p.u)
[12]	MCS-Simple Mapping step	0.0534	0.1254
[17]	k-shortest path algorithm	0.05256	0.12213
Proposed method	Streamlining approach-interconnection matrix	0.0529	0.1236

The results in Table IX demonstrate that the proposed method offers a highly competitive performance compared to other established reliability assessment techniques. Specifically, the LOLP for the proposed streamlining approach using the interconnection matrix is 0.0529, which is closely aligned with the k-shortest path algorithm (0.05256) and slightly lower than the MCS-Simple Mapping Step method (0.0534). Similarly, the EENS for the proposed method is 0.1236, showing a marginal difference from the k-shortest path algorithm (0.12213) and a noticeable improvement over the MCS-Simple Mapping Step (0.1254). These results highlight that the proposed method achieves nearly the same level of accuracy as the other techniques while significantly reducing computational complexity by focusing on interconnections and eliminating redundant failure states. This balance between precision and efficiency makes the proposed method well-suited for evaluating the reliability of complex cyber-physical systems.

Furthermore, recently, Bayesian Networks (BN) have emerged as an efficient tool in reliability evaluation, offering a probabilistic framework that can model complex dependencies and uncertainties. Considering its growing application, future research could explore how BN-based approaches can be adapted to handle interdependencies in

CPS, potentially enhancing the resilience and reliability analysis of interconnected systems. The study in [39] presents a novel methodology combining the Markov model and dynamic BN to evaluate the resilience of engineering systems under variable external disasters. Unlike traditional methods limited to fixed disaster scenarios, this approach adapts to diverse external disaster models by integrating real physical influences into the system's resilience evaluation. Through the combination of Markov models and DBNs, the overall system resilience is computed via the integral of the system's performance curve. Another study in [40] provides a comprehensive review of the application of BN in reliability evaluation over the past decades. It highlights how BN models are constructed and validated for various applications. The paper outlines the general steps involved in BN-based reliability evaluation, including modeling the BN structure, defining BN parameters, performing BN inference, and verifying the model. It also identifies current challenges and gaps in BN-based reliability evaluation and suggests future research directions in this area.

#### 4.2. Limitations

A limitation regarding the application of the simplified mapping step is the inherent challenge of determining the contribution of every components of the cyber network to the overall probability of a state. For instance, following the implementation of the streamlined mapping procedure, we adjust the likelihood of EU elements by considering the effects of failures in switches and servers. However, it remains unclear whether an EU failure is due to internal issues or related failures in switches or servers. This ambiguity can complicate the attribution of specific failures to individual cyber components and requires further refinement.

Moreover, while this research primarily focuses on static aspects of reliability assessment in smart grids, state estimation for dynamic analysis extends the understanding to the grid's dynamic response under various conditions. Dynamic state estimation involves real-time or near-real-time calculation of the network characteristics [26] [27]. These estimations are vital for assessing the transient and dynamic stability of the grid. Dynamic state estimation can capture the system's response to contingencies, disturbances, and

variations in generation and load, enabling operators to make informed decisions to maintain grid stability and reliability. In this context, it is recommended to integrate algorithms and methodologies for real-time dynamic state estimation. Additionally, incorporating models and analytical tools that address transient phenomena and voltage stability, as well as conducting contingency analysis under dynamic conditions, including simulations of the system's response to various contingencies, are suggested as potential directions for future research.

## 5. Conclusion and future work

The reliability of smart MGs stands as a critical concern for planners and operators, given the intricate dependency between CPS components. However, assessing the reliability of CPS proves to be a complex and time-consuming task. This study proposed an innovative approach to alleviate the complexity burden associated with the mapping task. Defining a connection matrix and outline proposed simple steps was introduced. By showcasing obtained updated probability for both bus and ring topologies, we demonstrate the effectiveness of our approach. The system state post-simplification accounts for the status of physical systems, servers, and EUs, thereby providing a comprehensive analysis inclusive of switches' operations and failures. To evaluate selected configurations, we employ an optimize DCLF analysis, updating the calculations to reflect maximum transmission line ratings as provided by the DTR system. Application of our method on a microgrid via various configurations and scenarios yields promising results, with LOLE and EENS computed using reduced system states

without sacrificing accuracy. The LOLE and EENS were calculated using evaluating  $2^{14}$  and  $2^{16}$  states from all possible  $2^{21}$  and  $2^{22}$  system states in case of utilizing bus and ring configurations. The results revealed that the network configuration significantly influences reliability indices, with approximately 36% and 41% enhancements in LOLE and EENS, respectively, observed by transitioning from bus to ring or star topology. Additionally, the findings highlight that added redundant component will not guarantee improving the reliability of the system. Moreover, the incorporation of the DTR rating yields a remarkable reduction in EENS index by up to 43.58%, underscoring its efficacy in enhancing system reliability.

Regarding future work, several avenues can be explored to further enhance the reliability assessment of CPS in smart grids. Firstly, integrating more advanced optimization techniques could help determine the optimal topology and placement of cyber components, improving overall system reliability. Machine learning and artificial intelligence methods can also be leveraged to predict potential failure scenarios and dynamically adjust the network configuration to prevent cascade failures. Moreover, future studies could focus on the economic implications of different reliability enhancement strategies, balancing the cost of implementing redundant components and advanced technologies against the benefits of increased reliability. Finally, exploring the impact of emerging technologies, such as blockchain for secure communications and advanced sensors for real-time monitoring, could further strengthen the resilience and reliability of smart grids.

## References

1. H. Jain, M. Kumar, and A. M. Joshi, "Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data injection," *Electr. Eng.*, vol. 104, no. 1, pp. 331–346, 2022, doi: 10.1007/s00202-021-01380-9.
2. M. Barani, V. V. Vadlamudi, and P. E. Heegaard, "Reliability analysis of cyber-physical microgrids: Study of grid-connected microgrids with communication-based control systems," *IET Gener. Transm. Distrib.*, vol. 15, no. 4, pp. 645–663, 2021, doi: 10.1049/gtd2.12049.
3. L. Yan, M. Sheikholeslami, W. Gong, M. Shahidehpour, and Z. Li, "Architecture, Control, and Implementation of Networked Microgrids for Future Distribution Systems," *J. Mod. Power Syst. Clean Energy*, vol. 10, no. 2, pp. 286–299, 2022, doi: 10.35833/MPCE.2021.000669.
4. T. C. Huang and Y. J. Zhang, "Reliability evaluation of microgrid considering incentive-based demand response," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 222, no. 1, 2017, doi: 10.1088/1757-899X/222/1/012017.
5. Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 5–20, 2013, doi: 10.1109/SURV.2012.021312.00034.

6. G. Andersson *et al.*, “Causes of the 2003 major grid blackouts in North America Europe, and recommended means to improve system dynamic performance,” *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, 2005, doi: 10.1109/TPWRS.2005.857942.
7. R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, “Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications,” *IEEE Access*, vol. 8, pp. 151019–151064, 2020, doi: 10.1109/ACCESS.2020.3016826.
8. B. Jimada-Ojuolape and J. Teh, “Impact of the Integration of Information and Communication Technology on Power System Reliability: A Review,” *IEEE Access*, vol. 8, pp. 24600–24615, 2020, doi: 10.1109/ACCESS.2020.2970598.
9. T. Adefarati and R. C. Bansal, “Reliability and economic assessment of a microgrid power system with the integration of renewable energy resources,” *Appl. Energy*, vol. 206, no. May, pp. 911–933, 2017, doi: 10.1016/j.apenergy.2017.08.228.
10. S. Bahramirad, W. Reder, and A. Khodaei, “Reliability-constrained optimal sizing of energy storage system in a microgrid,” *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 2056–2062, 2012, doi: 10.1109/TSG.2012.2217991.
11. J. Marqusee, W. Becker, and S. Ericson, “Resilience and economics of microgrids with PV, battery storage, and networked diesel generators,” *Adv. Appl. Energy*, vol. 3, no. June, p. 100049, 2021, doi: 10.1016/j.adapen.2021.100049.
12. B. Falahati, Y. Fu, and L. Wu, “Reliability assessment of smart grid considering direct cyber-power interdependencies,” *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1515–1524, 2012, doi: 10.1109/TSG.2012.2194520.
13. B. Falahati and Y. Fu, “Reliability assessment of smart grids considering indirect cyber-power interdependencies,” *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1677–1685, 2014, doi: 10.1109/TSG.2014.2310742.
14. H. Lei and C. Singh, “Power system reliability evaluation considering cyber-malfunctions in substations,” *Electr. Power Syst. Res.*, vol. 129, no. December, pp. 160–169, 2015, doi: 10.1016/j.epsr.2015.08.010.
15. M. Memari, A. Karimi, and H. Hashemi-Dezaki, “Clustering-based reliability assessment of smart grids by fuzzy c-means algorithm considering direct cyber-physical interdependencies and system uncertainties,” *Sustain. Energy, Grids Networks*, vol. 31, p. 100757, 2022, doi: <https://doi.org/10.1016/j.segan.2022.100757>.
16. M. Aslani, H. Hashemi-Dezaki, and A. Ketabi, “Reliability evaluation of smart microgrids considering cyber failures and disturbances under various cyber network topologies and distributed generation’s scenarios,” *Sustain.*, vol. 13, no. 10, 2021, doi: 10.3390/su13105695.
17. M. Gholami, M. Mohammadtaheri, and A. Gholami, “A new approach for reliability assessment of the smart microgrids using k-shortest path algorithms,” *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.*, vol. 0, no. 0, p. 1748006X231214337, doi: 10.1177/1748006X231214337.
18. M. Aslani, H. Hashemi-Dezaki, and A. Ketabi, “Analytical reliability evaluation method of smart micro-grids considering the cyber failures and information transmission system faults,” *IET Renew. Power Gener.*, vol. 16, no. 13, pp. 2816–2839, 2022, doi: 10.1049/rpg2.12541.
19. Y. Han, Y. Wen, C. Guo, and H. Huang, “Incorporating cyber layer failures in composite power system reliability evaluations,” *Energies*, vol. 8, no. 9, pp. 9064–9086, 2015, doi: 10.3390/en8099064.
20. H. Lei, C. Singh, and A. Sprintson, “Reliability modeling and analysis of IEC 61850 based substation protection systems,” *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2194–2202, 2014, doi: 10.1109/TSG.2014.2314616.
21. Y. Xue, M. Li, J. Luo, M. Ni, Q. Chen, and T. Yi, “Modeling Method for Coupling Relations in Cyber Physical Power Systems Based on Correlation Characteristic Matrix,” *Dianli Xitong Zidonghua/Automation Electr. Power Syst.*, vol. 42, pp. 11–19, 2018, doi: 10.7500/AEPS20170705006.
22. M. Li, M. Ni, Y. Xue, X. Chen, and W. Ding, “Hybrid Calculation Architecture of Cyber Physical Power System Based on Correlative Characteristic Matrix Model,” *8th Annu. IEEE Int. Conf. Cyber Technol. Autom. Control Intell. Syst. CYBER 2018*, pp. 584–588, 2019, doi: 10.1109/CYBER.2018.8688204.
23. A. H. Ahangar and H. A. Abyaneh, “Improvement of smart grid reliability considering various cyber network topologies and direct interdependency,” *Asia-Pacific Power Energy Eng. Conf. APPEEC*, vol. 2016-Decem, pp. 267–272, 2016, doi: 10.1109/APPEEC.2016.7779510.
24. M. Kim, Y. Kim, and N. Myoung, “A multi-level hierarchical communication network architecture for distributed generators,” *Electr.*

- Eng.*, vol. 97, no. 4, pp. 303–312, 2015, doi: 10.1007/s00202-015-0332-7.
25. C. Wang, T. Zhang, F. Luo, F. Li, and Y. Liu, “Impacts of Cyber System on Microgrid Operational Reliability,” *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 105–115, 2019, doi: 10.1109/TSG.2017.2732484.
  26. B. Jimada-Ojuolape and J. Teh, “Surveys on the reliability impacts of power system cyber–physical layers,” *Sustain. Cities Soc.*, vol. 62, no. July, p. 102384, 2020, doi: 10.1016/j.scs.2020.102384.
  27. O. Akinpelumi and K. Kopsidas, “Impact Analysis of Cyber-related Failures on Power System Reliability - A Review,” *2021 IEEE Madrid PowerTech, PowerTech 2021 - Conf. Proc.*, 2021, doi: 10.1109/PowerTech46648.2021.9495026.
  28. H. J. Jabir, J. Teh, D. Ishak, and H. Abunima, “Impact of demand-side management on the reliability of generation systems,” *Energies*, vol. 11, no. 8, pp. 1–19, 2018, doi: 10.3390/en11082155.
  29. S. Garip, Ş. Özdemir, and N. Altın, “Power system reliability assessment - A review on analysis and evaluation methods,” *J. Energy Syst.*, vol. 6, no. 3, pp. 401–419, 2022, doi: 10.30521/jes.1099618.
  30. C. M. Lai and J. Teh, “Comprehensive review of the dynamic thermal rating system for sustainable electrical power systems,” *Energy Reports*, vol. 8, pp. 3263–3288, 2022, doi: 10.1016/j.egyr.2022.02.085.
  31. L. Yang and J. Teh, “Review on vulnerability analysis of power distribution network,” *Electr. Power Syst. Res.*, vol. 224, no. May, p. 109741, 2023, doi: 10.1016/j.epsr.2023.109741.
  32. C. M. Lai, J. Teh, B. Alharbi, A. AlKassem, A. Aljabr, and N. Alshammari, “Optimisation of generation unit commitment and network topology with the dynamic thermal rating system considering N-1 reliability,” *Electr. Power Syst. Res.*, vol. 221, no. March, p. 109444, 2023, doi: 10.1016/j.epsr.2023.109444.
  33. J. Teh, C. M. Lai, and Y. H. Cheng, “Impact of the real-time thermal loading on the bulk electric system reliability,” *IEEE Trans. Reliab.*, vol. 66, no. 4, pp. 1110–1119, 2017, doi: 10.1109/TR.2017.2740158.
  34. B. Jimada-Ojuolape and J. Teh, “Impacts of Communication Network Availability on Synchronphasor-Based DTR and SIPS Reliability,” *IEEE Syst. J.*, vol. 16, no. 4, pp. 1–12, 2021, doi: 10.1109/jsyst.2021.3122022.
  35. B. Jimada-Ojuolape and J. Teh, “Composite Reliability Impacts of Synchronphasor-Based DTR and SIPS Cyber-Physical Systems,” *IEEE Syst. J.*, vol. 16, no. 3, pp. 3927–3938, 2022, doi: 10.1109/JSYST.2021.3132657.
  36. P. Nyeng and J. Østergaard, “Information and communications systems for control-by-price of distributed energy resources and flexible demand,” *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 334–341, 2011, doi: 10.1109/TSG.2011.2116811.
  37. M. Kezunovic, “Monitoring of power system topology in real-time,” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 10, no. C, pp. 1–10, 2006, doi: 10.1109/HICSS.2006.355.
  38. X. Liu, P. Wang, and P. C. Loh, “A Hybrid AC/DC Microgrid and Its Coordination Control,” *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 278–286, 2011, doi: 10.1109/TSG.2011.2116162.
  39. B. Cai *et al.*, “Resilience evaluation methodology of engineering systems with dynamic-Bayesian-network-based degradation and maintenance,” *Reliab. Eng. Syst. Saf.*, vol. 209, p. 107464, 2021, doi: <https://doi.org/10.1016/j.ress.2021.107464>.
  40. B. Cai *et al.*, “Application of Bayesian Networks in Reliability Evaluation,” *IEEE Trans. Ind. Informatics*, vol. 15, no. 4, pp. 2146–2157, 2019, doi: 10.1109/TII.2018.2858281.