Energy Engineering

Tech Science Press

DOI: 10.32604/ee.2024.050594

ARTICLE

Risk-Balanced Routing Strategy for Service Function Chains of Cyber-Physical Power System Considering Cross-Space Cascading Failure

He Wang, Xingyu Tong, Huanan Yu[*], Xiao Hu and Jing Bian

The Key Laboratory of Modern Power System Simulation and Control Renewable Energy Technology, Ministry of Education, Northeast Electric Power University, Jilin, 132000, China

[*]Corresponding Author: Huanan Yu. Email: yhn810117@163.com

Received: 11 February 2024   Accepted: 10 April 2024   Published: 19 August 2024

ABSTRACT

Cyber-physical power system (CPPS) has significantly improved the operational efficiency of power systems. However, cross-space cascading failures may occur due to the coupling characteristics, which poses a great threat to the safety and reliability of CPPS, and there is an acute need to reduce the probability of these failures. Towards this end, this paper first proposes a cascading failure index to identify and quantify the importance of different information in the same class of communication services. On this basis, a joint improved risk-balanced service function chain routing strategy (SFC-RS) is proposed, which is modeled as a robust optimization problem and solved by column-and-constraint generation (C-CG) algorithm. Compared with the traditional shortest-path routing algorithm, the superiority of SFC-RS is verified in the IEEE 30-bus system. The results demonstrate that SFC-RS effectively mitigates the risk associated with information transmission in the network, enhances information transmission accessibility, and effectively limits communication disruption from becoming the cause of cross-space cascading failures.

KEYWORDS

Cyber-physical power system; service function chain; risk balance; routing optimization; cascading failure

1 Introduction

1.1 Background

With the digitalization of the power system, the number of sensors, intelligent terminals, and information system decision-making units in the system has surged, and the power system on the physical side and the communication system on the information side are deeply coupled to form the cyber-physical power system (CPPS) [1,2]. Both sides are mutually interdependent, which improves the operating efficiency but also poses potential risks to the safety and reliability of CPPS [3]. Due to the large-scale adoption of Optical Fiber Composite Overhead Ground Wire (OPGW) [4], these two networks have a high degree of coupling at the topological level. The coupling of both function and structure makes it easy to form cross-space cyber-physical interaction cascading failures within CPPS [5], and the vulnerability superposition increases the risk of expanding the scope of failure.

For example, the Italian power grid in 2003 experienced a shutdown of power plants, causing several communication nodes to go offline. This resulted in the loss of control functionality, leading to further power outages in multiple substations and eventually escalating into a large-scale blackout

Copyright © 2024 The Authors. Published by Tech Science Press.
This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

event [6]. In the same year, the northeastern and midwestern regions of the United States, as well as Ontario, Canada, also experienced widespread power outages due to cascading failures. During this process, communication failures in cyber systems exacerbated the scale of the power outage [7]. In 2008, ice disasters in Southern China caused widespread disruption of transmission lines and communication links [8]. In 2015, the Ukrainian power grid experienced a cyberattack that resulted in the partial failure of the communication system [9], which significantly impacted the operation of the physical power grid and led to serious consequences, including regional blackouts. In December 2020, a natural wildfire in the state of Tamaulipas, Mexico, caused a trip in the 400 kV transmission lines connecting the central and northern grids. Subsequently, due to the untimely control measures of cyber system, the grid experienced widespread power flow transfer and frequency oscillations, ultimately resulting in a large-scale power outage incident [10].

The analysis of past cases shows that when the communication system fails or is attacked, the power nodes may fail or trigger protection mechanisms due to the loss of measurement and control support. This, in turn, leads to the interruption of power supply to certain communication equipment which will trigger a new cycle of failures. Cascading failures can persist over multiple cycles, ultimately resulting in a complete system breakdown. The most critical communication service affected by communication disruptions in the power system is the emergency control service carried out at the transmission layer. The loss of relevant service information directly impacts the post-fault operation adjustment and the topology of the power system. Therefore, in this paper, we focus on emergency control services which belong to the first-class service category.

1.2 Related Works

In practical power communication systems, the State Grid Corporation categorizes electric communication services into five classes. The first-class services, especially the emergency control services, directly relate to the secure and stable operation of the power system. It is implemented on the multi-service transport platform dusing time-division multiplexing (TDM) channels in an end-to-end circuit-switched manner. Not limited to this class of service, most communication solutions rely on synchronous network solutions such as TDM for static scheduling of data transmission. However, with the advancement of power grid informatization, this technology is gradually losing its advantages in addressing the growing demands for flexible configuration and rapid response to critical tasks in the power grid [11]. The emergence of technologies such as Software Defined Networking (SDN) and Network Function Virtualization (NFV) has overcome the limitations of traditional networks in areas such as Quality of Service (QoS), resource utilization, and transmission capacity. These technologies are capable to addressing data bursts in CPPS and meeting the evolving demands of the system [12]. SDN/NFV decouples dedicated network functions into unified hardware units and diverse Virtualized Network Functions (VNF). By dynamically deploying a series of VNFs, a Service Function Chain (SFC) can be flexibly and rapidly constructed to meet specific service requirements in electric communication. Service data only needs to flow through a sequence of VNFs deployed on network nodes for transmission and processing. The deployment and routing process of VNFs is referred to as VNF orchestration operation.

There are abundant studies on VNF orchestration. The authors of [13] propose an optimization problem that minimizes reliability degradation and cost while ensuring a strict delay constraint during parallel VNF processing and introduce a Tabu search-based algorithm to find sub-optimal solutions. Another work [14] is aiming at the transport security problem of VNF, a backup strategy based on VNF decomposition is proposed, which is described as a mixed integer linear programming problem, and solved by a delay-aware hybrid shortest path heuristic. In [15], the authors study the problem of differentiated routing considering SFC in SDN and NFV networks, the resource aware routing algorithm is proposed to solve the differentiated routing problem which is formulated as a binary integer programming model aiming to minimize the resource consumption cost of flows with SFC requests. In [16], the authors propose a deep reinforcement learning method with offline proximal policy optimization to solve the problem of VNF mapping and scheduling with the objective of maximizing the fairness of different services while ensuring the corresponding delay requirements. In [17], a dynamic SFC orchestration framework has been created in the context of the Industrial Internet of Things, and the joint optimization problem is decomposed into two subproblems: SFC selection and dynamic SFC orchestration. In the context of the power system, the authors in [18] propose the hybrid fault path recovery algorithm to solve the problem of communication link failures in wide area measurement systems leveraging the flexibility of SDN technology to quickly recover communication routes in response to individual communication link failures. In order to prevent the power communication network from failing due to grid-side failures, reference [19] proposes a strategy to find disjoint power supply routes for VNF orchestration which also helps in finding the most efficient way to route traffic through a network while minimizing the cost of managing the network's virtual functions.

1.3 Motivation

The rapid development of SDN and NFV technologies has endowed them with tremendous potential applications in the field of power communication. SDN and NFV can significantly enhance the flexibility and control capabilities of power communication systems, while also providing new solutions for addressing cross-space cascading failure issues in cyber-physical convergence scenarios. Due to the constraints imposed by various electrical parameters on energy flow, accurately adjusting the energy distribution on power grid lines is much more difficult than controlling information flow on the information side [20]. Therefore, regarding the problem of communication failures leading to the loss of emergency control services and subsequently exacerbating a single failure into cascading failures within the power grid, compared to constructing cascading failure defense mechanisms on the power grid side, we believe that optimizing routing strategies from the information side is a more efficient solution approach.

Therefore, in this paper, we seek to propose an SFC routing strategy (SFC-RS) to improve the accessibility of high-importance information in the network and reduce the probability of cascading failures in the system caused by communication disruptions.

To achieve these goals, the following issues need to be addressed. Firstly, it is necessary to identify high-importance information within the same class of communication services. Due to the varying roles of each node in the power grid, the probability and impact of cascading failures triggered by the interruption of emergency control service at respective nodes are different. Therefore, SFCs of the same service class have different levels of importance based on their destination nodes, and it is necessary to categorize the importance of information flows within the same class of communication services. Secondly, the decentralized circulation of high-importance information needs to be achieved. Currently, communication systems only differentiate information importance based on the class of services. The routing strategy implemented based on this will lead to the concentration of high-importance information in local areas or on single lines within the network. Once communication links are disrupted due to extreme disasters or network attacks, all services carried on them will be lost, thereby increasing the likelihood of triggering cascading failures. Therefore, it is essential to avoid concentrating the transmission paths of high-importance SFCs within the communication network to reduce the operational risks of the communication network.

1.4 Contributions

The contributions of this paper are summarized as follows:

1. To quantify the probability of cascading failures in CPPS, a cascading failure index (CFI) is proposed, followed by a method to evaluate the importance of information flows within the same class of service.

2. An improved risk balancing strategy is designed, and then a joint risk balancing optimization model for SFC routing deployment is proposed.

3. An indicator of weighted failure risk entropy is proposed based on the information entropy theory, which evaluates the optimization effect of SFC routing strategy.

The remaining sections are organized as follows. Section 2 introduces the SFC model and proposes the approach for measuring the importance of SFC. In Section 3, the risk balancing strategy is improved and the model of SFC-RS is proposed. And the model is solved by column-and-constraint generation (C-CG) algorithm in Section 4. Section 5 discusses performance evaluation results. Finally, Section 6 concludes this paper.

2 System Model and Evaluation Approach

2.1 Network Analysis of CPPS

CPPS is a typical interdependent network system, which can be divided into a communication layer and an electrical layer. Fig. 1 illustrates the interdependency between the two-layer networks, where power nodes and links, as well as communication nodes and links, represent two distinct entities located in the same physical space. In the power grid, power plants, substations, distributed power sources, etc., are abstracted as power nodes, power transmission lines are abstracted into links, denoted ν_P and ε_P, respectively, and the grid topology can be represented by an undirected graph $G_P = (\nu_P, \varepsilon_P)$.

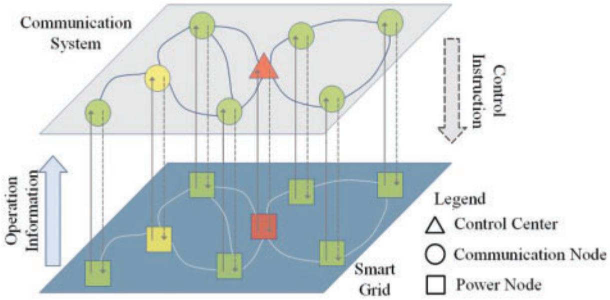


Figure 1: The interdependency of CPPS

The communication layer network consists of a physical topology network and a logical topology network that represents the SFC request. The physical network is defined by an undirected diagram $G_c = (\nu_c, \varepsilon_c)$, ν_c and ε_c represent the physical node set and link set in the communication network, $i, j \in \nu_c$ represent any two physical nodes, and $ij \in \varepsilon_c$ represents the physical link between nodes i and j; the logical topology network of SFC_k is defined by a directed graph $\overline{G}_k = (\overline{\nu}_k, \overline{\varepsilon}_k)$, where $\overline{\nu}_k$ and $\overline{\varepsilon}_k$ represent the node set and link set in the SFC_k logical topology, $\overline{i}, \overline{j} \in \overline{\nu}_k$ represent any two logical nodes, and $\overline{ij} \in \overline{\varepsilon}_k$ represents the logical link between the two nodes.

2.2 SFC Model

As shown in Fig. 2, a SFC_k consists of a source node, a destination node, and several VNFs. VNFs are deployed on network function virtualization infrastructures, which are the physical nodes of the communication network. Since the virtual functions that should be included in the formation of a particular network service have not been standardized. Therefore, a general expression is used in this paper to represent the SFC and its constituent VNFs [19]. M is the set of VNFs in the network, and $m \in M$ represents VNF_m. SFC_k in the network is defined as:

$$SFC_k = \left\{\mathrm{VNF}_1^k, \mathrm{VNF}_2^k, \ldots, \mathrm{VNF}_{|V_k|}^k\right\} \tag{1}$$

where $|V_k|$ is the length of the SFC_k, that is, the number of VNFs in the SFC_k; VNF_m^k is the $m-$ th VNF of this SFC_k. We define a binary variable z_i^m, where a value of 1 indicates that VNF_m is deployed on physical node i, and 0 otherwise. Since each VNF can only be hosted on one physical node, the following constraint should be met:

$$\sum_{i \in v_C} z_i^m = 1 \quad \forall m \in M \tag{2}$$

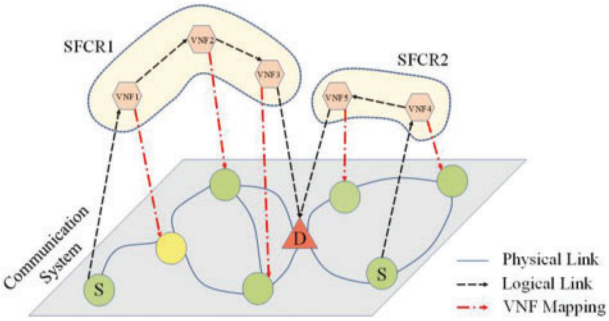


Figure 2: The mapping of VNF

2.3 SFC Importance Evaluation Approach

When the emergency control services are blocked due to the failure of communication facilities, the power nodes will lose the ability to promptly perform feedforward control on occurred faults, which will expand the fault scope and trigger cascading failures. The cross-space cascading failures triggered by communication disruptions actually belong to the cyber-physical interaction process. To quantify the impact of these blocked SFCs on the power system, reference [21] proposes a cyber-physical sensitivity analysis method to characterize the influence of information flow on physical state variables. In the cyber-physical interaction process, there are differences in the importance of physical state variables themselves. Therefore, when calculating the importance of SFCs, both cyber-physical sensitivity and the importance of physical state variables themselves should be considered.

We propose CFI to quantify the risk of cross-space cascading failures occurring in power system due to communication disruptions, thereby describing the importance of physical state variables themselves. In the event of a power grid failure and the loss of emergency control services, load transfer within the system will result in overloading of certain lines. Due to varying power transmission limits of each transmission line, lines with lower power transmission limits may not necessarily become overloaded due to the transfer of power from failed lines. Conversely, some lines with higher power transmission limits but already heavily loaded are more likely to experience failures. Therefore, the proximity of pre-failure transmission power to the line limit could be used to evaluate the probability of line failure. The proximity of line l is recorded as d_l:

$$d_l = \frac{1 - \dfrac{P_l}{P_{l,N}}}{1 - \dfrac{P_{l,\lim}}{P_{l,N}}}, l = 1, 2, \cdots, L \tag{3}$$

where P_l is the power flowing through the line l before the failure; $P_{l,N}$ is the reference power value of line l; $P_{l,\lim}$ is the power transmission limit of line l; L is the total number of lines in the network.

Implicit faults are also a major cause of triggering cascading failures, and they are related to power fluctuations [22]. After a failure occurs, the power of the failed line is redistributed in the network, and s_l is the power fluctuation amplitude of line l after redistribution:

$$s_l = \frac{\tilde{P}_{l-o}}{P_{l,\lim} - P_l}, l = 1, 2, \cdots, L \tag{4}$$

where $\tilde{P}_{l-o}$ is the power fluctuation caused on line l after line o failure:

$$\tilde{P}_{l-o} = B_{l-o} \cdot P_o + G_{l-k} \cdot \Delta P_k \tag{5}$$

where B_{l-o} is the branch breaking distribution factor; G_{l-k} is the generator transmission power transfer distribution factor; P_o is the power flowing through the line o before the failure; ΔP_k is the absolute value of power at the destination node of the blocked SFC_k.

Combining the above two parameters, the CFI of transmission line l can be defined as C_l:

$$C_l = \lambda \cdot d_l + (1 - \lambda) \cdot s_l, l = 1, 2, \cdots, L \tag{6}$$

where λ is the balance factor used to differentiate the emphasis on different risk factors. Combined with the index of line power before and after the failure, C_l reflects the probability of cascading failures occurring in normal lines after a coupled failure happens. The larger the value of C_l, the more susceptible the line is to experiencing cascading failures.

Then we use CFI to reflect the importance of physical state variables, and define the importance of SFC_k as follows:

$$I_k = \sum_{s \in S} \delta_s \cdot \left| s\left(\overline{\boldsymbol{x}}, \gamma_k\right) \cdot C_l^s \right| \tag{7}$$

where $s\left(\overline{\boldsymbol{x}}, \gamma_k\right)$ is the cyber-physical sensitivity; δ_s is the probability of the occurrence of failure scenario s; the failure scenarios of the power communication network can be expressed as $S = \{S_1, \ldots, S_n\}$, S is the failure matrix uncertainty set of the communication network $S \in \mathbb{Z}$: $\tilde{s}_{ij} \in S, \forall ij \in \varepsilon_c$, when the binary variable $\tilde{s}_{ij}$ takes a value of 1, it indicate that the physical link $ij \in \varepsilon_c$ fails, otherwise it is 0.

The SFC importance calculated by the above method will be applied as a key parameter to the proposed improved risk balancing strategy and the model of SFC-RS.

3 SFC-RS Modelling and Formulation

3.1 Improved Risk Balancing Strategy

Traditional risk balancing strategy divides the information importance according to the class of communication services [23], which ignores the fact that information belonging to the same services class also has different importance due to the varying levels of importance of different power nodes

[24]. Therefore, we propose a more targeted risk balancing strategy based on the importance of information and apply it to the SFC-RS.

Traditional risk balancing strategy defines the risk of link $ij \in \varepsilon_c$ as the product of service importance and link failure rate. In order to accurately quantify different information under the same service class, we replace the service importance with the importance of SFC calculated in Section 2, and define the improved link risk as shown in Eq. (8):

$$R(i,j) = I \cdot [1 - p(i,j)] \tag{8}$$

where $p(i,j)$ is the availability of the fiber link $ij \in \varepsilon_c$ with length $D(i,j)$. When multiple SFCs are carried on a physical link, the risk value is the sum of the risk values of each SFC:

$$R(i,j) = \sum_{k} I_k \cdot [1 - p(i,j)] \tag{9}$$

Further, the link risk value is constructed in the form of weight, and the risk route weight $W(i,j)$ of link $ij \in \varepsilon_c$ is defined:

$$W(i,j) = [-D(i,j)\ln A]\,\frac{R_l(i,j)}{R_M(i,j) - R(i,j)} \tag{10}$$

where A is the availability of fiber per unit length; $R_M(i,j)$ is the maximum risk value that link $ij \in \varepsilon_c$ can withstand. When the risk value of the link increases, the corresponding weight will increase significantly, which sensitively reflects the change of the link state.

3.2 Optimization Model of SFC-RS

Similar to traditional communication networks, NFV-enabled optical networks also face reliability issues in information transmission. Moreover, due to the execution of VNFs on virtualized platforms, they are more prone to errors compared to dedicated hardware. An effective way to guarantee reliability is to provide redundant backups and pathways for SFCs. In this paper, we consider the joint problem of risk balancing and reliable deployment of primary and backup routes for SFC, in order to improve the robustness of the communication system while reducing the centralized distribution of high-importance information in the network.

We first model the SFC routing deployment with joint risk balancing as a mathematical optimization problem. The binary variable $z_m^{\bar{i}}$ reflects that the logical node $\bar{i} \in \bar{v}_k$ is processed by VNF$_m$, when the value is 1, otherwise it is 0; the binary variables $x_{k,ij}^{\bar{ij}}$ and $y_{k,ij}^{\bar{ij}}$ indicate whether the primary and backup logical links $\bar{ij} \in \bar{\varepsilon}_k$ of SFC_k need to pass through the physical link $ij \in \varepsilon_c$, and the value is set to 1 if needed, otherwise it is 0.

For physical link $ij \in \varepsilon_c$, SFC cannot occupy more bandwidth resources than its available bandwidth b_{ij}:

$$\sum_{\bar{ij} \in \bar{\varepsilon}_k} \left(x_{k,ij}^{\bar{ij}} + y_{k,ij}^{\bar{ij}} \right) \le b_{ij} \quad \forall ij \in \varepsilon_c \tag{11}$$

For each SFC_k, it is necessary to ensure that the selected paths access all the contained VNFs in a specific order:

$$\begin{aligned} z_m^{\bar{i}} \cdot z_i^m &\le x_{k,ij}^{\bar{ij}} \quad \forall \bar{i} \in \bar{v}_k, \forall \overline{ij} \in \bar{\varepsilon}_k, \forall m \in M \\ z_m^{\bar{i}} \cdot z_i^m &\le \mathrm{y}_{k,ij}^{\bar{ij}} \quad \forall \bar{i} \in \bar{v}_k, \forall \overline{ij} \in \bar{\varepsilon}_k, \forall m \in M \end{aligned} \tag{12}$$

In SFC_k, each VNF corresponds to at most one logical node $\bar{i} \in \overline{\nu}_k$:

$$\sum_{m\in M} z_m^{\bar{i}} = 1 \quad \forall \bar{i} \in \overline{\nu}_k \tag{13}$$

In addition, it should also be ensured that the selected physical links are connected end-to-end in the network topology and that the primary and backup paths of SFC should not overlap:

$$\begin{gathered}
\textstyle\sum_{i\in\nu_C} \sum_{\bar{ij}\in\bar{\varepsilon}_k} \left(x_{k,ij}^{\bar{ij}} - x_{k,ji}^{\bar{ij}}\right) = \begin{cases} 1, i = s_k \\ -1, i = d_k \\ 0,\ \text{otherwise} \end{cases} \\
\textstyle\sum_{i\in\nu_C} \sum_{\bar{ij}\in\bar{\varepsilon}_k} \left(y_{k,ij}^{\bar{ij}} - y_{k,ji}^{\bar{ij}}\right) = \begin{cases} 1, i = s_k \\ -1, i = d_k \\ 0,\ \text{otherwise} \end{cases}
\end{gathered} \tag{14}$$

$$x_{k,ij}^{\bar{ij}} + y_{k,ij}^{\bar{ij}} \le 1 \forall k, \forall ij \in \varepsilon_c \tag{15}$$

Our starting point is to achieve risk-balanced primary and backup route planning. Therefore, the risk route weight is taken as the weighting factor for the decision variables $x_{k,ij}^{\bar{ij}}$ and $y_{k,ij}^{\bar{ij}}$. The weight is dynamically updated based on the state of networks to reflect the carrying relationship of the virtual link $\bar{ij} \in \bar{\varepsilon}_k$. It is recorded as:

$$\mathcal{R} = \sum_{k=1}^{K} I_k \left[\sum_{ij\in\varepsilon_C} W\left(ij\right) \cdot \left(x_{k,ij}^{\bar{ij}} + \tau \cdot y_{k,ij}^{\bar{ij}}\right)\right] \tag{16}$$

Simultaneously, we search for the worst-case failure scenario in the failure uncertainty set. The sum of the importance of each SFC in this scenario is used as the basis for measuring the impact of the failure scenario on the power system, it can be expressed by the following formula:

$$\mathcal{Q} = \sum_{k=1}^{K} H_k\left(\tilde{s}_{ij}\right) \cdot I_k \tag{17}$$

where H_k is the interrupt indicator coefficient of SFC_k, it takes a value of 1 when SFC_k is disrupted and 0 otherwise, the value of H_k depends on the uncertain variable $\tilde{s}_{ij}$:

$$\begin{gathered}
\tilde{u}_k \le \sum_{ij\in\varepsilon_C} x_{k,ij}^{\bar{ij}} \cdot \tilde{s}_{ij} \le \tilde{u}_k \cdot M \quad \forall k \\
\tilde{v}_k \le \sum_{ij\in\varepsilon_C} y_{k,ij}^{\bar{ij}} \cdot \tilde{s}_{ij} \le \tilde{v}_k \cdot M \quad \forall k \\
H_k = \tilde{u}_k \cdot \tilde{v}_k
\end{gathered} \tag{18}$$

among them, the uncertain variable $\tilde{s}_{ij}$ represents the state of the physical link $ij \in \varepsilon_c$, and when the value is 1, it indicates that the link is disrupted, otherwise it is 0. Each failure scenario corresponds to a specific set of $\tilde{s}_{ij}$. The auxiliary variables $\tilde{u}_k$ and $\tilde{v}_k$ are used to indicate whether the primary and backup routes of SFC_k are interrupted, which is 1 when interrupted, otherwise 0. M is a large enough value.

In summary, we construct the SFC route deployment with joint risk balancing as a two-stage robust optimization problem. The objective function can be expressed as:

$$\min_{x_{k,ij}^{\bar{ij}},y_{k,ij}^{\bar{ij}}} \left(\mu \cdot \mathcal{R} + \max_{S} \mathcal{Q}\right)$$
$$s.t.\ (2), (11), (12), (13), (14), (15), (18) \tag{19}$$

where μ is a small value used to prioritize the robust optimization objective.

The optimization model prioritizes allocating SFCs with a higher probability of triggering cascading failures after being blocked to network paths that have the lowest risk weights, which could improve the robustness of the routing mechanism and achieve autonomous adaptation.

3.3 Performance Evaluation Indicator

We adopt the load loss rate to reflect the severity of the impact on the power system caused by the loss of emergency control services due to communication disruptions:

$$R_L = \frac{\sum_{i=1}^{N} P_{loss,i}}{\sum_{i=1}^{N} P_{load,i}} \times 100\% \tag{20}$$

where N represents the total number of nodes. $P_{load,i}$ denotes the initial load of node i. $P_{loss,i}$ represents the load lost of node i.

However, since the purpose of this study is to reduce the probability of cross-space cascading failures by curbing the occurrence of information-side failures, merely assessing the severity of failures cannot reflect the optimization effect of SFC-RS. In order to measure the risk level of CPPS after optimization, drawing upon the concept of information entropy, a weighted failure risk entropy is proposed.

We calculate the sum of the importance of blocked SFC in N-2 failure scenarios, and given the blocked SFC importance sequence $R = \{R_1, R_2, \cdots, R_n\}$. The number of failure scenarios with importance $I_k \in (R_m, R_{m+1}]$ is denoted by s_m, the probability $P(m)$ of importance level being within the interval $(R_m, R_{m+1}]$ is:

$$P(m) = \frac{s_m}{\sum_{m=1}^{n-1} s_m} \tag{21}$$

The weighted risk distribution entropy is then defined as:

$$H = -\sum_{m=1}^{n-1} \bar{I}(m) P(m) \ln P(m) \tag{22}$$

where $\bar{I}(m)$ is the average importance value of all scenarios with importance $I_k \in (R_m, R_{m+1}]$. Assuming that $(R_m, R_{m+1}]$ contains t failure scenarios, then:

$$\bar{I}(m) = \frac{1}{t} \sum_{n=1}^{t} I_{mn} \tag{23}$$

According to the definition of entropy value, a smaller entropy value corresponds to fewer high-risk scenarios in the system, indicating a lower probability of triggering cross-space cascading failures.

4 Algorithm

The SFC-RS model proposed above is a typical Mixed Integer Programming (MIP) problem, which is difficult to solve, and it has been proven that problems of this kind are NP-hard. SFC-RS requires obtaining the optimal solution under the worst-case failure scenario. Among existing methods, Zeng et al. proposed the C-CG algorithm, which can effectively solve such two-stage robust optimization problems [25].

The C-CG algorithm is executed within a master-subproblem framework. In the initial state, the master problem only needs to consider the decision variables and constraints related to the first stage, which provides a suitable starting point for the subsequent optimization process. First, we define the master problem of SFC-RS:

$$MP\colon \min_{x,q} \boldsymbol{cx} + q \tag{24}$$

$$\begin{aligned}
s.t.\quad & G\boldsymbol{x} \geq g \\
& q \geq \boldsymbol{by}^{l} \quad \forall 1 \leq l \leq k \\
& D\boldsymbol{x} + E\boldsymbol{y}^{l} \geq f - R\boldsymbol{s}_{l}^{*} \quad \forall 1 \leq l \leq k \\
& H\boldsymbol{s}_{l}^{*} \leq a \quad \forall 1 \leq l \leq k \\
& \boldsymbol{x} \in Z, q \in R, \boldsymbol{y}^{l} \in R \quad \forall 1 \leq l \leq k \\
& \boldsymbol{s}_{l}^{*} \in R \times Z \quad \forall 1 \leq l \leq k
\end{aligned} \tag{25}$$

where $\boldsymbol{x}$ corresponds to the decision variable $x_{k,ij}^{ij}, y_{k,ij}^{ij}$ in SFC-RS; $\boldsymbol{cx}$ corresponds to the objective $\mathcal{R}$; q is the upper bound of the second stage objective function; s_{l}^{*} is the worst-case scenario for the second stage; Eq. (25) corresponds to the constraints in the preceding model. It is worth noting that due to the presence of nonlinear terms in the objective function and constraints proposed in Section 3, the Big-M method needs to be used to linearize them.

The objective of the subproblem is to solve the worst-case scenario based on the decisions made by the master problem. By solving the subproblem and gradually adding the parameters and related constraints corresponding to the worst-case scenario back to the master problem, the iterative process progressively improves the solution. The subproblem defined as follows:

$$SP\colon Q\left(\hat{x}\right) = \max_{s \in S} \max_{y} \boldsymbol{by} \tag{26}$$

$$\begin{aligned}
s.t.\quad & D\hat{\boldsymbol{x}} + E\boldsymbol{y} \geq f - R\boldsymbol{s} \\
& Hs \leq a \\
& \boldsymbol{y} \in R, \boldsymbol{s} \in R \times Z
\end{aligned} \tag{27}$$

where $\boldsymbol{y}$ represents the second-stage decision variables after linearization; $\boldsymbol{by}$ corresponds to the objective function $\mathcal{Q}$; $\hat{\boldsymbol{x}}$ represents the decision variable obtained after solving the master problem, and $\hat{\boldsymbol{x}}$ is known; Eq. (27) corresponds to the constraints related to the solutions of master problem.

Due to the large scale of uncertain scenarios in SFC-RS, it is not feasible to directly identify the worst-case scenario. Based on the solutions of previous subproblem, the C-CG algorithm modifies the parameters and constraints of the master problem in the next round, and then solves the master problem under the tightened conditions, and uses the obtained solution as known values to continue solving the subproblem. This iterative process gradually improves the feasible solution, converging towards results that closely approximate the worst-case scenario. The code process is shown in Algorithm 1.

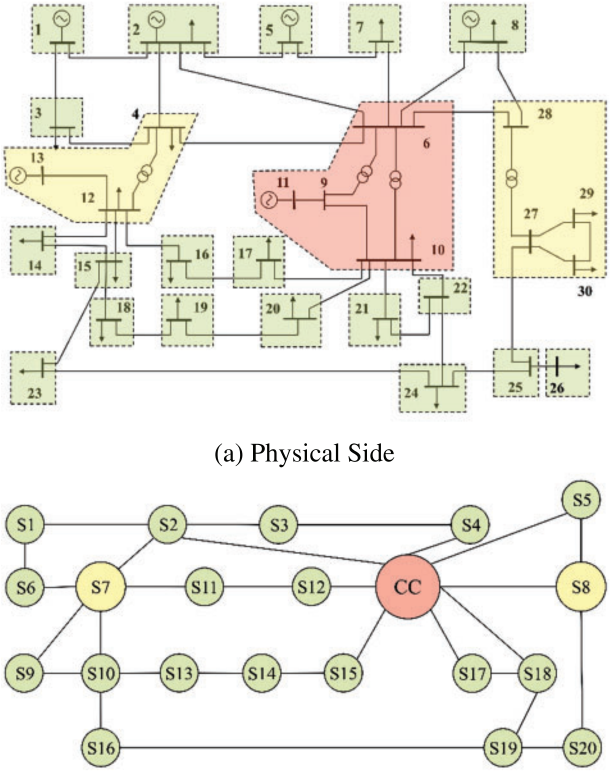
Algorithm 1: Column-and-Constraint Generation

```
1:  Set $LB = -\infty$, $UB = \infty$;
2:  Initialize $iter\_cnt = 0$, $\sigma \geq 0$;
3:  Solve the initial MP (without considering the uncertainty), and derive an optimal solution
    $\boldsymbol{x}_k^*, k = 1, \cdots, K$;
4:  Update $LB$ with $\boldsymbol{cx}_k^*$;
5:  With given $\boldsymbol{x}_k^*$,
6:  for $k = 1, \cdots, K$, do
7:      Call MIP solver to compute the subproblem;
8:  end for
9:  Update $UB = \min\left\{UB, \boldsymbol{cx}_k^* + Q\left(\boldsymbol{x}_k^*\right)\right\}$;
10: if $Q\left(\boldsymbol{x}_k^*\right)$ is feasible and bounded, then
11:     Create new variables $\boldsymbol{y}^{k+1}$ and add new constrains with $\boldsymbol{y}^{k+1}$:
            $q \geq \boldsymbol{by}^{k+1}$
            $Dx + \boldsymbol{Ey}^{k+1} \geq f - \boldsymbol{Rs}_{l+1}^*$
            $H\boldsymbol{s}_{l+1}^* \leq a$
        to MP;
12: else if $Q\left(\boldsymbol{x}_k^*\right)$ is unbounded, then
13:     Create new variables $\boldsymbol{y}^{k+1}$ and add new constraints with $\boldsymbol{y}^{k+1}$:
            $\boldsymbol{Dx} + \boldsymbol{Ey}^{k+1} \geq f - \boldsymbol{Rs}_{l+1}^*$
            $H\boldsymbol{s}_{l+1}^* \leq a$
        to MP;
14: end if
15: Call MIP solver to compute the master problem with new variables and constraints;
16: Derive an optimal solution $\left(\boldsymbol{x}_k^*, q_{k+1}^*, \boldsymbol{y}^{1*}, \cdots, \boldsymbol{y}^{k+1*}\right)$
17: Update $LB$ with $\boldsymbol{cx}_k^* + q_{k+1}^*$, $LB = \boldsymbol{cx}_k^* + q_{k+1}^*$;
18: if $UB - LB \leq \sigma$, then
19:     return $\boldsymbol{x}_{k+1}^*$ and terminate;
20: else
21: $iter\_cnt += 1$ and return to step 5;
22: end if
```

5 Simulation Results and Analysis

In this section, we apply the proposed SFC-RS to IEEE 30-bus system and the corresponding communication networks. The topologies of both networks are shown in Fig. 3.

The node CC is chosen as the control center because of the highest node degree. Considering the existence of transformers, the power nodes on both sides of the transformer are attributed to the same communication node. Due to the coupling characteristics of CPPS, for each node in the power network, there is a counterpart in the communication network corresponding to it, the two networks are highly coupled at the physical level.



(a) Physical Side

(b) Cyber Side

Figure 3: The topology of IEEE 30-bus system

We use Gurobi 9.5.2 to solve the optimization problem. The convergence threshold σ and the small value of μ the solver are both set to 10^{-4}. The balance factor is set to 0.5. The number of VNF type is set to 4. The length of each SFC is randomly distributed from 2 to 4, and VNFs of the same type are generated only once in each SFC. Set the link bandwidth to 30. Since the main objective of SFC-RS is to affect the operation of the power system by regulating the SFC paths, the communication delay is not considered, and the VNFs are allowed to be pre-deployed on communication nodes, representing scenarios where the communication infrastructure is shared.

According to the requirements of relevant Chinese standards, the first-class service must meet the planning objectives of N-2. In this paper, communication disruptions are presumed to be N-2 faults, while power grid failures are presumed to be N-1 faults. When both the primary and backup paths carrying the SFC are interrupted, the transmission of the SFC is obstructed. In actual power grid, the existing communication service routing optimization is artificially designed by using the experience of operators, and is mainly deployed based on the shortest-path routing model (SPRM) [20]. Therefore, this paper compares the effectiveness of the SPRM and the SFC-RS in the IEEE 30-node system.

5.1 Robustness Improvement Effects

Comparing the robustness, Fig. 4 illustrates the information transmission accessibility corresponding to each method. Analysis of Fig. 4 shows that in the worst-case scenario, SFC-RS has 3 nodes disconnected, while the maximum number of disconnected nodes in SPRM reaches 5. When dealing with N-2 failures, SFC-RS only reaches the maximum number of node disconnections in three scenarios, and the number of disconnected nodes in the remaining scenarios does not exceed two, which is much lower than the number of scenarios in SPRM where more than two nodes are disconnected. In addition, reference [26] quantifies the robustness of systems by analyzing the topology of the system after failures and calculating the proportion of surviving nodes to the total number of nodes in both the power and cyber systems. Similarly, following this method for robustness assessment, when more than 3 SFCs are blocked, it means that the number of lost nodes exceeds 3, and at least 15% of the emergency control services in the power system will fail. When SPRM is applied, if the disrupted links are No.4 and No.8, No.7 and No.16, or No.11 and No.16, the service interruption rate will be as high as 25%, posing a serious threat to the safety and stability of CPPS.

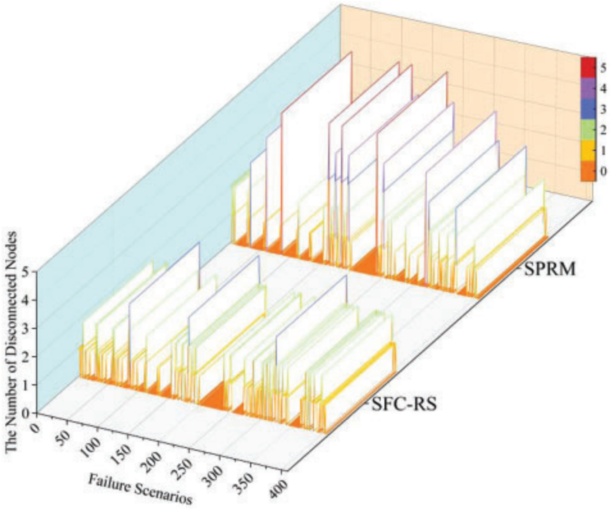


Figure 4: Comparison of accessibility in N-2 scenarios

The severity of the impact on the power system caused by the loss of emergency control services due to communication disruptions is represented by the load loss rate. Table 1 shows the load loss rates of both methods in response to N-2 failures, with both average and maximum values being lower than those of SPRM when SFC-RS is applied.

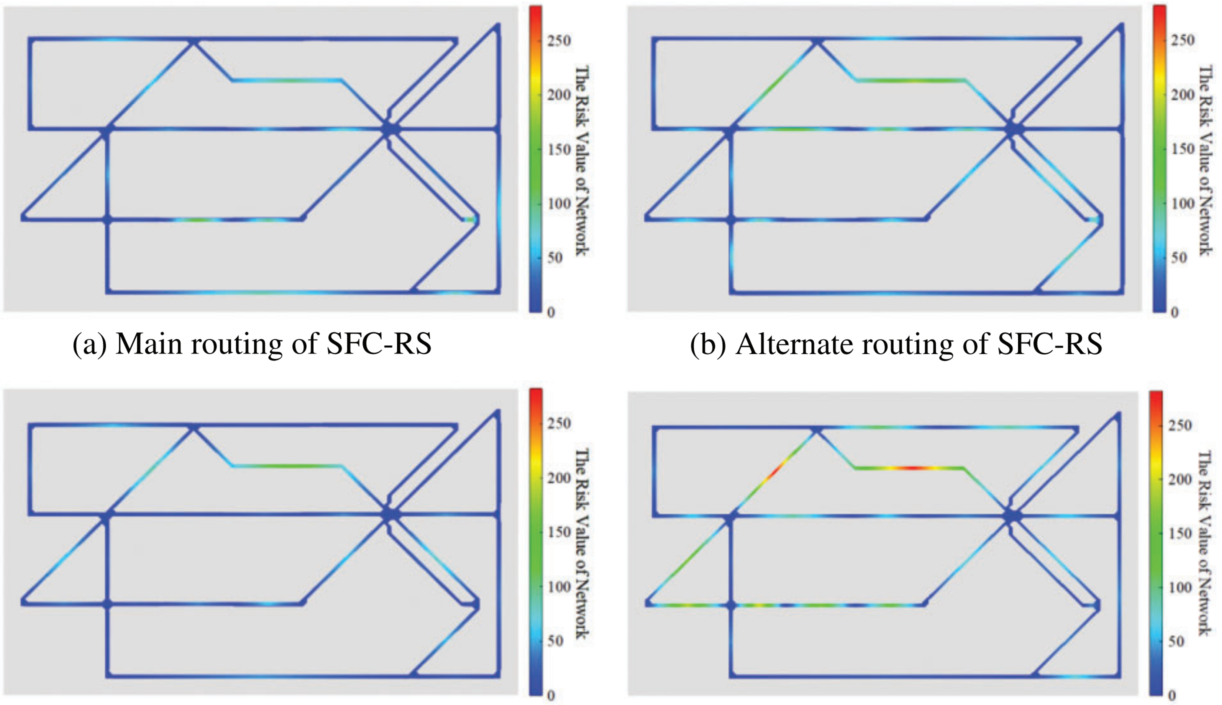
Table 1: Load loss rate under two methods

	SFC-RC	SPRM
Average	4.57%	6.38%
Max	22.08%	25.57%

From the effect of information reachability and load loss rate, it can be seen SFC-RS effectively improves the robustness of CPPS.

5.2 Risk Balancing Effects

Fig. 5 shows the risk distribution of SFCs carried by each physical link when the two algorithms are applied in the IEEE 30-bus communication system topology, and the color from dark to light indicates that the risk value on the line gradually increases. Comparing Figs. 5a and 5c, it could be found that the information is mainly concentrated in the upper half of the network when SPRM is used, because SPRM preferentially selects the path with the lowest cost, so that the information is collected on the path with a smaller weight, resulting in the centralized distribution of SFC. In contrast, SFC-RS takes the risk route weight as the weighting factor and dynamically updates the risk route weights in the network after assigning paths for the previous SFC. When allocating paths for a new SFC, SFC-RS seeks the path with the minimum risk route weight rather than the lowest cost path. This approach avoids information concentration in a specific area or on a particular link.



(a) Main routing of SFC-RS

(b) Alternate routing of SFC-RS

(c) Main routing of SPRM

(d) Alternate routing of SPRM

Figure 5: Comparison of risk distribution

However, compared to Fig. 5c, the overall risk value of Fig. 5a is slightly higher (there are more highlighted paths than Fig. 5c), because SFC-RS is essentially a type of shortest-path algorithms, the difference is that SFC-RS seeks the minimum link risk, which leads to individual SFC-RS assigned paths being longer compared to paths obtained using SPRM, and then causes an increase in the overall risk value. However, the original intention of SFC-RS is to reduce the probability of cross-space cascading failures through the effective adjustment of the information side. In this regard, the exceeding of risk value in an individual area or link is more dangerous than the slight risk increasing of the overall network. It could be concluded that SFC-RS slightly increases the average risk in exchange for the robustness of communication and the risk balance of network. From the view of the effect, such sacrifice is well worth it. The comparison between Figs. 5b and 5d further confirms this fact.

5.3 Verification of Entropy Value

We use the weighted failure risk entropy to assess the effectiveness of SFC-RS in achieving the objective of reducing the risk of cross-space cascading failures by suppressing information-side failures. Taking the blocked SFC importance sequence$R = \{0, 100, 200, \cdots, 2500\}$, by traversing the N-2 failure scenarios in the IEEE 30-bus system, the importance values of the blocked SFCs are statistically counted as shown in Fig. 6. By incorporating the impact of risk-balanced considerations into the robust optimization model, SFC-RS exhibits significantly lower blocked SFCs importance value compared to SPRM. These data are calculated by using the weighted failure risk entropy to obtain the entropy values, the results are given in Table 2.

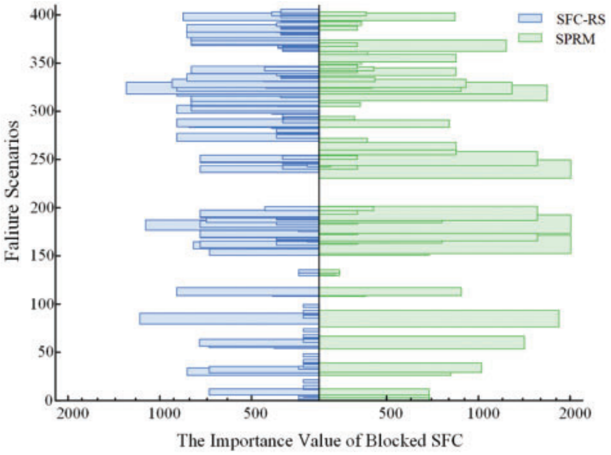


Figure 6: Comparison of the SFC importance value blocked in different scenarios

Table 2: Comparison of entropy

	SFC-RC	SPRM
Entropy value	495.057	601.126

According to the calculated results, the entropy value of SFC-RS is significantly lower than that of SPRM, which confirms the effectiveness of achieving the research objectives through SFC-RS.

6 Future Work

An important direction for future work is to incorporate dynamic line rating (DLR) into the assessment of SFC importance. This paper primarily assesses the risk of cascading failures and determines the importance of SFCs by considering the effects of both explicit and implicit failures. The calculation process adopts the static line rating (SLR) method to account for the load conditions of transmission lines. However, recent research articles have shown that the adoption of DLR in system analysis can provide a more realistic reflection of the load status of the power grid [27,28]. A more realistic system analysis will enable us to arrange SFCs more precisely, thereby minimizing the possibility of communication disruptions exacerbating cascading failures in the power grid. Therefore, we will proceed with further research from this perspective.

7 Conclusion

This paper first proposes cascading failure index for the approach of information importance evaluation, which achieves the quantification and identification of different information in the same class of communication services. And then the risk balancing strategy is improved by using the importance evaluation approach, making it more accurate in reflecting the risk distribution. Considering the influence of communication risk and the uncertainty of disruption, a joint risk-balanced service function chain routing strategy is proposed and modeled as a two-stage robust optimization problem. Simulation results verified the superiority of SFC-RS compared with the shortest-path routing model. SFC-RS effectively enhances information accessibility and the transmission robustness, achieves the decentralized circulation of high-importance information. The objective of reducing cross-space cascading failures caused by communication disruptions through information-side regulation has been achieved.

Acknowledgement: None.

Funding Statement: This research is funded by the National Natural Science Foundation of China under Grant 52177074.

Author Contributions: The authors confirm contribution to the paper as follows: Study conception and design: He Wang, Xingyu Tong; data collection: Huanan Yu; analysis and interpretation of results: He Wang, Xingyu Tong, Huanan Yu; draft manuscript preparation: Xingyu Tong, Xiao Hu, Jing Bian. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The authors confirm that the data supporting the findings of this study are available within the article.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Y. Li *et al.*, "An effective node-to-edge interdependent network and vulnerability analysis for digital coupled power grids," *Int. Trans. Electr. Energy Syst.*, vol. 2022, pp. 1–13, Sep. 2022. doi: 10.1155/2022/5820126.
2. 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, Aug. 2020. doi: 10.1109/ACCESS.2020.3016826.
3. X. Gao, M. Peng, C. K. Tse, and H. Zhang, "A stochastic model of cascading failure dynamics in cyber-physical power systems," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4626–4637, Jan. 2020. doi: 10.1109/JSYST.2020.2964624.
4. B. Ti, G. Li, M. Zhou, and J. Wang, "Resilience assessment and improvement for cyber-physical power systems under typhoon disasters," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 783–794, Sep. 2022. doi: 10.1109/TSG.2021.3114512.
5. A. Behfarnia and A. Eslami, "Error correction coding meets cyber-physical systems: Message-passing analysis of self-healing interdependent networks," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2753–2768, Apr. 2017. doi: 10.1109/TCOMM.2017.2698480.
6. Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 530–538, Oct. 2016. doi: 10.1109/TSG.2015.2478888.
7. U.S.-Canada power system outage task force. "Final report on the August 14, 2003 blackout in the united states and canada," 2004. Accessed: Jun. 03, 2024. [Online]. Available: https://www3.epa.gov/region1/npdes/merrimackstation/pdfs/ar/AR-1165.pdf
8. J. Wang, Y. Su, and J. Zhou, "Practice and experience in dispatching of southern power grid during rare ice disaster at beginning of year 2008," in *Proc. 4th Int. Conf. Elect. Utility Deregulation Restructuring Power Technol. (DRPT)*, 2011, pp. 1869–1874.

9. G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 Ukraine blackout: Implications for false data injection attacks,” *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Nov. 2017. doi: 10.1109/TPWRS.2016.2631891.
10. S. Djunisic, “Fire, high renewables share caused Mexico’s Dec. 28 blackout, experts say,” Accessed: Jun. 03, 2024. [Online]. Available: https://renewablesnow.com/news/fire-high-renewables-share-caused-mexicos-dec-28-blackout-experts-say-746746/
11. N. Suhaimy, N. A. M. Radzi, W. S. H. M. Ahmad, K. H. M. Azmi, and M. A. Hannan, “Current and future communication solutions for smart grids: A review,” *IEEE Access*, vol. 10, pp. 43639–43668, Apr. 2022. doi: 10.1109/ACCESS.2022.3168740.
12. J. Gil Herrera and J. F. Botero, “Resource allocation in NFV: A comprehensive survey,” *IEEE Trans. Netw. Serv. Manag.*, vol. 13, no. 3, pp. 518–532, Aug. 2016. doi: 10.1109/TNSM.2016.2598420.
13. N. Promwongsa *et al.*, “Ensuring reliability and low cost when using a parallel VNF processing approach to embed delay-constrained slices,” *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 4, pp. 2226–2241, Oct. 2020. doi: 10.1109/TNSM.2020.3029108.
14. L. Qu, C. Assi, M. J. Khabbaz, and Y. Ye, “Reliability-aware service function chaining with function decomposition and multipath routing,” *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 2, pp. 835–848, Dec. 2020. doi: 10.1109/TNSM.2019.2961153.
15. J. Pei, P. Hong, K. Xue, and D. Li, “Resource aware routing for service function chains in SDN and NFV-enabled network,” *IEEE Trans. Serv. Comput.*, vol. 14, no. 4, pp. 985–997, Jun. 2021. doi: 10.1109/TSC.2018.2849712.
16. Z. Kuai, T. Wang, and S. Wang, “Fair virtual network function mapping and scheduling using proximal policy optimization,” *IEEE Trans. Commun.*, vol. 70, no. 11, pp. 7434–7445, Sep. 2022. doi: 10.1109/TCOMM.2022.3211071.
17. H. Chen, S. Wang, G. Li, L. Nie, X. Wang and Z. Ning, “Distributed orchestration of service function chains for edge intelligence in the industrial internet of things,” *IEEE Trans. Ind. Inform.*, vol. 18, no. 9, pp. 6244–6254, Dec. 2022. doi: 10.1109/TII.2021.3131757.
18. T. Duan and V. Dinavahi, “Fast path recovery for single link failure in SDN-enabled wide area measurement system,” *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1645–1653, Dec. 2022. doi: 10.1109/TSG.2021.3131682.
19. P. Kong and Y. Jiang, “Vnf orchestration and power-disjoint traffic flow routing for optimal communication robustness in smart grid with cyber-physical interdependence,” *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 4, pp. 4479–4490, Apr. 2022. doi: 10.1109/TNSM.2022.3165219.
20. L. Xu, Q. Guo, T. Yang, and H. Sun, “Robust routing optimization for smart grids considering cyber-physical interdependence,” *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5620–5629, Dec. 2019. doi: 10.1109/TSG.2018.2888629.
21. S. Xin, Q. Guo, H. Sun, C. Chen, J. Wang and B. Zhang, “Information-energy flow computation and cyber-physical sensitivity analysis for power systems,” *IEEE Jour. Emer. Select. Top. Circu. Syste.*, vol. 7, no. 2, pp. 329–341, Jan. 2017. doi: 10.1109/JETCAS.2017.2700618.
22. Y. Liu, M. Peng, X. Gao, and H. Zhang, “Probabilistic vulnerability assessment of transmission lines considering cascading failures,” *Processes*, vol. 9, no. 11, pp. 1994, Nov. 2021. doi: 10.3390/pr9111994.
23. B. Li, C. Lu, B. Qi, Y. Sun, and J. Han, “Risk and traffic based service routing optimization for electric power communication network,” *Int. J. Electr. Power Energy Syst.*, vol. 137, p. 107782, May 2022. doi: 10.1016/j.ijepes.2021.107782.
24. B. Ti, J. Wang, G. Li, and M. Zhou, “Operational risk-averse routing optimization for cyber-physical power systems,” *CSEE J. Power Energy Syst.,* Jan. 2022. doi: 10.17775/CSEEJPES.2021.00370.
25. B. Zeng and L. Zhao, “Solving two-stage robust optimization problems using a column-and-constraint generation method,” *Oper. Res. Lett.*, vol. 41, no. 5, pp. 457–461, Sep. 2013. doi: 10.1016/j.orl.2013.05.003.
26. S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, “Catastrophic cascade of failures in interdependent networks,” *Nature*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010. doi: 10.1038/nature08932.

27. B. Jimada-Ojuolape and J. Teh, "Composite reliability impacts of synchrophasor-based dtr and sips cyber-physical systems," *IEEE Syst. J.*, vol. 16, no. 3, pp. 3927–3938, Jan. 2022. doi: 10.1109/JSYST.2021.3132657.
28. B. Jimada-Ojuolape and J. Teh, "Impacts of communication network availability on synchrophasor-based dtr and sips reliability," *IEEE Syst. J.*, vol. 16, no. 4, pp. 6231–6242, Nov. 2022. doi: 10.1109/JSYST.2021.3122022.