EMS communication routings’ optimisation to enhance power system security considering cyber-physical interdependence

Qinglai Guo1,*, Shujun Xin2, Luo Xu1, Hongbin Sun1

1Department of Electrical Engineering, Tsinghua University, Beijing 100084, People’s Republic of China
2State Power Economic Research Institute, Beijing 102209, People’s Republic of China
*E-mail: guqinglai@tsinghua.edu.cn

Abstract: Energy management system (EMS) is one of the most essential categories of the advanced applications in current cyber-physical power systems. However, because of the tight coupling relationship between a power network and EMS’s communication network, a physical break-line fault may be accompanied by a communication line outage, which may result in regional unobservability and uncontrollability. To maximally avoid and eliminate such operation risks, referring to current EMS’s ‘active + standby’ communication configuration scheme in China, the authors propose a dynamic routing optimisation mechanism for its standby communication routings, assigning the most reliable communication lines to the most important information. Such optimisation considers two factors: information’s significance and the reliability of communication lines. By introducing cyber-physical sensitivity index and path-branch incidence matrix, both factors can be expressed numerically. In the case study, the authors optimise the standby communication routings for a power flow corrective control application under different scenarios. The results verify the effectiveness and superiority of their approach.

1 Introduction

Thanks to the introduction of information and communications technology (ICT), traditional power grids have gradually evolved into cyber-physical smart grids [1–4]. Energy management systems (EMSs) play an important role in all smart applications. With comprehensive and wide perception and regulation, an EMS helps to ensure a physical power grid’s safe and reliable operation [5–7].

An EMS’s communication network supports the control centre’s awareness and control ability for the entire power network [8–10]. Communication lines, such as fibres, are mostly set up along the power transmission lines, thus the topologies of a physical power grid and its corresponding power communication network are always highly coupled [11]. For example, optical fibre composite overhead ground wire combines fibre and ground wire, and the fibre is often located inside the overhead ground wire [12]. Therefore, when extreme weather descends upon a regional power system and leads to serious device failures, such as pole collapse, power transmission lines and their corresponding communication lines are likely to be destroyed simultaneously [13, 14]. The break-line faults in EMS’s communication network may result in the control centre losing communication to some areas, thereby leading to inappropriate feedback control actions on physical power grids. Such risks could further trigger or aggravate physical operation failures. For example, in coastal power networks, the loss of a crucial substation’s communication often leads to serious regional blackouts. Therefore, to maximise the reliability of energy management processes, it is necessary to properly allocate the information flow inside an EMS’s communication network by optimising its communication routings.

Many ICT-related researches have addressed the issue of communication configuration and optimisation, with methods including routing optimisation algorithms [15], queue control [16, 17], communication network design [18] and software-defined networks (SDNs for short) [19, 20]. Through configuring information transmission paths by adjusting communication routers and channels, we can improve the operation efficiency of the communication network, for example reducing routing hops and communication time, maximising data interchange, and balancing the communication load. However, the optimisation objectives for the above-mentioned approaches only focus on the communication network itself, but the core value of an EMS should be supporting a power grid’s safe and stable operation. Therefore, when optimising the communication routings for an EMS, it is necessary to first consider the requirements of the power system’s operation and control, rather than the state of its communication network.

To guarantee safety and reliability of power system dispatching, current EMSs are mostly installed on separate communication networks owned by private electricity utilities rather than public ones [21]. In addition, to avoid mistakenly mutual interferences among different signals, a power utility’s communication and automation divisions prefer to determine a fixed communication routing scheme between the control centre and all substations while generating the dispatching plan. In other words, the communication links between substations and the control centre can be regarded as isolated and fixed during operation. Currently, to further increase the reliability of EMSs’ dispatching, system designers and operators attempt to utilise communication redundancy by configuring a standby communication scheme occupying different channels. If the communication of an active link is blocked by an accident, the control centre can promptly switch to the standby one. With this ‘active + standby’ mechanism, proper coordination between two groups of communication routings can effectively decrease the influence of communication outages on EMS services and control.

Considering this background, an effective method for optimising EMS’s communication is to optimise its communication routings between substations and the control centre. Notably, to adapt to dynamic operation scenarios and external environments, different load distributions and weather conditions, for example, an EMS needs to make different control decisions, in which the information significance and the importance of channels under different scenarios should be accordingly different. Therefore, an EMS’s communication optimisation should be a dynamic process rather than fixed. Considering that the constructed communication network and the enabled active communication routings cannot be discretionarily manipulated, in this paper we propose a dynamic optimisation mechanism for standby communication routings. In other words, we are trying to re-schedule the standby communication routings on-line considering the cyber-physical interdependence, and ensure that the most ‘important’ information will be deployed to the most ‘reliable’ communication channel.
Such a mechanism could help to improve the reliability of power system operation and energy management processes.

This paper is organised as follows: In Section 2, we propose a matrix-based optimisation model. In Section 3, we take a power flow corrective control (PFCC) application as an example to illustrate how to apply the optimisation mechanism to real EMSs’ configuration, and study three different scenarios. The results verify the effectiveness and superiority of our theory. Finally, in Section 4, we provide a summary and a future outlook.

2 Optimisation model for an EMS’s standby communication routings

2.1 Optimisation idea and general model

According to researches [5, 6], the significance of different information in an EMS should be different. For example, for a coordinated voltage control application, voltage measurements of different buses have different contributions to the decision-making process, of which the pilot-bus measurements are most important. Correspondingly, cyber contingencies on different information might affect power systems differently. As a matter of fact, the essence of communication scheme optimisation is to properly allocate different information in a communication network according to its significance and the communication environment, so that the most important information can be transmitted by the most reliable channels.

According to the analysis above, such an optimisation should be determined by two main factors:

i. Significance of information, which refers to how much an information value could affect power system operation, i.e. the seriousness of the impact of a cyber-contingency on a physical power system. According to Xin et al. [6], information's significance can be described as its cyber-physical sensitivity index and can be calculated based on the operation state of a power network and its EMS application.

ii. Reliability of a communication line, which can be represented by the influence of a communication line's interruption on an EMS's communication. The less likely a failure is to occur, and the less information the failure affects, the more reliable a communication line is. As mentioned in Section 1, in order to avoid conflicts among different services or signals, the routing tables of an electric power communication network are usually configured in advance rather than automatically addressed, thus the impact of any communication failure can be quantitatively assessed by topology analysis.

Indeed, the two above-mentioned factors determine the extent to which a communication line outage affects physical operation. For the former factor (significance of information), because an EMS generates control decisions based on state measurements, the information significance should be determined by physical operation states including voltage level, load distribution and switch states. In this paper, we define those different operation states as physical operation scenarios. Notably, a physical power grid may be faced with numerous possible operation scenarios. While for the latter factor (reliability of a communication line), it can be described with communication risks a communication network may be confronted with. Therefore, in order to maximally eliminate the impact that a power system suffers from communication vulnerabilities, an EMS’s communication optimisation should take into consideration both physical operation scenario/communication risk sets as well as their occurrence probabilities. The schematic diagram for such an idea is presented in Fig. 1.

As mentioned in Section 1, the goal of our standby communication optimisation is to reduce the risk communication failures poses to physical operation while properly configuring the communication resources, such as channels. For a certain EMS application, assuming that its physical state variables are defined as vector $x$, the substation measurements are represented by vector $z$, and the final control signals issued by the control centre are represented by vector $y$, the general optimisation model can be described by the following equation:

$$\min \sum_{x \in \mathcal{N}} \sum_{y \in \Psi} (s(\mathbf{x}, \mathbf{z}) \cdot \Delta s(\mathbf{x}, \mathbf{z}) + s(\mathbf{x}, \mathbf{y}) \cdot \bar{\Delta} y(\mathbf{x}, \mathbf{y})) \cdot q \cdot r$$

where $\mathcal{N} = \{x\}$ and $\mathcal{R} = \{r\}$, respectively, represent the communication outage set and the corresponding possibilities ($k$ represents the number of an outage), and $\Psi = \{\Psi\}$ and $\mathcal{Q} = \{q\}$, respectively, represent the physical operation scenario set and the possibilities ($q$ refers to the possibility of the $k$th operation scenario $\Psi$). $s(\mathbf{x}, \mathbf{z})$ and $s(\mathbf{x}, \mathbf{y})$ refer to the sensitivity indices, respectively, between virtual quantity $z$ and selective physical state variables. $c$ refers to the fibre's maximum occupancy rate, which is often utilised to evaluate the balance degree of a communication.
network. In power communication systems, different substations’ routings usually occupy different channels, thus \( c \) can be represented by maximum quantity of the occupied channels in a fibre. Finally, \( \Lambda \) is a small quantity.

\( \Delta z(\chi_{l}) \) and \( \Delta y(\chi_{l}) \) represent the impact of communication outage \( \chi_{l} \) on the measurement and control signals’ transmission between the control centre and the substations. Assuming that there are \( n \) substations, \( \Delta z(\chi_{l}) \) and \( \Delta y(\chi_{l}) \) can be abstracted in the following form:

\[
\Delta z(\chi_{l}) = \begin{bmatrix}
\Delta z_{1}(\chi_{l}) \\
\vdots \\
\Delta z_{n}(\chi_{l})
\end{bmatrix}^{T},
\Delta y(\chi_{l}) = \begin{bmatrix}
\Delta y_{1}(\chi_{l}) \\
\vdots \\
\Delta y_{n}(\chi_{l})
\end{bmatrix}^{T}.
\]

To be specific, the elements of \( \Delta z(\chi_{l}) \) and \( \Delta y(\chi_{l}) \) are defined as follows:

\[
\Delta z_{i} = \begin{cases}
1, & \chi_{i} \text{ blocks the uploading of substation } i's \text{ measurement } z_{i} \\
0, & \text{others}
\end{cases},
\Delta y_{i} = \begin{cases}
1, & \chi_{i} \text{ blocks the control signal } y' \text{ issuing to substation } i \\
0, & \text{others}
\end{cases}.
\]

The first half of (1) represents the expected impact that the anticipated risks make on power system operation. The final \( \Lambda \cdot c \) is introduced to balance the information distribution. In such an optimisation model, \( N = \{z_{i}\} \), \( R = \{q_{i}\} \), \( \Psi = \{\Psi_{i}\} \) and \( Q = \{q_{i}\} \) can be pre-assessed according to the prediction results, e.g. weather forecasting and load forecasting reports; sensitivity indices \( s(x, z) \) and \( s(x, y) \) can be calculated according to the method described in research [6] based on the system's information-energy flow model.

Finally, the key to building such an optimisation model is to quantitatively express the vectors \( \Delta z(\chi_{l}) \) and \( \Delta y(\chi_{l}) \) by mappings from communication outage \( \chi_{l} \). Notably, both the active and standby communication routings could affect \( \Delta z(\chi_{l}) \) and \( \Delta y(\chi_{l}) \)’s values. Therefore, in the following two sub-sections, we first introduce a path-branch incidence matrix to describe the routing schemes, and utilise such a matrix expressing \( \Delta z(\chi_{l}) \) and \( \Delta y(\chi_{l}) \).

### 2.2 Topological expression for communication routings

Similar to a physical power network, the topology of a power communication network can also be modelled as a graph. Defining the substation (node) set as \( N = \{N_{1}, N_{2}, ..., N_{n}\} \) and the communication line (branch) set as \( b = \{b_{1}, b_{2}, ..., b_{m}\} \), a power communication network can be expressed as graph \( G(N, b) \).

Indeed, a routing scheme, whether active or on standby, refers to the sum of the links between all substations and the control centre, and each link can be described as a path from a substation to the control centre, which consists of a group of end-to-end branches. In this research, the active up-link and down-link sets are described as \( G^{u} \) and \( G^{d} \), respectively, and the standby up-link and down-link sets are similarly described as \( G^{s} \) and \( G^{p} \). As the formats of the four link sets should be similar, here we only take \( G^{u} \) as an example to illustrate the definitions of the elements.

Define

\[
G^{u} = \{\text{path}(1), ..., \text{path}(n)\},
\]

where \( \text{path}(j) \) represents the standby up-link from substation \( j \) to the control centre. For any \( 1 \leq j \leq n \), we have

\[
\text{path}(j) = \{N'(j, 1), ..., N'(j, \text{Len}(j) + 1); b'(j, 1), ..., b'(j, \text{Len}(j))\},
\]

in which

\[
\forall 1 \leq k \leq \text{Len}(j) + 1, \ N'(j, k) \in N \\
\forall 1 \leq l \leq \text{Len}(j), \ b'(j, l) \in b.
\]
\[ T = \overrightarrow{T} = \overleftarrow{T} \]

\[
\begin{bmatrix}
 b_1 \\
 b_2 \\
 b_3 \\
 b_4 \\
 b_5 \\
 b_6 \\
 b_7 \\
 b_8 \\
 b_9 \\
 b_{10} \\
 b_{11} \\
 b_{12} \\
 b_{13} \\
 b_{14} \\
 b_{15}
\end{bmatrix}
\]

\[
\begin{bmatrix}
 s_1 \\
 s_2 \\
 s_3 \\
 s_4 \\
 s_5 \\
 s_6 \\
 s_7 \\
 1 \\
 1 \\
 0 \\
 1 \\
 1 \\
 1 \\
 1 \\
 0 \\
 1 \\
 1
\end{bmatrix}
\]

Assuming that communication line 8 is interrupted by an accident (see the red star in Fig. 3), substations 6, 9 and 10's communication should be blocked (see the red circles and line in Fig. 3), which exactly corresponds to the non-zero element in \( b_8 \)'s row vector in matrix (10), i.e.

\[
b_8 \rightarrow T_8 = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \\ s_8 \\ s_9 \\ s_{10} \end{bmatrix} = [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1] \\
\]

### 2.3 Expression of communication outage impacts

In this section, we utilise the previously proposed path-branch incidence matrices to express \( \Delta z(\chi) \) and \( \Delta y(\chi) \) in (1).

For a certain communication interruption scenario \( \chi \), assume the faulty communication lines are set as

\[
b(\chi) = \{b_1^\prime \ldots b_{\text{size}(\chi)}^\prime \} \subset b.
\]

In this scenario, all the links related to \( b(\chi) \) should be terminated, thus the blocked information transmission can be described as the sum of the row vectors corresponding to \( b(\chi) \). Thanks to the 0–1 duality of path-branch incidence matrices, such a set operation can be equally transformed as multiplications among vectors.

According to the definitions in (8), the impact of \( \chi \) on active/standby communication can be expressed as

\[
\Delta z(\chi) = \alpha(n) - \alpha(n) - T(\chi) \cdot (\chi)^T, \ldots
\]

\[
\Delta y(\chi) = \alpha(n) - \alpha(n) - T(\chi) \cdot (\chi)^T, \ldots
\]

\[
\Delta z(\chi) = \alpha(n) - \alpha(n) - T(\chi) \cdot (\chi)^T, \ldots
\]

\[
\Delta y(\chi) = \alpha(n) - \alpha(n) - T(\chi) \cdot (\chi)^T, \ldots
\]

where \( \alpha(n) \) refers to an \( n \)-dimensional column vector whose elements are all +1. Operator \( \cdot \) represents the multiplication between two column vectors with the same dimension. Assume

\[
\begin{bmatrix}
 y_1 \\
 \vdots \\
 y_k
\end{bmatrix} \cdot \begin{bmatrix}
 \beta_1 \\
 \vdots \\
 \beta_k
\end{bmatrix} = \begin{bmatrix}
 y_1 \cdot \beta_1 \\
 \vdots \\
 y_k \cdot \beta_k
\end{bmatrix}
\]

When an EMS is configured with ‘active + standby’ communication routings, only when a substation's active and standby link to the control centre are interrupted simultaneously, can its communication be terminated. Therefore, \( \chi \)'s final impacts

---

**Fig. 2** Cyber-physical model for the IEEE 14 bus test system and the active communication routings

**Fig. 3** Impact of communication line 8's interruption on information transmission

\[ \text{IET Cyber-Phys. Syst., Theory Appl., 2018, Vol. 3 Iss. 1, pp. 44-53} \]

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/)
on up-link/down-link data can be described as the intersection of the active and standby
\[
\Delta z(\chi) = \Delta z^s(\chi) \cap \Delta z^f(\chi) = \Delta z^s(\chi) \ast \Delta z^f(\chi) \]
\[
\Delta y(\chi) = \Delta y^s(\chi) \cap \Delta y^f(\chi) = \Delta y^s(\chi) \ast \Delta y^f(\chi)
\]
(15)
Substituting (13) into (15), the impacts of any communication outage can be expressed as a mapping from four path-branch incidence matrices \( \overline{T}, \overline{F}, \overline{T}^l \) and \( \overline{T}^r \). To be specific, when optimising the standby communication routings, \( \overline{T} \) and \( \overline{F} \) can be regarded as known, thus \( \Delta z(\chi) \) and \( \Delta y(\chi) \) can be reformulated as a function of \( \overline{T}^l \) and \( \overline{T}^r \). Therefore, in this optimisation model, the optimisation variables should be \( \overline{T}^l \) and \( \overline{T}^r \).

2.4 Optimisation model for the standby communication routings

After substituting (13) and (15) into (1), we can reformulate the optimisation model for the standby communication routings as (16), in which the definitions for the most variables can be referred to (1), (13) and (14). In particular, we define (see (16))
\[
A^* \{a^*_{j,k}\} = A \cdot A^T
\]
(17)
in which \( A \) is the node-branch incidence matrix of the communication network \( G(N, b) \), with elements defined as follows:
\[
a(j,k) = \begin{cases} 1, & N_j = b_k; \text{start} \\ -1, & N_j = b_k; \text{end} \\ 0, & N_j \notin b_k \end{cases}
\]
(18)
where \( a(j,k) \) refers to the element in the \( j \)th row and \( k \)th column, and \( b_k \) start and \( b_k \) end, respectively, refer to the start node and end node of directed branch \( b_k \). According to the definition, only when vertices \( N_j \) and \( N_j \) are directly connected by communication lines can the element be non-zero.

In (16), the optimisation objective is to minimise the expected impacts of the possible communication risks; optimisation variables are matrices \( \overline{T}^l \) and \( \overline{T}^r \), corresponding to standby up-link and down-link sets, and the constraints are the connectivity of all links. Currently, communication system designers and engineers often use the genetic algorithm to study discrete path planning problems because of its guarantee for paths’ connectivity [22–24]. Therefore, in this paper, we also introduce the genetic algorithm to achieve this optimisation.

3 Case study: optimisation supporting PFCC application

In this section, we take a certain advanced EMS application as an example, i.e. the PFCC application, to illustrate our optimisation theory’s application as well as its effectiveness.

3.1 Brief introduction of PFCC

PFCC is an energy management technique for power system dispatching and is widely applied in most power systems [25, 26]. During a power system’s operation, different fluctuations of loads and generations, as well as randomly occurring device failures, may result in overloads in different power transmission lines. Such events relate to different operation scenarios in our case study. The primary goal of PFCC is to eliminate such overloads by regulating the load distributions and generator outputs. Other than in extreme emergency scenarios, a PFCC application does not perform load shedding.

To illustrate the cyber-optimisation issue, a simplified model of PFCC is adopted as follows:
\[
\text{min} \| \Delta P_r \|_l \\
\text{s.t.} \quad \text{diag}(d^p) \cdot (A^p)^T \cdot \left( B^p \right)^{-1} \cdot \Delta P_r + \text{p}^{\text{line}, \Psi} = \text{p}^{\text{line}, \Psi, \text{ref}}
\]
(19)
where superscript ‘line’ represents the transmission line, and superscript ‘\( \Psi \)’ represents the generator. Vector \( P^{\text{line}, \Psi} \) represents the transmission power of the overloaded lines under operation scenario \( \Psi \), and vector \( P^{\text{line}, \Psi, \text{ref}} \) represents the transmission limits of those lines. In power system analysis theory, matrix \( B \) is defined as a highly sparse susceptance matrix, i.e. the imaginary part of the node-branch admittance matrix. Vector \( d^p \) contains the susceptance information, \( \text{diag}(d^p) \) is the diagonal matrix with the vector \( d^p \) on the diagonal, and matrix \( A \) refers to the power network’s node-branch incidence matrix. To be specific, in this equation, \( A^p \) and \( B^p \), respectively, represent the power system’s susceptance and node-branch incidence matrices under operation scenario \( \Psi \). Although additional information may also affect the PFCC’s decisions by adding extra constraints to optimisation (16), such as power range and uncertainty indices, \( P^{\text{line}, \Psi} \) and \( P^{\text{line}, \Psi, \text{ref}} \) affect such closed-loop control most. For this reason, we present such a simplified model to better illustrate the contribution of our cyber-optimisation approach, i.e. allocating the most essential information to the most stable channels.

If we only consider a simple PFCC model without inequality constraints, the optimisation (19) can be simplified into a linear mapping from \( P^{\text{line}, \Psi} \) and \( P^{\text{line}, \Psi, \text{ref}} \) to \( \Delta P_r \):
\[
\Delta P_r = \left(C^pight)^T \left((C^p) \cdot (C^p)^T\right)^{-1} \left(P^{\text{line}, \Psi, \text{ref}} - P^{\text{line}, \Psi}\right)
\]
(20)
in which
\[
C^p = \text{diag}(d^p) \cdot (A^p)^T \cdot \left( B^p \right)^{-1}
\]
(21)

3.2 PFCC’s vulnerabilities: cyber-physical break-line faults

As mentioned in Section 1, an EMS’s communication network’s structure is often tightly coupled with its physical power grid’s structure. Therefore, a break-line fault occurring in the power grid might be accompanied by a failure on its coupled communication

\[
\begin{align*}
\text{min} & \sum_{g^l, g^l,c \in k, \Psi=\Psi} (\text{diag}(s^l(\Psi)) \cdot e^l \cdot \Delta z(\chi) + \text{diag}(s^f(\Psi)) \cdot e^f \cdot \Delta y(\chi)) \cdot r_k \cdot q_j) \quad + \Lambda \cdot c \\
\text{s.t.} & \forall 1 \leq j \leq n, \\
& \forall 1 \leq k_1 \leq \text{Len}(j), \forall 1 \leq k_2 \leq \text{Len}(j) + 1, \ k_2 \neq k_1 \\
& N^l(j, k_2) \neq N^l(j, k_2) = \text{start} \\
& N^l(j, k_2) + 1 = b^l(j, k_2). \text{end} = b^l(j, k_2) + 1. \text{start}
\end{align*}
\]
(16)
line, which may block information transmission inside the EMS. In this case study, such accidents are defined as cyber-physical break-line faults.

A cyber-physical break-line fault could result in both power flow redistribution and communication outages, and the former impact may cause power overloads, while the latter one may seriously hinder the EMS's measurement and control actions, thus further aggravating operation risks, such as observable or uncontrollable power overloads. Take an example to illustrate the mechanism of cyber-physical break-line fault. For the IEEE-14 bus system presented in Fig. 2, we consider the active communication routings and introduce a cyber-physical break-line fault on the power/communication line connecting substation 1 and substation 5 (i.e. bus 1 and bus 5). The graph-based assessment of such a failure is briefly presented in Fig. 4.

In the physical power grid, such a fault breaks the power transmission line between bus 1 and bus 5 (see the right subfigure in Fig. 4). In addition, because of the topology coupling between the power grid and the communication network, the communication between substation 1 and substation 5 should also be blocked, which means that the control centre cannot issue the control command to bus 1’s generator (see the left subfigure in Fig. 4). Unfortunately, in this condition, if the output of bus 1’s generator remains the same, most of the power flow of power transmission line (S1–S5) will be transferred to power transmission line (S1–S2), resulting in serious overloads, which could possibly trigger a cascading failure.

The aforementioned analysis illustrates the impact of a cyber-physical break-line fault on a PFCC’s communication as well as the necessity for a standby communication configuration. To ensure the reliable and safe operation of a power system, power system operators are required to dynamically optimise the standby communication routings according to the risk scenario, thereby reducing such cyber-physical negative impacts by switching between two routing schemes.

### 3.3 Cyber-physical sensitivity analysis for PFCC

Before generating the optimisation model (16), it is first necessary to obtain the cyber-physical sensitivity indices for z and y. To be specific, for PFCC application, z refers to $P_{\text{line}}$, $\Psi$, and y refers to control command $\Delta P_g$. Utilising the method discussed in research [6], we can generate the information-energy flow model for such a cyber-physical power system based on the decision function (21). The model for an IEEE-14 bus system is presented in Fig. 5.

For a power transmission line, assume that any terminals’ communication loss could affect its observability [27], based on which we can briefly estimate the cyber-physical sensitivity indices between information values $P_{\text{line}}$, $\Psi$, $\Delta P_g$ and line overload according to the method discussed in [6]:

$$s(P_{\text{line}}) = \begin{cases} 1, & b_i^l \in b^l_{\text{overload}} \\ 0, & b_i^l \notin b^l_{\text{overload}} \end{cases}$$

and line overload

$$s(\Delta P_g) = C^{\Psi}_{j}$$

in which $b^l_{\text{overload}}$ represents the set of the overloaded power transmission lines, $b_i^l$ represents the i-th power transmission line, and $C^{\Psi}_{j}$ refers to $C^\Psi$’s row vector corresponding to the i-th generator (see (21) for $C^\Psi$’s definition).

Substituting the above sensitivity indices into the optimisation model (16), and solving the problem with the genetic algorithm, we
can optimise standby communication routings for different scales of power systems under different load conditions and risk scenarios. In the following subsection, we will propose three scenarios and analyse their optimised routings to illustrate the effectiveness and superiority of our approach.

3.4 Standby communication routings’ optimisation for different scenarios

3.4.1 Consider power load fluctuations: During power system operation, power loads on different buses may fluctuate with numerous factors, such as time, temperature and season, leading to different power flow distribution inside the power network. Thus, a dynamic optimisation for EMS’s communication routing is required to adapt to the current load distribution and ensure safe operation. An ideal communication scheme should first guarantee the communication reliability for the most significant measurement and control signals.

In this case, the physical system is set as the IEEE 14-bus system with an PFCC application, whose structure and coupled communication network are shown in Fig. 2. The probability of a power line outage is set as 0.02%, and the conditional probability for a cyber-physical break-line fault is set as 30%. The maximum quantity of broken power lines is set as 3.

In an IEEE 14-bus system, the generation and load are concentrated in the upper-half. Our case study considers a load fluctuation scenario in the bottom-half network, in which the power load of each bus is tripled in a control period (see the red dotted box in Fig. 6). In this scenario, power transmission lines (S1–S2) and (S1–S5) are most vulnerable to overloading (see the left sub-graph in Fig. 6), thus the control centre needs to preferentially regulate substations S1, S4 and S5’s generation output based on substations S1, S2 and S5’s measurements. Accordingly, these substations should be the pivotal substations for this operation scenario. After optimisation for the standby communication routings, a comparison between three pivotal substations’ active and standby links to the control centre is presented in the right sub-graph in Fig. 6.

In the right sub-graph, the yellow circles represent the pivotal substations, the black lines represent active routings, and the green/orange dotted lines represent standby up-links/down-links. Symbols * and # refer to the uploaded measurements and issued control signals, respectively. With careful analysis of the optimised routings, we can determine that all three pivotal substations’ standby links do not overlap the active links, and they also avoid passing those communication lines coupled with the overloaded power lines (i.e. branch (S1–S2) and branch (S1–S5)). Such a configuration maximises the observation and controlling capacity of the control centre, thus helping to avoid unobservable and uncontrollable overload accidents. In addition, our optimised communication scheme also minimises the routing hops as well as separates the up and down links, thus reducing the outage probability and balancing the communication load.

3.4.2 Consider extreme weather conditions: Power systems may be faced with different operation risks, extreme weather, for example. Therefore, system operators need to forecast the possible risks and pointedly carry out corresponding communication configuration schemes. In this case study, we compare two standby routing schemes optimised under two different risk scenarios.

The power system we choose is again the IEEE 14-bus system, whose parameters and outage probabilities are set to the same as in the former case. Consider the following two extreme weather scenarios:

i. A tornado hits at the location of substation 2, and the break-line probabilities for those related power lines are increased to 30%.

ii. A tornado hits the bottom-half area, and the break-line probabilities for power lines (S9–S5), (S6–S10) and (S7–S8) are increased to 30%.

The impacts of two extreme weather scenarios are labelled in the left sub-graph in Fig. 7, and the comparison between their standby communication routings are shown in the right. In Fig. 7, symbols * and # refer to the uploaded measurements and issued control signals; the red and blue lines refer to vulnerable and normal communication lines; and the dotted lines represent existing unused communication lines. The thickness of the lines represents the occupation rates.

In scenario 1, the tornado attacks a heavy-load area, and the control centre is highly capable of regulating substations S1 and S5’s generation outputs. Therefore, in our optimised routing scheme, most of the EMS’s communication is carried by the communication lines in the bottom half, among which communication line (S4–S5), with comparatively fewer routing hops, carries the most. Although the links are not the shortest, such a routing scheme could guarantee the reliability of the closed-loop control for the entire power grid.

As for scenario 2, all vulnerable power lines are light loaded. In other words, their break-line faults do not affect the power flow distribution much. Therefore, under the reliable-communication premise, our proposed optimisation mechanism carries out a communication scheme with minimum routing hops and a balanced information distribution. As the network’s communication lines are more vulnerable than the rest, because of their high cyber-physical break-line possibilities, most communication is carried by the upper-half network. In our standby scheme, the upper-half substations’ routings satisfy mutual-exclusion and shortest-path principles, while the bottom-half substations’ routings maximally avoid those vulnerable communication lines.

Accordingly, these substations should be the pivotal substations for this operation scenario. After optimisation for the standby communication routings, a comparison between three pivotal substations’ active and standby links to the control centre is presented in the right sub-graph in Fig. 6.
3.4.3 Consider regional failure of the power system: Power systems may also be faced with regional failure accidents caused by extreme weather. Such failures do not only affect the system’s energy flow distribution, but also change the topology and the connectivity of both the power and communication networks, which may even block other substations’ communication to the control centre. In this case, we utilise the IEEE-39 bus power system as an example to illustrate the efficiency of our optimisation mechanism against such failures.

The power network and its corresponding EMS communication network are presented in Fig. 8. According to the graph, substations S1, S11 and S17 are directly connected with the control centre (see stars in three colours). The active communication routings generated by the shortest path algorithm are presented in Fig. 8b, in which the green, blue and yellow circles refer to a substation being linked to the control centre via S1, S11 and S17, respectively, and the coloured arrows/lines illustrate the general communication routings from the substations to the control centre.

Consider the scenario that substations S18 and S17 are highly likely to quit operation (the vulnerable substations and power lines are labelled by red stars). The optimised standby communication scheme is shown in Figs. 8c and d. The two sub-graphs,
respective ly, show two separate groups of substations whose communication routings pass S1 and S11, and these two substation groups are marked by green and blue circles/dotted lines, respectively. The occupied communication lines for each group are labelled by their corresponding colour, e.g. green and blue. With careful comparison between the active (Fig. 8b) and standby (Figs. 8c and d) routings, we can determine that the labelled colours for any substation are different. In other words, all substations’ active and standby routings connect to the control centre via different substations among S1, S11 and S17, reflecting the mutual exclusivity of the two schemes.

In addition, in this scenario, power transmission lines (S14–S15), (S16–S24), (S23–S24) and (S21–S22) are most vulnerable to overloading (see the bold red lines in Fig. 8a). Based on the information-energy flow analysis theory discussed in [1], we can estimate that substations S16, S19–S24 and S33–S35 are most important for PFCC decisions against the assumed risk; these are labelled in purple round frames in Figs. 8b–d. In the shortest-path-based primary communication scheme, these pivotal substations communicate with the control centre via vulnerable substation S17 and communication lines (S16–S17) and (S16–S21), which may easily be affected by extreme weather. To avoid such negative effects, the optimised standby routings for these substations avoid those vulnerable substations or communication lines and link to the control centre via substation S11 instead. Indeed, in Figs. 8c and d, it is clear that no substation communicates with the control centre via high-risk substation S17. Admittedly, from the perspective of communication, some substations’ standby routings via S1 or S11 are not as efficient as via S17, for example, S3 and S14, but the sacrifice in communication time and routing hops is intended to lower the operation risk of EMS. Therefore, even though the arrows in Figs. 8c and d are markedly longer than the arrows in Fig. 8b, our ‘detoured’ standby routing scheme successfully avoids those vulnerable substations and communication lines, thus guaranteeing the reliability of communication.

### 3.5 Brief summary for simulation results

After analysing the optimised communication plans for the proposed three scenarios, we have noticed that our routing configuration mechanism possess following four characteristics:

i. avoiding overlapping with the active routings;

ii. avoiding passing the channels with high break-line risks;

iii. avoiding passing the channels coupled with heavy-loaded power transmission lines;

iv. reducing the routing hops and balancing the communication load.

Notably, routing hops and communication balance are the last things we think of in our optimisation. However, these two factors are often primary consideration for communication configuration [15]. To better compare two optimisation mechanisms, we select the most vulnerable scenarios, i.e. scenarios in Subsection 3.4.2 (1) and Subsection 3.4.3 to perform optimisation using both methods. The results are proposed in Table 1. According to the results, shortest-routing optimisation could achieve less router hops. However, the configuration plan computed with our mechanism could ensure the minimum expectations of both the over-loaded-line quantities and overloading amount, which can also be dynamically adjusted according to cyber-physical risk scenarios. Such comparison indicates that even though our method may not be optimal from the perspective of communication networks, it can better support the safe and reliable operation of EMS and power systems than traditional communication optimisation mechanisms.

### 4 Conclusion

To better support the safe operation of power systems, we have discussed the optimisation mechanism for current EMSs’ communication routings. Different from traditional network planning and configuration methods, the goal of our approach is to minimise the impact of communication risks on power system operation. Referring to current ‘active + standby’ configuration convention, we have proposed a dynamic optimisation model for EMSs’ standby communication routings to adapt to changing operation environments and risk scenarios, which guarantees that the most important information can be transmitted by the most reliable channels.

The optimisation model is determined by two main factors: information significance, which can be described as cyber-physical sensitivity index, and communication reliability, which can be represented by the seriousness of a communication break-line risk’s impact on EMS’s communication. For the latter factor, we introduce a path-branch incidence matrix to describe the routing scheme, in which each row vector corresponds to the information blocked by a communication line’s interruption. With such a definition, the mechanism by which a communication outage affects information transmission can be quantitatively expressed using vectors’ multiplications.

To illustrate the concepts and methods, we have utilised our proposed mechanisms studying a typical closed-loop control application –PFCC under three different scenarios, and the results verify the effectiveness of our approach. All three case studies indicate that the optimised standby routings do not overlap with the active routings, and avoid passing those channels with high break-line risks or coupling with heavy-loaded power transmission lines. Even though the optimised scheme may not be optimal from the perspective of communication networks, it can better support the safe and reliable operation of power systems. As future SDN-based EMSs will allow network administrators to programmatically control communication network behaviour dynamically via open interfaces, such optimisation mechanisms have great application potential.

### 5 Acknowledgment

This work was supported by National Key R&S Program of China under grant no. 2017YFB0903000.

### 6 References

[1] Xin, S., Guo, Q., Wang, J., et al.: ‘Information masking theory for data protection in future cloud-based energy management’, IEEE Trans. Smart Grid, 2017, doi: 10.1109/TSG.2017.2693345, in press

[2] He, H., Yan, J.: ‘Cyber-physical attacks and defences in the smart grid: a survey’, IET Cyber-Phys. Syst. Theory Appl., 2016, 1, (1), pp. 13–27

[3] Wu, D., Ma, F., Javadi, M., et al.: ‘Fast screening severe cyber attacks via transient energy-based impact analysis’, CSEE J. Power Energy Syst., 2016, 2, (5), pp. 28–34

[4] Shi, X., Li, Y., Cao, Y., et al.: ‘Cyber-physical electrical energy systems: challenges and issues’, CSEE J. Power Energy Syst., 2015, 1, (2), pp. 36–42

[5] Xin, S., Guo, Q., Sun, H., et al.: ‘Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems’, IEEE Trans. Smart Grid, 2015, 6, (5), pp. 2375–2385

[6] Xin, S., Guo, Q., Sun, H., et al.: ‘Energy-information flow computation and cyber-physical sensitivity analysis for power systems’, IEEE J. Emerg. Sel. Top. Circuits Syst., 2017, 7, (2), pp. 329–341

[7] Qi, J., Hahn, A., Liu, X., et al.: ‘Cybersecurity for distributed energy resources and smart inverters’, IET Cyber-Phys. Syst. Theory Appl., 2016, 1, (3), pp. 28–39

[8] Hadjiaidu, N., Tranchita, C., Roxel, B., et al.: ‘Modeling cyber and physical interdependencies – application in ICT and power grids’. IEEE/PES Power Systems Conf. Exposition, PSCE, Seattle, WA, USA, March 2009, pp. 1–6.
Lei, H., Singh, C., Sprintson, A.: ‘Reliability modeling and analysis of IEC 61850 based substation protection systems’, IEEE Trans. Smart Grid, 2014, 5 (5), pp. 1–9

Li, H., Essey, A.T., Zhang, J., et al.: ‘Optimal energy management for industrial microgrids with high-penetration renewables’, Prot. Control Mod. Power Syst., 2017, 2 (12), pp. 1–14

Liu, R., Vellaiathurai, C., Buswas, S.: ‘Analyzing the cyber-physical impact of cyber events on the power grid’, IEEE Trans. Smart Grid, 2015, 6 (5), pp. 2444–2453

Kanemaru, K., Ooura, K., Ibuki, S., et al.: ‘Application of a power line maintenance information system using OPGW to the Nishi-Gunma UHV line’, IEEE Trans. Power Deliv., 1995, 10 (1), pp. 511–517

Yates, D., Luna, B.Q., Rasmussen, R., et al.: ‘Stormy weather: assessing climate change hazards to electric power infrastructure: a sandy case study’, IEEE Power Energy Mag., 2014, 12 (5), pp. 66–75

Li, H., Treinish, L.A., Hosking, J.R.M.: ‘A statistical model for risk management of electric outage forecasts’, IBM J. Res. Dev., 2010, 54 (3), pp. 8:1–8:11

Ling, T.: ‘Optimal allocation of channels in an alternate route’, IEEE Trans. Commun., 1964, 12 (2), pp. 185–191

Hassan, N.U.L., Assaad, M.: ‘Dynamic resource allocation in multi-service OFDMA systems with dynamic queue control’, IEEE Trans. Commun., 2011, 59 (6), pp. 1664–1674

Chen, J., Lau, V.K.N.: ‘Delay analysis of max-weight queue algorithm for time-varying wireless ad hoc networks-control theoretical approach’, IEEE Trans. Signal Process., 2013, 61 (1), pp. 99–108

Wu, J., To, C., Lau, F.: ‘Optimizing performance of communication networks: an application of network science’, IEEE Trans. Circuits Syst. Express Briefs, 2014, 62 (1), pp. 95–99

Simmhan, Y., Kumbhare, A.G., Cao, B., et al.: ‘An analysis of security and privacy issues in smart grid software architectures on clouds’, Proc. 2011 IEEE 4th Int. Conf. Cloud Computing, CLOUD, Washington, DC, USA, July 2011, pp. 582–589

Fu, Y., Bi, J., Chen, Z., et al.: ‘A hybrid hierarchical control plane for flow-based large-scale software-defined networks’, IEEE Trans. Netw. Serv. Manag., 2015, 12 (2), pp. 117–131

Steinhauer, F.: ‘Propagation and interaction of ethernet packets with ieee 61850 sampled values in power utility communication networks’. 12th IET Int. Conf. Developments in Power System Protection, Copenhagen, Denmark, April 2014, pp. 1–4

Gelenbe, E., Liu, P., Lainé, J.: ‘Genetic algorithms for route discovery’, IEEE Trans. Syst. Man Cybern. B Cybern., 2006, 36 (6), pp. 1247–1254

Al-faiz, M.Z., Sabry, S.S.: ‘Optimal linear quadratic controller based on genetic algorithm for TCP/AQM router’. Int. Conf. Future Communication Networks, Baghdad, Iraq, April, 2012, pp. 78–83

Di Fatta, G., Hoffmann, F., Re, G.L., et al.: ‘A genetic algorithm for the design of a fuzzy controller for active queue management’, IEEE Trans. Syst. Man Cybern. C Appl. Rev., 2003, 33 (3), pp. 313–324

Roald, L., Misra, S., Krause, T., et al.: ‘Corrective control to handle forecast uncertainty: a chance constrained optimal power flow’, IEEE Trans. Power Syst., 2017, 32 (2), pp. 1626–1637

Zhang, W., Xu, Y., Dong, Z., et al.: ‘Robust security-constrained optimal power flow using multiple microgrids for corrective control under uncertainty’, IEEE Trans. Ind. Inform., 2016, 3203 (3), pp. 1–1

Tang, Y., Li, F., Wang, Q., et al.: ‘Quantitative evaluation of communication system fault effect on real-time load control of power system’, Electr. Power Autom. Equip., 2017, 37 (2), pp. 90–96