A fault-tolerance control method of load frequency based on reverse behavior reconstruction

Fei Xue\(^1\)*, Hanhua Zhang\(^2\), Shuang Zhang\(^3\), Lei Zhou\(^4\), Ting Yang\(^5\), Hao Li\(^6\)

\(^1\)Electric Power Research Institute of State Grid Ningxia Electric Power Co., LTD Yinchuan, China
\(^2\)Electric Power Research Institute of State Grid Ningxia Electric Power Co., LTD Yinchuan, China
\(^3\)Electric Power Research Institute of State Grid Ningxia Electric Power Co., LTD Yinchuan, China
\(^4\)Electric Power Research Institute of State Grid Ningxia Electric Power Co., LTD Yinchuan, China
\(^5\)Tianjin University, The School of Electrical Engineering and Automation, Tianjin China
\(^6\)Tianjin University, The School of Electrical Engineering and Automation, Tianjin China

* Corresponding author: tjuxf1010@126.com

Abstract—The access of a high proportion of renewable energy and the large-scale application of open sharing communication network are the two main characteristics of modern interconnected power grid. However, the tight coupling between the cyber and physical subsystem makes the malicious network attack and sudden physical failure more likely to cause the collapse of the interconnected power grid. Therefore, a reverse behavior reconstruction strategy is proposed, which does not need to obtain a priori fault information and only depends on the input and output measurements of the system, so as to realize fault tolerance as much as possible. The simulation experiments show that the proposed strategy can achieve the frequency fault tolerance and has better practicability and applicability under complex and diverse fault conditions.

1. INTRODUCTION

In the interconnected power grid with a large number of the distributed generation, the stability between regions strongly depends on the normal operation of the cyber and power subsystem. For the physical subsystem, various faults occur in the power equipment, such as hydraulic leakage, blade fracture and other faults, causing an off-grid failure of renewable energy. For the cyber subsystem, false data injection, data packet loss and communication network delay can cause the control center make a wrong decision or the actuator cannot receive control commands in time. When the interconnected power grid has cyber and physical faults, the performance of traditional analysis and design methods...
will decline sharply or even fail to work normally. Therefore, it is necessary to design a new fault-tolerance control strategy to make the system run safely and stably when the corresponding fault occurs.

The existing research of active fault-tolerance control (AFTC) generally realizes fault identification by designing observers. For example, reference [1] designed a series of redundant observers and controllers for power real-time control systems with sensor faults, and selected the most matching observer and controller by defining the observed signal index. For the load frequency control (LFC) problem of interconnected power systems considering system parameter uncertainty, a distributed filtering strategy has been proposed in [2] to effectively estimate the system state. Reference [3] studies the design of multiarea LFC strategy considering cyber delay and aperiodic DoS attack.

However, the traditional observer based AFTC strategy relies too much on a priori fault information and accurate system parameters in the process of selecting the best matching controller. To solve the above problems, a reverse behavior reconstruction strategy that does not depend on a priori system parameters is proposed to realize rapid frequency fault-tolerance for cyber and physical faults. The remainder of this article is organized as follows. Section II introduces the fault library and preset controller library. Section III presents a reverse behavior reconfiguration method, which is verified by case studies in Section IV. Finally, Section V concludes the paper.

2. Fault library and preset controller library

2.1. Control Model

The controlled object model under normal conditions is given as:

\[
\begin{aligned}
\frac{d}{dt} x(t) &= Ax(t) + Bu(t) + H \omega(t) \\
y(t) &= Cx(t) + Du(t)
\end{aligned}
\]  

(1)

Where \(x, u, \omega\) and \(y\) indicate the state variables, input variables, external disturbance variables and output variables, respectively. Matrix \(A, B, H, C, D\) are proper dimensional matrix.

It is noteworthy that: the model is not limited to a certain scene or system object, but has better universal representation. Although the interconnected system is nonlinear, the linearization method at the equilibrium point can be used to linearize the system. The model error caused by this linearization process can be considered in the controller design process.

2.2. Fault library

As can be seen from Figure 1, due to the introduction of cyber subsystem, all kinds of uncertain factors (such as delay, packet loss and cyber attack) in the process of data transmission bring new security risks to real-time control systems in the interconnected power system. Although there are many fault types, they can be divided into three categories according to the impact of faults:
1) Data fault: This type of fault is mostly caused by the aging of sensors and actuators or malicious tampering of data. The measured electrical parameters seriously deviate from the real value. Under the data fault, the control parameters and measurement parameters meet the following relationship:

\[
\begin{align*}
\dot{u}_f(t) &= G^f G^c u(t) \\
\dot{y}_f(t) &= Y^f Y^p y(t)
\end{align*}
\]

(2)

Where subscript \( f \) indicates the fault state, \( I^p = \text{diag}(\gamma P 1, \gamma P 2, \ldots, \gamma P p) \) is the physical fault matrix of actuator. \( I^c = \text{diag}(\gamma C 1, \gamma C 2, \ldots, \gamma C p) \) refers to the cyber fault matrix between controller and actuator. \( \Psi^f = \text{diag}(\psi C 1, \psi C 2, \ldots, \psi C q) \) represent cyber fault matrix between sensor and controller. \( \Psi^p = \text{diag}(\psi P 1, \psi P 2, \ldots, \psi P q) \) indicates physical fault matrix of sensor. Take \( \gamma P i \) and \( \gamma C i \) for example, \( \gamma P i = 0 \) means actuator \( i \) fails completely, \( \gamma P i = 1 \) indicates actuator \( i \) works normally, \( \gamma P i \in (0, 1) \) represents actuator \( i \) has partial failure. \( \gamma C i = 1 \) indicates that the cyber transmission is normal, \( \gamma C i \in (\gamma_{\text{min}}, \gamma_{\text{max}}) \), \( \gamma C i \neq 1 \) indicates data tampering attack in cyber subsystem, \( \gamma_{\text{min}}, \gamma_{\text{max}} \in \mathbb{R} \) represents the ratio of the tampered value to the original real value.

2) Delay fault: Due to the transmission channel congestion or malicious cyber attack, the transmission delay of measurement data and control commands increases and then the data become uncertain or meaningless owing to the loss of its timeliness. Under the delay fault, there is no negligible delay in the control command or measurement data from the source node to the root node. Assume that \( \tau_c \) and \( \tau_a \) respectively indicate the data delay from the sensor to the control center and from the control center to the actuator. Under normal state and delay fault state, the control commands output by the controller are \( u'(t) \) and \( u(t) \) respectively, the system state variables received by the control center are \( y'(t) \) and \( y(t) \) respectively. The following relationship can be satisfied:

\[
\begin{align*}
\dot{u}(t) &= u'(t + \tau_a) \\
\dot{y}(t) &= y(t + \tau_a)
\end{align*}
\]

(3)

Further, Padé approximation technology is used to approximate the above pure time-delay links. For details, please refer to [4].

3) Component fault: The original structure and operation mode will be fundamentally changed by the internal component fault. The abnormality of state space description, that is:

\[
\begin{align*}
\dot{x}(t) &= A' x(t) + B' u(t) + H' \phi(t) \\
y(t) &= C' x(t) + D' u(t)
\end{align*}
\]

(4)

Where A', B', H', C', D' represent the controlled system matrix after the component fault occurs.

2.3 Hybrid fault system modeling

Based on the mathematical modeling of three types of faults, assuming the augmented vector \( X=[x, x_{ca}, x_a]^T \), \( x_{ca}(t) \) and \( x_a(t) \) are the intermediate variables introduced by Padé approximation. The state equation of real-time control system of interconnected power grid considering cyber and physical hybrid faults is established as:

\[
\begin{align*}
\dot{x}(t) &= A' x(t) + B' u(t) + H' \phi(t) \\
y(t) &= C' x(t) + D' u(t)
\end{align*}
\]

(5)

Where \( A = A' \), \( B = B' T' I^c \), \( H = H' \), \( C = \Psi^c \Psi^p C' \), \( D = \Psi^c \Psi^p D' T' I^c \).

2.4 Preset controller Library

Obviously, the real-time control system described in (5) has model uncertainty: 1) the linearization modeling of controlled system will produce errors. 2) the actual operating parameters of the controlled system deviate from the nominal value. 3) Padé approximation of network delay will also bring errors. Therefore, the controller design must be robust to model uncertainty. Based on the hybrid \( H_0/H_n \)
method proposed in [5], this paper designs the basic controller to realize the robust control. Due to the space limitation of the article, the design process of $H_2/H_\infty$ method is not described in detail here.

Considering that the controlled system has $M$ normal working scenarios and $N$ typical fault scenarios, the number of controllers in the basic library is $M+N$, assuming that $\Sigma_\mu=\{\Sigma_1, \Sigma_2, \ldots, \Sigma_M(M+N)\}$ represents the set of controllers designed for specific operation scenarios, which has the following general form:

$$
\Sigma_{\mu}j: \begin{cases} 
\frac{d}{dr}x_{\mu j}(t)=A_{\mu j}x_{\mu j}(t)+B_{\mu j}(r(t)-y'(t)) \\
u'(t)=C_{\mu j}x_{\mu j}(t)+D_{\mu j}(r(t)-y'(t)) 
\end{cases} (6)
$$

Where $j=1, 2, \ldots, M+N$, $x_{\mu j}(t)$ indicates the intermediate variable introduced into the controller, $A_{\mu j}, B_{\mu j}, C_{\mu j}, D_{\mu j}$ are the controller system matrices.

2.5 Dynamic behavior modeling

The controlled system (5) and controller (6) are essentially linear differential equations with constant coefficients. The intersection of their solution sets restricts the value space of the dynamic behavior of the closed-loop system. Therefore, the signal vector is defined as $s(t)=[s(t), r(t), y(t), u'(t)]^T$, the dynamic behavior of the controlled system and the controller can be described as:

Controlled system:

$$
B_{p}=[s=(r, y', u')^T][N_{p1}(\xi) 0 D_p(\xi) -N_p(\xi)]s(t)=0
$$

Controller:

$$
B_{\mu}=[s=(r, y', u')^T][0 N_{\mu}(\xi) -N_{\mu}(\xi) D_{\mu}(\xi)]s(t)=0
$$

Where $\xi=\frac{d}{dt}$, $N_{p1}(\xi), N_{p2}(\xi), D_p(\xi), N_{\mu}(\xi), D_{\mu}(\xi)$ are proper dimensional polynomial matrix and can be strictly proved in [6]:

1) $\{N_{p1}(\xi), N_{p2}(\xi), D_p(\xi), N_{\mu}(\xi), D_{\mu}(\xi)\}$ are mutually prime and all revertible polynomial matrices; 
2) $D-1 p(\xi)N_{p1}(\xi), D-1 p(\xi)N_{p2}(\xi)$, and $D-1 c(\xi)N_{\mu}(\xi)$ are true rational polynomial matrices.

According to (7) and (8), the controlled system and the controller are interconnected through common variables $[r(t), y(t), u'(t)]^T$. In addition, the preset controllers meet the $H_2/H_\infty$ performance, that is, through the design of the controller $\Sigma_c$, the external disturbance $\omega(t)$ of the controlled system can always attenuate within the design requirements.

3. REVERSE BEHAVIOR RECONFIGURATION

3.1 Reverse reconstruction module

The core of the AFTC method is to put the best-matched controller into the controller loop. However, the traditional fault identification method requires accurate prior system parameters and a large number of state parameters, and there is a risk of mismatch between the controller and the controlled system, resulting in fault-tolerance failure.

Therefore, a AFTC strategy that does not rely on fault identification is proposed in the paper. As shown in Figure 2, the core is to use only the output $y(t)$ of the controlled system, the control command $u'(t)$ and the existing controller library $\Sigma_c$ to reversely reconstruct the dynamic behavior of the closed-loop system in a parallel mode, which is recorded as $\{\hat{B}_1, \hat{B}_2, \ldots, \hat{B}_{M+N}\}$. By calculating the dynamic performance index between $\{\hat{B}_j\} (j=1, 2, \ldots, M+N)$, the controller with the best index result is selected to put into the control loop, so as to realize accurate switching. Therefore, the proposed AFTC strategy consists of the following three parts: 1) dynamic behavior reverse reconstruction module; 2) performance index calculation module; 3) controller switching module.
Based on the analysis in Section II, the dynamic behavior of the controller $\Sigma_{ij}$ can be completely reconstructed only through $y'(t)$ and $u'(t)$, without accurate priori system operating parameters and fault information. The dynamic behavior of the reconstructed controller is satisfied:

$$\hat{r}_j(t) = N_{ij}^{-1}(\xi)D_{ij}(\xi)u'(t) + y(t),\; t \in [(m-1)T_s, mT_s)$$

(9)

Where $\hat{r}_j(t)$ is the reconstruction reference input of $\Sigma_{ij}$.

3.2. Performance index calculation module

The function of this module is to calculate the performance index of the dynamic behavior of the parallel reconstructed controller in any detection cycle $[(m-1)T_s, mT_s)$. The goal of control system is that the output $y'(t)$ can track the reference input $r(t)$ in real time, so this paper considers the $MSE$ (Mean Square Error) index of the error between the reconstructed reference input $\hat{r}_j(t)$ and the output $y'(t)$ as a performance index, that is:

$$MSE = \frac{1}{T_s} \int_{mT_s}^{(m+1)T_s} (\hat{r}_j(t) - y'(t))^2 \, dt$$

(10)

This index can accurately represent the control error of different controllers in the case of information uncertainty.

3.3. Controller switching module

The function of the controller selection module is to select the most matching controller in the next time interval according to the calculated performance index $MSE$, and the number value of the selected controller can be expressed as:

$$\sigma(t) = \arg\min\{MSE_i(t), t \in [mT_s, (m+1)T_s]\}$$

(11)

4. SIMULATION ANALYSIS

This paper takes the three-area interconnected power system as the research object for simulation experiments. Table 1 shows the seven possible cases of the three-area interconnected system. This paper uses comparison method to verify: the passive fault-tolerance control (PFTC) strategy considering the progressive stability of all fault cases proposed in [7] and the active fault-tolerant control strategy based on fault identification (fault identification AFTC) proposed in [3].

| Case | Instruction                                                                 |
|------|-----------------------------------------------------------------------------|
| 1    | Area 1, Area 2, Area 3 operate normally                                     |
| 2    | Area 1 has data faults, Area 2, Area 3 operate normally                    |
| 3    | Area 2 has delay faults, Area 1, Area 3 operate normally                   |
| 4    | Area 3 has component faults, Area 1, 2 operate normally                    |
| 5    | Area 1, 2 has data and delay faults, Area 3 operate normally               |
| 6    | Area 1, 3 has data and component faults, Area 2 operate normally           |
| 7    | Area 2, 3 has data and component faults, Area 1 operate normally           |
| 8    | Area 1, 2 and 3 has data, delay and component faults                       |

TABLE 1. THE SCENARIOS OF OPERATING
According to Figure 3, when the PFTC strategy is adopted, the mean square error (MSE) of $\Delta f_1$ and $\Delta P_{tie1}$ is generally greater than that of AFTC, and only slightly better than the AFTC strategy in cases 2 and 6 (the MSE of $\Delta f_1$ and $\Delta P_{tie1}$ in other cases is at least high 18.40% and 220%). The performance index of the proposed AFTC strategy is roughly similar to that of the fault identification-AFTC strategy in terms of control performance, but because the proposed scheme only relies on the input and output parameters of the controlled system when selecting the best-matching controller. It does not need to rely on accurate prior knowledge of system parameters, and can achieve similar fault tolerance effects, so it is more practical.

![Figure 3. MSE of $\Delta f_1$ and $\Delta P_{tie1}$ in each fault case](image)

5. CONCLUSION
In view of the risk that the interconnected power system is vulnerable to malicious cyber attacks and sudden physical failures, this paper proposes a reverse behavior reconstruction method. It only depends on the input and output measurements of the system, which effectively overcomes the limitation that the traditional AFTC method based on parameter identification must rely on priori system parameters. Future research will focus on further improving the controller expansion mechanism to achieve complete fault tolerance to unknown faults.

ACKNOWLEDGMENT
Financial support should be acknowledged here. This work was supported by the Key Research and Development Program of Ningxia Hui Autonomous Region (2021BDE931017) and the Science and technology project of State Grid Ningxia Electric Power Co., Ltd (5229DK20005F).

REFERENCES
[1] Khosravani Saeid, Moghaddam Iman Naziri, Afshar Ahmad, Karrari Mahdi, “Wide-area measurement-based fault tolerant control of power system during sensor failure,” in Electrical Power Systems Research, vol. 137, pp. 66-75, 2016.
[2] Hu Zhijian, Liu Shichao, Yang Liu, Wu Ligang. “Distributed fuzzy filtering for load frequency control of non-linear interconnected power systems under cyber-physical attacks,” in IET Control Theory and Applications, vol. 14, pp. 527-538, 2020.

[3] Cheng Zihao, Yue Dong, Hu Ssonglin, Xie Xiangpeng, Huang Chongxin, “Detection-based weighted H\(_\infty\) LFC for multi-area power systems under DoS attacks,” in IET Control Theory and Applications, vol. 13, pp. 1909-1919, 2019.

[4] Zheng Chengde, Zhang Huaguang, Tian Hong. “Generalized homogeneous multivariate matrix Pade-type approximants and Pade approximants,” in IEEE Transactions on Automatic Control, vol. 52, pp. 2160-2165, 2007.

[5] Khosrowjerdi MJ, Nikoukhah R, Sarari-Shad N. “A mixed H\(_2\)/H\(_\infty\) approach to simultaneous fault detection and control,” in Automatica, vol. 40, pp. 261-267, 2004.

[6] T Jain, J Yame, D Sauter. “Active fault-tolerant control systems: a behavioral system theoretic perspective,” in Berlin: Springer Press, pp. 15-18, 2018.

[7] Sevillal F, Jaimoukha I, Chaudhuri B, et al. “Fault-tolerant control design to enhance damping of inter-area oscillations in power grids,” in International Journal of Robust and Nonlinear Control, vol. 24, pp. 1304-1316, 2013.