Quantifying Resilience of Wide-Area Damping Control Against Cyber Attack Based on Switching System Theory

Yifan Zhao, *Graduate Student Member, IEEE*, Wei Yao, *Senior Member, IEEE*, Chuan-Ke Zhang, *Senior Member, IEEE*, Xing-Chen Shangguan, *Graduate Student Member, IEEE*, Lin Jiang, *Member, IEEE*, and Jinyu Wen, *Member, IEEE*

***Abstract*—Since the cyber attack on the communication network will deteriorate the performance of wide-area damping controllers (WADCs) or even cause instability, many resilient WADCs are developed to mitigate the adverse influence of cyber attacks recently. However, there is a lack of quantitative indexes to guide the controller design in order to achieve the trade-off between attack resilience and damping performance. To address this problem, an index is proposed to quantify the strongest attack that the power system with a given WADC can tolerate, which is called as resilience margin. Firstly, the power system with a WADC subjected to cyber attack is modeled as a switching system consisting of stable and unstable subsystems. Then, based on switching system theory, the definition of resilience margin is presented. To calculate the resilience margin, the Lyapunov stability analysis is implemented on the switching power system to derive a practical calculation algorithm, which combines the bisection method and the linear matrix inequalities (LMIs) technology. The case study on the 16-machine 68-bus system with a voltage source converter based high voltage direct current system is performed. Simulation results demonstrate the effectiveness of the calculation algorithm and the significance of the resilience margin in the design of WADC.**

***Index Terms*—Wide-area damping control, cyber attack, switching system, resilience margin, maximum acceptable attack frequency.**

I. Introduction

With the increasing integration of renewable energy and the wide use of power electronic equipment, the problem of inter-area low-frequency oscillations in a large-scale power system is becoming more and more prominent [1]. Compared with the local power system stabilizers (LPSS), wide-area damping controller (WADC)/wide-area PSS plays an important role in addressing this problem due to the fact that its input is the remote signals with high observability on inter-area modes [2]. Meanwhile, the rapid development of information and communication technology (ICT) and wide-area measurements system (WAMS) enable WADCs to obtain remote signals via the wide-area communication network [3].

Nevertheless, the open communication network is not immune to cyber attacks [4]. The blackouts caused by cyber attacks in Ukraine and Venezuela proved that cyber incidents could have severe consequences on the grid operation. Reports from the government [5], [6] and many studies [7], [8] have indicated that WAMS is at high risk of being attacked since it consists of enormous sensors and communication networks involving complex information exchange and transmission. Once the remote signals are corrupted by cyber attacks, the performance of WADC will be seriously weakened, or the whole system may lose stability [9]–[11]. Consequently, the researches that analyze and defend the cyber attack on WADC have attracted wide attention.

To handle the impact of cyber attack on WADC, many works have been done. One of the most effective methods is to establish an attack-resilient system (ARS), which consists of an attack detection mechanism and an attack-resilient controller [12], [13]. The main idea of this system is to set a data preprocessor to detect if data packets are corrupted by cyber attacks before they enter the controller. Once a cyber attack occurs, the alarm sent by the attack detection mechanism will guide the resilient controller to mitigate the influence of the attack. Lots of algorithms based on machine learning [12], [13], spoof-catching [14] or Kirchhoff's law [15] have been developed to detect denial of service (DoS) attack [16] and deception attack (including false data injection attack (FDIA) and replay attack) [12], [13], [17]–[22]. However, the researches about the design of attack-resilient controller are inadequate compared with those about attack detection because it is difficult to judge how reliable a given-WADC can be in the face of cyber attacks. Designers of the resilient WADCs are often caught between attack resilience and damping performance. Consequently, an index to quantify attack resilience is needed to help the designers achieve the trade-off between attack resilience and damping performance. Unfortunately, related studies are still very few.

Manuscript received August 14, 2021; revised November 30, 2021; accepted January 22, 2022. Date of publication January 26, 2022; date of current version April 22, 2022. This work was supported by the National Natural Science Foundation of China under Grant 52022035. Paper no. TSG-01301-2021. *(Corresponding author: Wei Yao.)*

Yifan Zhao, Wei Yao, and Jinyu Wen are with the State Key Laboratory of Advanced Electromagnetic Engineering and Technology, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: yf_zhao2181@hust.edu.cn; w.yao@hust.edu.cn; jinyu.wen@hust.edu.cn).

Chuan-Ke Zhang and Xing-Chen Shangguan are with the School of Automation, China University of Geosciences, Wuhan 430074, China (e-mail: ckzhang@cug.edu.cn; star@cug.edu.cn).

Lin Jiang is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool L69 3GJ, U.K. (e-mail: ljiang@liverpool.ac.uk).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2022.3146375.

Digital Object Identifier 10.1109/TSG.2022.3146375

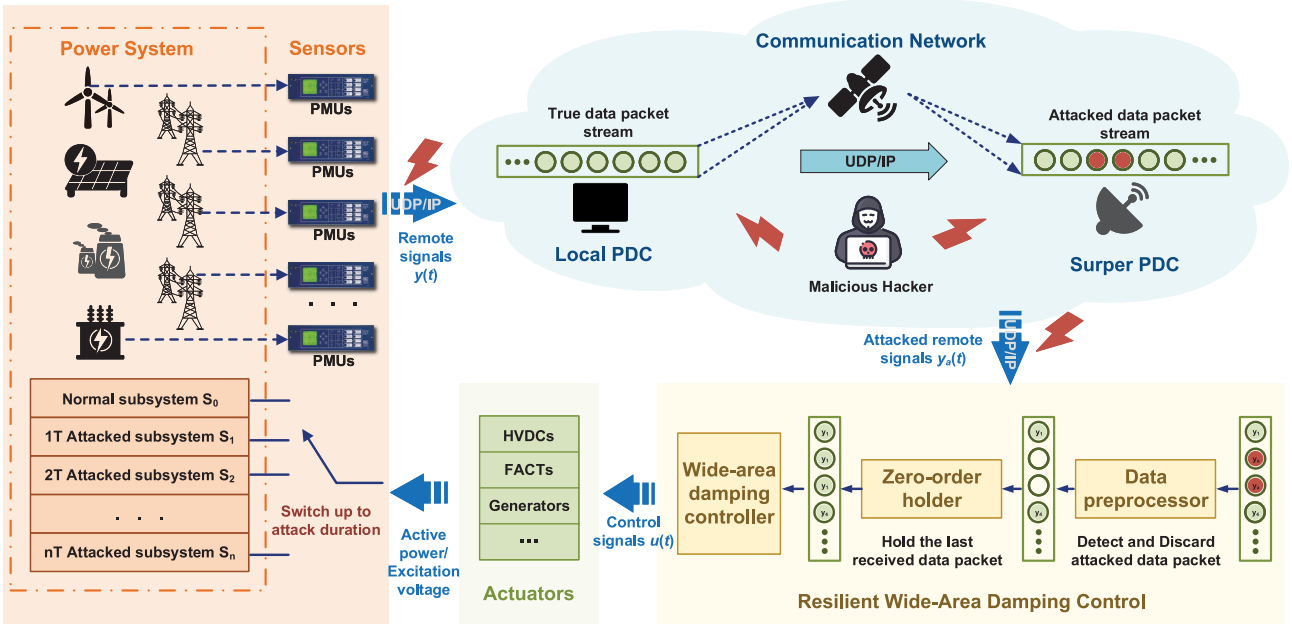


Fig. 1. Structure of resilient wide-area damping control subjected to cyber attack.

References [23] and [24] have made some attempts to quantify resilience/attack. In [23], the impact of the DoS attack is modeled as the Hadamard product of the gain matrix, and the $\mathcal{H}_2$ norm of the post-attack closed-loop system is unitized to represent the resilience index. Similarly, an uncertain attack matrix Δ is multiplied to the gain matrix to describe cyber attacks in [24], whose influence is that the eigenvalues of the closed-loop system may be removed to the right-half plane. The resilience index is defined as the distance that an attack Δ can make. Nevertheless, the above two indexes can only reflect how powerful a cyber attack is likely to turn a system into an unstable one instead of the system will lose stability. A cyber attack always lasts for only a short time (the detailed explanation is presented in Remark 1), which means that the system will turn back into a stable system when the attack disappears or is cleared. Then the system may stay stable eventually. The switching system theory provides a different view to address this problem [25]–[27]. The whole system can be modeled as a hybrid system made up of a stable subsystem (normal system) and some unstable subsystems (attacked systems), which can stay stable with an approximate switching sequence. By analyzing the relationship between the switching signals and the stability of the system, a new index can be obtained.

Motivated by the above discussions, this paper models the power system with WADC as a closed-loop switching system and employs Lyapunov stability analysis for the switching system such that a novel quantitative index called resilience margin and corresponding calculation algorithm is proposed to guide the design of WADC. Especially, the main contributions of this paper can be summarized as follows:

- The power system with WADC considering cyber attacks with different durations is modeled as different subsystems, including a normal subsystem and some attacked subsystems. Then a closed-loop switching power system is established by connecting adjacent subsystems.
- Based on the switching system theory, a novel quantitative index called resilience margin is proposed. Moreover, the Lyapunov stability analysis is performed on the established switching power system to derive an algorithm for calculating the resilience margin combining the bisection method and the linear matrix inequalities (LMIs) technology.
- To demonstrate the effectiveness of the calculation algorithm and the significance of the resilience margin in designing WADC, the case study is carried out on a 16-machine 68-bus power system with a voltage source converter based high voltage direct current system (VSC-HVDC). Simulation results reveal the trend of the resilience margin with the gain of lead-leg WADC, attack duration, and operating condition. These conclusions guide the selection of the optimal gain so that attack resilience and damping performance can be balanced.

The remainder of this paper is organized as follows. Section II establishes the closed-loop switching power system with WADC considering cyber attacks. The definition and calculation algorithm of resilience margin are presented in Section III. In Section IV, case study of 16-machine 68-bus power system with VSC-HVDC is performed to demonstrate the effectiveness of the calculation algorithm and the significance of resilience margin. Section V concludes the paper.

II. Modeling of Power System With WADC Based on Switching System Theory Considering Cyber Attacks

The structure of the power system with WADC is illustrated in Fig. 1, where the dynamics of the nonlinear power system is typically described as a set of differential-algebraic equations (DAEs) [28]. To facilitate the analysis of low-frequency

oscillations, the DAEs are linearized around an equilibrium point, and a balanced model order reduction method based on normalized coprime factors [29] is performed for improving efficiency [23], [30], [31]. Then, a networked-reduced linearized power system model is obtained as follows:

$$\begin{cases} \dot{\bar{\boldsymbol{x}}}(t) = \bar{\boldsymbol{A}}\bar{\boldsymbol{x}}(t) + \bar{\boldsymbol{B}}\bar{\boldsymbol{u}}(t) \\ \bar{\boldsymbol{y}}(t) = \bar{\boldsymbol{C}}\bar{\boldsymbol{x}}(t) \end{cases} \tag{1}$$

where $\bar{\boldsymbol{x}}(t)$, $\bar{\boldsymbol{u}}(t)$, $\bar{\boldsymbol{y}}(t)$ are the state vector, the control vector and the output vector. $\bar{\boldsymbol{A}}$, $\bar{\boldsymbol{B}}$ and $\bar{\boldsymbol{C}}$ are the reduced state-space matrices. Specially, the output vector $\bar{\boldsymbol{y}}(t)$ refers to the remote signals while the control vector $\bar{\boldsymbol{u}}(t)$ refers to the control signals generated by WADC, which can be selected using modal controllability/observability approaches [2], [32] to obtain the best performance for damping the unstable and/or poorly damped modes.

As shown in Fig. 1, the WADC is installed with the actuators and implemented over the WAMS, consisting of phasor measurement units (PMUs), phasor data concentrators (PDCs), and communication channels. The remote signals $y(t)$ are firstly sampled by sensors (PMUs) at a fixed frequency and then transmitted to the local PDCs and super PDCs in turn. The communication between them can be via any communication medium and protocol. Here, fiber optics is adopted to ensure the feedback control as real-time as possible. And the User Datagram Protocol/Internet Protocol (UDP/IP) is used, during which the data is transmitted in the form of data packets one by one. Due to cyber attacks, the final data packet, denoted by $y_a(t)$, may be different from the original one or even cannot arrive at the WADC. Therefore, a zero-order holder (ZOH) is implemented before the WADC to hold the last received packet until the newer one comes. The WADC generates control-commands and then delivers them to the actuators, referring to the flexible AC transmission systems (FACTs) [31], the HVDCs [33], or the generators [2] in general.

A. Influence of Cyber Attack on WADC

For a WADC, a good damping performance can only be achieved under the promise of security objectives, including confidentiality, integrity, authenticity, and availability. However, these objectives cannot be ensured once the attack occurs. For example, to launch a deception attack or a DoS attack, the hackers must hijack the communication networks via GPS spoofing or other means, a breach of confidentiality. In more detail, the deception attack will replace the original data packet with the false one that has been designed carefully. Then the communication will no longer be integrated and authoritative. The perpetrators of the DoS attack seek to deplete network resources to block the communication. In this paper, we pay particular interest in these two kinds of attacks and try to analyze them in a unified way from the view of WADC. To this end, Assumption 1 is presented as follows:

Assumption 1: Effective attack detection mechanism has been adopted before the controllers. Once the false data resulting from the deception attack is detected, the whole data packet will be discarded. Then the ZOH will hold the last received signal. Consequently, the influences of the deception attack and DoS attack are the same from the view of the controllers.

Why the above assumption is reasonable is explained as follows. Many references have been published recently to address the problem of detecting attacks, as it says in the Introduction. The dynamic watermarking-based defense approach proposed in [34] can ensure confidentiality. The attacks that affect the data integrity can be detected with the machine learning method developed in [12]. In our recent work [20], an information technology security system including data encryption and data decryption is also developed aiming at detecting the deception attack. Therefore, it is feasible to implement an effective and practical attack-detection mechanism. Apart from the deception attack and the DoS attack, other types of attack can also be incorporated into the proposed analysis method as long as they can be detected by the existing means.

According to Assumption 1, whatever value the data itself is tampered with by cyber attacks, great or tiny, it remains in its data packet and will be detected and discarded. Therefore, the influence of any type of attack is all that the controller cannot receive timely packets. In other words, the controller will operate in only two states. One is the normal state when the controller can receive a real-time data packet. The other is the attacked state when the real-time data packet is discarded so that the controller cannot receive it. Assume that the remote signals $\boldsymbol{y}(t)$ are sampled periodically at $0 < t_{S1} < t_{S2} < \cdots < t_{Sk} < \cdots$, and the sampling period is denoted with T. Then, we have $t_{Sk} - t_{S(k-1)} = T,\ \forall k = 1, 2, 3, \ldots$ When a cyber attack occurs, the input of the actuators $\boldsymbol{u}(t)$ cannot be updated timely since the controller does not generate a new command. Therefore, a new updating sequence is defined for the actuators: $0 < t_{A1} < t_{A2} < \cdots < t_{Ak} < \cdots$. Here, cyber attacks can be represented with just two parameters: the attack duration and the attack frequency. The detailed definition can be found in Assumptions 2 and 3. The new sampling period of the actuators is dependent on the attack duration and denoted by $h_k = t_{Ak} - t_{A(k-1)} = m_k T, m_k \in \{1, 2, \ldots, m_{max}\}$.

Assumption 2: For a power system where the sampling period of the sensors is T, the system suffers attack during $[kT, (k+m)T)$ with $m \in \{1, 2, \ldots, m_{max}\}$ such that the data packets at sampling time $\{kT, (k+1)T, \ldots, (k+m-1)T\}$ are discarded or blocked. Then, the attack duration is defined as $mT, m \in \{1, 2, \ldots, m_{max}\}$.

Assumption 3: During a certain period, the times the power system is attacked are denoted by $\kappa 1$, and $\kappa 2$ represents the number of normal transmissions without attack. Then, the attack frequency f_u is defined as $\kappa 1/(\kappa 1 + \kappa 2)$.

Remark 1: For the hackers, the limitation of attack resources is in conflict with the huge number of sensors, communication facilities, and hosts of the power system. A practical solution is to launch random attacks. Consequently, the selected remote signals will only be attacked with a certain probability. Furthermore, even if the hackers obtain the information about the critical facilities, the increasing energy/power budget [35] and the growing risk of being detected will force them to limit the duration of the attack to a shorter level. For instance, the low-rate shrew distributed

DoS attack with a shorter duration and a lower frequency is designed in [36] to make the attack resource-saving and stealthy.

With the redefined sampling period, the attack model can be illustrated with (2).

$$\bar{\boldsymbol{u}}(t_k)^* = \begin{cases} \bar{\boldsymbol{u}}(t_{k-1}) & t \in [t_{k-1}, t_{k-1} + t_{ad}) \\ \bar{\boldsymbol{u}}(t_k) & t \in [t_{k-1} + t_{ad}, t_{k-1} + h_k) \end{cases} \tag{2}$$

where $\bar{\boldsymbol{u}}(t_k)^*$ and $\bar{\boldsymbol{u}}(t_k)$ represent the attacked and original input signal, respectively. h_k is the redefined period, and t_{ad} is the moment when the attack disappears. It is worth mentioning that the attack model of (2) is different from those reported in previous references, which aim at detecting or mitigating attacks. For those studies, the magnitude of the attack is an essential parameter since the attack and the normal grid dynamics or contingencies can both cause a sudden magnitude change, making it difficult to tell the two apart. However, the focus of this paper is to propose a quantitative resilience index and corresponding calculation method. Attack detection is just a prerequisite but not the point. Therefore, attack duration and attack frequency are enough to represent the established attack model.

Based on the above discussions, the power system with WADC can be considered as a non-uniformly sampled-data system [37]. The attack duration is positively correlated with the redefined sampling period. When attack duration, attack frequency, or both reach a high level, the system may become unstable. Consequently, the resilience of the system can be quantified with the parameters of attack duration and attack frequency.

B. Closed-Loop Switching System Modeling

Considering the influence of the attack, the state-space of the power system (1) can be rewritten as follows:

$$\begin{cases} \dot{\bar{\boldsymbol{x}}}(t) = \bar{\boldsymbol{A}}\bar{\boldsymbol{x}}(t) + \eta\bar{\boldsymbol{B}}\bar{\boldsymbol{u}}(t_k) + (1-\eta)\bar{\boldsymbol{B}}\bar{\boldsymbol{u}}(t_{k-1}) \\ \bar{\boldsymbol{y}}(t) = \bar{\boldsymbol{C}}\bar{\boldsymbol{x}}(t) \qquad t \in [t_k, t_{k+1}) \end{cases} \tag{3}$$

where $\eta = 0$ or 1. $\eta = 0$ means that the system is subjected to cyber attacks while $\eta = 1$ represents that the system is not subjected to cyber attacks. To moderate the influence of cyber attacks, the executing period of the actuators, denoted by T_0, is assumed to be much smaller than the sampling period of the sensors and satisfies $T_0 = T/n, n \in \{1, 2, \dots\}$. Then, the sampling period of the system in (3) is $h_k = mnT_0$. The time slots of the input of the actuators $\bar{\boldsymbol{u}}(t)$ under this control strategy is illustrated in Fig. 2. It can be seen that there exist two control signals simultaneously in the interval of h_k when the system suffers attacks. Hence, the system (3) is reconstructed as the following discrete model.

$$\begin{cases} \bar{\boldsymbol{x}}(t_{k+1}) = \bar{\boldsymbol{A}}(h_k)\bar{\boldsymbol{x}}(t_k) + \bar{\boldsymbol{B}}(h_k)\bar{\boldsymbol{u}}(t_k) \\ \qquad\qquad + \bar{\boldsymbol{B}}(h_{k-1})\bar{\boldsymbol{u}}(t_{k-1}) \\ \bar{\boldsymbol{y}}(t_k) = \bar{\boldsymbol{C}}\bar{\boldsymbol{x}}(t_k) \end{cases} \tag{4}$$

where

$$\bar{\boldsymbol{A}}(h_k) = e^{\bar{\boldsymbol{A}}h_k}, \ \bar{\boldsymbol{B}}(h_k) = \int_{n_1(k)T_0}^{h_k} e^{\bar{\boldsymbol{A}}s}\bar{\boldsymbol{B}}ds$$

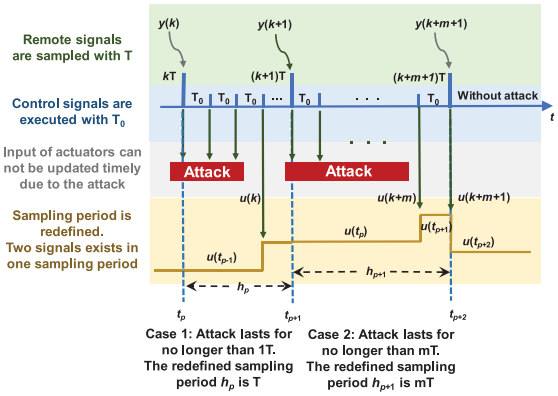


Fig. 2. Time slots of signals in WADC system under cyber attack.

$$\bar{\boldsymbol{B}}(h_{k-1}) = \int_0^{n_1(k)T_0} e^{\bar{\boldsymbol{A}}s}\bar{\boldsymbol{B}}ds$$

Define

$$\bar{\boldsymbol{A}}_0 = e^{\bar{\boldsymbol{A}}T_0}, \ \bar{\boldsymbol{B}}_0 = \int_0^{T_0} e^{\bar{\boldsymbol{A}}s}\bar{\boldsymbol{B}}ds$$

Then, we can obtain

$$\bar{\boldsymbol{A}}(h_k) = \bar{\boldsymbol{A}}_0^{mn}, \ \bar{\boldsymbol{B}}(h_k) = \sum_{j=n_1(k)}^{mn-1} \bar{\boldsymbol{A}}_0^j\bar{\boldsymbol{B}}_0$$

$$\bar{\boldsymbol{B}}(h_{k-1}) = \sum_{j=0}^{n_1(k)-1} \bar{\boldsymbol{A}}_0^j\bar{\boldsymbol{B}}_0$$

where $\bar{\boldsymbol{A}}_0^j$ denotes $\bar{\boldsymbol{A}}_0$ to the power of j, $j \in \{0, 1, 2, \dots, mn\}$. Thus, the system (4) can be stated as follows:

$$\begin{cases} \bar{\boldsymbol{x}}(t_{k+1}) = \bar{\boldsymbol{A}}_0^{mn}\bar{\boldsymbol{x}}(t_k) + \sum_{j=n_1(k)}^{mn-1} \bar{\boldsymbol{A}}_0^j\bar{\boldsymbol{B}}_0\bar{\boldsymbol{u}}(t_k) \\ \qquad\qquad + \sum_{j=0}^{n_1(k)-1} \bar{\boldsymbol{A}}_0^j\bar{\boldsymbol{B}}_0\bar{\boldsymbol{u}}(t_{k-1}) \\ \bar{\boldsymbol{y}}(t_k) = \bar{\boldsymbol{C}}\bar{\boldsymbol{x}}(t_k) \end{cases} \tag{5}$$

where $n_1(k) \in \{1, 2, \dots, mn\}$. When $n_1(k)$ takes different values, the system (5) will be correspond to different forms in terms of different intervals h_k. Consequently, the system (5) can be reconstructed as a switching system model as follows:

$$\begin{cases} \bar{\boldsymbol{x}}(t_{k+1}) = \bar{\boldsymbol{A}}_0^{mn}\bar{\boldsymbol{x}}(t_k) + \bar{\boldsymbol{B}}_{\sigma(t_k)}\bar{\boldsymbol{u}}(t_k) + \hat{\bar{\boldsymbol{B}}}_{\sigma(t_k)}\bar{\boldsymbol{u}}(t_{k-1}) \\ \bar{\boldsymbol{y}}(t_k) = \bar{\boldsymbol{C}}\bar{\boldsymbol{x}}(t_k) \end{cases} \tag{6}$$

where $\bar{\boldsymbol{B}}_{\sigma(t_k)} = \sum_{j=n_1(k)}^{mn-1} \bar{\boldsymbol{A}}_0^j\bar{\boldsymbol{B}}_0$, $\hat{\bar{\boldsymbol{B}}}_{\sigma(t_k)} = \sum_{j=0}^{n_1(k)-1} \bar{\boldsymbol{A}}_0^j\bar{\boldsymbol{B}}_0$, and $\sigma(t_k) = n_1(k)$ denotes the switching signals, which means that the system switches from the attacked subsystem to the normal subsystem at $\sigma(t_k)T_0$ during an interval h_k. Furthermore, $\sigma(t_k) = 0$ represents that the system has not been attacked during a whole interval h_k. Instead, when the system is subjected to a cyber attack that lasts for all the interval h_k, $\sigma(t_k)$ reaches its maximum value mn.

In the system (6), every subsystem corresponds to a value for the switching signal $\sigma(t_k)$, and there are at most $mn + 1$ subsystems for an interval h_k. The subsystem is assumed to be stable with $\sigma(t_k) = 0$, meaning no attack occurs. When $\sigma(t_k) = 1, 2, \dots, mn$, the system gets more and more unstable. Assume that the activation number of the subsystem $\sigma(t_k)$ is

$n_{\sigma(t_k)}$ over $[t_0, t_k)$, then the activation number of the stable and unstable subsystems are n_0 and $\sum_{j=1}^{mn} n_j$, respectively. The existing frequency of the unstable subsystems is denoted as $f_u = \sum_{j=1}^{mn} n_j/(n_0 + \sum_{j=1}^{mn} n_j)$, which is also regarded as the attack frequency combining with Assumption 3.

Further, the dynamic model of the WADC can be incorporated into the above open-loop switching power system. For any linear WADC, its state-space can be written as follows [30]:

$$\begin{cases} \boldsymbol{x}_c(t_{k+1}) = \boldsymbol{A}_c\boldsymbol{x}_c(t_k) + \boldsymbol{B}_c\boldsymbol{u}_c(t_k) \\ \boldsymbol{y}_c(t_k) = \boldsymbol{C}_c\boldsymbol{x}_c(t_k) + \boldsymbol{D}_c\boldsymbol{u}_c(t_k) \end{cases} \tag{7}$$

where $\boldsymbol{x}_c(t_k)$, $\boldsymbol{y}_c(t_k)$, $\boldsymbol{u}_c(t_k)$ are state vector, output vector and control vector of the WADC, respectively. And $\boldsymbol{A}_c$, $\boldsymbol{B}_c$, $\boldsymbol{C}_c$, $\boldsymbol{D}_c$ are state matrix, input matrix, output matrix and feedforward matrix of the WADC, respectively.

Redefining the state vector $\boldsymbol{x}(t) = [\bar{\boldsymbol{x}}^T(t), \boldsymbol{x}_c^T(t)]^T$ and the output vector $\boldsymbol{y}(t) = [\bar{\boldsymbol{y}}^T(t), \boldsymbol{y}_c^T(t)]^T$, then the closed-loop switching power system is obtained as follows:

$$\begin{cases} \boldsymbol{x}(t_{k+1}) = \boldsymbol{A}_{\sigma(t_k)}\boldsymbol{x}(t_k) + \boldsymbol{B}_{\sigma(t_k)}\boldsymbol{x}(t_{k-1}) \\ \boldsymbol{y}(t_k) = \boldsymbol{C}\boldsymbol{x}(t_k) \end{cases} \tag{8}$$

where

$$\boldsymbol{A}_{\sigma(t_k)} = \begin{bmatrix} \bar{\boldsymbol{A}}_0^{mn} + \bar{\boldsymbol{B}}_{\sigma(t_k)}\bar{\boldsymbol{D}}_c\bar{\boldsymbol{C}} & \bar{\boldsymbol{B}}_{\sigma(t_k)}\bar{\boldsymbol{C}}_c \\ \bar{\boldsymbol{B}}_c\bar{\boldsymbol{C}} & \bar{\boldsymbol{A}}_c \end{bmatrix},$$

$$\boldsymbol{B}_{\sigma(t_k)} = \begin{bmatrix} \hat{\bar{\boldsymbol{B}}}_{\sigma(t_k)}\boldsymbol{D}_c\bar{\boldsymbol{C}} & \hat{\bar{\boldsymbol{B}}}_{\sigma(t_k)}\bar{\boldsymbol{C}}_c \\ 0 & 0 \end{bmatrix}, \quad \boldsymbol{C} = \begin{bmatrix} \bar{\boldsymbol{C}} & 0 \\ 0 & \boldsymbol{C}_c \end{bmatrix}$$

The main idea of the process of modeling the closed-loop switching system can be illustrated with Fig. 3.

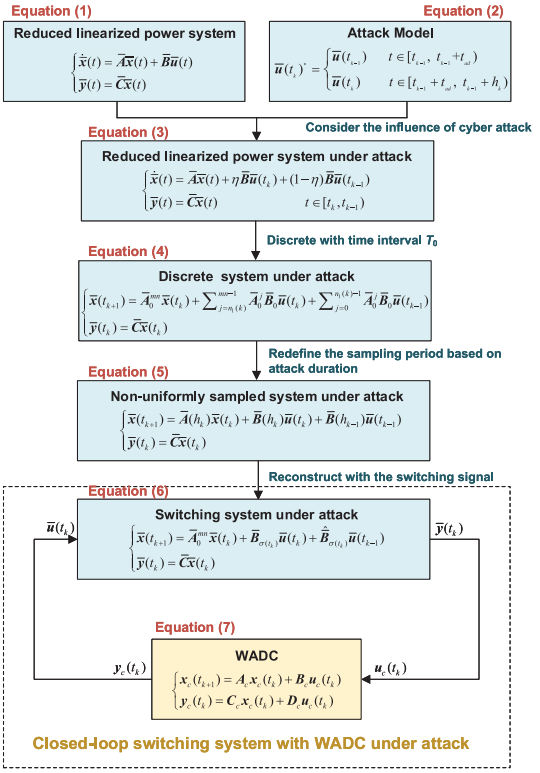


Fig. 3. Modeling sequence for the closed-loop switching power system with WADC.

III. Definition and Calculation of Resilience Margin

So far, the closed-loop power system is modeled as a switching power system that consists of stable and unstable subsystems. According to the statement in [38], the switching system can stay stable even if there exist unstable subsystems as long as the activation frequency of unstable subsystems is limited below a certain value. Since the system subjected to the cyber attack with different attack durations corresponds to different subsystems, the attack frequency can be approximated to the activation frequency of the unstable subsystems. Therefore, the definition of the resilience margin is presented as Definition 1.

Definition 1: Assume that the cyber attack that system suffers each time lasts for no longer than a specific duration, the resilience margin of the system with a given WADC, denoted as f_{MAF}, is defined as the maximum acceptable attack frequency without losing stability.

A. Exponential Stability Analysis of Switching Power System

To calculate the resilience margin, a sufficient criterion for the exponential stability of the switching system proposed in [25], [38] is applied. A brief overview of its main idea has been presented as follows.

Firstly, the definitions of exponential stability and average dwell time (ADT) of a switching system are expressed in Definitions 2 and 3.

Definition 2: If for every initial state $\boldsymbol{x}(t_0)$, there exist positive constants c and $\lambda < 1$ such that the inequality $\|\boldsymbol{x}(t_k)\| \le c\lambda^{t_k}\|\boldsymbol{x}(t_0)\|$ holds. Then the system (8) is said to be exponentially stable.

Definition 3: For any given switching signal $\sigma(t_k)$ and $t_k > 1$, let $N_\sigma[t_0, t_k)$ denote the switching number over the time interval $[t_0, t_k)$. If there exist $N_0 \ge 0$, $t_a \ge 0$ such that $N_\sigma[t_0, t_k) \le N_0 + t_k/t_a$, t_a is defined as the average dwell time of the switching signal $\sigma(t_k)$, and N_0 is defined as the chatter bound.

Denote n_j as the activation number of the subsystem S_j over $[t_0, t_k)$, $j \in \{1, 2, \ldots, mn\}$. Theorem 1 provides a sufficient criterion for the exponential stability of the system (8).

Theorem 1: For the system (8), if there exist positive constants $\lambda_j > 0$, $\lambda < 1$ and $\mu \ge 1$ and approximate matrices $P_j \ge 0$, $Q_j \ge 0$, $j \in \{1, 2, \ldots, mn\}$, such that the following inequalities hold

$$\Gamma_j = \begin{bmatrix} \boldsymbol{A}_j^T\boldsymbol{P}_j\boldsymbol{A}_j - \lambda_j^2\boldsymbol{P}_j + \boldsymbol{Q}_j & \boldsymbol{A}_j^T\boldsymbol{P}_j\boldsymbol{B}_j \\ \boldsymbol{B}_j^T\boldsymbol{P}_j\boldsymbol{A}_j & \boldsymbol{B}_j^T\boldsymbol{P}_j\boldsymbol{B}_j - \lambda_j^2\boldsymbol{Q}_j \end{bmatrix} < 0 \tag{9}$$

$$\boldsymbol{P}_\alpha \le \mu\boldsymbol{P}_\beta, \boldsymbol{Q}_\alpha \le \mu\boldsymbol{Q}_\beta, \alpha, \beta \in \{1, 2, \ldots, mn\} \tag{10}$$

$$f_u \le \frac{\ln\lambda - \ln\lambda_0}{\ln\lambda_b - \ln\lambda_0} \tag{11}$$

$$\frac{\ln\mu}{2\ln(1/\lambda)} < T_a \tag{12}$$

where, T_a is the ADT as defined in Definition 3, λ_0 is the exponential decay rate of stable subsystem with $\sigma(t_k) = 0$, and $\lambda_b = \max(\lambda_p), \lambda_p | p \in \{1, 2, \ldots, mn\}$ denotes the maximum exponential decay rate among the rates of all the unstable subsystems with $\sigma(t_k) = \{1, 2, \ldots, mn\}$. Then, the system (8) is exponentially stable with an exponential decay rate of $\rho(\lambda, T_a) = \lambda \mu^{1/(2T_a)}$.

Remark 2: Due to the randomness of the cyber attack, the ADT cannot be obtained in advance. Nevertheless, it can be inferred from its definition that the ADT T_a is no longer than the sampling period of sensors T. Thus, the inequality (12) in Theorem 1 can be replaced with (13).

$$\frac{\ln \mu}{2 \ln(1/\lambda)} < T \tag{13}$$

The proof of Theorem 1 can be found in [38] and omitted here.

B. Calculation of Resilience Margin

Considering Theorem 1, the inequality (11) provides an upper bound of the acceptable attack frequency for a certain system without losing stability. Therefore, the calculation of the resilience margin is converted into an optimal problem (14). Notice that the resilience margin is a monotone increasing function in λ and a decrease in λ_b. The optimal solution will be achieved with the maximum value of λ and the minimum value of λ_b. As for the selection of λ_0, it needs to poll from 0 to 1 to find an approximate value. Based on this, the following procedure is proposed to solve (14):

$$\begin{aligned} \max \ & f_u = \frac{\ln \lambda - \ln \lambda_0}{\ln \lambda_b - \ln \lambda_0} \\ s.t. \ & (9), \ (10), \ (13) \\ & P_j > 0 \\ & Q_j > 0 \\ & 0 < \lambda_0 < \lambda < 1 < \lambda_b. \end{aligned} \tag{14}$$

1) Choose a sufficiently small initial value for λ_0 satisfying $\Gamma_0 < 0$.
2) When λ_0 is determined, the minimum value for every $\lambda_j, j \in \{1, 2, \ldots, mn\}$ should be calculated by solving Γ_j. However, the matrix inequality (9) cannot be solved directly since it is nonlinear due to λ_j^2 and P_j or Q_j. A practical solution is to fix λ_j^2 and check the feasibility of the inequality over $P_j > 0$ and $Q_j > 0$. Then, the LMIs technology can be applied and solved through MATLAB/YALMIP toolbox. On that basis, the bisection approach is adopted to search for every minimum λ_j that satisfies $\Gamma_j < 0$. At last, λ_b is the maximum of all minimum λ_j.
3) With determined λ_0 and λ_b, the objective function f_u depends only on λ now. It is easy to find the maximum λ that satisfies (13). Furthermore, the resilience margin $f_{MAF|\lambda_0}$ at the current value of λ_0 can be obtained.
4) Update $\lambda_0 = \lambda_0 + \Delta\lambda_0$, and repeat the step 2) and step 3) until $\Gamma_0 < 0$ is no longer satisfied or $\lambda_0 \geq 1$, where $\Delta\lambda_0$ is the step size. Then compare $f_{MAF|\lambda_0}$ corresponding to all possible values of λ_0 and choose the maximum value as the f_{MAF}.

The details of the procedure are presented in Algorithm 1.

Algorithm 1 Find the Resilience Margin f_{MAF}

Require: System parameters $\boldsymbol{A}_{\sigma(t_k)}$, $\boldsymbol{B}_{\sigma(t_k)}$. Sampling periods of actuator T_0 and sensor $T = nT_0$. The longest attack duration $m_{max}T$.

Ensure: Resilience margin f_{MAF}

Initialization:
Set scalar μ, initial λ_0, step size $\Delta\lambda_0$.
Set parameters of bisection approach: lower bound λ_{min}, upper bound λ_{max}, tolerance λ_{ac}.
$f_{MAF} \to 0$, $\rho \to 0$
while $\lambda_0 < 1$ and $\Gamma_0 < 0$ **do**
  for j $= 1 : mn$ **do**
    1) Calculate λ_j such that (9) and (10) are satisfied by bisection approach.
    2) Set $\rho = 1$ if λ_j is a valid solution.
  end for
  if $\rho = 1$ **then**
    1) Set $\lambda_b = \max\{\lambda_\mathrm{j}, \mathrm{j} = 1, 2, \ldots, \mathrm{mn}\}$.
    2) Find maximum λ satisfying (13) and $\lambda_b > \lambda > \lambda_0$.
    3) Calculate $f_{MAF|\lambda_0} = \frac{\ln \lambda - \ln \lambda_0}{\ln \lambda_b - \ln \lambda_0}$.
  end if
  if $f_{MAF|\lambda_0} > f_{MAF}$ **then**
    Set $f_{MAF} = f_{MAF|\lambda_0}$ and save λ, λ_0.
  end if
  Clear array λ_j and set $\lambda_0 = \lambda_0 + \Delta\lambda_0$.
end while

C. Summary of Application Steps

Detailed application of resilience margin in the design of WADC can be summarized as the following steps. For those WADCs with fixed parameters, all four steps are performed offline. And then, the parameters remain fixed when WADCs are put into use online. For those WADCs whose parameters need to be adjusted to realize adaptivity, Steps 1 and 2 are recommended to be performed offline under a series of typical operating conditions to form a model library. Then the controller designer can select the linearized model of the power system with the most similar operating conditions from the library to perform online calculation and parameter update, avoiding the difficulty of online model identification caused by the complexity of the model and the potential impact of attacks.

Step 1 Obtain the reduced linearized model of the power system, excluding the WADC. Firstly, establish the detailed non-linear full-order test system models using the power system simulation toolbox (PSST) [39] based on MATLAB/Simulink. Then, the Linear Analysis Toolbox is adopted to linear the original model in terms of a certain operating point. After that, the order of the system is reduced by the balanced model order reduction method based on normalized coprime factors, remaining the

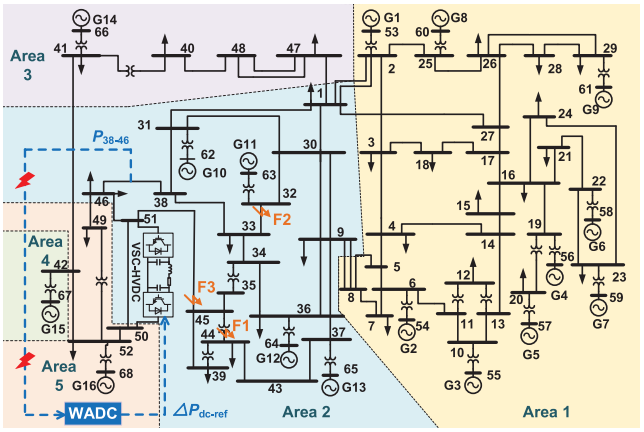


Fig. 4. The diagram of 16-machine 68-bus power system with VSC-HVDC.

dynamics characteristics of inter-area oscillations (typically ranging from 0.2Hz to 2.5Hz).

Step 2 Establish the closed-loop switching model of the power system considering the influence of cyber attacks. Discrete the reduced linearized power system with the sampling period $mT, m \in \{1, 2, \ldots, m_{max}\}$, respectively. The systems with a sampling period of $mT, m \in \{1, 2, \ldots, m_{max}\}$ are the different subsystems. Then, the WADC model is linked to every subsystem to form the closed-loop subsystems. The whole closed-loop system is the combination of all the subsystems.

Step 3 Calculate the resilience margin. Based on the model established in Step 2, the resilience margin f_{MAF} can be calculated using Algorithm 1.

Step 4 Determine the WADC parameters based on resilience margin and desired damping performance. By choosing a set of WADC parameters and repeating Step 2 and Step 3, the relationship between the WADC parameters and the resilience margin is obtained. Considering the variation of damping ratio with WADC parameters, the best parameters can be determined.

IV. Case Study

The case study is carried out based on the 16-machine 68-bus New England-New York power system with VSC-HVDC, as shown in Fig. 4. It consists of five areas, and the parameters are given in [40]. Using MATLAB/Simulink, the test system model excluding WADC is represented as a 135th-order nonlinear dynamic model, in which each generator is described with 6th-order DAEs equipped with an excitation system. The VSC-HVDC located between bus 50 and 51 is represented as 19th-order DAEs. Then, the test system is linearized, and order-reduced to 20^{th} order [30].

Under the basic operating condition, the VSC-HVDC delivers 1196MW rated power. All the generators are equipped with PSSs except for G14 and G15. There exists an unstable damping mode with a damping ratio of −0.0069. Thus, the classical lead-lag WADC is designed for this mode using the method described in [2] and can be represented as:

$$H_{WADC}(s) = K_a \frac{T_\omega s}{1 + T_\omega s} \left(\frac{1 + T_1 s}{1 + T_2 s} \right)^2 \tag{15}$$

where T_ω is a washout constant and is set to be 2s. And T_1 and T_2 are two phase-compensation constants whose values are designed according to the conventional phase compensation method described in [40]. Assume that R^i is the residue of the transfer function G of the closed-loop system with regard to the i_{th} mode, also the weakest mode targeted for design. Then, the phase needed to be compensated is obtained by (16), denoted with ϕ

$$\phi = 180^\circ - arg(R^i) \tag{16}$$

Since the phase that each block can compensate is 30°-50°, two blocks are used here to make the compensated phase achieve 60°-100°. T_1 and T_2 can be determined with (17) and (18).

$$\alpha = \frac{1 - \sin(\phi/2)}{1 + \sin(\phi/2)} \tag{17}$$

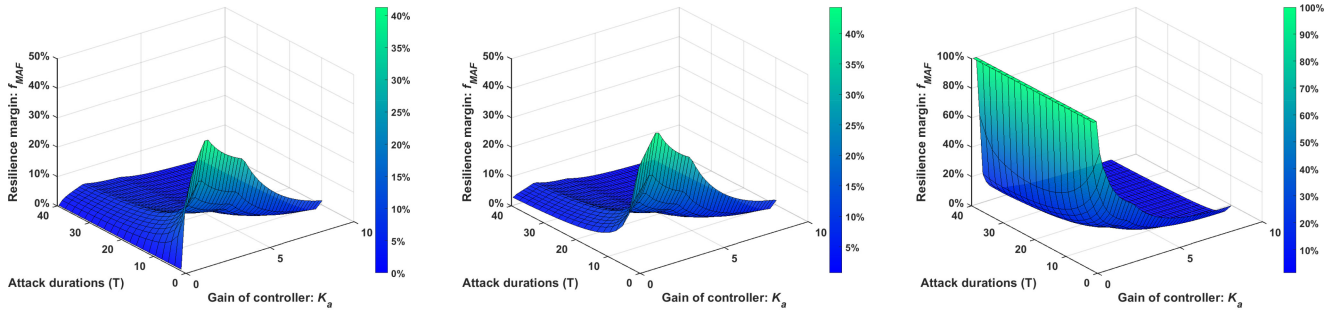
$$T_1 = \frac{1}{2\pi f_i \sqrt{\alpha}}, \quad T_2 = \alpha T_1 \tag{18}$$

where f_i is the oscillation frequency for i_{th} mode. Here, they are determined as $T_1 = 0.4860$s, $T_2 = 0.1716$s.

Then, controller gain K_a is the only parameter to be determined, the value of which plays an important role in deciding both damping ratio and resilience margin. Thus, it should be designed by the trade-off between damping ratio and resilience margin. It is worth noting that T_1 and T_2 also contribute to the resilience margin. But it is complex and unnecessary to consider it when designing all parameters. Compared with T_1/T_2, controller gain K_a has a greater impact on the resilience margin. It is enough only to adjust K_a. When the controller design is completed, resilience margin sensitivity analysis can be applied to verify the designed parameters using the similar analysis method proposed in [41], which propose a method to analyze the delay margin sensitivity to the controller parameters.

Based on controllability/observability analysis, the AC tie line active power P_{38-46} is selected as the input signal, and the WADC is chosen to be installed with the control system of VSC-HVDC. When the disturbance occurs, the WADC adjusts the delivered active power of VSC-HVDC by providing an additional active power reference $\Delta P_{\text{dc-ref}}$ to damp out the oscillations.

To prove the proposed method is applicable under various operating conditions, two more operating conditions (O.C.) are discussed. Through adjusting the active power of machine G16, the power flow of the whole system changes as well. As a result, HVDC delivers different active power, and the damping ratio is adjusted to be negative (−0.0069), close to zero (−0.0006), and positive but small (0.0279), respectively. These three damping ratios indicate that the system will fall into divergent oscillation, persistent oscillation, and damping oscillation with a slow convergence rate after faults, respectively, covering most cases where a WADC is needed. Under every O.C., three-phase-ground fault is applied, and their locations



(a) O.C.1 (b) O.C.2 (c) O.C.3

Fig. 5. Resilience margin f_{MAF} of different attack durations (1T−40T) and gains of WADC (K_a : 0.1 − 8.6) under three operating conditions.

TABLE I
DIFFERENT OPERATING CONDITIONS FOR THE TEST SYSTEM

O.C. No.	*P_{50-51} (MW)*	*Damping Ratios*	*Fault Setting*
1	1196	-0.0069	Three-phase-ground fault of line 44-45 near bus 44 and switch off line 44-45 after 100 ms and reclose it after 800 ms
2	1102	-0.0006	Three-phase-ground fault of line 32-33 near bus 32 and switch off line 32-33 after 100 ms, the line does not reclose
3	585	0.0279	Three-phase-ground fault of line 45-51 near bus 45 and switch off line 45-51 after 100 ms and reclose it after 800 ms

TABLE II
RESILIENCE MARGIN f_{MAF} OF DIFFERENT ATTACK DURATIONS AND GAINS UNDER THREE OPERATING CONDITIONS

O.C. No.	*Attack Durations*	*Resilience Margin f_{MAF}*					
		$K_a = 0.1$	$K_a = 0.9$	$K_a = 1.5$	$K_a = 2.5$	$K_a = 5.5$	$K_a = 8.5$
1	10T	0.00%	9.52%	12.89%	10.59%	4.36%	2.05%
	20T	0.00%	5.33%	7.41%	6.08%	2.47%	1.16%
	30T	0.00%	3.91%	5.50%	4.51%	1.81%	0.84%
	40T	0.00%	3.26%	4.61%	3.77%	1.51%	0.71%
2	10T	7.96%	12.40%	14.21%	10.74%	3.97%	2.10%
	20T	4.36%	7.10%	8.28%	6.21%	2.26%	1.20%
	30T	3.20%	5.31%	6.22%	4.64%	1.67%	0.88%
	40T	2.72%	4.52%	5.29%	3.93%	1.42%	0.75%
3	10T	100.00%	25.40%	15.88%	11.15%	4.25%	3.59%
	20T	100.00%	16.27%	9.65%	6.66%	2.50%	2.12%
	30T	100.00%	13.43%	7.59%	5.14%	1.90%	1.61%
	40T	100.00%	13.36%	7.08%	4.72%	1.77%	1.54%

are denoted with F1, F2, F3 depicted in Fig. 4. The overview of three operating conditions is shown in Table I.

A. Resilience Margin Under Three Operating Conditions

Firstly, the reduced linearized model is discretized in terms of the sampling period T of PMUs, set to be 0.02s. The executing period of the actuator is assumed as $T_0 = T/n = 0.005$s with $n = 4$. Then the results under three operating conditions are calculated through Algorithm 1 and shown in Fig. 5 by choosing a set of controller gains (K_a : 0.1 − 8.6) and attack durations with $\mu = 1.00001$. The attack duration ranges from 1T to 40T, indicating that the maximum attack duration may be 0.02s-0.8s. Part of the data in Fig. 5 is shown in Table II but more data is omitted due to the limitation of space. Besides, the damping ratio as a function of the controller gain is also shown in Fig. 6.

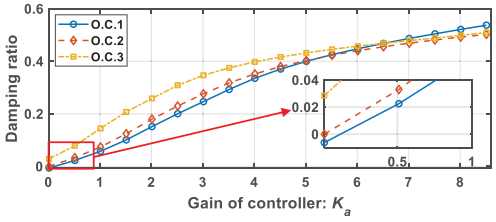


Fig. 6. The trend of the damping ratio of system with gain of WADC (K_a : 0.1 − 8.6) under three operating conditions.

Based on the obtained results, some observations about the relationship between the resilience margin and gain of WADC, attack duration, and operating condition of the system can be revealed. Specially, these observations are summarized and discussed as follows.

- The resilience margin increases firstly and then decreases with the increase of gain of WADC when the damping ratio of the system without WADC is negative, as shown in Fig. 5 (a) and (b). As shown in Fig. 6, the damping ratio under O.C.1 and O.C.2 rises from a negative value (−0.0069 under O.C.1 and −0.0006 under O.C.2) as the gain increases, which means the system is unstable itself when the gain is minor or even equal to zero (that is, there is no WADC). Therefore, resilience margin f_{MAF} is close to zero. But then, the increase of gain promotes the stability of the system such that the resilience margin increases as well and reaches its maximum when the gain is about 1.5, as illustrated in Table II. Nevertheless, the adverse influence out of attacks will also be multiplied by the gain. This effect predominates when the gain is larger than 1.5 such that the resilience margin begins to decrease.
- The resilience margin decreases all the time as the gain of WADC increases when the damping ratio of the system without WADC is positive, as shown in Fig. 5 (c). f_{MAF} can be approximated to 100% under O.C.3 since the system is stable even if there is no WADC (damping ratio is 0.0279). Consequently, the resilience margin only has a downward trend with the gain due to the cyber attack.
- The attack duration and the resilience margin are inversely proportional to each other. For the system with a given-gain WADC, resilience margin f_{MAF} decreases as the attack duration increases from 1T to 40T no matter

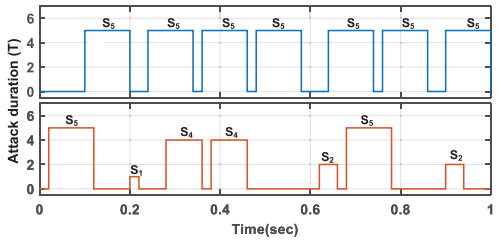


Fig. 7. The details of two types of cyber attack.

which operating condition the system is under, according to Fig. 5. This trend is consistent with the fact that the attack with a longer duration has a more severe impact on the stability of the system so that the acceptable attack frequency is less.

- Under the operating condition with a heavy power flow, the system has less resilience margin. Comparing the subfigures of Fig. 5, it can be seen that f_{MAF} is smaller under O.C.1 than those under O.C.2 and O.C.3 with a given WADC gain and attack duration in most cases.

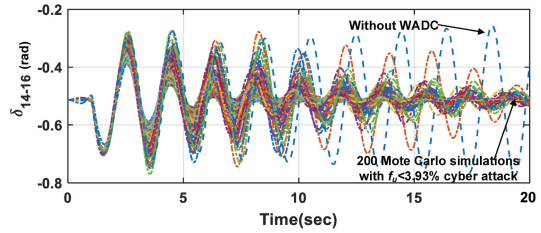
B. Monte Carlo Simulation Verification

Since Assumption 2 only ensures that the attack duration is below a certain upper bound, the practical attack duration can be any length less than the bound. Besides, the attack frequency is just a statistical indicator over an interval according to Assumption 1. The practical cyber attack will take on various forms even when the maximum attack duration and attack frequency are given. As shown in Fig. 7, the two types of attack share the same attack parameters (The maximum attack duration is 5T and the attack frequency is 13.73%) over $t = [0, 1)$ but take on different forms and thus have different degrees of impact on the system. The attack duration of the first type of attack, denoted with *attack type 1*, is fixed, while that of the second type, denoted with *attack type 2*, is a random value no more than 5T. To deal with the randomness of the attack, Monte Carlo simulations (MCSs) are adopted to provide a statistical view to verify the calculation results. Note that the attack frequency can only be calculated after the simulation instead of preset before the simulation since it is a statistical concept. Therefore, the attack frequency of MCSs is presented in the form of attack frequency ranges.

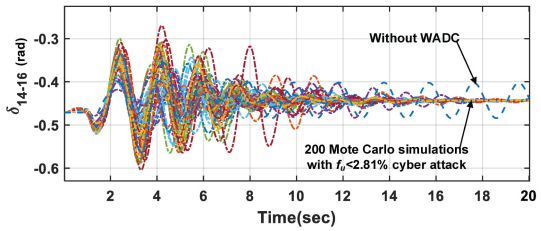
First of all, the examples of each operating condition with given controller gain and maximum attack duration are selected as follows to perform the simulations. The attack frequencies are limited below their resilience margins.

- *O.C. 1:* The system with a WADC of $K_a = 2.3$ suffers $f_u \in [0, 3.93\%)$ attack with an attack duration of 40T.
- *O.C. 2:* The system with a WADC of $K_a = 4.1$ suffers $f_u \in [0, 2.81\%)$ attack with an attack duration of 30T.
- *O.C. 3:* The system with a WADC of $K_a = 0.7$ suffers $f_u \in [0, 19.27\%)$ attack with an attack duration of 10T.

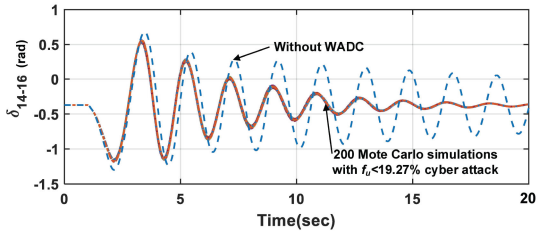
200 MCSs (half of attack type 1 and half of attack type 2) are carried out under every operating condition, respectively. The cases where attack frequency is below the resilience margin are picked up, and their number are 109/200, 101/200, 196/200, respectively. The simulation results of the selected



(a) O.C.1: The system with WADC of $K_a = 2.3$ suffers $f_u \in [0, 3.93\%)$ attack with attack duration of 40T



(b) O.C.2: The system with WADC of $K_a = 4.1$ suffers $f_u \in [0, 2.81\%)$ attack with attack duration of 30T



(c) O.C.3: The system with WADC of $K_a = 0.7$ suffers $f_u \in [0, 19.27\%)$ attack with attack duration of 10T

Fig. 8. Dynamic responses of the system without WADC and the system subjected to resilience marginal cyber attack under three operating conditions.

cases are illustrated in Fig. 8, in which the relative angle between G14 and G16 δ_{14-16} is unitized to represent the system dynamic response. According to Fig. 8, all the curves show the better damping performance than that of the system without WADC under every operating condition. It can be concluded that the damping performance of the WADC can be sufficiently promised when the attack frequency is no larger than the calculated resilience margin.

Furthermore, taking O.C.1 as an example, 2000 MCSs (half of attack type 1 and half of attack type 2) are carried out and sorted into five groups according to their attack frequency, as shown in Fig. 9. The maximum attack frequency of 2000 simulations is 13.23%, and the resilience margin is 3.93%. The number of cases in every group is 412/2000, 472/2000, 474/2000, 345/2000, 297/2000. The ITAE is an index widely used in the control field to compare the performance of different controllers [42] and is defined as ITAE $= \int_{t_1}^{t_2} t|e(t)|\,\mathrm{dx}$, where $e(t)$ represents the difference relative to its steady-state value of δ_{14-16}. Large ITAE denotes terrible performance. Through the violin diagram, Fig. 9 depicts the numerical distribution of ITAE in all 2000 simulations (the black box in the middle), as well as the fitted probability density (the pink/blue part around). Key indicators of the data in Fig. 9 have also been illustrated in Table III. Combing Fig. 9 and Table III, it can be seen that the ITAE of the system with a larger attack frequency gets a higher mean regardless of attack types. The

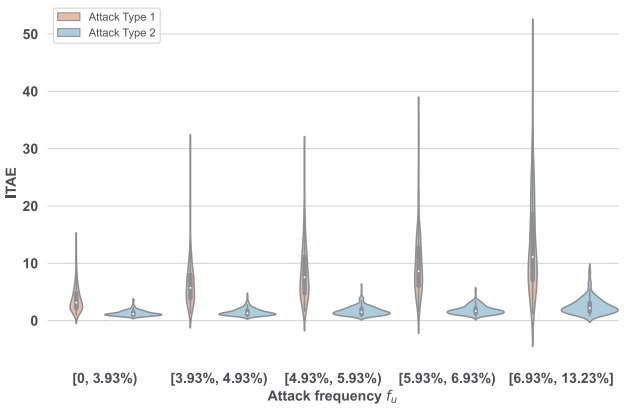


Fig. 9. The distribution of ITAE in 2000 simulations with different attack frequencies.

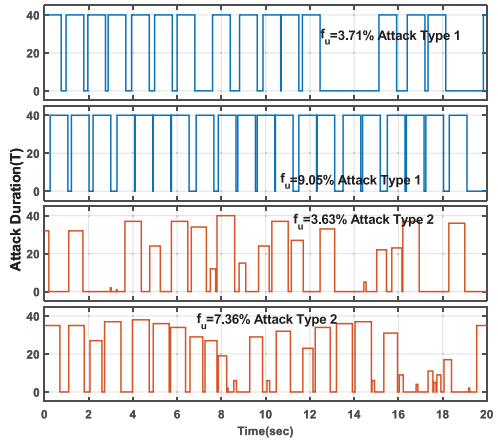
TABLE III
ITAE OF 2000 SIMULATIONS WITH DIFFERENT ATTACK FREQUENCIES

Attack Frequency		*Mean*	*Maximum*	*Minimum*	*Standard Deviation*
Attack Type 1	[0, 3.93%)	3.7418	13.8110	0.9963	2.2142
	[3.93%, 4.93%)	6.3886	29.8627	1.2986	3.7771
	[4.93%, 5.93%)	8.6006	28.6503	1.6786	5.1070
	[5.93%, 6.93%)	9.7671	35.1809	1.5806	5.3236
	[6.93%, 13.93%]	13.1165	46.8273	1.2490	8.0620
Attack Type 2	[0, 3.93%)	1.2710	3.5006	0.6500	0.4738
	[3.93%, 4.93%)	1.4653	4.4214	0.6411	0.6179
	[4.93%, 5.93%)	1.6925	5.8670	0.6447	0.7889
	[5.93%, 6.93%)	1.8078	5.2485	0.6254	0.7317
	[6.93%, 13.93%]	2.5235	8.7931	0.7934	1.4099

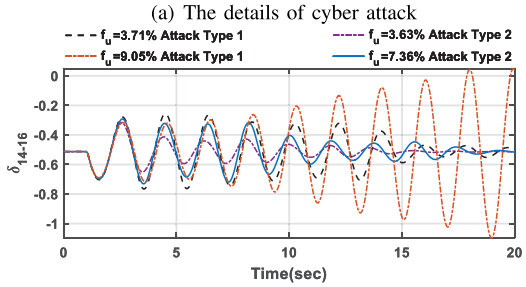
maximum and the minimum also follow the same trend with the mean, although, at some points, it is not monotonically changing due to randomness of attack. Therefore, it can be concluded that the system is more likely to fall into unstable when subjected to attacks with a larger frequency.

In addition, the curves corresponding to the maximum ITAE of group 1 ($f_u < f_{MAF} = 3.93\%$) are picked up to represent the worst possible influence of attack when the attack frequency is no larger than the calculated resilience margin in terms of every attack type. Similarly, the curves corresponding to the maximum ITAE of all groups are also picked up to denote the worst system performance of all the simulations in terms of every attack type. The four selected curves are shown in Fig. 10. It can be seen that the system can stay stable eventually under all cases except for that of $f_u = 9.05\%$ attack type 1. Therefore, it can be inferred that the simulated resilience margin is no larger than 9.05%.

Remark 3: Notice that the calculated resilience margin is conservative compared with the simulated one. On the one hand, this conservatism comes from the limitation of the algorithm itself since Theorem 1 provides a sufficient condition for exponential stability. On the other hand, the severest influence that a given-frequency attack can bring may still not be found even if lots of MCSs have been done in this paper. Thus, the true resilience margin will be smaller than the simulated one but larger than the calculated one. Nevertheless, the conservatism does not affect the trend of the relationship between the calculated resilience margin and the gain of the



(a) The details of cyber attack



(b) Dynamic responses of the system

Fig. 10. Dynamic responses of the system with $K_a = 2.3$ WADC subjected to different attack frequencies under O.C.1.

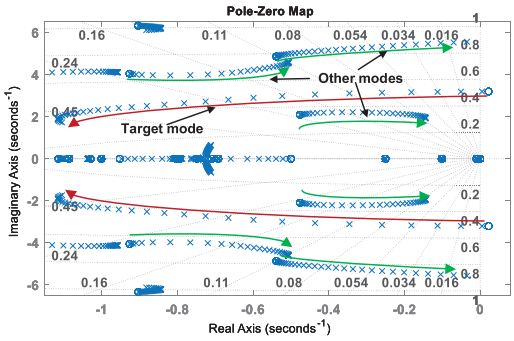
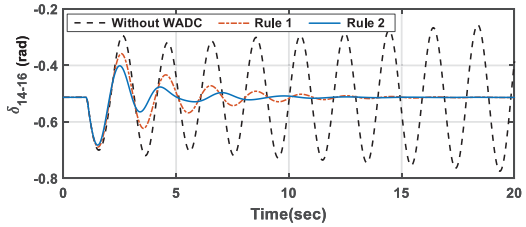


Fig. 11. Root locus of the closed-loop power system ($K_a : 0 - 10$).

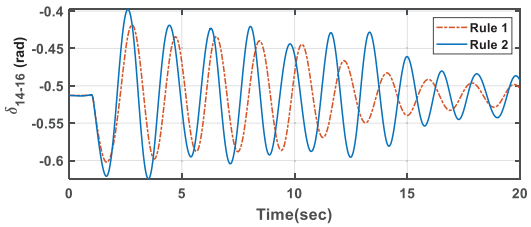
WADC so that it is still of great significance in guiding the design of WADC. By designing a better Lyapunov function, less conservative results may be obtained in the future.

C. WADC Design Based on Resilience Margin

At last, the significance of the resilience margin in designing WADC is confirmed with the example of choosing the best controller gain for (15). When the system is not implemented with a WADC, the damping ratio is -0.0069 under O.C.1. The WADC of (15) is designed targeting promote the damping ratio of this mode. The root locus of the closed-loop system is illustrated in Fig. 11, in which controller gain ranges from 0 to 10. It can be seen that the increase of K_a not only promotes the damping ratio of the target mode but also may reduce the damping ratio of other modes, which limits the infinite rise of K_a. Besides, even for the target mode, the damping



(a) There is no cyber attack



(b) The system suffers $f_u \in [0, 15\%)$ type 2 attack with an attack duration of 40T

Fig. 12. Dynamic responses of the system with WADC designd following different rules under O.C.1.

ratio does not always increase as the controller gain increases due to an output limitation module in the controller. However, considering that the analysis of this paper is based on the linearized system, the nonlinear limitation module will increase the complexity of the proposed method. Therefore, the output limitation module is neglected in the switching system model established.

Two different rules to select the optimal gain are firstly presented as follows. Rule 2 is the traditional rule that only considers the damping performance. While Rule 1 aims at achieving a trade-off between damping performance and resilience with the proposed resilience index considered. Considering that the cyber attack is destructive, a WADC should be as resilient as possible when ensuring the oscillations can be suppressed.

- *Rule 1:* Make the resilience margin as high as possible under the premise that all modes are adequately damped.
- *Rule 2:* Promote the damping ratio of the target mode as much as possible under the premise that all other modes would not be affected too much.

Moreover, these two rules can be illustrated with (19) and (20), respectively.

$$\max_{K_a} \ f_{MAF} \quad s.t. \ \ \zeta_i > 0.1 \ i = 1, 2, \ldots, n-1 \tag{19}$$

$$\max_{K_a} \ \zeta_w \quad s.t. \ \ \zeta_i > 0.1 \ i = 1, 2, \ldots, w-1, w+1, \ldots, n-1 \tag{20}$$

where ζ_i denotes the damping ratio of i_{th} mode, and $\zeta_i > 0.1$ is ensured to provide enough damping. ζ_w is the damping ratio of the target mode. $n-1$ is the total number of electromechanical modes. f_{MAF} is the defined resilience margin.

According to the results of Fig. 5 and Table II, the largest resilience margin is achieved when the controller gain is about 1.5. Then the resilience margin decreases with the growth of the gain. The damping ratios of the four modes highlighted in Fig. 11 are shown in Table IV. Mode 1 refers to the target mode, while modes 2-4 denote the other three modes. It can be seen that damping ratios of all four modes are larger than 0.1, satisfying the requirement of Rule 1. Thus, the optimal gain for Rule 1 is determined as 1.5. In addition, when the gain continues to grow from 1.5, the damping ratio of the target mode increases until the gain is bigger than 3.5, when the damping ratio of mode 4 will be less than 0.1. Then Rule 2 will not be met. Therefore, the optimal gain for Rule 2 is chosen as 3.5.

TABLE IV
DAMPING RATIOS OF DIFFERENT MODES FOR THE SYSTEM WITH WADC DESIGNED ACCORDING TO RULE 1 AND 2

Rule No.	*Optimal Gain*	*Damping Ratios*			
		Mode 1	*Mode 2*	*Mode 3*	*Mode 4*
1	1.5	0.101	0.215	0.139	0.108
2	3.5	0.292	0.149	0.137	0.102

Then time-domain simulation is carried out to compare the role of two rules in designing a controller when there is/is not an attack. Fig. 12 (a) shows the dynamic responses of the system with a WADC designed according to different rules when there is no attack. It can be seen that the system with a WADC designed following Rule 1 can suppress the oscillations effectively but is still worse than that with WADC designed following Rule 2, which means Rule 2 is indeed more effective when there is no attack. However, when the system is subjected to the same $fu \in [0, 15\%)$ type 2 attack with an attack duration of 40T, as shown in Fig. 12 (b), the response with the maximum ITAE of 200 MCSs indicate that the damping performance of the system with the WADC designed following Rule 1 performs better than that with the WADC designed following Rule 2. Here, the response with maximum ITAE in 200 MCSs is ensured to perform worst, which is also regarded as the worst consequence an attack can cause. These observations indicate that considering the proposed resilience margin when designing WADC can effectively improve the performance of the controller in the face of attack, which verifies the significance of the proposed index in designing WADC.

Note that it is not the key of this paper to design a resilient WADC based on the proposed index. The above discussion only provides a simple example to apply the proposed resilience margin. But the scope of application is not limited to the presented lead-leg controller. By analyzing the relationship between parameters of WADC and resilience margin, any resilient controller, including multiple inputs and multiple outputs (MIMO) WADC, can also be designed with the steps of Section III-C as long as it can be represented with the state space of (7).

V. CONCLUSION

This paper proposes a novel index named resilience margin to quantify the resilience of the system with a given WADC against cyber attacks. An algorithm combining the bisection method and the LMIs technology has been developed to calculate the resilience margin based on the Lyapunov stability

analysis of the switching system. Simulation results of the 16-machine 68-bus system with VSC-HVDC confirm that the system can stay sufficiently stable when the cyber attack is below the calculated resilience margin.

It is also found that the resilience margin goes up at first and then goes down as the gain of lead-leg WADC increases when the damping ratio of the system without WADC is negative but only has a downward trend when the damping ratio is positive. In addition, for the system with a given-gain WADC, the resilience margin is inversely proportional to the attack duration. The power flow will also affect the resilience margin. Based on these observations, the optimal gain is determined such that the trade-off between attack resilience and damping performance can be ensured.

The above results demonstrate the effectiveness of the calculation algorithm and the significance of the proposed resilience margin in the design of WADC. Future work will focus on decreasing the conservatism of the calculation results by establishing more accurate models with the output limitation module in the controller considered and making the proposed index adapt to the conditions where attacks occur in multiple channels. Based on the proposed index, it is also an interesting topic to study how to design WADC achieving coordination of various objectives such as damping performance, resilience, adaptivity to operating conditions, and robustness to parameter perturbations and time-delay.

REFERENCES

[1] S. Q. Bu, W. Du, and H. F. Wang, "Investigation on probabilistic small-signal stability of power systems as affected by offshore wind generation," *IEEE Trans. Power Syst.*, vol. 30, no. 5, pp. 2479–2486, Sep. 2015.

[2] M. E. Aboul-Ela, A. A. Sallam, J. D. McCalley, and A. A. Fouad, "Damping controller design for power system oscillations using global signals," *IEEE Trans. Power Syst.*, vol. 11, no. 2, pp. 767–773, May 1996.

[3] J. Wang, C. Fu, and Y. Zhang, "Design of WAMS-based multiple HVDC damping control system," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 363–374, Jun. 2011.

[4] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389–1407, Jul. 2017.

[5] "Roadmap to achieve energy delivery systems cybersecurity," U.S. Dept. Energy, Germantown, MD, USA, Rep., 2011.

[6] *Critical Infrastructure Protection (CIP)*, NERC Standard, 2016.

[7] A. Bindra, "Securing the power grid: Protecting smart grids and connected power systems from cyberattacks," *IEEE Power Electron. Mag.*, vol. 4, no. 3, pp. 20–27, Sep. 2017.

[8] H. M. Khalid and J. C.-H. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026–2037, Jul. 2016.

[9] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[10] W. Yao, L. Jiang, J. Wen, Q. Wu, and S. Cheng, "Wide-area damping controller for power system interarea oscillations: A networked predictive control approach," *IEEE Trans. Control Syst. Technol.*, vol. 23, no. 1, pp. 27–36, Jan. 2015.

[11] Y. Shen, W. Yao, J. Wen, H. He, and L. Jiang, "Resilient wide-area damping control using GrHDP to tolerate communication failures," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2547–2557, May 2019.

[12] G. Ravikumar and M. Govindarasu, "Anomaly detection and mitigation for wide-area damping control using machine learning," *IEEE Trans. Smart Grid*, early access, May 18, 2020, doi: 10.1109/TSG.2020.2995313.

[13] V. K. Singh and M. Govindarasu, "A cyber-physical anomaly detection for wide-area protection using machine learning," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3514–3526, Jul. 2021.

[14] J. F. O'Brien and D. Roberson, "Synchrophasor spoofing detection and remediation for wide-area damping control," *Electr. Power Syst. Res.*, vol. 199, Oct. 2021, Art. no. 107445.

[15] B. Chen, S.-I. Yim, H. Kim, A. Kondabathini, and R. Nuqui, "Cybersecurity of wide area monitoring, protection, and control systems for HVDC applications," *IEEE Trans. Power Syst.*, vol. 36, no. 1, pp. 592–602, Jan. 2021.

[16] N. Chockalingam, A. Chakrabortty, and A. Hussain, "Mitigating denial-of-service attacks in wide-area LQR control," in *Proc. IEEE PES Gen. Meeting*, Nov. 2016, pp. 1–5.

[17] S. Liu, I. Zenelis, Y. Li, X. Wang, Q. Li, and L. Zhu, "Markov game for securing wide-area damping control against false data injection attacks," *IEEE Syst. J.*, vol. 15, no. 1, pp. 1356–1365, Mar. 2021.

[18] M. Li and Y. Chen, "Wide-area robust sliding mode controller for power systems with false data injection attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 922–930, Mar. 2020.

[19] M. Ayar, S. Obuz, R. D. Trevizan, A. S. Bretas, and H. A. Latchman, "A distributed control approach for enhancing smart grid transient stability and resilience," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 3035–3044, Nov. 2017.

[20] W. Yao *et al.*, "Resilient wide-area damping control for inter-area oscillations to tolerate deception attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4238–4249, Sep. 2021.

[21] Y. Zhao *et al.*, "Resilient adaptive wide-area damping control to mitigate false data injection attacks," *IEEE Syst. J.*, vol. 15, no. 4, pp. 4831–4842, Dec. 2021.

[22] K. Mahapatra, M. Ashour, N. R. Chaudhuri, and C. M. Lagoa, "Malicious corruption resilience in PMU data and wide-area damping control," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 958–967, Mar. 2020.

[23] L. D. Marinovici and H. Chen, "Framework for analysis and quantification of wide-area control resilience for power systems," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 864–872, Mar. 2020.

[24] T. Ding *et al.*, "Quantifying cyber attacks on industrial MMC-HVDC control system using structured pseudospectrum," *IEEE Trans. Power Electron.*, vol. 36, no. 5, pp. 4915–4920, May 2021.

[25] X.-C. ShangGuan *et al.*, "Switching system-based load frequency control for multi-area power system resilient to denial-of-service attacks," *Control Eng. Pract.*, vol. 107, Feb. 2021, Art. no. 104678.

[26] T. Li, W. Zhang, and L. Yu, "Improved switched system approach to networked control systems with time-varying delays," *IEEE Trans. Control Syst. Technol.*, vol. 27, no. 6, pp. 2711–2717, Nov. 2019.

[27] Y. Shen, W. Zhang, H. Ni, D. Zhang, and L. Yu, "Guaranteed cost control of networked control systems with DoS attack and time-varying delay," *Int. J. Control Autom. Syst.*, vol. 17, no. 4, pp. 811–821, 2019.

[28] J. Machowski, Z. Lubosny, J. W. Bialek, and J. R. Bumby, *Power System Dynamics: Stability and Control*. Hoboken, NJ, USA: Wiley, 2020.

[29] M. G. Safonov and R. Y. Chiang, "A Schur method for balanced-truncation model reduction," *IEEE Trans. Autom. Control*, vol. 34, no. 7, pp. 729–733, Jul. 1989.

[30] W. Yao, L. Jiang, Q. H. Wu, J. Y. Wen, and S. J. Cheng, "Delay-dependent stability analysis of the power system with a wide-area damping controller embedded," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 233–240, Feb. 2011.

[31] A. K. Singh, R. Singh, and B. C. Pal, "Stability analysis of networked control in smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 381–390, Jan. 2015.

[32] A. Heniche and I. Karnwa, "Control loops selection to damp inter-area oscillations of electrical networks," *IEEE Trans. Power Syst.*, vol. 17, no. 2, pp. 378–384, May 2002.

[33] Y. Shen, W. Yao, J. Wen, H. He, and W. Chen, "Adaptive supplementary damping control of VSC-HVDC for interarea oscillation using GrHDP," *IEEE Trans. Power Syst.*, vol. 33, no. 2, pp. 1777–1789, Mar. 2018.

[34] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6816–6827, Nov. 2018.

[35] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, May 2005, pp. 46–57.

[36] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, "On a mathematical model for low-rate shrew DDoS," *IEEE Trans. Inf. Forensics Security*, vol. 9, pp. 1069–1083, 2014.

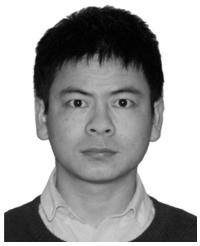
[37] J. Cheng, J. H. Park, H. R. Karimi, and H. Shen, "A flexible terminal approach to sampled-data exponentially synchronization of Markovian neural networks with time-varying delayed signals," *IEEE Trans. Cybern.*, vol. 48, no. 8, pp. 2232–2244, Aug. 2018.
[38] W. Zhang and L. Yu, "New approach to stabilisation of networked control systems with time-varying delays," *IET Control Theory Appl.*, vol. 16, no. 12, pp. 263–268, Dec. 2008.
[39] W. Yao, J. Wen, S. Cheng, and L. Jiang, "Development of a MATLAB/Simulink based power system simulation toolbox," *Power Syst. Technol.*, vol. 36, no. 6, pp. 95–101, Jun. 2012.
[40] P. Kundur, *Power System Stability and Control*. New York, NY, USA: McGrawHill, 1994.
[41] C. Li, Y. Cao, C. Duan, and K. Zhang, "A feasible delay margin sensitivity analysis method," *IEEE Trans. Power Syst.*, vol. 36, no. 3, pp. 2713–2716, May 2021.
[42] A. Bartoszewicz and A. Nowacka-Leverton, "ITAE optimal sliding modes for third-order systems with input signal and state constraints," *IEEE Trans. Autom. Control*, vol. 55, no. 8, pp. 1928–1932, Aug. 2010.

Yifan Zhao (Graduate Student Member, IEEE) received the B.S. degree in electrical engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2019, where he is currently pursuing the Ph.D. degree.

His current research interests include control and stability analysis of cyber physical power system and application of cyber security in smart grid.

Wei Yao (Senior Member, IEEE) received the B.S. and Ph.D. degrees in electrical engineering from the Huazhong University of Science and Technology (HUST), Wuhan, China, in 2004 and 2010, respectively.

He was a Postdoctoral Researcher with the Department of Power Engineering, HUST from 2010 to 2012 and a Postdoctoral Research Associate with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, U.K., from 2012 to 2014. He has been a Professor with the School of Electrical and Electronics Engineering, HUST. His current research interests include power system stability analysis and control, renewable energy, HVDC and DC Grid, and application of artificial intelligence in smart grid.



Chuan-Ke Zhang (Senior Member, IEEE) received the B.S. degree in automation and the Ph.D. degree in control science and engineering from Central South University, Changsha, China, in 2007 and 2013, respectively.

He was a Research Associate with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, U.K., from 2014 to 2016. He is currently a Professor with the School of Automation, China University of Geosciences, Wuhan, China. His current research interests include time-delay systems and power systems.

Xing-Chen Shangguan (Graduate Student Member, IEEE) received the B.S. degree in automation and the Ph.D. degree in control science and engineering from the China University of Geosciences, Wuhan, China, in 2016 and 2021, respectively.

He was a joint Ph.D. student with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, U.K., from 2018 to 2020. His current research interests include power systems, time-delay systems, and sampled-data systems.

Lin Jiang (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from the Huazhong University of Science and Technology, Wuhan, China, in 1992 and 1996, respectively, and the Ph.D. degree in electrical engineering from the University of Liverpool, Liverpool, U.K., in 2001.

He is currently working as a Reader of Electrical Engineering with the University of Liverpool. His current research interests include the optimization and control of smart grids, electrical machines, power electronics, and renewable energy.

Jinyu Wen (Member, IEEE) received the B.S. and Ph.D. degrees in electrical engineering from the Huazhong University of Science and Technology (HUST), Wuhan, China, in 1992 and 1998, respectively.

He was a visiting student from 1996 to 1997 and a Research Fellow from 2002 to 2003 with the University of Liverpool, Liverpool, U.K., and a Senior Visiting Researcher with the University of Texas at Arlington, Arlington, USA, in 2010. From 1998 to 2002, he was the Director Engineer with XJ Electric Company Ltd., China. In 2003, he joined HUST, where he is currently a Professor with the School of Electrical and Electronics Engineering. His current research interests include renewable energy integration, energy storage, multi-terminal HVDC, and power system operation and control.