A Butterfly Effect: Attack-Induced Heterogeneous Equilibrium Points of High-Voltage DC Systems

Jiazuo Hou, *Member, IEEE*, Hanchen Deng, *Graduate Student Member, IEEE*, and Jimmy Chih-Hsien Peng, *Senior Member, IEEE*

***Abstract*—High-voltage direct-current (HVDC) system plays a vital role in enabling long-distance, bulk power transfers between regions. It is intrinsically a cyber-physical system, and is vulnerable to cyber intrusions, threatening both HVDC converters and their interconnected grids. To this end, attack-induced HVDC behaviors were investigated by identifying heterogeneous equilibrium points in the cyber-attack injection space of two-terminal line-commutated converter (LCC) HVDC systems. The combined effects of both intra-station switching control and inter-station current margin control were considered. Therein, this paper derived the closed-form cyber-attack capability boundaries by identifying the worst-case scenarios regarding power imbalance, over-current, and over-voltage. Closed-form bifurcation hyperplanes were then formulated to classify non-smooth or discontinuous attack-induced equilibrium points. They showcase an attack-induced butterfly effect of HVDC systems, where *infinitesimally small cyber-attacks* across bifurcation hyperplanes trigger a chain of control malfunctions. Such outcome leads to dramatic changes in the HVDC operation status, e.g., reversals in power and voltage across HVDC. Attack-induced HVDC behaviors, including the *infinitesimal-attack-high-impact* phenomenon, were validated by establishing a hardware-in-the-loop HVDC cybersecurity testbed using a STM32F429-based cyber-attack prototype and a Real Time Digital Simulator (RTDS).**

***Index Terms*—Bifurcation, butterfly effect, cybersecurity testbed, hardware-in-the-loop, heterogeneous equilibrium points, high-voltage direct-current (HVDC), infinitesimal-attack-high-impact, switching control.**

NOMENCLATURE

α_C, α_V, α_m	firing angles of DC current control, DC voltage control, minimum firing angle control at #1 station
α	selected firing angle of intra-station coordination control at #1 station
β_C, β_V, β_m	firing angles of DC current control, DC voltage control, minimum firing angle control at #2 station; $\beta'_m := \pi - \beta_m$
β	selected firing angle of intra-station coordination control at #2 station
I_1, I_2	DC current measurement at #1 and #2 stations
I_1^*, I_2^*	DC current control reference
I_m^*	margin of inter-station coordination control
ΔI_1, ΔI_2	cyber-attack injection on DC current
$\Delta I'_1$, $\Delta I'_2$	equivalent DC current control reference under cyber-attack
$I_{1,0}$, $I_{2,0}$	consequent equilibrium point of DC current under cyber-attack
V_1, V_2	DC voltage measurement at #1 and #2 stations
V_1^*, V_2^*	DC voltage control reference
ΔV_1, ΔV_2	cyber-attack injection on DC voltage
$\Delta V'_1$, $\Delta V'_2$	equivalent DC voltage control reference under cyber-attack
$V_{1,0}$, $V_{2,0}$	consequent equilibrium point of DC voltage under cyber-attack
$\boldsymbol{y}$	a set collecting ΔI_1, ΔV_1, ΔI_2, and ΔV_2
$\boldsymbol{y}'$	a set collecting $\Delta I'_1$, $\Delta V'_1$, $\Delta I'_2$, and $\Delta V'_2$
$P_{1,0}$, $P_{2,0}$	consequent equilibrium point of DC power under cyber-attack
$k_{p,1C}$, $k_{i,1C}$	proportional-integral coefficients of DC current control at #1 station
$k_{p,1V}$, $k_{i,1V}$	proportional-integral coefficients of DC voltage control at #1 station
$k_{p,2C}$, $k_{i,2C}$	proportional-integral coefficients of DC current control at #2 station
$k_{p,2V}$, $k_{i,2V}$	proportional-integral coefficients of DC voltage control at #2 station
L_1, L_2, L	smoothing reactance at #1 and #2 stations and their sum
R_1, R_2	equivalent commutation resistance at #1 and #2 stations
R_d	resistance of DC transmission line
R	sum of R_1, R_2, and R_d
U_1, U_2	ideal no-load voltage at #1 and #2 stations
V_{a1}, V_{a2}	root-mean-square value of line-to-line grid-side AC voltage
T_1, T_2	transformer ratio
B_1, B_2	number of series-connected six-pulse converters
s	Laplace operator

Manuscript received 15 February 2024; revised 17 May 2024; accepted 27 May 2024. Date of publication 5 June 2024; date of current version 23 October 2024. This work was supported by the Singapore Ministry of Education Academic Research Fund Tier 1 under Grant A-8000214-01-00. Paper no. TSG-00254-2024. *(Corresponding author: Jimmy Chih-Hsien Peng.)*

The authors are with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore (e-mail: houjz@nus.edu.sg; e1143502@u.nus.edu; jpeng@nus.edu.sg).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2024.3409704.

Digital Object Identifier 10.1109/TSG.2024.3409704

I. INTRODUCTION

HIGH-VOLTAGE direct-current (HVDC) systems serve as the backbones for long-distance bulk power transmission [1], integration of renewable resources [2], and

interconnection of asynchronous AC grids [3]. In recent decades, the power industry has witnessed over 300 gigawatts of installed HVDC projects around the world and additional 150 gigawatts planned in the next decade [4]. The HVDC market size is estimated at 13.78 billion U.S. dollars in 2024 [5].

One main function of HVDC systems is accurately and rapidly maintaining the power balances of interconnected AC grids [6]. The high controllability of HVDC system is underpinned by its closed-loop feedback controls (e.g., DC current/voltage control), which rely on trustworthy measurements collected from metering devices and transmitted over communication networks [2]. An HVDC system is intrinsically a cyber-physical system with potential cyber vulnerabilities. General cyber-attack events in power systems have been increasingly reported [7], resulting in severe physical damages to power utilities [8]. Therein, it has been physically demonstrated that cyber-attacks could maliciously alter the measurements of HVDC converter stations [9] by compromising their sensors [10], [11], communication links [12], [13], etc. This threatens the secure operation of both HVDC converters and interconnected AC grids [14].

In response, equipment vendors [15], [16], [17] revised their security measures in accordance to the industry standards, e.g., IEC 60919 [18]. For instance, Siemens Energy [15] provided a cybersecurity service portfolio for HVDC systems to identify cyber vulnerabilities and respond to cyber incidents. One of its competitor–Hitachi Energy–supplied a HVDC cybersecurity solution to reduce vulnerabilities and remediate security gaps [16], [17]. At the same time, research in cybersecurity of HVDC systems have gained significant traction, specifically in addressing the vulnerabilities under different HVDC controls. For example, [19] proposed a rule-based cybersecurity enhancement method for the HVDC wide-area damping control in suppressing inter-area oscillations. In the context of using HVDC to provide ancillary service, [20] reported a squeeze-excitation double conventional neural network for boosting the cybersecurity of the control framework. Furthermore, an event-triggered strategy for DC power control of multi-infeed HVDC systems against non-simultaneous cyber-attacks was developed in [21]. Advancement in quantifying the impact of cyber-attack on the stability margin of HVDC systems was made in [22]. The work considered the interplay of vector current control and phase-locked loop control, providing a holistic assessment of the HVDC performance. Apart from enhancing cybersecurity in the control framework, progress was also made in the monitoring domain. For example, [9] reported the use of a Kalman filter-based method to detect cyber-attacks on the voltage measurements of a consensus-based HVDC distributed controller.

To date, most existing studies focus on the cybersecurity of one specific HVDC controller, which is only a part of the hierarchical HVDC control architecture that is jointly characterized by 1) the *intra-station coordination* of multiple closed-loop feedback controls inside each HVDC station, e.g., the 'min-max' switching control [23]; and 2) the *inter-station coordination* between two HVDC stations, e.g., the current margin control [6]. This leads to an interdependent nonlinear switching framework, which is not only illustrated in the IEC 60919 standard [18] but also widely deployed in practical HVDC projects [23].

Therefore, an intriguing question arises: *Considering the intra-station and inter-station coordination controls, how would the HVDC system behave under cyber-attacks*? This question is analogous to the *chaos theory* that focuses on the disorder and irregularities of deterministic nonlinear dynamical systems [24], e.g., the atmosphere's behaviors in weather science [25], the three-body problem in astronomy [26], the Van der Pol oscillator in radio engineering [27], etc. Generally, there are two aspects of concern: 1) the system's behaviors given certain initial inputs; and 2) the sensitive dependence on and ripple effects of initial inputs, i.e., the *butterfly effect* [25]. Similarly, we have the following research questions:

- *Attack-induced Equilibrium Points:* What would be the HVDC equilibrium points, i.e., steady-state operation points, under different cyber-attacks?
- *Worst Attack-induced Consequences:* What and when are the most damaging consequences regarding attack-induced power mismatch, over-current, and over-voltage?
- *Attack-induced Butterfly Effects:* Would a small perturbation of cyber-attack ripple out and eventually cause large differences in attack-induced outcomes?

Inspired by the chaos theory, this work investigates the attack-induced HVDC behaviors by identifying heterogeneous equilibrium points and their bifurcation hyperplanes in the cyber-attack injection space. To the best of our knowledge, this is the first time an attack-induced butterfly effect of HVDC systems is presented, where an infinitesimally small ripple of cyber-attack triggers a series of control malfunctions, leading to power and voltage reversals. The contributions are summarized as follows:

- Investigate the closed-form heterogeneous attack-induced equilibrium points for two-terminal line-commutated converter (LCC) HVDC systems. Both intra-station switching control and inter-station current margin control are addressed in the study.
- Derive the analytical cyber-attack capability boundaries considering the maximum attack-induced power surplus/deficit, the maximum/minimum attack-induced DC current/voltage, and the closed-form sufficient conditions to achieve these extreme points.
- Formulate the bifurcation hyperplanes to classify non-smooth and even discontinuous attack-induced HVDC equilibrium points. That is, catastrophic changes in the HVDC operation status, e.g., power/voltage reversals, can be triggered by an infinitesimally small cyber-attack, indicating a butterfly effect.
- Experimentally verify the proposed attack-induced HVDC behaviors by establishing a hardware-in-the-loop HVDC cybersecurity testbed. The setup is based on a STM32F429-based cyber-attack prototype and a Real Time Digital Simulator (RTDS).

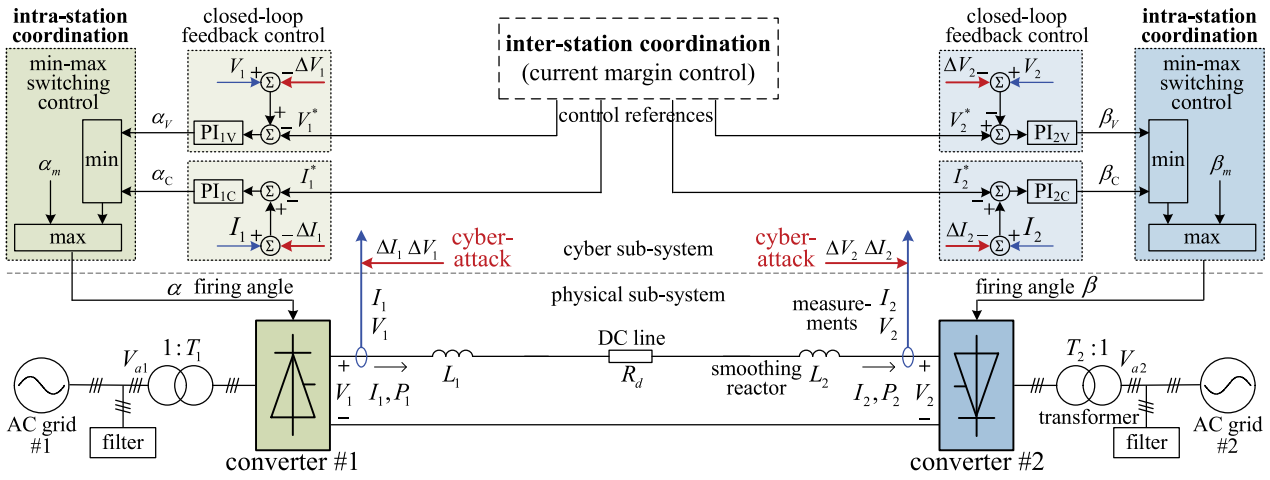


Fig. 1. A hierarchical control architecture of a two-terminal LCC HVDC transmission system with intra-station and inter-station coordination controls.

II. Attack-Induced Heterogeneous Equilibrium Points of HVDC Systems

This section investigates the attack-induced equilibrium points of HVDC systems in the cyber-attack injection space.

A. An HVDC Hierarchical Control Structure With Intra-Station and Inter-Station Coordination

A two-terminal LCC HVDC system, as shown in Fig. 1, is widely utilized for bulk power transmission between AC grid #1 and AC grid #2 via two converter stations. To accurately transmit power and maintain power balances of two AC grids, the HVDC system is operated in a hierarchical manner, including three folds [18], [23]: 1) the *closed-loop feedback control* in each station, i.e., DC current control and DC voltage control that consistently eliminate the differences between preset references (I_1^*, V_1^*, I_2^*, V_2^*) and real-time measurements (I_1, V_1, I_2, V_2); 2) the *intra-station coordination control* in each station, i.e., the switching control that strategically selects a firing angle α (or β) in station #1 (or #2) from three different controls, including α_C (or β_C) of DC current control, α_V (or β_V) of DC voltage control, and α_m (or β_m) of the minimum firing angle control; and 3) the *inter-station coordination control* between two stations, i.e., the current margin control that presets proper DC current/voltage references to construct a desired operation point. Each converter is required to function as either a rectifier for AC/DC power conversion or an inverter for DC/AC power conversion [28], whose role is interchangeable via the current margin control, leading to a reversal of power flow direction if needed [6].

B. Two Control Curves of HVDC Systems

The converter #1 (or #2) in a two-terminal LCC HVDC system can be equivalent to a Thevenin circuit with a DC voltage source $U_1\cos\alpha$ (or $U_2\cos(\pi-\beta)$) and a series-connected resistor R_1 (or R_2) [18]. R_1 and R_2 represent the equivalent commutation resistance. U_1 and U_2 represent the ideal no-load voltages:

$$U_1 = 3\sqrt{2}V_{a1}T_1B_1/\pi \tag{1}$$

$$U_2 = 3\sqrt{2}V_{a2}T_2B_2/\pi \tag{2}$$

where V_{a1} and V_{a2} represent the root-mean-square value of line-to-line AC voltage in Fig. 1. T_1 and T_2 represent the transformer ratio. B_1 and B_2 represent the number of series-connected six-pulse converters. The two Thevenin circuits are interconnected via two smoothing reactors L_1 and L_2 and a DC line resistance R_d, yielding the DC current and voltage in frequency domain [18], [23]:

$$I_1 = I_2 = (U_1\cos\alpha - U_2\cos(\pi-\beta))/(Ls+R) \tag{3}$$

$$V_1 = -I_1R_1 + U_1\cos\alpha \tag{4}$$

$$V_2 = I_2R_2 + U_2\cos(\pi-\beta) \tag{5}$$

where $R = R_1 + R_2 + R_d$ and $L = L_1 + L_2$. s denotes the Laplace operator.

As shown in Fig. 1, the DC voltage (V_1 and V_2), DC current (I_1 and I_2), and DC power ($P_1 = V_1I_1$ and $P_2 = V_2I_2$) are determined by firing angles (α and β), which are consistently and concurrently regulated by four proportional-integral (PI) controllers, i.e., $\mathrm{PI}_{1C} = k_{p,1C} + k_{i,1C}/s$, $\mathrm{PI}_{1V} = k_{p,1V} + k_{i,1V}/s$, $\mathrm{PI}_{2C} = k_{p,2C} + k_{i,2C}/s$, $\mathrm{PI}_{2V} = k_{p,2V} + k_{i,2V}/s$. Afterward, the consequent firing angles (α_C, α_V, β_C, and β_V) and the minimum firing angle (α_m and β_m) are coordinated via the switching control, i.e., the 'min-max' control selectors in each converter [18], [29]:

$$\begin{aligned}\alpha &= \max\{\alpha_m,\ \min\{\alpha_C,\ \alpha_V\}\}\\ &= \max\left\{\alpha_m,\ \min\left\{(I_1 - I_1^*)\mathrm{PI}_{1C},\ (V_1 - V_1^*)\mathrm{PI}_{1V}\right\}\right\}\end{aligned} \tag{6}$$

$$\begin{aligned}\beta &= \max\{\beta_m,\ \min\{\beta_C,\ \beta_V\}\}\\ &= \max\left\{\beta_m,\ \min\left\{(I_2 - I_2^*)\mathrm{PI}_{2C},\ (V_2^* - V_2)\mathrm{PI}_{2V}\right\}\right\}\end{aligned} \tag{7}$$

That is, the minimum firing angle limits the outputs of DC current/voltage controls. As a result, the feedback controls (PI_{1C} and PI_{1V}), the minimum firing control α_m, and their 'min-max' switching control of converter #1 in (6), jointly create a steady-state control curve in (I_1, V_1) plane in Fig. 2, including two line segments (i.e., the vertical and horizontal solid green lines) and a ray (i.e., the dashed green line). Similarly, the control curve of converter #2 in (I_2, V_2) plane includes two line segments (i.e., the vertical and horizontal solid blue lines) and a ray (i.e., the dashed blue line). Without loss of generality, we assume the desired power transmission

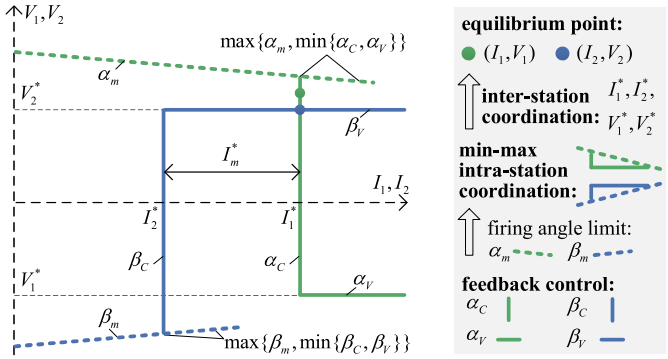


Fig. 2. Control curves and their corresponding equilibrium points of a two-terminal HVDC system in (I, V) plane in the absence of cyber-attacks.

direction in Fig. 1 is from AC grid #1 to #2. Then, the inter-station coordination control, i.e., the current margin control, sets $I_m^* = I_1^* - I_2^* > 0$, $V_1^* < 0$ and $V_2^* > 0$. Combing the control curves of two converters into the same (I, V) plane in Fig. 2, the intersection points, including the green point (I_1, V_1) and the blue point (I_2, V_2), are the equilibrium points for converter #1 and #2, respectively. That is, after presetting control references, the HVDC equilibrium point would be eventually achieved although the two converters are independently controlled and do not rely on inter-station communication, yielding a decentralized but coordinated manner.

C. Cyber-Attack Assumptions

The hierarchical control architecture of HVDC systems relies on trustworthy measurements collected by metering devices and transmitted by communication devices in real time. This is a cyber-physical system that has been physically demonstrated in [9]. Essentially, HVDC measurements can be altered via compromising the sensors [10], [11], and communication links [12], [13].

Cyber-attacks with fewer prerequisites are generally easier to launch [30]. To avoid prohibitive cyber-attack requirements, the attacks in this paper are assumed as follows:

1) *No prior knowledge* about the HVDC systems, including system parameters, network topology, control principles, etc, is required;
2) *No reading access* to the operation status of HVDC systems is required;
3) *No writing access* to control references (i.e., I_1^*, V_1^*, I_2^*, V_2^*), which are preset by the control center and transmitted to HVDC station in a top-down manner, is required;
4) *Limited writing access* to control measurements (i.e., I_1, V_1, I_2, V_2), which are consistently collected by metering devices and transmitted by communication devices in a bottom-up manner, is required.

Cyber-attacks in the form of data injections, i.e., ΔI_1, ΔV_1, ΔI_2, ΔV_2 shown in Fig. 1, can be executed by compromising communication devices, e.g., merging units [31], and communication protocols, e.g., IEC 61850 [3]. Note that the techniques for hacking the communication networks are outside the scope of this work.

D. Attack-Induced Correction of Closed-Loop Feedback Control

Let the control measurement $x \in \{I_1, V_1, I_2, V_2\}$, the control reference $x^* \in \{I_1^*, V_1^*, I_2^*, V_2^*\}$, and the cyber-attack $\Delta x \in \{\Delta I_1, \Delta V_1, \Delta I_2, \Delta V_2\}$. Let $G(s)$ represents the closed-loop transfer function between x and x^*. Since x is designed to consistently track x^* for closed-loop feedback controls, we have

$$\lim_{s\to 0} G(s) = \lim_{s\to 0} x(s)/x^*(s) = 1 \tag{8}$$

If cyber-attack Δx is added to the actual measurement x, then the on-screen measurement instantly become

$$x' = x - \Delta x \neq x^* \tag{9}$$

Mathematically, this is equivalent to a difference between the actual measurement x and a compromised reference $x^* + \Delta x$:

$$(x - \Delta x) - x^* = x - \left(x^* + \Delta x\right) \tag{10}$$

Then, the closed-loop feedback control would rapidly correct the difference within the control timescale, e.g., tens of milliseconds for DC current/voltage control [6]. Under steady-state, the resulting corrective reaction would lead to the actual measurement

$$\begin{aligned}\lim_{t\to\infty} x(t) &= \lim_{s\to 0} sx(s) = \lim_{s\to 0} sG(s)\left(x^* + \Delta x\right)/s \\ &= x^* + \Delta x\end{aligned} \tag{11}$$

while the on-screen measurement is

$$\lim_{t\to\infty} x'(t) = \lim_{s\to 0} sG(s)x^*/s = x^* \tag{12}$$

This leads to a stealthy deviation Δx between the on-screen measurement and the actual measurement under steady-state. In other words, by compromising the measurements x, the cyber-attacks Δx manage to equivalently manipulate the references x^* without having the writing access to any control references.

E. Attack-Induced Equilibrium Points of the Two-Terminal HVDC Systems

The control references $x^* + \Delta x$ determine the relative positions of two steady-state control curves as shown in Fig. 2. For instance, a positive cyber-attack ΔI_1 (or ΔI_2) would move the vertical solid green line (or the vertical solid blue line) rightward, while a negative cyber-attack would move leftward. A positive cyber-attack ΔV_1 (or ΔV_2) would move the horizontal solid green line (or the horizontal solid blue line) upward, while a negative cyber-attack would move downward. Afterward, the attack-induced deviations would possibly trigger the switching control that shifts from one feedback control to another one, leading to another system with different differential-algebraic equations and thus different equilibrium points. This threatens the secure operation of power systems [32].

Therefore, we propose the following propositions to identify the equilibrium points under various cyber-attack injections on measurements. Let $[\Delta I_1', \Delta V_1', \Delta I_2', \Delta V_2'] :=$

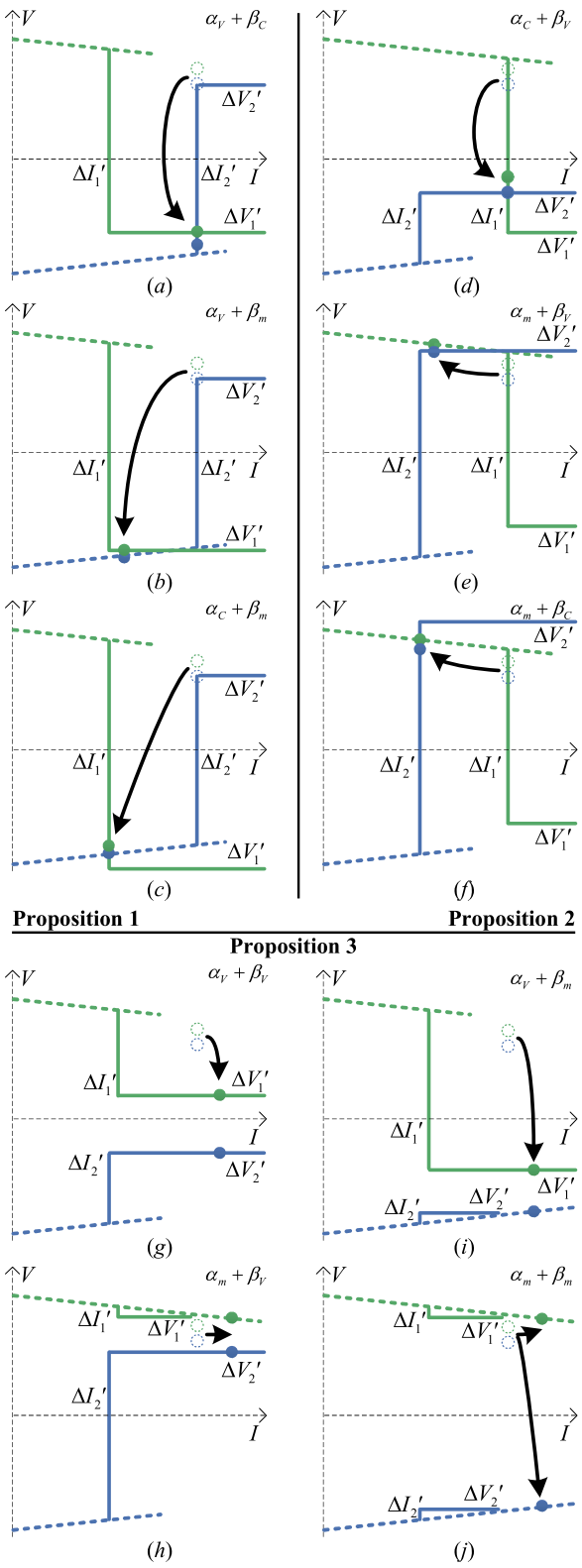


Fig. 3. Equilibrium points of HVDC systems under different cyber-attack injections. (*a*), (*b*), (*c*) correspond to equilibrium points (16), (18), (19) in Proposition 1, respectively; (*d*), (*e*), (*f*) correspond to equilibrium points (21), (23), (24) in Proposition 2, respectively; (*g*), (*h*), (*i*), (*j*) correspond to equilibrium points (27), (18), (23), (30) in Proposition 3, respectively.

$[\Delta I_1, \Delta V_1, \Delta I_2, \Delta V_2] + [I_1^*, V_1^*, I_2^*, V_2^*]$. Let $\beta_m' := \pi - \beta_m$. Let the subscript 0 denotes the equilibrium points.

Proposition 1 (Attack-induced Heterogeneous Equilibrium Points):

1) If the cyber-attacks satisfy conditions (13), (14), and (15), where

$$\Delta V_2' > \Delta V_1' \tag{13}$$
$$\Delta I_2' - \Delta I_1' > 0 \tag{14}$$
$$\Delta V_1' > \Delta I_2'(R_2 + R_d) + U_2 \cos \beta_m' \tag{15}$$

then the attack-induced equilibrium point is (16) and depicted in Fig. 3(a).

$$I_{1,0} = I_{2,0} = \Delta I_2' \tag{16a}$$
$$V_{1,0} = \Delta V_1' \tag{16b}$$
$$V_{2,0} = \Delta V_1' - \Delta I_2' R_d \tag{16c}$$

2) If the cyber-attacks violate condition (15), but satisfy conditions (13), (14), and (17), where

$$\Delta V_1' > \Delta I_1'(R_2 + R_d) + U_2 \cos \beta_m' \tag{17}$$

then the attack-induced equilibrium point is (18) and depicted in Fig. 3(*b*).

$$I_{1,0} = I_{2,0} = \frac{\Delta V_1' - U_2 \cos \beta_m'}{R_2 + R_d} \tag{18a}$$
$$\text{(16b)} \tag{18b}$$
$$V_{2,0} = \frac{\Delta V_1' R_2 + R_d U_2 \cos \beta_m'}{R_2 + R_d} \tag{18c}$$

3) If the cyber-attacks violate condition (17), but satisfy conditions (13), and (14), then the attack-induced equilibrium point is (19) and depicted in Fig. 3(*c*).

$$I_{1,0} = I_{2,0} = \Delta I_1' \tag{19a}$$
$$V_{1,0} = \Delta I_1'(R_2 + R_d) + U_2 \cos \beta_m' \tag{19b}$$
$$V_{2,0} = \Delta I_1' R_2 + U_2 \cos \beta_m' \tag{19c}$$

Proof: See the Appendix.

Proposition 2 (Attack-Induced Heterogeneous Equilibrium Points):

1) If the cyber-attacks violate condition (14), but satisfy conditions (13), and (20), where

$$\Delta V_2' < -\Delta I_1'(R_1 + R_d) + U_1 \cos \alpha_m \tag{20}$$

then the attack-induced equilibrium point is (21) and depicted in Fig. 3(*d*).

$$\text{(19a)} \tag{21a}$$
$$V_{1,0} = \Delta V_2' + \Delta I_1' R_d \tag{21b}$$
$$V_{2,0} = \Delta V_2' \tag{21c}$$

2) If the cyber-attacks violate conditions (14), and (20), but satisfy conditions (13), and (22), where

$$\Delta V_2' < -\Delta I_2'(R_1 + R_d) + U_1 \cos \alpha_m \tag{22}$$

then the attack-induced equilibrium point is (23) and depicted in Fig. 3(e).

$$I_{1,0} = I_{2,0} = \frac{-\Delta V_2' + U_1 \cos \alpha_m}{R_1 + R_d} \tag{23a}$$

$$V_{1,0} = \frac{\Delta V_2' R_1 + R_d U_1 \cos\alpha_m}{R_1 + R_d} \quad (23b)$$

(21c) (23c)

3) If the cyber-attacks violate conditions (14), and (22), but satisfy condition (13), then the attack-induced equilibrium point is (24) and depicted in Fig. 3(*f*).

(16a) (24a)

$$V_{1,0} = -\Delta I_2' R_1 + U_1 \cos\alpha_m \quad (24b)$$

$$V_{2,0} = -\Delta I_2' (R_1 + R_d) + U_1 \cos\alpha_m \quad (24c)$$

Proof: Similar to the proof of Proposition 1 in the Appendix.

Proposition 3 (Attack-Induced Heterogeneous Equilibrium Points):

1) If the cyber-attacks violate condition (13), but satisfy conditions (25), and (26), where

$$\Delta V_1'(R_1 + R_d) - \Delta V_2' R_1 < R_d U_1 \cos\alpha_m \quad (25)$$

$$\Delta V_1' R_2 - \Delta V_2'(R_2 + R_d) < -R_d U_2 \cos\beta_m' \quad (26)$$

then the attack-induced equilibrium point is (27) and depicted in Fig. 3(*g*).

$$I_{1,0} = I_{2,0} = \frac{\Delta V_1' - \Delta V_2'}{R_d} \quad (27a)$$

(16b), (21c) (27b)

2) If the cyber-attacks violate conditions (13), and (25), but satisfy condition (28), where

$$\Delta V_2' R > R_2 U_1 \cos\alpha_m + (R_1 + R_d) U_2 \cos\beta_m' \quad (28)$$

then the attack-induced equilibrium point is (18) and depicted in Fig. 3(*h*).

3) If the cyber-attacks violate conditions (13), and (26), but satisfy condition (29), where

$$\Delta V_1' R < (R_2 + R_d) U_1 \cos\alpha_m + R_1 U_2 \cos\beta_m' \quad (29)$$

then the attack-induced equilibrium point is (23) and depicted in Fig. 3(*i*).

4) If the cyber-attacks violate conditions (13), (25), and (26), then the attack-induced equilibrium point is (30) and depicted in Fig. 3(*j*).

$$I_{1,0} = I_{2,0} = \frac{U_1 \cos\alpha_m - U_2 \cos\beta_m'}{R} \quad (30a)$$

$$V_{1,0} = \frac{(R_2 + R_d) U_1 \cos\alpha_m + R_1 U_2 \cos\beta_m'}{R} \quad (30b)$$

$$V_{2,0} = \frac{R_2 U_1 \cos\alpha_m + (R_1 + R_d) U_2 \cos\beta_m'}{R} \quad (30c)$$

Proof: See the Appendix.

III. Worst Attack-Induced Equilibrium Points of HVDC Systems

This section investigates what are the worst cases and when they occur, i.e., the most damaging consequences with respect to the attack-induced power mismatch, DC current, and DC voltage.

A. Attack-Induced Power Surplus and Power Deficit

Proposition 4 (Maximum Attach-Induced Power Surplus and Power Deficit): A locally maximum value of the attack-induced power transmission from AC Grid #1 is

$$P_{1,0,\max} = (U_1 \cos\alpha_m)^2 / (4R_1) \quad (31)$$

which is achieved when 1) $\Delta I_2' = U_1 \cos\alpha_m/(2R_1)$ if the conditions of Proposition 2(*c*) are satisfied; or 2) $\Delta V_2' = (R_1 - R_d) U_1 \cos\alpha_m/(2R_1)$ if the conditions of Proposition 2(*b*) or Proposition 3(*b*) are satisfied.

A locally minimum value of the attack-induced power transmission from AC Grid #1 is

$$P_{1,0,\min} = -\left(U_2 \cos\beta_m'\right)^2 / (4(R_2 + R_d)) \quad (32)$$

which is achieved when 1) $\Delta I_1' = -U_2 \cos\beta_m'/(2(R_2 + R_d))$ if the conditions of Proposition 1(*c*) are satisfied; or 2) $\Delta V_1' = U_2 \cos\beta_m'/2$ if the conditions of Proposition 1(*b*) or Proposition 3(*c*) are satisfied.

A locally maximum value of the attack-induced power transmission into AC Grid #2 is

$$P_{2,0,\max} = (U_1 \cos\alpha_m)^2 / (4(R_1 + R_d)) \quad (33)$$

which is achieved when 1) $\Delta I_2' = U_1 \cos\alpha_m/(2(R_1 + R_d))$ if the conditions of Proposition 2(*c*) are satisfied; or 2) $\Delta V_2' = U_1 \cos\alpha_m/2$ if the conditions of Proposition 2(*b*) or Proposition 3(*b*) are satisfied.

A locally minimum value of the attack-induced power transmission into AC Grid #2 is

$$P_{2,0,\min} = -\left(U_2 \cos\beta_m'\right)^2 / (4R_2) \quad (34)$$

which is achieved when 1) $\Delta I_1' = -U_2 \cos\beta_m'/(2R_2)$ if the conditions of Proposition 1(*c*) are satisfied; or 2) $\Delta V_1' = (R_2 - R_d) U_2 \cos\beta_m'/(2R_2)$ if the conditions of Proposition 1(*b*) or Proposition 3(*c*) are satisfied.

Proof: See the Appendix.

B. Extreme Values of Attack-Induced DC Current/Voltage

The HVDC systems also need to ensure the secure operation of two converters to avoid over-current and over-voltage:

Proposition 5 (Maximum and Minimum Attack-Induced DC Current): The minimum attack-induced DC current is

$$I_{1,0,\min} = I_{2,0,\min} = 0 \quad (35)$$

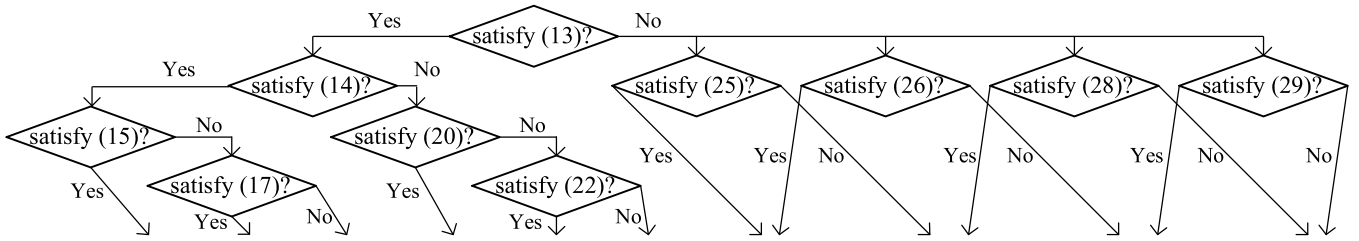
which is achieved when 1) $\Delta V_1' = U_2 \cos\beta_m'$ if the conditions of Proposition 3(*c*) are satisfied; or 2) $\Delta V_2' = U_1 \cos\alpha_m$ if the conditions of Proposition 3(*b*) are satisfied; or 3) $\Delta I_1' = 0$ if the conditions of Proposition 2(a) are satisfied; or 4) $\Delta I_2' = 0$ if the conditions of Proposition 1(a) are satisfied.

A locally maximum attack-induced DC current is (30a) if the conditions of Proposition 3(*d*) are satisfied. In addition, the maximum attack-induced DC current is

$$I_{1,0,\max} = I_{2,0,\max} = \begin{cases} \Delta I_1' \to +\infty \text{ if Proposition 1}(c) \\ \Delta I_2' \to +\infty \text{ if Proposition 2}(c) \end{cases} \quad (36)$$

Proof: See the Appendix.

By comparison, the maximum and minimum attack-induced DC voltages, e.g., $V_{2,0}$, are addressed in Proposition 6. They help to tune the over-voltage parameters for HVDC converters.



proposition	1(*a*)	1(*b*)	1(*c*)	2(*a*)	2(*b*)	2(*c*)	3(*a*)	3(*b*)	3(*c*)	3(*d*)
equilibrium point	(16) in Fig. 3(*a*)	(18) in Fig. 3(*b*)	(19) in Fig. 3(*c*)	(21) in Fig. 3(*d*)	(23) in Fig. 3(*e*)	(24) in Fig. 3(*f*)	(27) in Fig. 3(*g*)	(18) in Fig. 3(*h*)	(23) in Fig. 3(*i*)	(30) in Fig. 3(*j*)
case study in Fig. 7	RXYY′	YXZZ′	XZT	RUVV′ HED	GHEF VUWW′	IFGG′ UWP	AKC	AKMA′	CKNN′	NKMM′

Fig. 4. A tree diagram outlining the eight types of attack-induced equilibrium points classified by ten cyber-attack bifurcation hyperplanes.

Proposition 6 (Maximum and Minimum Attack-Induced DC Voltage): A locally maximum attack-induced DC voltage is

$$V_{1,0,\max} = V_{2,0,\max} = U_1 \cos \alpha_m \tag{37}$$

which is achieved when $\Delta V_2' = U_1 \cos \alpha_m$ if the conditions of Proposition 3(*b*) is satisfied.

A locally minimum attack-induced DC voltage is

$$V_{1,0,\min} = V_{2,0,\min} = U_2 \cos \beta_m' \tag{38}$$

which is achieved when $\Delta V_1' = U_2 \cos \beta_m'$ if the conditions of Proposition 3(*c*) is satisfied.

Proof: See the Appendix.

IV. Attack-Induced Butterfly Effect in HVDC Systems

This section investigates the cyber-attack bifurcation hyperplanes and an attack-induced butterfly effect of HVDC systems. Here, infinitesimally small perturbations of cyber-attacks will trigger a series of control malfunctions, and eventually lead to power and voltage reversals.

A. Cyber-Attack Bifurcation Hyperplanes

Let $\boldsymbol{y} := [\Delta I_1, \Delta V_1, \Delta I_2, \Delta V_2]^T \in \mathbb{R}^4$ and $\boldsymbol{y}' := [\Delta I_1', \Delta V_1', \Delta I_2', \Delta V_2']^T := \boldsymbol{y} + [I_1^*, V_1^*, I_2^*, V_2^*]^T \in \mathbb{R}^4$. Three convex sets are defined as follows [33]:

Definition 1: A hyperplane is a set of the form $\{\boldsymbol{x} \mid \boldsymbol{a}^T\boldsymbol{x} = b\}$. A halfspace is a set of the form $\{\boldsymbol{x} \mid \boldsymbol{a}^T\boldsymbol{x} \le b\}$. A polyhedron is a set of the form $\{\boldsymbol{x} \mid \boldsymbol{a}_i^T\boldsymbol{x} \le b_i, \forall i\}$.

According to Propositions 1 to 3, there are eight types of attack-induced equilibrium points $(I_{1,0}, V_{1,0}, I_{2,0}, V_{2,0})$, i.e., (16), (18), (19), (21), (23), (24), (27), and (30). These points manifest different qualitative properties. In other words, the attack-induced equilibrium point fails to maintain its qualitative behavior under *infinitesimally small perturbation* of cyber-attacks $\boldsymbol{y}'$ across some hyperplanes in the cyber-attack injection space $\boldsymbol{y}'$. These hyperplanes, therefore, are termed as cyber-attack bifurcation hyperplanes [34]. Note that the bifurcation hyperplanes distinguish eight types of equilibrium points that are all locally stable, while the Hopf bifurcation (or saddle-node bifurcation) distinguishes equilibrium points that are either stable or unstable as the real eigenvalue (or a pair of conjugate eigenvalues) crosses the imaginary axis of the complex plane [34].

TABLE I
Cyber-Attack Bifurcation Hyperplanes and Attack-Induced Equilibrium Points in Propositions

Propositions		**Cyber-attack bifurcation hyperplanes** $\{\boldsymbol{y}' \mid \boldsymbol{a}_i^T\boldsymbol{y}' = b_i\}$				**Attack-induced equilibrium points** $(I_{1,0}, V_{1,0}, I_{2,0}, V_{2,0})$
1	(*a*)	(13)	(14)	(15)		(16) in Fig. 3(*a*)
	(*b*)			not (15)	(17)	(18) in Fig. 3(*b*)
	(*c*)				not (17)	(19) in Fig. 3(*c*)
2	(*a*)		not (14)	(20)		(21) in Fig. 3(*d*)
	(*b*)			not (20)	(22)	(23) in Fig. 3(*e*)
	(*c*)				not (22)	(24) in Fig. 3(*f*)
3	(*a*)	not (13)	(25)	(26)		(27) in Fig. 3(*g*)
	(*b*)		not (25)	(28)		(18) in Fig. 3(*h*)
	(*c*)		(29)	not (26)		(23) in Fig. 3(*i*)
	(*d*)		not (29)	not (28)		(30) in Fig. 3(*j*)

As shown in Table I and Fig. 4, cyber-attacks $\boldsymbol{y}'$ on a two-terminal LCC HVDC system create ten cyber-attack bifurcation hyperplanes:

$$\left\{\boldsymbol{y}' \in \mathbb{R}^4 \mid \boldsymbol{a}_i^T\boldsymbol{y}' = b_i\right\},\ i = 1, 2, \ldots, 10 \tag{39}$$

They are corresponding equality versions of the inequalities, i.e., the halfspaces (13), (14), (15), (17), (20), (22), (25), (26), (28), (29), respectively:

1) $\boldsymbol{a}_1 = [0, 1, 0, -1]^T$, $b_1 = 0$;
2) $\boldsymbol{a}_2 = [1, 0, -1, 0]^T$, $b_2 = 0$;
3) $\boldsymbol{a}_3 = [0, 1, -(R_2 + R_d), 0]^T$, $b_3 = U_2 \cos \beta_m'$;
4) $\boldsymbol{a}_4 = [-(R_2 + R_d), 1, 0, 0]^T$, $b_4 = U_2 \cos \beta_m'$;
5) $\boldsymbol{a}_5 = [R_1 + R_d, 0, 0, 1]^T$, $b_5 = U_1 \cos \alpha_m$;
6) $\boldsymbol{a}_6 = [0, 0, R_1 + R_d, 1]^T$, $b_6 = U_1 \cos \alpha_m$;
7) $\boldsymbol{a}_7 = [0, R_1 + R_d, 0, -R_1]^T$, $b_7 = R_d U_1 \cos \alpha_m$;
8) $\boldsymbol{a}_8 = [0, R_2, 0, -(R_2 + R_d)]^T$, $b_8 = -R_d U_2 \cos \beta_m'$;
9) $\boldsymbol{a}_9 = [0, 0, 0, R]^T$, $b_9 = R_2 U_1 \cos \alpha_m + (R_1 + R_d) U_2 \cos \beta_m'$;
10) $\boldsymbol{a}_{10} = [0, R, 0, 0]^T$, $b_{10} = (R_2 + R_d) U_1 \cos \alpha_m + R_1 U_2 \cos \beta_m'$.

As a result, the ten halfspaces can divide a sufficiently large hyperbox $\underline{\boldsymbol{y}'} \le \boldsymbol{y}' \le \overline{\boldsymbol{y}'}$ into ten four-dimensional polyhedrons, which correspond to Fig. 3(a)-(*j*), respectively. For instance, according to Proposition 1(a), three halfspaces (13), (14), (15)

correspond to three hyperplanes $\{\boldsymbol{y}'|\boldsymbol{a}_i^T\boldsymbol{y}' = b_i, i = 1, 2, 3\}$, respectively. The three halfspaces and the hyperbox jointly create a polyhedron with an attack-induced equilibrium point (16) in Fig. 3(a). Similar formulations can be applied to Fig. 3(*b*)-(*j*).

B. Butterfly Effect Due to Discontinuous Equilibrium Points

The eight types of attack-induced equilibrium points are non-smooth or discontinuous across the ten cyber-attack bifurcation hyperplanes in the cyber-attack injection space $\boldsymbol{y}'$. For instance, the attack-induced equilibrium points (16) and (21) are classified by the bifurcation hyperplane $\{\boldsymbol{y}' \mid \Delta I_1' = \Delta I_2'\}$, leading to a typical $V_{2,0} < 0$ in (16c) and a typical $V_{2,0} > 0$ in (21c). This indicates discontinuous attack-induced steady-state DC voltage $V_{2,0}$ (i.e., a voltage reversal), and thus DC power $P_{2,0}$ (i.e., a power reversal) across this hyperplane. In the two-terminal HVDC system, the intra-station coordination control and inter-station coordination control jointly create a switching control architecture, which is mathematically a discontinuous but piecewise-smooth nonlinear system. Therefore, the discontinuous surfaces (see Fig. 7 and Fig. 8 in case study) or points (see Fig. 9 in case study) would lead to an infinite rate of change of steady-state DC voltage/power due to small cyber-attack perturbations across this hyperplane. In short, small perturbations of one or multiple cyber-attacks that slightly affect one or multiple HVDC measurements, if they are next to any of these bifurcation hyperplanes, manage to dramatically affect the whole HVDC system's properties and behaviors, showcasing a butterfly effect.

In chaos theory, the butterfly effect is characterized in two folds [25]: 1) an insignificant change in the system input triggers a chain of events that reshape the system; and 2) the insignificant input change eventually results in a significant change in the system output. Similarly, the infinitesimal-attack-high-impact phenomenon in HVDC systems can not be achieved in an instant manner due to the existence of smoothing reactors that guarantee continuous DC current. Instead, a cyber-attack perturbation across these bifurcation hyperplanes would set off a chain of control malfunctions in a cascading manner:

- Step 1 (**Intra-station Reaction**): The cyber-attack activates the corrective action of one corresponding closed-loop feedback control;
- Step 2 (**Inter-station Reaction**): Two intra-station switching controls in both two converters are triggered due to the inter-station electrical connection;
- Step 3 (**Full Reaction**): The corrective actions of all four closed-loop feedback controls are activated, leading to another trigger of multiple switching controls;
- Step 4 (**Another Equilibrium**): The HVDC system finally converges to another type of equilibrium point.

In essence, the attack-induced butterfly effect of HVDC systems is jointly created by the extrinsic cyber-attacks and the intrinsic non-linearity, including the cosine functions (4) and (5), the differential equations in PI controls and smoothing reactors (3), and the switching controls (6) and (7). Since a cyber-attack injection could be too small to differential it from regular dynamics or system contingencies, such infinitesimal-attack-high-impact phenomenon would jeopardize the HVDC systems as well as the interconnected AC grids. On this point, it would be challenging to propose corresponding cyber-defense strategies such as detection methods and mitigation methods. This is outside the scope of this work, and require a future investigation.

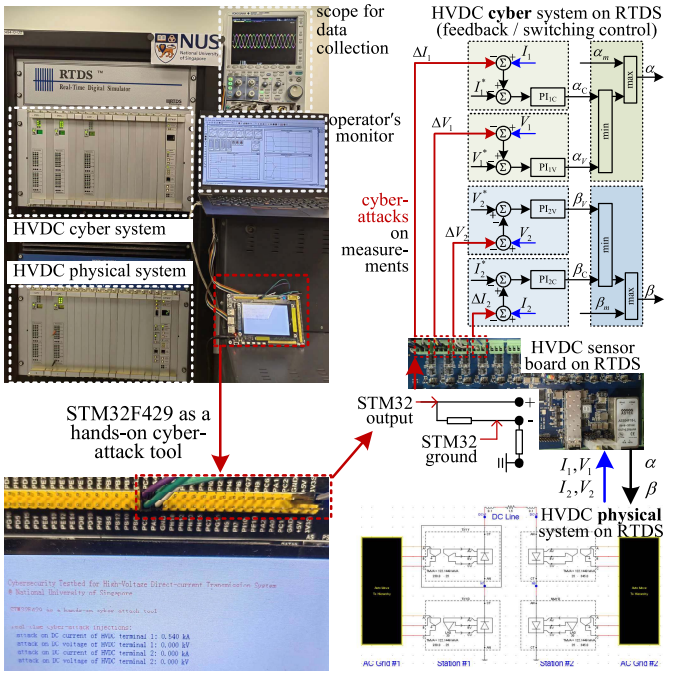


Fig. 5. A hardware-in-the-loop HVDC cybersecurity testbed using a RTDS for modeling HVDC cyber-physical systems and a STM32F429-based cyber-attack prototype for cyber-attack injections.

V. Extension to Different HVDC Systems

There are mainly two types of HVDC transmission systems: 1) the thyristor-based LCC HVDC systems with higher power and voltage ratings; and 2) the insulated gate bipolar transistors (IGBT)-based voltage-source-converter (VSC) HVDC systems with additional controllability of the reactive power. According to IEC 60919 standard [18] and IEC 62543 standard [35], both LCC HVDC and VSC HVDC systems operate in a hierarchical control architecture with inter-station coordination control. Therein, LCC HVDC system adopts the current margin control, while VSC HVDC system utilizes strategies including leader/follower control, voltage droop control, and voltage margin control. In this regard, the attack-induced behaviors of a LCC HVDC system in this study can be extended to a VSC HVDC system with consideration of its equivalent circuit, intra-station control, and inter-station control.

VI. Experimental Case Studies

A hardware-in-the-loop HVDC cybersecurity testbed is constructed to verify the cyber-attack HVDC behaviors. Referring to Fig. 5, the testbed is composed of 1) a STM32F429-based cyber-attack prototype to perform cyber-attack injections; and

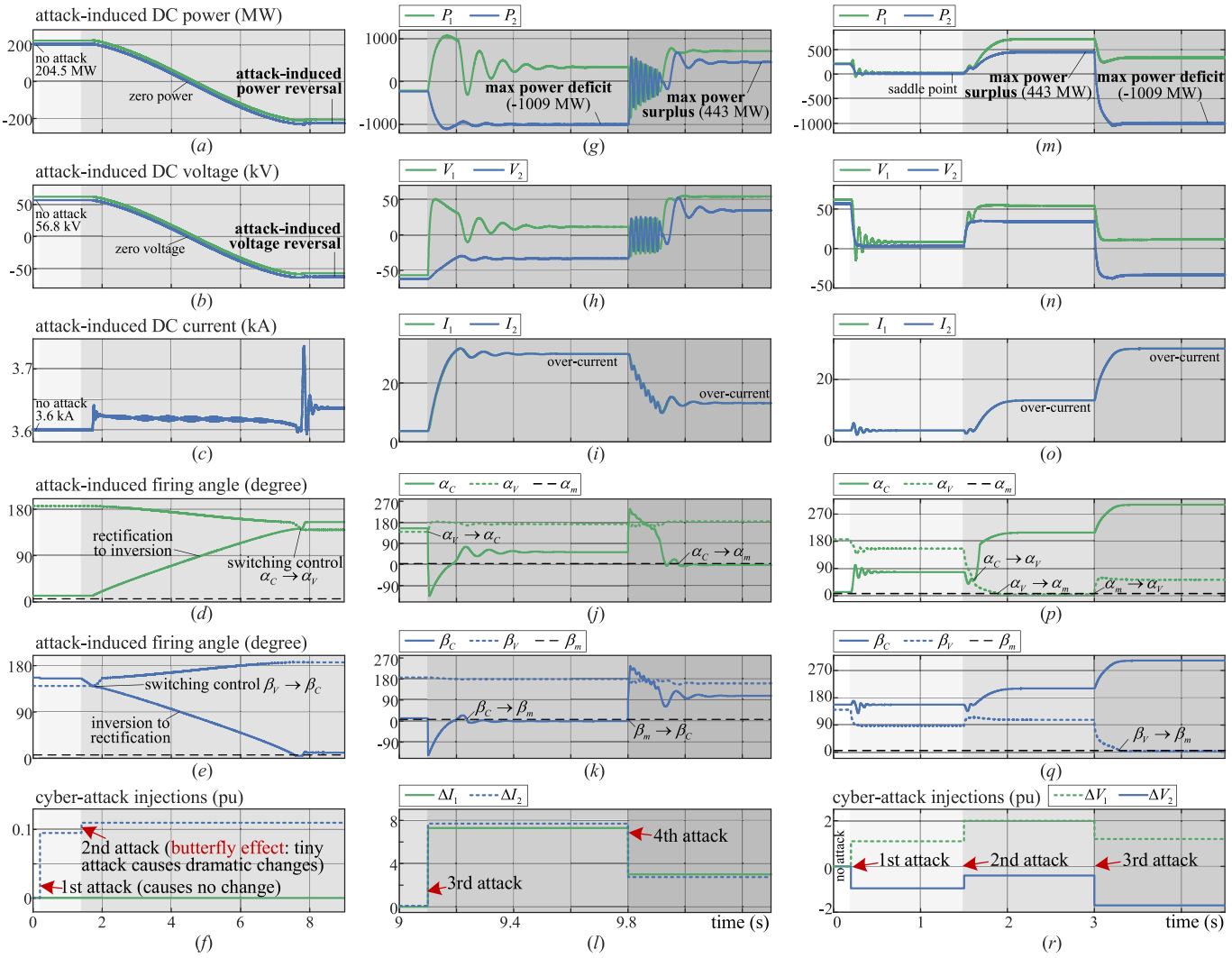


Fig. 6. Attack-induced DC power/voltage/current and firing angles. (a)-(l) with four cyber-attacks (ΔI_1, ΔI_2). (m)-(r) with three cyber-attacks (ΔV_1, ΔV_2).

2) an electromagnetic transient simulator, i.e., RTDS, for modeling HVDC cyber-physical systems.

A. A Hardware-in-the-Loop HVDC Cybersecurity Testbed

As a cyber-physical system, a two-terminal LCC HVDC system is modeled with a physical sub-system and a cyber sub-system in RTDS in Fig. 5. Referring to Fig. 1, the HVDC physical sub-system in RTDS is composed of two 12-pulse converters (i.e., two series-connected 6-pulse converters), two transformers, two smoothing reactors, two AC grids, and a DC transmission line. The HVDC cyber sub-system in RTDS consists of feedback controls (i.e., DC current/voltage controls), minimum firing angle controls, intra-station and inter-station controls as shown in Fig. 1. The control measurements I_1, V_1, I_2, and V_2 are collected and transmitted from the HVDC physical sub-system to the cyber sub-system. In addition, we design a STM32F429-based cyber-attack prototype to inject four additional measurements, i.e., ΔI_1, ΔV_1, ΔI_2, and ΔV_2. The digital-to-analog converter (DAC) at STM32F429 is programmed to output the four-channel signals, which are physically interconnected to four channels of the analog-to-digital converter (ADC) of a RTDS sensor board and then transmitted to the HVDC cyber sub-system in RTDS. As shown in Fig. 5, each analog output signal from STM32F429 needs to connect a three-terminal analog input in the RTDS sensor board.

The voltage, current, and power bases are 56.8 kV, 3.6 kA, and 204.48 MW, respectively. $V_{a1} = 230$ kV, $V_{a2} = 345$ kV, $T_1 = 25:230$, $T_2 = 25:345$, $B_1 = B_2 = 2$. This yields $U_1 = U_2 = 67.5$ kV. $R_1 = 1.05\ \Omega$, $R_2 = 1.12\ \Omega$, $R_d = 1.5\ \Omega$, $L_1 = L_2 = 0.1$ H, $\alpha_m = \beta_m = 5$ degree, $k_{p,1C} = k_{p,2C} = 45$ degree/pu, $k_{i,1C} = k_{i,2C} = 4500$ degree/s/pu, $k_{p,1V} = k_{p,2V} = 35$ degree/pu, $k_{i,1V} = k_{i,2V} = 2250$ degree/s/pu.

B. Validation of Attack-Induced HVDC Behaviors

In the absence of cyber-attacks, the original control references are $I_1^* = 1$ pu, $V_2^* = 1$ pu, $I_2 = 0.9$ pu, and $V_1^* = -1$ pu. Thus, the original equilibrium point is determined by DC current control α_C at HVDC converter #1 and DC voltage control β_V at HVDC converter #2, leading to $I_{1,0} = I_{2,0} = 1$ pu, $V_{2,0} = 1$ pu, and DC power transmission $P_{2,0} = V_{2,0}I_{2,0} = 1$ pu. The cyber-attacks are designed in two folds, including four times of DC current attack ΔI_1 and ΔI_2 in Fig. 6(a)-(l) and three times of DC voltage attack ΔV_1 and ΔV_2 in

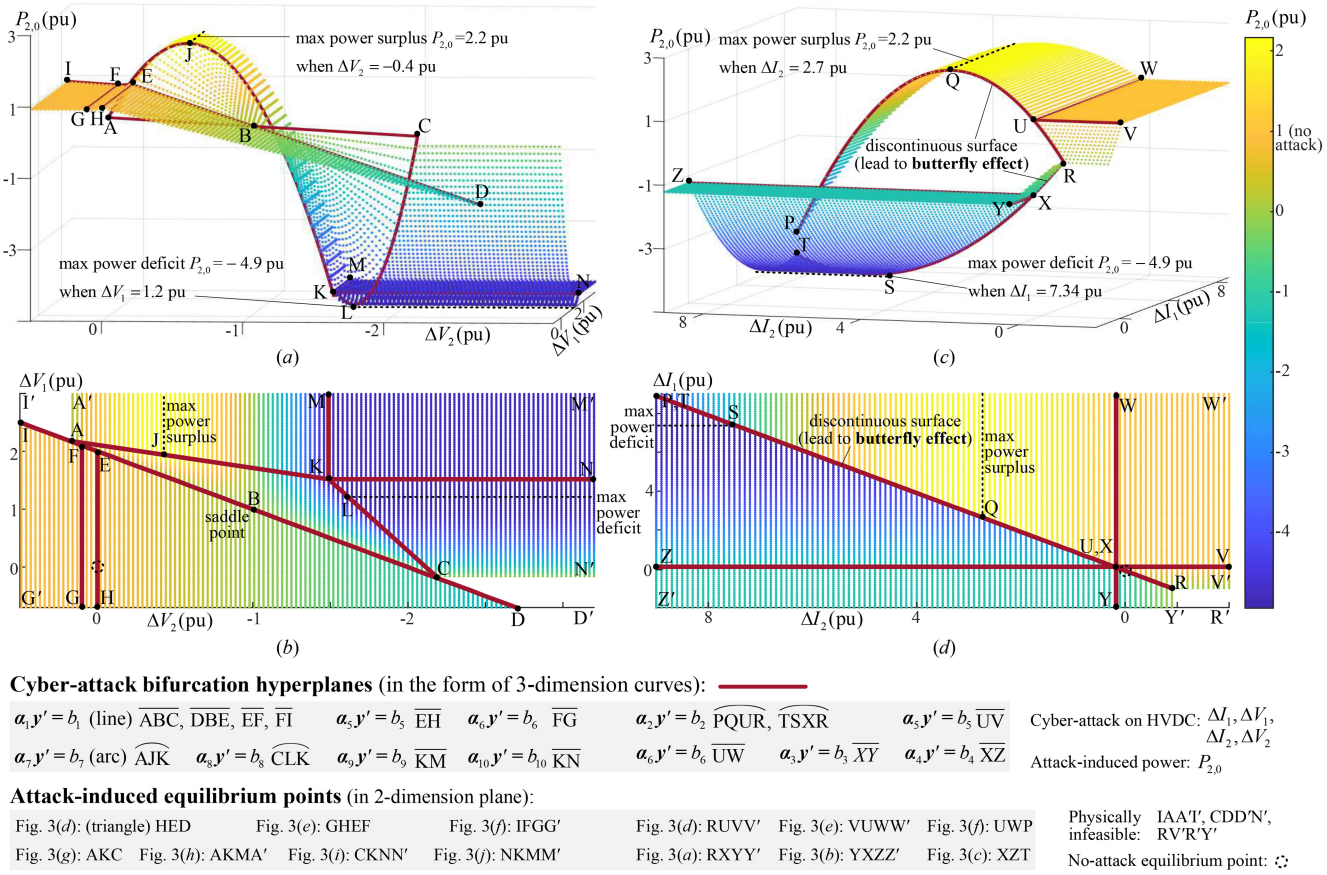


Fig. 7. Cyber-attack bifurcation hyperplanes that classify non-smooth and even discontinuous attack-induced equilibrium points of HVDC systems. (a)(*b*) in the $(\Delta V_1, \Delta V_2)$ cyber-attack injection space. (*c*)(*d*) in the $(\Delta I_1, \Delta I_2)$ cyber-attack injection space.

Fig. 6(*m*)-(*r*). Specifically, Fig. 6(*f*) indicates the cyber-attack injections of the first and the second $(\Delta I_1, \Delta I_2)$ attacks. As a result, the attack-induced DC power, DC voltage, DC current, firing angles in #1 station, and firing angles in #2 station are recorded by the testbed and depicted in Fig. 6(a)-(e), respectively. Similarly, the third and fourth $(\Delta I_1, \Delta I_2)$ cyber-attacks are performed in Fig. 6(l), leading to attack-induced HVDC behaviors in Fig. 6(*g*)-(*k*). In addition, the $(\Delta V_1, \Delta V_2)$ cyber-attacks are performed in Fig. 6(*r*), leading to attack-induced HVDC behaviors in Fig. 6(*m*)-(*q*). For brevity, the attack-induced DC voltage (or DC current) with high-order harmonics is filtered by a first-order (or second-order) filter.

The first cyber-attack in Fig. 6(*f*) is injected with $\Delta I_2 = 0.095$ pu at $t = 0.2$ s, which only causes negligible changes in β_C in Fig. 6(e) and no changes in the control modes of HVDC systems. This indicates that poorly designed cyber-attacks would not necessarily have impacts on HVDC systems. As shown in Fig. 2, $\Delta I_2 = 0.095$ pu pushes the blue vertical line rightward, but it fails to change the equilibrium points since the current margin $I_m^* = 0.1$ pu. Thus, the blue vertical line still remains on the left of the green vertical line.

In contrast, the second cyber-attack is injected at $t = 1.4$ s with additional $\Delta I_2 = 0.015$ pu as illustrated in Fig. 6(*f*). This is a tiny offset, but it sets off a series of events in a cascading manner:

1) Intra-station Reaction: The cyber-attack instantly activates corrective actions of DC current control PI_{2C} during $t = [1.40, 1.73]$ s;
2) Inter-station Reaction: The switching controls of two converters are triggered, leading to $\beta_V \to \beta_C$ at $t = 1.73$ s in Fig. 6(e) and $\alpha_C \to \alpha_V$ at $t = 7.75$ s in Fig. 6(*d*);
3) Full Reaction: The corrective actions of all the four PI controls are activated during $t = [1.73, 8]$ s;
4) Another Equilibrium: The HVDC system converges to another equilibrium point with unexpected voltage reversal and power reversal at $t = 8$ s in Fig. 6(a)(*b*).

This verifies the attack-induced butterfly effect.

Moreover, according to (34), the maximum power deficit $P_{2,0,\min} = -1009$ MW $= -4.9$ pu and is achieved when: 1) $\Delta I_1 = 7.3$ pu, i.e., the third cyber-attack in Fig. 6(*l*); or 2) $\Delta V_1 = -4.9$ pu, i.e., the second cyber-attack in Fig. 6(*r*). Similarly, according to (33), the maximum power surplus $P_{2,0,\max} = 443$ MW $= 2.2$ pu and is achieved when: 1) $\Delta I_2 = 2.7$ pu, i.e., the fourth cyber-attack in Fig. 6(*l*); or 2) $\Delta V_2 = -0.4$ pu, i.e., the third cyber-attack in Fig. 6(*r*). In addition, attack-induced over-current is observed in Fig. 6(*i*)(*o*), indicating that the HVDC system may shut down due to the damage of converters.

In summary, the second cyber-attack in Fig. 6(*a*)-(*f*) verifies the attack-induced equilibrium points in Proposition 1(*a*). The third and fourth cyber-attacks in Fig. 6(*g*)-(*l*) verify Proposition 1(*c*) and Proposition 2(*c*), respectively; The first, second, and third cyber-attacks in Fig. 6(*m*)-(*r*) verify Proposition 3(*a*), Proposition 3(*b*), and Proposition 3(*c*), respectively.

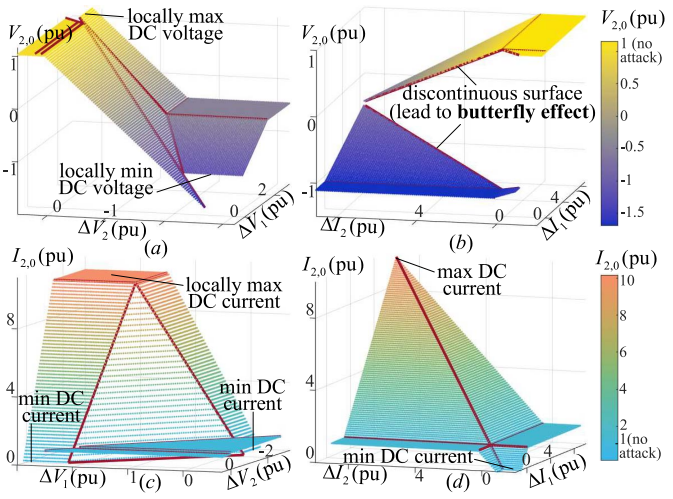


Fig. 8. Cyber-attack bifurcation hyperplanes (i.e., red solid curves) and attack-induced steady-state DC voltage and current of HVDC systems. (a)(b) attack-induced DC voltage in the $(\Delta V_1, \Delta V_2)$ and $(\Delta I_1, \Delta I_2)$ cyber-attack injection space. (c)(d) attack-induced DC current in the $(\Delta V_1, \Delta V_2)$ and $(\Delta I_1, \Delta I_2)$ cyber-attack injection space.

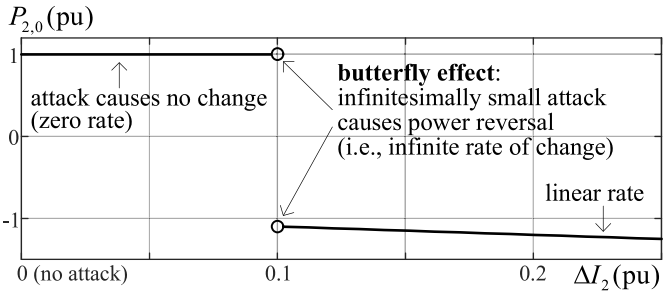


Fig. 9. Discontinuous point-induced butterfly effect, indicating that infinitesimal cyber-attacks lead to dramatic changes of HVDC equilibrium points.

C. Validation of Proposed Attack-Induced Equilibrium Points

To verify the proposed eight types of attack-induced equilibrium points and ten cyber-attack bifurcation hyperplanes, the attack-induced DC power $P_{2,0}$ is depicted in the cyber-attack injection space, i.e., $(\Delta V_1, \Delta V_2)$ in Fig. 7(a)(b) and $(\Delta I_1, \Delta I_2)$ in Fig. 7(c)(d), respectively. For instance, Fig. 7(a)(b) depict seven types of attack-induced DC power $P_{2,0}$, i.e., Fig. 3(d)-(j), which are separated by seven cyber-attack bifurcation hyperplanes $\{\boldsymbol{y}' \mid \boldsymbol{a}_i^T \boldsymbol{y}' = b_i\}$, $i = 1, 5, 6, 7, 8, 9, 10$. These 4-dimensional bifurcation hyperplanes in $\boldsymbol{y}'$ space are projected into 3-dimensional (or 2-dimensional) curves in Fig. 7(a) (or Fig. 7(b)). Note that some areas, e.g., the trapezoid CDD′N′, are physically infeasible due to the non-negative DC current constraints of LCC HVDC systems. Note that the no-attack DC power in Fig. 7 is 1 pu, whereas cyber-attacks could lead to either power surplus or power deficit.

Moreover, Fig. 7(c)(d) depict six attack-induced DC power, i.e., Fig. 3(a)-(f), which are characterized by five cyber-attack bifurcation hyperplanes $\{\boldsymbol{y}' \mid \boldsymbol{a}_i^T \boldsymbol{y}' = b_i\}$, $i = 2, 3, 4, 5, 6$. The attack-induced equilibrium points $P_{2,0}$ can be discontinuous, implying dramatic transitions of equilibrium points caused by infinitesimally small perturbations of cyber-attacks ΔI_1 and ΔI_2. This threatens the power system secure operation. For instance, if only ΔI_2 is injected while ΔI_1, ΔV_1, and ΔV_2 are fixed to zero, then Fig. 9 indicates 1) zero rate, i.e., no-impact attack; 2) infinite rate, i.e., infinitesimal-attack-high-impact phenomenon; and 3) linear rate. This property is supported by the observation from the RTDS-based HVDC cybersecurity testbed in Fig. 6. Furthermore, the zero rate in Fig. 9 demonstrates why the first cyber-attack in Fig. 6(a)-(f) fails to change the equilibrium point.

An attack-induced DC voltage $V_{2,0}$ is depicted in Fig. 8(a)(b). The discontinuous surface is also observed, implying the butterfly effect. By comparison, the attack-induced DC current $I_{2,0}$ is depicted in Fig. 8(c)(d), where the minimum $I_{2,0}$ is 0 due to the physically irreversible DC current of LCC HVDC systems [28]. On the other hand, the maximum $I_{2,0}$ is infinite as long as the cyber-attack injections are sufficiently large, which is dangerous for the HVDC operation.

VII. Conclusion

HVDC transmission system plays a critical role in bulk power delivery and renewable integration, while the intrinsic cyber-physical properties and cyber deficiencies make it vulnerable to cyber-attacks. This paper investigates the attack-induced behaviors of a two-terminal LCC HVDC system in the cyber-attack injection space. Cyber-attack bifurcation hyperplanes are characterized by classifying heterogeneous attack-induced equilibrium points. In addition, this paper identifies the attack-induced butterfly effect of HVDC systems, where minuscule perturbations will ripple out and eventually result in dramatic changes in HVDC operation status.

The proposed attack-induced HVDC behaviors have been successfully validated using a hardware-in-the-loop HVDC cybersecurity testbed, which is composed of a RTDS for modeling HVDC cyber-physical systems, and a STM32F429-based cyber-attack prototype for injecting cyber-attack on measurements. The testbed successfully showcases multiple abrupt power reversals, voltage reversals, and over-current under different cyber-attacks. In addition, the maximum attack-induced power surplus (i.e., 2.2 pu compared to the original 1 pu) and deficit (i.e., -4.9 pu compared to 1 pu) and the stationary points have been verified. More importantly, the attack-induced butterfly effect is observed when an infinitesimally small cyber-attack perturbation (e.g., $\leq$ 0.015 pu) was injected into one HVDC measurement. This is sufficient to trigger cascading control malfunctions of HVDC systems, leading to power and voltage reversals. Such an infinitesimal-attack-high-impact phenomenon threatens not only the frequency stability of interconnected AC grids, but also the secure operation of HVDC converters.

Appendix

Proofs of Propositions

Proof of Proposition 1: As shown in Fig. 2, the condition (14) indicates that the green vertical solid line is to the left of the blue vertical solid line. The condition (13) indicates that the green horizontal solid line is below the blue horizontal solid line, while the condition (15) indicates that the green

horizontal solid line is above the intersection point of the blue dashed line and the blue vertical solid line. The three conditions result in Fig. 3(a), in which the control PI_{1V} and PI_{2C} are selected for converter #1 and #2, respectively. This leads to $\alpha = \alpha_V = (V_1 - V_1^*)(k_{p,1V} + k_{i,1V}/s)$ and $\beta = \beta_C = (I_2^* - I_2)(k_{p,2C} + k_{i,2C}/s)$. Then, considering (3)-(5) and applying the steady state $s = 0$, we obtain the equilibrium point (16). Similar proofs can be applied to the equilibrium points (18) and (19). ■

Proof of Proposition 3: Let $(I_{1,0,\Delta V_1'}, \Delta V_1')$ denotes the intersection point of the green horizontal solid line and the green dashed line in Fig. 2, where $I_{1,0,\Delta V_1'} = (\Delta V_1' - U_1 \cos\alpha_m)/(-R_1)$. Let $(I_{2,0,\Delta V_2'}, \Delta V_2')$ denotes the intersection point of the blue horizontal solid line and the blue dashed line in Fig. 2, where $I_{2,0,\Delta V_2'} = (\Delta V_2' - U_2 \cos\beta_m')/R_2$. Figure 3(*g*) indicates the equilibrium point where the control PI_{1V} and PI_{2V} are selected, yielding $I_{1,0} = I_{2,0} = (\Delta V_1' - \Delta V_2')/R_d$ in (27). This equilibrium point is achieved if the vertical line $I_{1,0}$ (or $I_{2,0}$) is to the left of the two intersection points $(I_{1,0,\Delta V_1'}, \Delta V_1')$ and $(I_{2,0,\Delta V_2'}, \Delta V_2')$. Thus, we have $I_{1,0,\Delta V_1'} > I_{1,0}$ and $I_{2,0,\Delta V_2'} > I_{2,0}$, yielding (25) and (26) in Proposition 3(a). Similar proofs can be applied to Fig. 3(*h*)(*i*)(*j*) in Proposition 3(*b*)(*c*)(*d*), respectively. ■

Proof of Proposition 4: Take $P_{2,0,\max}$ as an example, according to Proposition 2(*b*) and Proposition 3(*b*), we have $P_{2,0} = \Delta V_2'(-\Delta V_2' + U_1 \cos\alpha_m)/(R_1 + R_d)$, which is a quadratic equation of $\Delta V_2'$ and has a locally maximum value (33) that is achieved at the stationary point $\Delta V_2' = U_1 \cos\alpha_m/2$. Moreover, according to Proposition 2(*c*), we have $P_{2,0} = \Delta I_2'(-\Delta I_2'(R_1+R_d)+U_1 \cos\alpha_m)$, which is a quadratic equation of $\Delta I_2'$ and has a locally maximum value (33) that is achieved at the stationary point $\Delta I_2' = U_1 \cos\alpha_m/(2(R_1+R_d))$. Similar proofs can be applied to $P_{2,0,\min}$, $P_{1,0,\max}$, and $P_{1,0,\min}$. ■

Proof of Proposition 5: Due to the physical limitation of thyristor-based LCC HVDC systems, the minimal DC current is 0 pu. This can be achieved by forcing $I_{1,0} = I_{2,0} = 0$ in (23a) of Proposition 3(*c*), or (18a) of Proposition 3(*b*), or (21a) of Proposition 2(a), or (16a) of Proposition 1(a). By comparison, the maximum attack-induced DC current could be infinite as $\Delta I_1'$ or $\Delta I_2'$ increases in Proposition 2(a) or Proposition 1(a), respectively. ■

Proof of Proposition 6: The minimal attack-induced DC current is 0 pu due to the physical limitation of LCC-based HVDC systems. Applying $I_{1,0} = I_{2,0} = 0$ into (23a) of Proposition 3(*c*) yields $V_{2,0,\max}$ in (37). Applying $I_{1,0} = I_{2,0} = 0$ into (18a) of Proposition 3(*b*) yields $V_{1,0,\max}$ in (37). Similar proof can be applied to $V_{1,0,\min}$ and $V_{2,0,\min}$ in (38). ■

ACKNOWLEDGMENT

The authors would like to thank Dr. Aram Kirakosyan with the Independent Electricity System Operator (IESO), Ontario, Canada, for the insightful suggestions regarding cyber vulnerabilities and threats in practical HVDC systems.

REFERENCES

[1] A. Alassi, S. Bañales, O. Ellabban, G. Adam, and C. MacIver, "HVDC transmission: Technology review, market trends and future outlook," *Renew. Sustain. Energy Rev.*, vol. 112, pp. 530–554, Sep. 2019.

[2] D. Roberson et al., "Improving grid resilience using high-voltage DC: Strengthening the security of power system stability," *IEEE Power Energy Mag.*, vol. 17, no. 3, pp. 38–47, May/Jun. 2019.

[3] D. Van Hertem et al., "Substations for future HVDC grids: Equipment and configurations for connection of HVDC network elements," *IEEE Power Energy Mag.*, vol. 17, no. 4, pp. 56–66, Jul./Aug. 2019.

[4] *The Operational and Market Benefits of HVDC to System Operators*, Brattle Group, Boston, MA, USA, 2023. [Online]. Available: https://www.brattle.com/wp-content/uploads/2023/09/The-Operational-and-Market-Benefits-of-HVDC-to-System-Operators-Full-Report.pdf

[5] *HVDC Transmission Market Size & Share Analysis-Growth Trends & Forecasts (2024-2029)*, Mordor Intelligence, Hyderabad, Telangana, 2024. [Online]. Available: https://www.mordorintelligence.com/industry-reports/global-hvdc-transmission-systems-market-industry

[6] V. K. Sood, *HVDC and FACTS Controllers: Applications of Static Converters in Power Systems* (Power Electronics and Power Systems). Boston, MA, USA: Springer, 2004.

[7] *Power Systems in Transition: Challenges and Opportunities Ahead for Electricity Security*, Int. Energy Agency, Paris, France, 2020. [Online]. Available: https://iea.blob.core.windows.net/assets/cd69028a-da78-4b47-b1bf-7520cdb20d70/Power_systems_in_transition.pdf

[8] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[9] C. Burgos-Mellado et al., "Cyber-attacks in modular multilevel converters," *IEEE Trans. Power Electron.*, vol. 37, no. 7, pp. 8488–8501, Jul. 2022.

[10] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks," *IEEE Trans. Circuits Syst. II*, vol. 68, no. 2, pp. 717–721, Feb. 2021.

[11] Y. Chen, W. Qiu, X. Liu, and Y. Kang, "A parallel control framework of analog proportional integral and digital model predictive controllers for enhancing power converters cybersecurity," *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 1, pp. 1258–1269, Feb. 2022.

[12] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—Challenges and vulnerabilities," *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5326–5340, Oct. 2021.

[13] Y. Wang, S. Mondal, C. Deng, K. Satpathi, Y. Xu, and S. Dasgupta, "Cyber-resilient cooperative control of bidirectional interlinking converters in networked AC/DC microgrids," *IEEE Trans. Ind. Electron.*, vol. 68, no. 10, pp. 9707–9718, Oct. 2021.

[14] E. Taherzadeh, H. Radmanesh, S. Javadi, and G. B. Gharehpetian, "Circuit breakers in HVDC systems: State-of-the-art review and future trends," *Prot. Control Modern Power Syst.*, vol. 8, no. 3, pp. 1–16, 2023.

[15] *Cyber Security for HVDC & FACTS-Cyber Security Services*, Siemens Energy, Munich, Germany, 2021. [Online]. Available: https://assets.siemens-energy.com/siemens/assets/api/uuid:2ec35f7e-6264-4c33-a857-08cfddb53d08/se-ff-en-cyber-security.pdf

[16] *Cyber Security Services HVDC and FACTS*, Hitachi Energy, Zürich, Switzerland, 2021. [Online]. Available: https://search.abb.com/library/Download.aspx?DocumentID=9AKK107680A8598&LanguageCode=en&DocumentPartId=&Action=Launch

[17] R. Nuqui, "Cyber attack resilient HVDC system (CARDS) (final scientific/technical report)," ABB Inc., Zürich, Switzerland, Rep. DE-OE0000824, 2019. [Online]. Available: https://www.osti.gov/biblio/1810571

[18] *Performance of High-Voltage Direct Current (HVDC) Systems with Line-Commutated Converters-Part-1: Steady-State Conditions*, IEC Standard TR 60919-1, 2020.

[19] Y. Zhao, W. Yao, C.-K. Zhang, X.-C. Shangguan, L. Jiang, and J. Wen, "Quantifying resilience of wide-area damping control against cyber attack based on switching system theory," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2331–2343, May 2022.

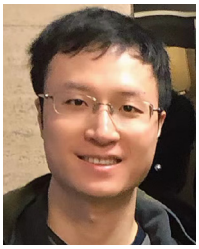
[20] K. Sun, W. Qiu, W. Yao, S. You, H. Yin, and Y. Liu, "Frequency injection based HVDC attack-defense control via squeeze-excitation double CNN," *IEEE Trans. Power Syst.*, vol. 36, no. 6, pp. 5305–5316, Nov. 2021.

[21] J. Hou, S. Lei, W. Yin, W. Sun, and Y. Hou, "Cybersecurity enhancement for multi-infeed high-voltage DC systems," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 3227–3240, Jul. 2022.

[22] 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.

[23] D. Jovcic, *High Voltage Direct Current Transmission: Converters, Systems and DC Grids*. Hoboken, NJ, USA: Wiley, 2019.

[24] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963.
[25] E. Lorenz, *The Essence of Chaos*. Seattle, WA, USA: Univ. Washington Press, 1993.
[26] I. Newton, *Philosophiae Naturalis Principia Mathematica*. Douglasville, GA, USA: G. Brookman, 1833.
[27] B. Van Der Pol and J. Van Der Mark, "Frequency demultiplication," *Nature*, vol. 120, no. 3019, pp. 363–364, Sep. 1927. [Online]. Available: https://doi.org/10.1038/120363a0
[28] P. Kundur, *Power System Stability and Control*. New York, NY, USA: McGraw-Hill, 1994.
[29] D. Liberzon, *Switching in Systems and Control*. Birkhäuser Boston, MA, USA: Springer, 2003.
[30] W.-L. Chin, C.-H. Lee, and T. Jiang, "Blind false data attacks against AC state estimation based on geometric approach in smart grid communications," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6298–6306, Nov. 2018.
[31] B. Chen, H. Kim, S.-I. Yim, A. Kondabathini, and R. F. 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.
[32] M. Muniappan, "A comprehensive review of DC fault protection methods in HVDC transmission systems," *Prot. Control Modern Power Syst.*, vol. 6, no. 1, pp. 1–20, 2021.
[33] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[34] H. K. Khalil, *Nonlinear Systems*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 1996.
[35] *High-Voltage Direct Current (HVDC) Power Transmission Using Voltage Sourced Converters (VSC)*, IEC Standard TR 62543:2011+A2:2017, 2017.



Jiazuo Hou (Member, IEEE) received the B.E. degree from Zhejiang University, China, in 2016, the M.E. degree from the Huazhong University of Science and Technology, China, in 2019, and the Ph.D. degree from The University of Hong Kong, Hong Kong, SAR, in 2023. He was a visiting Ph.D. student with Imperial College London. He is currently a Postdoctoral Research Fellow with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. His research interests include cyber–physical–social resilience, inverter-interfaced power system, and high-voltage direct-current power transmission.

Hanchen Deng (Graduate Student Member, IEEE) received the B.E. degree in communication engineering from Beijing Jiaotong University, China, in 2023, and the M.Sc. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2024, where he is currently pursuing the Ph.D. degree. His research interests include inverter-interfaced power system, stability analysis of microgrids, and signal processing.

Jimmy Chih-Hsien Peng (Senior Member, IEEE) received the B.E. and Ph.D. degrees in electrical and computer engineering from the University of Auckland, Auckland, New Zealand, in 2008 and 2012, respectively.

He is currently an Associate Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. In 2013, he was appointed as a Visiting Scientist with the Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA, USA, where he later became a Visiting Assistant Professor in 2014. His research interests include power system dynamics, inverter-based resources, and computational social science.