Vulnerability Assessments for Power-Electronics-Based Smart Grids

Jinan Zhang, Jin Ye, Lulu Guo, Fangyu Li, Wenzhan Song
School of Electrical and Computer Engineering
University of Georgia, Athens, Georgia, USA
jinan.zhang@uga.edu, jin.ye@uga.edu, lulu.guo@uga.edu, fangyu.li@uga.edu, wsong@uga.edu

***Abstract*—In this paper, a novel method is proposed to evaluate the cyber security of the power-electronics-based smart grids (PESG). The proposed method considers the performance and stability of both the individual inverter and the grid. To our knowledge, this is a first attempt to evaluate the performance and stability of PESG due to cyber attacks. We first develop impedance-based modeling and cyber-attack modeling for PESG. Then we propose innovative two security criteria to evaluate the security of PESG, including stability-based and metrics-based. For metrics-based criteria, we propose to use both total harmonic distortion (THD) and space phasor model (SPM) to evaluate the inverter performance. The simulation results with a two-inverter-based power grid verify the validity and accuracy of the proposed security evaluation method. Results have shown that the performance and stability of PESG are significantly affected by cyber attacks, and thus there is indeed a need to further study cyber security issues of PESG.**

***Index Terms*—cyber attacks, PESG, stability, impedance-based modeling, SPM, THD**

I. Introduction

As smart grids are evolving into an advanced cyber-physical system, cyber security becomes increasingly important to operators in the power grid. The high integration with the cyber system not only brings the evolution of power gird but also extends the attack surfaces and their ultimate impacts. In particular, communication technology updating offers more possibilities for the application of the Internet of Things (IoT) in a physical system. A typical example is shown in Fig.1, where a large amount of power electronics and controllers are deployed in a power grid, which is referred to as power-electronics-based smart grids (PESG) thereafter. Once hackers compromise any of the controllers in the electrical system, a series of cascaded damages will occur inevitably. For instance, in 2010, the Stuxnet worm infected supervisory control and data acquisition (SCADA) of the power system [1]. In 2015, a cyber attack made several substations disconnected to the primary grid for three hours in Ukrainian [2]. Therefore, more attention should be paid to the cyber-physical security of the smart grids.

The impacts of cyber attacks on the grid or other physical systems were studied extensively. In [3], the authors discussed the limitation of the existing security measures with consideration of cyber-infrastructure. In [4], a novel approach is proposed to evaluate the risk of cyber attack considering the dependence on cyber-infrastructure. In [5]–[7], the impact of data integrity attacks on power electronics, drive, and electric vehicles are analyzed. A novel method is proposed for system condition monitoring and fault diagnosis in a power grid in [8]. A data-driven detection method of cyber and physical attack is applied in the power grid with PVs [9].

Although the power community has been aware of the importance of grid security, cyber attacks on power electronics systems are not well studied. This paper will focus on evaluating the performance and stability of PESG under a variety of cyber attacks. To our knowledge, this is a first attempt to evaluate the performance and stability of PESG due to cyber attacks. In order to assess the vulnerability of the PESG under cyber attacks, we propose a novel evaluation methodology. The contributions are as follows: (1) Novel impact indexes are introduced to evaluate the device performance under cyber attacks. (2) An improved impedance-based method is proposed to assess device-level and system-level stability. (3) Through combining the impact indexes and stability analysis, a novel approach is proposed to evaluate PESG due to cyber attacks comprehensively.

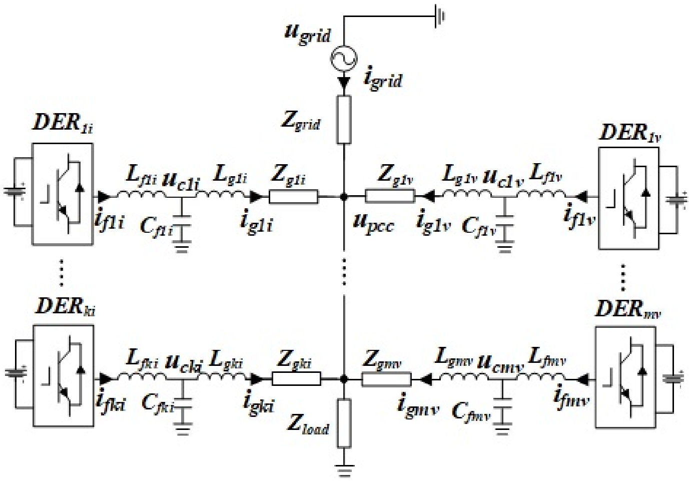

Fig. 1. A power electronics based Smart Grids

II. Power Electronics based Smart Grids (PESG) And Cyber Attack Modeling

In general, to connect distributed energy resources (DER) to the grid, DC/AC inverters work as interfaces. Voltage source inverters (VSIs) and current source inverters (CSIs) are considered as standard interfaces that connect DERs to the grid. DER models based on VSIs and CSIs are introduced respectively in the following section. As shown in Fig. 1, DC voltage represents a solar panel, a wind turbine, or other DERs, providing a DC voltage. Variable symbols description are shown in TABLE I.

TABLE I
NOMENCLATURE

Symbol	Description
DER_{ki}	kth DER is modeled as CSI
DER_{mv}	mth DER is modeled as VSI
L_{fki}	Inverter side inductance in DER_{ki}
C_{fki}	Capacitor in DER_{ki}
L_{gki}	Grid side inductance in DER_{ki}
Z_{gki}	Impedance connecting DER_{ki} to grid
L_{fmv}	Inverter side inductance in DER_{mv}
C_{fmv}	Capacitor in DER_{mv}
L_{gmv}	Grid side inductance in DER_{mv}
Z_{gmv}	Impedance connecting DER_{mv} to grid
Z_{mvv}	Virtual impedance in controller of DER_{mv}
i_{fki}	Inverter-side current in DER_{ki}
u_{cki}	Filter capacitor voltage in DER_{ki}
i_{gki}	Grid-side current in DER_{ki}
i_{fmv}	Inverter-side current in DER_{mv}
u_{cmv}	Filter capacitor voltage in DER_{mv}
i_{gmv}	Grid-side current in DER_{mv}
$i_{fkd,qi}$	i_{fki} in d-q frame
$i^*_{fkd,qi}$	$i_{fkd,qi}$ reference in controller
$i_{gkd,qi}$	i_{gki} in d-q frame
$u_{kd,qi}$	PCC voltage of DER_{ki} in d-q frame
$u^*_{rmd,qv}$	Voltage reference generated by droop control loop
$u_{cmd,qv}$	u_{cmv} in d-q frame
$u^*_{cmd,qv}$	$u_{cmd,qv}$ reference in controller
$i_{fmd,qv}$	i_{fmv} in d-q frame
$i^*_{fmd,qv}$	$i_{fmd,qv}$ reference in controller
$i_{gmd,qv}$	i_{gmv} in d-q frame
$u_{md,qv}$	PCC voltage of DER_{mv} in d-q frame
$u_{mvd,qv}$	virtual impedance voltage droop of DER_{mv} in d-q frame

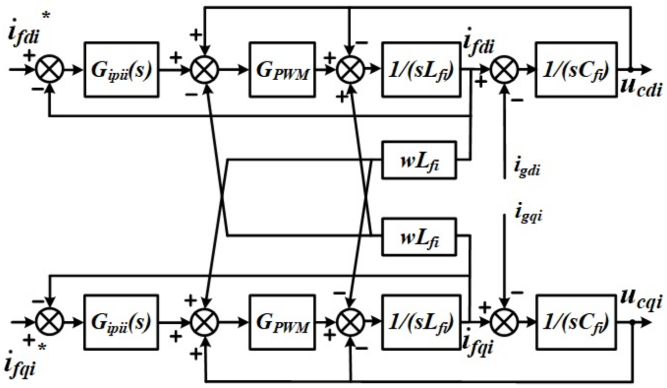

Fig. 2. Current control loop in the CSI

A. Impedance-based Modeling for CSI

To clearly demonstrate, letter k is overlooked in the derivation in CSI. Fig. 2 illustrates current control loop in the CSI. $i^*_{fd,qi}$ comes from outer power control loop in inverter controller.

$$\begin{bmatrix} i_{fdi} \\ i_{fqi} \end{bmatrix} = G_{ii}(s) \begin{bmatrix} i^*_{fdi} \\ i^*_{fqi} \end{bmatrix} \tag{1}$$

$$G_{ii}(s) = \frac{G_{ipii}(s)G_{ipi}(s)G_{PWM}(s)}{1 + G_{ipii}(s)G_{ipi}(s)G_{PWM}(s)}, \tag{2}$$

where $G_{ipii} = k_{ipi} + k_{iii}/s$, $G_{ipi} = 1/(sL_{fi})$. G_{ii} is closed transfer function. PWM is used to generate a control signal to the inverter so that the inverter produces a voltage that is the same as the controller output voltage. Thus, G_{PWM} represents inverter and PWM, which is assumed as one here. Then, grid side current can be calculated as,

$$\begin{bmatrix} i_{gdi} \\ i_{gqi} \end{bmatrix} = G_{ii}(s) \begin{bmatrix} i^*_{fdi} \\ i^*_{fqi} \end{bmatrix} - Y_{oi}(s) \begin{bmatrix} u_{cdi} \\ u_{cqi} \end{bmatrix} \tag{3}$$

$$Y_{oi}(s) = \begin{bmatrix} s * C_{fi} & -\omega * C_{fi} \\ \omega * C_{fi} & s * C_{fi} \end{bmatrix} \tag{4}$$

Based on grid side feeder impedance, the $i_{gd,qi}$ is also calculated as

$$\begin{bmatrix} i_{gdi} \\ i_{gqi} \end{bmatrix} = \frac{Z_{oi}(s)G_{ii}(s)}{Z_{oi}(s) + Z_{gi}(s)} \begin{bmatrix} i^*_{fdi} \\ i^*_{fqi} \end{bmatrix} - \frac{I_{2*2}}{Z_{oi}(s) + Z_{gi}(s)} \begin{bmatrix} u_{di} \\ u_{qi} \end{bmatrix} \tag{5}$$

$$Z_{gi}(s) = \begin{bmatrix} R_{gi} + s * L_{gi} & -\omega * L_{gi} \\ \omega * L_{gi} & R_{gi} + s * L_{gi} \end{bmatrix} \tag{6}$$

where $Z_{oi} = I_{2*2}/Y_{oi}$, I_{2*2} is an identity matrix.

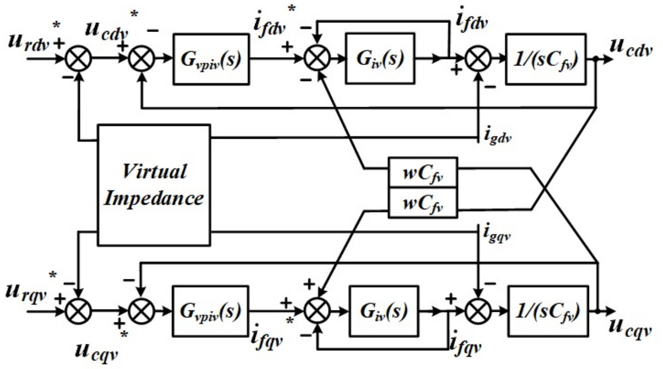

Fig. 3. Voltage and current control loop in the VSI

B. Impedance-based Modeling for VSI

Fig. 3 shows the inner voltage and current loops in the VSI. To clearly express, letter m is overlooked in the derivation. The u^*_{rdv} and u^*_{rqv} come from the droop control loop. This droop control loop is to realize active power-frequency and reactive power-voltage control method, which is derived as

$$\begin{aligned} \omega &= \omega_0 + k_p(P_0 - P) \\ E &= E_0 + k_q(Q_0 - Q) \end{aligned} \tag{7}$$

Where ω is frequency reference and E is voltage magnitude reference, ω_0 and E_0 are the nominal frequency and voltage, P and Q are the instantaneous active power and reactive power, P_0 and Q_0 is the power reference. To decouple the active and reactive power, virtual impedance is brought into the voltage control loop. The virtual makes inverter output impedance more inductive. The virtual impedance voltage drop is calculated as

$$\begin{bmatrix} u_{vdv} \\ u_{vqv} \end{bmatrix} = \begin{bmatrix} R_v + s * L_v & -\omega * L_v \\ \omega * L_v & R_v + s * L_v \end{bmatrix} \begin{bmatrix} i_{gdv} \\ i_{gqv} \end{bmatrix} \quad (8)$$

$$Z_v(s) = \begin{bmatrix} R_v + s * L_v & -\omega * L_v \\ \omega * L_v & R_v + s * L_v \end{bmatrix} \quad (9)$$

where the R_v and L_v are the virtual resistance and inductance. Then, u^*_{rdv} and u^*_{rqv} can be expressed as

$$\begin{bmatrix} u^*_{rdv} \\ u^*_{rqv} \end{bmatrix} = \begin{bmatrix} u^*_{cdv} \\ u^*_{cqv} \end{bmatrix} + \begin{bmatrix} u_{vdv} \\ u_{vqv} \end{bmatrix} \quad (10)$$

According to the Fig. 3, $G_{iv}(s)$ is the closed-loop transfer function of current control loop in VSI, which is derived as

$$G_{iv}(s) = \frac{G_{ipiv}(s) G_{ipv}(s) G_{PWM}(s)}{1 + G_{ipiv}(s) G_{ipv}(s) G_{PWM}(s)} \quad (11)$$

where $G_{ipiv} = k_{ipv} + k_{iiv}/s$, $G_{ipv} = 1/(sL_{fv})$, G_{PWM}=1. Thus, the closed-loop transfer function of current control loop is shown as,

$$G_{vv}(s) = \frac{G_{vpiv}(s) G_{vpv}(s) G_{iv}(s)}{1 + G_{vpiv}(s) G_{vpv}(s) G_{iv}(s)} \quad (12)$$

where $G_{vpiv} = k_{vpv} + k_{viv}/s$, $G_{vpv} = 1/(sC_{fv})$. The u_{cdv} and u_{cqv} can be calculated as,

$$\begin{bmatrix} u_{cdv} \\ u_{cqv} \end{bmatrix} = G_{vv}(s) \begin{bmatrix} u^*_{cdv} \\ u^*_{cqv} \end{bmatrix} - \begin{bmatrix} Z_{outv}(s) & 0 \\ 0 & Z_{outv}(s) \end{bmatrix} \begin{bmatrix} i_{gdv} \\ i_{gqv} \end{bmatrix} \quad (13)$$

$$Z_{ov}(s) = \begin{bmatrix} Z_{outv}(s) & 0 \\ 0 & Z_{outv}(s) \end{bmatrix} \quad (14)$$

$$Z_{outv}(s) = \frac{G_{vpv}(s)}{1 + G_{vpiv}(s) G_{vpv}(s) G_{iv}(s)} \quad (15)$$

Considering the virtual impedance voltage drop, the inverter output voltage is derived as,

$$\begin{bmatrix} u_{cdv} \\ u_{cqv} \end{bmatrix} = G_{vv}(s) \begin{bmatrix} u^*_{rdv} \\ u^*_{rqv} \end{bmatrix} - (G_{vv}(s) Z_v(s) + Z_{ov}(s)) \begin{bmatrix} i_{gdv} \\ i_{gqv} \end{bmatrix} \quad (16)$$

$$Z_{ovv} = G_{vv}(s) Z_v(s) + Z_{ov}(s) \quad (17)$$

Also, the PCC(Point of Common coupling) voltage is obtained considering the Z_{gv} voltage drop as following equations.

$$\begin{bmatrix} u_{dv} \\ u_{qv} \end{bmatrix} = G_{vv}(s) \begin{bmatrix} u^*_{rdv} \\ u^*_{rqv} \end{bmatrix} - (Z_{ovv}(s) + Z_{gv}(s)) \begin{bmatrix} i_{gdv} \\ i_{gqv} \end{bmatrix} \quad (18)$$

$$Z_{gv}(s) = \begin{bmatrix} R_{gv} + s * L_{gv} & -\omega * L_{gv} \\ \omega * L_{gv} & R_{gv} + s * L_{gv} \end{bmatrix} \quad (19)$$

C. Cyber Attack Modeling for PESG

To analyze the impact of cyber attack, we consider two types of cyber attacks in this paper. The attack model considers power electronics controllers being hijacked directly, including parameter modification, fake measurement, and attack duration time. For clear description, we denote the cyber attacks as,

$$\begin{aligned} \hat{p}(t) &= \gamma p(t), \quad t \in T_{attack} \\ \hat{y}(t) &= \alpha y(t), \quad t \in T_{attack} \end{aligned} \quad (20)$$

where p and $\hat{p}$ represent the power electronics parameter and modified parameter; y and $\hat{y}$ are the measurements and fake measurements, respectively; $T_{attack} = [T_0, T_0 + T]$; γ and α can be greater or smaller than 1.

III. Proposed Two-step Cyber Security Criteria for PESG

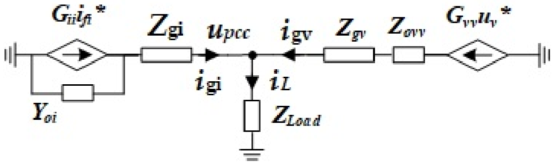

Fig. 4. Impedance model of a PESG

In this section, we propose innovative two security criteria to evaluate the performance and stability of PESG due to a variety of cyber attacks. To clearly illustrate the methodology, a impedance model of PESG is shown in Fig. 4.

A. Stability-based Cyber Security Criteria

To analyze the impact of the cyber attack on the whole system, two stability methodologies are proposed to access the operation status of this PESG in this section.

1) Impedance-based stability criteria: As discussed in the above section, the PESG impedance model in Fig. 4 can be derived as,

$$\begin{bmatrix} i_{gd,qv} \\ i_{gd,qi} \\ i_{loadd,q} \end{bmatrix} = G_n \begin{bmatrix} u^*_{rd,qv} \\ i^*_{fd,qi} \\ 0 \end{bmatrix} - Z_n u_{pccd,q} \quad (21)$$

$$G_n = \begin{bmatrix} \frac{G_{vv}}{Z_{ovv}(s) + Z_{gv}(s)} & 0 & 0 \\ 0 & \frac{Z_{oi} G_{ii}}{Z_{oi}(s) + Z_{gi}(s)} & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad (22)$$

$$Z_n = \begin{bmatrix} \frac{I_{2*2}}{Z_{ovv}(s) + Z_{gv}(s)} \\ \frac{I_{2*2}}{Z_{oi}(s) + Z_{gi}(s)} \\ -\frac{I_{2*2}}{Z_{Load}(s)} \end{bmatrix} \quad (23)$$

Based on Kirchoff's circuit laws, voltage at node PCC is expressed as,

$$u_{pccd,q} = G_{im} \begin{bmatrix} \frac{G_{vv}}{Z_{ovv}(s) + Z_{gv}(s)} \\ \frac{Z_{oi} G_{ii}}{Z_{oi}(s) + Z_{gi}(s)} \end{bmatrix}^T \begin{bmatrix} u^*_{rd,qv} \\ i^*_{fd,qi} \end{bmatrix} \quad (24)$$

$$G_{im} = (\frac{I_{2*2}}{Z_{Load}(s)} + \frac{I_{2*2}}{Z_{oi}(s) + Z_{gi}(s)} + \frac{I_{2*2}}{Z_{ovv}(s) + Z_{gv}(s)})^{-1} \tag{25}$$

The current in different branch can be calculate using equation (21), thus $i_{loadd,q}$ is derived as,

$$i_{loadd,q} = \frac{T_m}{I + T_m}\left(\frac{G_{vv}(s)u^*_{rd,qv}}{Z_{ovv}(s) + Z_{gv}(s)} + \frac{Z_{oi}(s)G_{ii}(s)i^*_{fd,qi}}{Z_{oi}(s) + Z_{gi}(s)}\right) \tag{26}$$

$$T_m = \frac{I_{2*2}}{Z_{Load}(s)} / \left(\frac{I_{2*2}}{Z_{oi}(s) + Z_{gi}(s)} + \frac{I_{2*2}}{Z_{ovv}(s) + Z_{gv}(s)}\right) \tag{27}$$

where $\frac{T_m}{1+T_m}$ can be defined as a small loop gain to assess the system stability with Nyquist stability criterion (NSC). By applying the NSC to the impedance ratio T_m that can be expressed as

$$P(T_m) - N_{-1,j0}(T_m) = 0 \tag{28}$$

We can assess the system stability. Here $P(\cdot)$ denotes the numbers of RHP (Right Half Plane) poles, and $N_{-1,j}(\cdot)$ is the number of the times the Nyquist trajectory encircles the critical points (-1, j0) in the anti-clockwise direction [10]. If the NSC criterion can be satisfied, the system is considered to be stable.

However, during a cyber attack, some parameters in the inverter controller are maliciously modified, thus modifying both the closed-loop transfer function and output impedance, especially in the VSI. Specifically, if T_m alone is used to assess the stability of the system, some poles in the transfer function could be overlooked. Therefore, to evaluate the stability under a cyber attack, we calculate the poles of the closed-loop transfer function of the controller in advance.

2) Small signal stability criteria: To evaluate the system level, the small-signal stability evaluation method is used in this section. VSI's capacitor voltage and CSI's inductance current is denoted as following,

$$\begin{bmatrix} u_{cd,qv} \\ i_{gd,qi} \end{bmatrix} = G_c \begin{bmatrix} u^*_{rd,qv} \\ i^*_{fd,qi} \end{bmatrix} + Z_c u_{pccd,q} \tag{29}$$

$$G_c = \begin{bmatrix} \frac{Z_{gv}(s)G_{vv}(s)}{Z_{ovv}(s)+Z_{gv}(s)} & 0 \\ 0 & \frac{Z_{oi}(s)G_{ii}(s)}{Z_{oi}(s)+Z_{gi}(s)} \end{bmatrix} \tag{30}$$

$$Z_c = \begin{bmatrix} \frac{Z_{ovv}(s)}{Z_{ovv}(s)+Z_{gv}(s)} \\ -\frac{I_{2*2}}{Z_{oi}(s)+Z_{gi}(s)} \end{bmatrix} \tag{31}$$

Accoring to equation (24), (29) is manipulated as,

$$\begin{bmatrix} u_{cd,qv} \\ i_{gd,qi} \end{bmatrix} = (G_c + Zc \begin{bmatrix} \frac{G_{im}G_{vv}}{Z_{ovv}(s)+Z_{gv}(s)} \\ \frac{G_{im}Z_{oi}G_{ii}}{Z_{oi}(s)+Z_{gi}(s)} \end{bmatrix}^T) \begin{bmatrix} u^*_{rd,qv} \\ i^*_{fd,qi} \end{bmatrix} \tag{32}$$

Generally, the small signal model of the PESG is derived as,

$$\begin{bmatrix} \Delta u_{cd,qv} \\ \Delta i_{gd,qi} \end{bmatrix} = (G_c + Z_c H) \begin{bmatrix} \Delta u^*_{rd,qv} \\ \Delta i^*_{fd,qi} \end{bmatrix} \tag{33}$$

where $H = [\frac{G_{im}G_{vv}}{Z_{ovv}(s)+Z_{gv}(s)} \frac{G_{im}Z_{oi}G_{ii}}{Z_{oi}(s)+Z_{gi}(s)}]$. The eigenvalues of closed transfer function matrix $G_{clm} = G_c + Z_c H$ can access the stability of whole system. Once anyone of eigenvalues shift to RHP, the grid is not stable.

B. Index-based Cyber Security Criteria

Io order to offer an insight into the impact of a cyber attack on the PESG, we propose to use the total harmonic distortion (THD), which indicates the current harmonics caused by the attack. The index can be expressed as

$$THD_i = \sqrt{[I^2_{i2} + ... + I^2_{in}]/I^2_{i1}}, \tag{34}$$

where $I_1 ... I_n$ are the amplitudes of the phase current in frequency domain, and I_n is current amplitude of the nth harmonic [11]. Generally, THD_i should be less than 5%.

The space phasor model (SPM) is proposed as a supplement of the THD. This index shows unbalance and distortion of voltage in the grid, which is derived by

$$SPM_u = |2(V_a + aV_b + a^2V_c)/3| \tag{35}$$

where $a = e^{j2\pi/3}$, and the absolute value of SPM_u is around 1 pu. Here, it takes 10% margin for harmonic distortion and voltage magnitude variations. To describe the characteristic of the inverter performance, we calculate THD_i and SPM_u according to the different periods, such as normal (before an attack), attack, and after the attack.

IV. Simulation Results

As shown in Fig. 4, for a PESG developed in the MATLAB, the simulation is conducted to assess system stability and security under cyber attacks. Table II shows parameters of inverters in the PESG. Here, cyber attacks on the VSI's inverter controller and sensors are analyzed, which causes unexpected performance degradation at both the inverter and the system levels. Fig. 5 illustrates grid voltage u_{pcc} and load current i_{load} in normal condition.

TABLE II
INVERTER PARAMETER

Parameter	Symbol	Value
DC voltage	V_{DC}	900
Droop coefficients in VSI	k_p, k_p	0.00157, 0.0076
Virtual Impedance in VSI	R_v, L_v	2, 30mH
Voltage Loop PI in VSI	k_{vpv}, k_{viv}	0.015, 10
Current Loop PI in VSI	k_{ipv}, k_{iiv}	70, 400
Power Loop PI in CSI	k_{ppi}, k_{pii}	0.005, 0.1
Current Loop PI in CSI	k_{ipi}, k_{iii}	70, 400
Inverter side inductance in VSI	L_{fv}, R_{fv}	8mH, 0.3Ω
Grid side inductance in VSI	L_{gv}, R_{gv}	11mH, 2.5Ω
Capacitor in VSI and CSI	C_{fv}, C_{fi}	$4.7\mu F$
Inverter side inductance in CSI	L_{fi}, R_{fi}	8mH, 0.3Ω
Grid side inductance in CSI	L_{gi}, R_{gi}	10mH, 2.4Ω

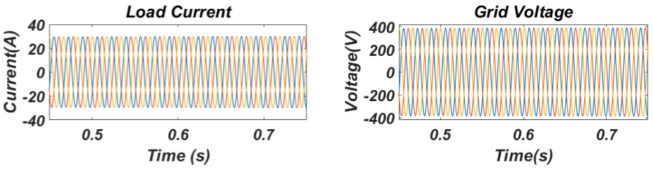

Fig. 5. Grid Voltage and Load Current

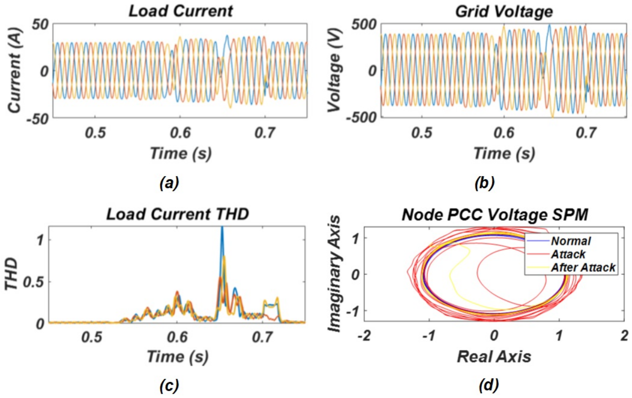

Fig. 6. i_{load}, u_{pcc}, THD and SPM in Case 1

A. Case 1

A cyber attack occurs at VSI's controller. The proportion parameter in PI controller is modified from 70 to 0.7, which can be represented by $\hat{p} = 0.01p, T_{attack} = 0.5 - 0.7s$. Fig. 6 shows load current i_{load} and PCC node voltage u_{pcc}. It can be observed that voltage and current deflect their normal status. There is a tremendous increase in THD in Fig. 6(c). Also, voltage SPM illustrates the voltage performance during the attack. In Fig. 6(d), the blue, red, and yellow trajectories represent three different periods of voltage distortion, which is before-attack (normal), attack, and after-attack, respectively. The normal current is the blue cycle, a unit cycle. When a cyber attack occurs, the blue cycle turns into a red cycle, in which a deviation is generated. When the attack stops, the red cycle becomes yellow, which means the system recovers to normal conditions. Because it takes a little time for the system to restore, the yellow one is not a standard unit circle. Based on the distorted current and voltage, it can be speculated that the inverter controller might be unstable due to this cyber attack.

To evaluate system status, both impedance-based and small-signal stability methods are applied. Figs. 7 (a,b) are the Nyquist plot and pole-zero map of a small loop gain T_m. Obviously, discrepancy between $P(T_m)$ and $N_{-1,j0}(T_m)$ equals two, which means the system is unstable. Also, there are several eigenvalues of closed transfer matrix G_{clm} shift to the RHP in Fig. 7(c). To figure out the cause of the instability operation status, the pole-zero map of the closed transfer function of VSI's controller is drawn in Fig. 7(d), which concludes that VSI's controller is destroyed due to cyber attacks.

B. Case 2

A cyber attack compromises VSI's controller sensor. The inductance current $i_f(t)$ is changed into a fake one, $\hat{i_f}$, expressed as $\hat{y} = 0.1y$, $T_{attack} = 0.5 - 0.7s$. Fig. 8(a,b) shows the load current i_{load} and node PCC voltage u_{pcc}. Both i_{load} and u_{pcc} deviate from their normal waveform due to the wrong measurement. Fig. 8(c,d) describes the distortion degree of load current and grid voltage. Impedance-based and small signal stability methods are applied to evaluate system status. The difference between $P(T_m)$ and $N_{-1,j0}(T_m)$ is obtained easily from Fig. 9 (a,c). Thus, the system is unstable because $P(T_m) - N_{-1,j0}(T_m) = 2$. The same conclusion is also made from Fig. 9(c), in which several eigenvalues of G_{clm} move to RHP.

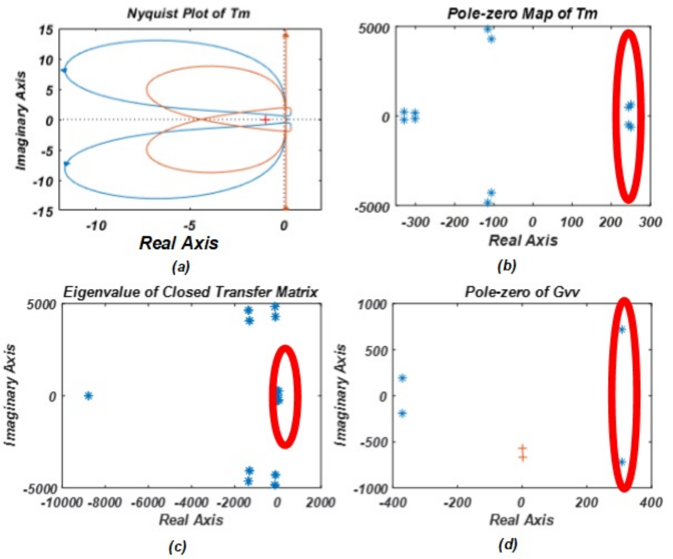

Fig. 7. Nyquist and PZ map plot of T_m, Eigenvalue, and G_{vv} PZ map in Case 1

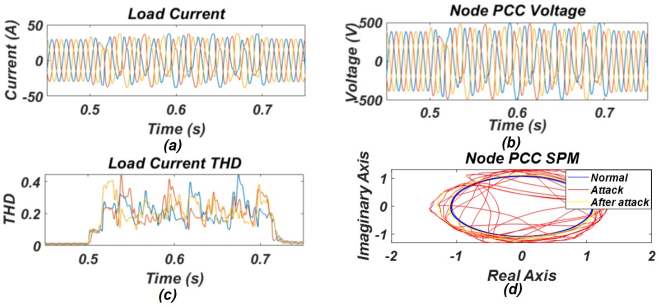

Fig. 8. i_{load}, u_{pcc}, THD and SPM in Case 2

C. Case 3

According to case one and case two , two security assessment criteria are effective for PESG due to cyber attacks. To monitor system status, these methods are also used to exhibit the system vulnerability under cyber attacks. When an inverter controller sensor is attacked, the system will enter into different operation region under different PI parameters in the controller. In this section, two cyber attacks temper sensor and controller in VSI successively. They can be indicated as $\hat{y} = 0.4y$ (attack I), $T_{yattack} = 0.5 - 0.7s$, $\hat{p} = 0.07p$ (attack II), $T_{pattack} = 0.6 - 0.7s$. Load current i_{load} and node PCC voltage u_{pcc} are drawn in Fig. 10(a,b). In the period-I (0.5-0.6s), VSI's controller sensor is attacked. In Fig. 10(c,d), THD and SPM show that this sensor attack's impact is limited, and

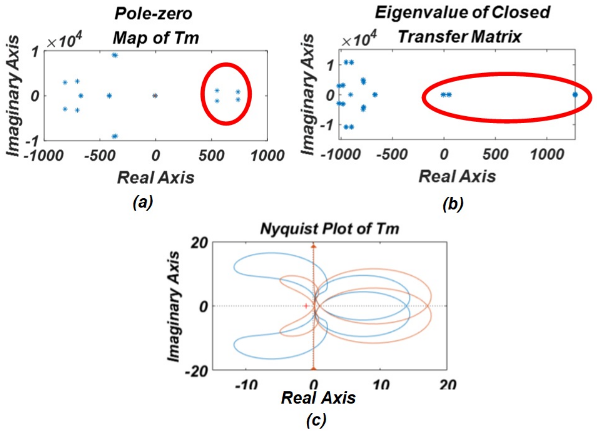

Fig. 9. Nyquist and PZ Map plot of T_m, and Eigenvalue of Closed Transfer Matrix in Case 2

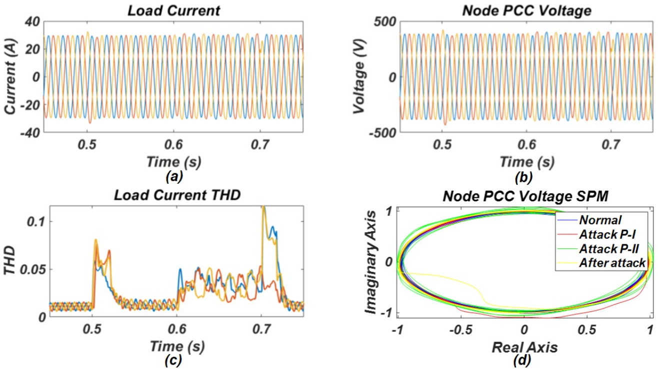

Fig. 10. i_{load}, u_{pcc}, THD and SPM in Case 3

the system is still stable during the period-I. The second attack, which changes the PI parameter in the current loop of VSI's controller, begins at 0.6s. According to Fig. 11(a,b), system is still stable, since $P(T_m) - N_{-1,j0}(T_m) = 0$. But from Fig. 10(c,d), distortion appears in the current and voltage in period-II(0.6-0.7s). THD of load current i_{load} approaches 5%. The green circle is not a unit one, which means deviation is generated in voltage waveform.

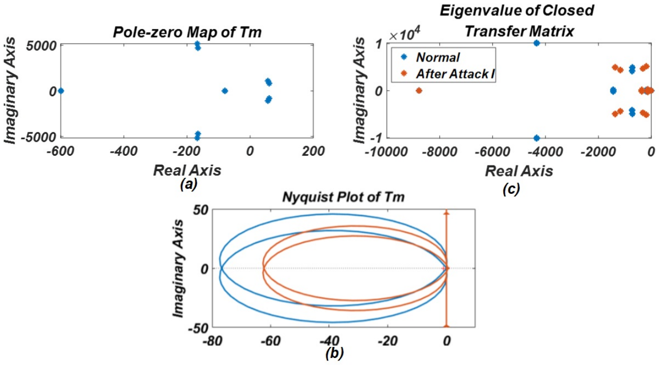

Fig. 11. i_{load}, u_{pcc}, THD and SPM in Case 3

The eigenvalues of the closed transfer function matrix in different situations are shown in Fig. 11(c) to further analyze the security of PESG. Compared with the normal condition, eigenvalues move closer to RHP after sensor attack. It also exhibits that the inverters' controller parameter has significant impacts on the system security operation margin. Thus, the system is more likely to collapse due to cyber attacks on PI parameters. This also explains why current and voltage distortion appear in period-II. Thus, two stability methods help operators evaluate security vulnerability.

V. Conclusion

This paper presents a comprehensive methodology to assess the stability and security under cyber attacks. For validation, two parallel inverters based power grid is modeled; two performance indexes and two stability assessment methodologies are proposed to evaluate the system condition under different cyber attacks. To obtain insight into impacts of a cyber attack, the evaluation index calculation considers three different time periods. A comprehensive assessment methodology that combines evaluation index and stability criterion is validated by simulation, which could be used for evaluation of the system vulnerability.

Acknowledgment

Our research is sponsored by NSF-ECCS-1946057.

References

[1] R. McMillan, "Siemens: Stuxnet worm hit industrial systems," *Computerworld*, vol. 14, 2010.

[2] T. Conway, R. Lee, and M. Assante, "Analysis of the cyber attack on the ukrainian power grid," *Retrieved from Electricity Information Sharing and Analysis Center website: https://ics. sans. org/media/E-ISAC_SANS_Ukraine_DUC_5. pdf*, 2016.

[3] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2011.

[4] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2011.

[5] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Impact analysis of data integrity attacks on power electronics and electric drives," in *2019 IEEE Transportation Electrification Conference and Expo (ITEC)*. IEEE, 2019, pp. 1–6.

[6] B. Yang, L. Guo, and J. Ye, "Real-time simulation of electric vehicle powertrain: hardware-in-the-loop (hil) testbed for cyber-physical security," in *2020 IEEE Transportation Electrification Conference and Expo (ITEC)*. IEEE, 2020.

[7] L. Guo, B. Yang, and J. Ye, "Enhanced cyber-physical security of steering stability control system for four-wheel independent drive electric vehicles," in *2020 IEEE Transportation Electrification Conference and Expo (ITEC)*. IEEE, 2020.

[8] B. Yang, F. Li, J. Ye, and W. Song, "Condition monitoring and fault diagnosis of generators in power networks," in *2019 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2019, pp. 1–5.

[9] F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, and W. Song, "Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–12, 2020, early access.

[10] W. Cao, "Impedance-based stability analysis and controller design of three-phase inverter-based ac systems," 2017.

[11] B. Yang, L. Guo, F. Li, J. Ye, and W.-Z. Song, "Vulnerability assessments of electric drive systems due to sensor data integrity attacks," *IEEE Transactions on Industrial Informatics*, 2019.