Cyber-Physical Attack Leveraging Subsynchronous Resonance

Bosong Li, Baosen Zhang, Daniel S. Kirschen
Department of Electrical and Computer Engineering
University of Washington

***Abstract*—This paper discusses how a cyber attack could take advantage of torsional resonances in the shaft of turbo-generators to inflict severe physical damage to a power system. If attackers were able to take over the control of a battery energy storage device, they could modulate the injection of this device at a frequency that matches one of the sub-synchronous resonance frequencies of a generator. Small changes in injection might be sufficient to excite one of these mechanical resonances, resulting in metal fatigue and ultimately a catastrophic failure in the shaft of the generator. Using a state-space model of the electro-mechanical system, the paper develops transfer functions linking the magnitude of the malicious injections to the magnitude of oscillations in the speed and angle of the various masses connected to the shaft. Numerical results from a two-area power system demonstrate the existence of vulnerable frequencies and show that damaging mechanical oscillations can be triggered without causing easily detectable signals at the generator terminals.**

***Index Terms*—Cyber attack, cyber-physical attack, battery energy storage, sub-synchronous resonance, state space analysis**

I. Introduction

While a cyber attack [1], [2] [3], [4] [5], [6] cripples a power system until the malicious software has been expurgated, a physical attack that destroys a major piece of equipment can take months to repair. To carry out a physical attack, the adversary must get in close proximity to the target equipment, which is expensive and difficult to carry out without detection. On the other hand, a cyber-physical attack does not require the malicious actor to get in close proximity of the target equipment. Instead, the attacker infiltrates some aspect of the control infrastructure of the power system and manipulates it to create physical damage [7]. Idaho National Laboratory demonstrated the feasibility of this type of attack by taking over the protection system of a generator and manipulating its synchronization until the generator self-destructed [8].

To avoid detection and countermeasures, malicious manipulations of the control system should remain small. It is therefore important to explore how an attacker could use resonances to amplify their effects. Because their output can be modulated at high frequency, battery energy storage systems (BESS) represent an ideal vector for this type of attack. Furthermore, because the number of BESS deployed in power systems is increasing rapidly, the attack surface is growing [9] [10] [11].

This paper explores how a malicious actor could damage large turbo-generators by taking over the control of a BESS and using it to inject small amounts of power at frequencies corresponding to the torsional sub-synchronous resonance (SSR) frequencies in the shaft of some generators. SSR is a condition of the electric power system where with a turbine generator exchanges energy with the rest of the system at one or more of the natural frequencies of the combined system below the synchronous frequency of the system [12]. While sub-synchronous oscillations between the various masses connected to the shaft of the generator typically remain small, they cause metal fatigue and can over time lead to a catastrophic failure of this shaft [13].

Physical and control countermeasures can be taken to avoid SSR [14]. Capacitor compensation can be added to the system, but the investment cost of such infrastructure measures is high. Protective relays can also be used to detect oscillations at the generator terminals. However, as this paper will show, it is possible to induce mechanical oscillations that are hard to detect at the generator terminals.

To demonstrate the feasibility of cyber-physical attacks that leverage sub-synchronous resonances, this paper develops a state-space model of the combined electromechanical system. From this state space model, we derive transfer functions linking the magnitude of the disturbances created by the subverted BESS and the angular frequency of the various masses connected to the shaft of a generator. These transfer functions exhibit resonance frequencies that an attacker could target. A relatively low-power BESS could therefore trigger sub-synchronous resonances that could ultimately destroy large generators while remaining hard to detect.

The remainder of the paper is organized as follows: Section II describes a state-space model of the system dynamics that combines the swing equations of the generator, the mechanical characteristics of the shaft system, as well as the power flow equations. Section III derives transfer functions relating the BESS injections to the angular frequency and position of the various masses connected to the generator shaft. Section IV describes numerical studies that illustrate the frequency-domain analysis and correlate it with time-domain simulations. Section V discusses possible countermeasures. Section VI concludes and discusses further work.

II. Model of System Dynamics

A. Notation

In this paper, the rated angular velocity in electrical rad/s is denoted by $\omega_0 = 2\pi f_0$, where frequency $f_0 = 60$ Hz. Assuming the number of field poles $p_f = 2$, we employ ω_{0m}

as the rated angular velocity in mechanical rad/s, and $\omega_{0m} = (2/p_f)\omega_0 = 377$ rad/s.

Each generator contains a five-mass torsional system. This paper denotes the speed and angle deviation of each rotor from the steady-state values respectively with $\omega_g, \omega_{s1}, \omega_{s2}, \omega_{s3}, \omega_{s4}$ and $\theta_g, \theta_{s1}, \theta_{s2}, \theta_{s3}, \theta_{s4}$. The subscription gi represents the terminal of generator i, while the subscriptions $s1 - s4$ represent the other turbine sections. We further define $\Delta\omega$ and $\Delta\theta$ as the speed and angle difference between two adjacent masses connecting to the same shaft. A torsional system of generator i is presented in Fig. 1 with the variables illustrated, where the shaft between two adjacent masses is denoted using a double subscript as $12, 23, 34$ and 45.

In the following formulation, the variables and parameters are employed with their per-unit values if not specially mentioned.

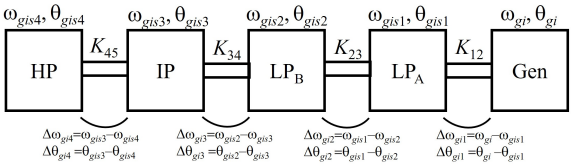

Fig. 1. Five-Mass Torsional System.

B. State-Space Model

We investigate the dynamics of generators considering the swing equations of the generator rotor together with the torsional characteristics of the shaft system shown below in (1)-(2) and (3)-(11).

$$\dot{\omega}_g = \frac{\omega_{0m}}{2H_g}\ (P_M - P_e - D_g \cdot \omega_g) \tag{1}$$

$$\dot{\theta}_g = \omega_g \tag{2}$$

$$\dot{\omega}_g = \frac{\omega_{0m}}{2H_g}\ \big(K_{12}(\theta_{s2} - \theta_g) - D_g \cdot \omega_g - P_e\big) \tag{3}$$

$$\dot{\omega}_{s1} = \frac{\omega_{0m}}{2H_{s1}}\ \big(K_{23}(\theta_{s3} - \theta_{s2}) - K_{12}(\theta_{s2} - \theta_g) - D_{s1} \cdot \omega_{s1} + P_{s1}\big) \tag{4}$$

$$\dot{\omega}_{s2} = \frac{\omega_{0m}}{2H_{s2}}\ \big(K_{23}(\theta_{s3} - \theta_{s2}) - K_{12}(\theta_{s2} - \theta_{s1}) - D_{s2} \cdot \omega_{s2} + P_{s2}\big) \tag{5}$$

$$\dot{\omega}_{s3} = \frac{\omega_{0m}}{2H_{s3}}\ \big(K_{34}(\theta_{s4} - \theta_{s3}) - K_{23}(\theta_{s3} - \theta_{s2}) - D_{s3} \cdot \omega_{s3} + P_{s3}\big) \tag{6}$$

$$\dot{\omega}_{s4} = \frac{\omega_{0m}}{2H_{s4}}\ \big(-K_{34}(\theta_{s4} - \theta_{s3}) - D_{s4} \cdot \omega_{s4} - P_{s4}\big) \tag{7}$$

$$\dot{\theta}_{s1} = \omega_{s1} \tag{8}$$

$$\dot{\theta}_{s2} = \omega_{s2} \tag{9}$$

$$\dot{\theta}_{s3} = \omega_{s3} \tag{10}$$

$$\dot{\theta}_{s4} = \omega_{s4} \tag{11}$$

In (3)-(7), parameters D and H are respectively the damping coefficient and inertia constant of each rotor section. Parameter K is the shaft stiffness. Note that (1) and (3) illustrate the dynamics of the generator rotor in different forms. Furthermore, the mechanical torque on the generator rotor equals the electrical torque in the steady state, i.e. $P_M = P_e$. We can therefore combine (1) and (3) as (12).

$$\dot{\omega}_g = \frac{\omega_{0m}}{2H_g}\ \big(K_{12}(\theta_{s2} - \theta_g) - D_g \cdot \omega_g - P_M\big) \tag{12}$$

Hence the dynamics of a generator considering the shaft system is fully described by (2), (4)-(11), and (12). In a power system containing n generators, we take the rotor speed $\boldsymbol{\omega}$ and angular displacement $\boldsymbol{\theta}$ of each generator as state variable $\mathbf{x} = [\boldsymbol{\omega}^T, \boldsymbol{\theta}^T]^T$, where $\boldsymbol{\omega}$ and $\boldsymbol{\theta}$ are both vectors of length $5n$ illustrated in details as:

$$\boldsymbol{\omega} = [\underbrace{\omega_{g1}, \omega_{g2}, ..., \omega_{gn}}_{n}, \underbrace{\omega_{g1s1}, ..., \omega_{g1s4}, ..., \omega_{gns1}, ..., \omega_{gns4}}_{4n}]^T \tag{13}$$

$$\boldsymbol{\theta} = [\underbrace{\theta_{g1}, \theta_{g2}, ..., \theta_{gn}}_{n}, \underbrace{\theta_{g1s1}, ..., \theta_{g1s4}, ..., \theta_{gns1}, ..., \theta_{gns4}}_{4n}]^T \tag{14}$$

In the steady state, the mechanical power P_M of the generator rotor in (12) equals the electrical power. By substituting the load bus angular displacement in the power flow and power balance equations with state variables, we write the mechanical power using the angular displacement vector $\boldsymbol{\theta}$ and load vector $\mathbf{L}$:

$$\mathbf{P_M} = \mathbf{P_e} = \mathbf{A_e}\boldsymbol{\theta} + \mathbf{B_e}\mathbf{L} \tag{15}$$

where $\mathbf{P_M} = [P_{Mg1}, P_{Mg2}, ..., P_{Mgn}]^T$. The matrices $\mathbf{A_e}$ and $\mathbf{B_e}$ depend on the system admittance matrix and topology. Since the focus of this paper is on the oscillations between different masses in the generator, we take a load bus to be the slack bus to emphasis generators internal dynamics.

This paper further denotes the input power on each mass of the generator shaft system with a 4-dimensional vector $\mathbf{P_{gi}} = [P_{gis1}, P_{gis2}, P_{gis3}, P_{gis4}]^T = P_{Mgi} \cdot \mathbf{B_{f}}_{gi}$, where the coefficient vector $\mathbf{B_{f}}_{gi}$ contains the fraction of the total turbine power generated by each turbine in the steady-state. Following the pattern of state variables $\boldsymbol{\omega}$ and $\boldsymbol{\theta}$, the input power vector $\mathbf{P_I} = [\mathbf{P_M}^T, \mathbf{P_{g1}}^T, ..., \mathbf{P_{gn}^T}]^T$ is defined as:

$$\mathbf{P_I} = \mathbf{B_I} \cdot \mathbf{P_M} = \mathbf{B_I}\mathbf{A_e}\boldsymbol{\theta} + \mathbf{B_I}\mathbf{B_e}\mathbf{L} \tag{16}$$

$$\mathbf{B_I} = \begin{bmatrix} \mathbf{I_{n\times n}} \\ \mathbf{B_F} \end{bmatrix} \tag{17}$$

$$\mathbf{B_F} = \begin{bmatrix} \mathbf{B_{f}}_{g1} & & & \\ & \mathbf{B_{f}}_{g2} & & \\ & & \ddots & \\ & & & \mathbf{B_{f}}_{gn} \end{bmatrix} \tag{18}$$

where $\mathbf{I_{n\times n}}$ is an n by n identity matrix. The $4n \times n$-dimensional coefficient matrix $\mathbf{B_F}$ is constructed by matrices $\mathbf{B_{f}}_{g1}, \mathbf{B_{f}}_{g2}, ..., \mathbf{B_{f}}_{gn}$ indicating how much input power each turbine provides in a generator.

We therefore build the state-space model of the whole power system as follows:

$$\begin{bmatrix} \dot{\boldsymbol{\omega}} \\ \dot{\boldsymbol{\theta}} \end{bmatrix} = \begin{bmatrix} \mathbf{A_{11}} & \mathbf{A_{12}} \\ \mathbf{A_{21}} & \mathbf{A_{22}} \end{bmatrix} \begin{bmatrix} \boldsymbol{\omega} \\ \boldsymbol{\theta} \end{bmatrix} + \mathbf{B} \cdot \mathbf{L} \tag{19}$$

The system matrix $\boldsymbol{A}$ consists of four parts, where:

$$\mathbf{A_{11}} = -\frac{\omega_{0m}}{2}\mathbf{diag}(-\frac{D_g}{H_g}, -\frac{D_{s1}}{H_{s1}}, -\frac{D_{s2}}{H_{s2}}, -\frac{D_{s3}}{H_{s3}}, -\frac{D_{s4}}{H_{s4}}) \tag{20}$$

$$\mathbf{A_{12}} = \mathbf{B_I}\mathbf{A_e} + \frac{\omega_{0m}}{2}\begin{bmatrix} -\frac{K_{12}}{H_g} & \frac{K_{12}}{H_g} & & & & \\ \frac{K_{12}}{H_{s2}} & -\frac{K_{12}+K_{23}}{H_{s2}} & \frac{K_{23}}{H_{s2}} & & & \\ & \frac{K_{23}}{H_{s3}} & -\frac{K_{23}+K_{34}}{H_{s3}} & \frac{K_{34}}{H_{s3}} & & \\ & & \frac{K_{34}}{H_{s4}} & -\frac{K_{34}+K_{45}}{H_{s4}} & \frac{K_{45}}{H_{s4}} & \\ & & & \frac{K_{45}}{H_{s5}} & -\frac{K_{45}}{H_{s5}} \end{bmatrix} \tag{21}$$

The sub-matrix $\mathbf{A_{21}} = \mathbf{I_{5n\times 5n}}$ is an identity matrix, while sub-matrix $\mathbf{A_{22}} = \mathbf{0}$ is a zero matrix. The input matrix $\mathbf{B} = \mathbf{B_I}\mathbf{B_e}$ according to (16).

III. Transfer Function Magnitude Analysis

With access to the BESS on a load bus, potential attackers can inject oscillatory signals into the system, illustrated mathematically as (22), where the attack signal ΔL is a square-wave signal. This paper assumes a square-wave attack signal because it is created by an energy storage device by constantly changing between the charging and discharging states. Moreover, we built a model predictive control (MPC) problem to maximize the oscillation of the generator terminal variables, and the optimal solution to this problem was a square wave.

$$\dot{\mathbf{x}} = \begin{bmatrix} \mathbf{A_{11}} & \mathbf{A_{12}} \\ \mathbf{A_{21}} & \mathbf{A_{22}} \end{bmatrix} \mathbf{x} + \mathbf{B}(\mathbf{L} + \Delta\mathbf{L}) \tag{22}$$

All the elements of the attack signal $\Delta\mathbf{L}$ are 0 except for the element corresponding to the load bus where the malicious energy storage device resides. We assume the oscillatory signal magnitude is 1 p.u. of the base power considering the limited power and capacity of the attack energy storage device. The only factor that affects the system oscillation is, therefore, the frequency of input signal $\Delta\mathbf{L}$. To explore the impact of the injected oscillatory signal frequency on each rotor of the generators in the system, we investigate two output signals denoted as (23) and (24). To explore the impact of the oscillatory signal injection on the generator terminal and the torsional system, we define the following output:

$$\mathbf{y_1} = \begin{bmatrix} \boldsymbol{\omega} \\ \boldsymbol{\theta} \end{bmatrix} = \mathbf{C_1}\mathbf{x} + \mathbf{D_1}(\mathbf{L} + \Delta\mathbf{L}) \tag{23}$$

$$\mathbf{y_2} = \begin{bmatrix} \Delta\boldsymbol{\omega} \\ \Delta\boldsymbol{\theta} \end{bmatrix} = \mathbf{C_2}\mathbf{x} + \mathbf{D_2}(\mathbf{L} + \Delta\mathbf{L}) \tag{24}$$

where output $\mathbf{y_1}$ is the generator terminal variables. The output $\mathbf{y_2}$ contains torsional variables showing the speed and angle differences between the rotors connecting to the same shaft. Output $\mathbf{y_2}$ is further explained in (25)-(28).

$$\Delta\boldsymbol{\omega} = [\Delta\boldsymbol{\omega}_{g1}, \Delta\boldsymbol{\omega}_{g2}, ..., \Delta\boldsymbol{\omega}_{gn}]^T \tag{25}$$

$$\Delta\boldsymbol{\theta} = [\Delta\boldsymbol{\theta}_{g1}, \Delta\boldsymbol{\theta}_{g2}, ..., \Delta\boldsymbol{\theta}_{gn}]^T \tag{26}$$

For generator i, $\Delta\boldsymbol{\omega}_{gi}$ and $\Delta\boldsymbol{\theta}_{gi}$ are both 4-dimensional vectors:

$$\Delta\boldsymbol{\omega_{gi}} = [\omega_{gi}-\omega_{gis1}, \omega_{gis1}-\omega_{gis2}, \omega_{gis2}-\omega_{gis3}, \omega_{gis3}-\omega_{gis4}]^T \tag{27}$$

$$\Delta\boldsymbol{\theta_{gi}} = [\theta_{gi}-\theta_{gis1}, \theta_{gis1}-\theta_{gis2}, \theta_{gis2}-\theta_{gis3}, \theta_{gis3}-\theta_{gis4}]^T \tag{28}$$

We analyze the magnitudes of the transfer functions between the input signal $\Delta\mathbf{L}$ and the output signals in (23) and (24) over the frequency spectrum from 0Hz to 60Hz. The magnitudes of the transfer functions $|\Gamma_1|_j$ and $|\Gamma_2|_k$ correspond respectively to the jth generator terminal variable and the kth torsional variable of a generator.

$$|y_1(j\omega_a)|_j = |\Gamma_1(j\omega_a)|_j \cdot |\Delta L(j\omega_a)| \tag{29}$$

$$|y_2(j\omega_a)|_k = |\Gamma_2(j\omega_a)|_k \cdot |\Delta L(j\omega_a)| \tag{30}$$

Equations (29) and (30) show that with the same oscillatory input signal, the oscillation magnitudes of the generator terminal variables as well as the torsional variables are determined by the magnitude of the corresponding transfer function. With an oscillatory input signal at frequency ω_a, if the magnitude $|\Gamma_2(j\omega_a)|_k$ is higher than $|\Gamma_1(j\omega_a)|_j$ as shown in (31), the internal torsional system of the generator suffers a more severe oscillation compared to the generator terminal.

$$|\Gamma_2(j\omega_a)|_k > |\Gamma_1(j\omega_a)|_j, j, k \in the\ same\ generator \tag{31}$$

Additionally, the protection system is usually designed to prevent the generator terminal rotor from significant oscillation, i.e., damping the frequencies that lead to high $|\Gamma_1(j\omega_a)|_i$ values. The input oscillation frequencies denoted in (31) therefore remain commonly neglected. A ratio parameter R_M is further defined in (32) as the ratio between the transfer function magnitudes of the torsional output and the terminal output.

$$R_M(\omega_a) = \frac{|\Gamma_2(j\omega_a)|_k}{|\Gamma_1(j\omega_a)|_i}, i, k \in the\ same\ generator \tag{32}$$

The higher the ratio R_M is, the more severe the oscillation inside the generator shaft system occurs while the measurements at the generator terminal remain close to the steady-state values. If the attack frequency ω_a in (32) is lower than the nominal frequency, i.e. $\omega_a < \omega_0$, the input attack signal leads to subsynchronous oscillation of the generator. Such oscillation is easily neglected in the power system, for the generator terminal measurements stay nearly unchanged. However, the subsynchronous oscillation will cause mechanical fatigue and fracture in the long term. In addition to the theoretical analysis in the frequency domain, we also testify the vulnerability leveraging SSR in the time domain, shown with the numerical studies in the following section.

IV. A Two-area System Example

To investigate the existence of the vulnerability presented in this paper in the power system, we employ a commonly used two-area system for numerical studies shown in Fig. 2.

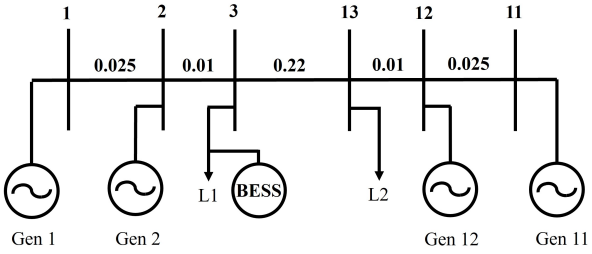

Fig. 2. Two-area System

In Fig. 2, the line reactances are shown in p.u. on 230 kW and 100 MW [14]. A linear system is considered here with a single circuit tie line. And an energy storage device is integrated to Bus 3 to inject malicious input signal with a magnitude of 1 MW, which is 1 p.u.. The power transfer from Area 1 to Area 2 is 400 MW, where L1 = 970 MW and L2 = 1770 MW. Four identical generating units Gen 1, Gen 2, Gen 11, and G 12, are respectively loaded to 700 MW, 670 MW, 670 MW, and 700 MW, with a five-mass torsional system each. The inertia constant, power fraction, and shaft stiffness of the generator torsional system are presented in Table I.

TABLE I
GENERATOR TORSIONAL SYSTEM PARAMETERS

Rotor	HP	IP	LP_B	LP_A	Gen
Inertia	0.0929	0.1556	0.8587	0.8842	0.8684
Power Fraction	0.30	0.26	0.22	0.22	

Shaft	HP-IP	IP-LP_B	LP_B-LP_A	LP_A-Gen
Shaft Stiffness	19.303	34.929	52.038	70.858

All values in p.u.

A. Frequency-Domain Analysis

While the damping factor of the generator terminal is commonly neglected, i.e. $D_{g1} = D_{g2} = D_{g11} = D_{g12} = 0$, the damping factor of each mass in the torsional system strongly affects the transfer function magnitudes according to our tests. The impact of the mass damping factor on the transfer function magnitude is depicted in Fig. 3. Note that such impact on each generator is similar, we take Gen 1 as an example to avoid repeating. In Fig. 3, the transfer function magnitude curves of rotor speed ω and angular displacement θ are respectively normalized. Thus the y-axis ranges from 0 to 1. The $|\Gamma|_\theta$ curves in Fig. 3 see their maximums with the input signal frequencies close to 0Hz. The maximums of the $|\Gamma|_\theta$ curves are significantly higher than the other $|\Gamma|_\theta$ values, which indicates the most notable oscillation occurs when the input signals approximate DC signals. With the increase of mass damping factor, the $|\Gamma|_\omega$ curve becomes smoother and moves upward. A more significant oscillation is therefore expected due to the higher values of the magnitude $|\Gamma|_\omega$. Hence it is reasonable for us to employ a low damping factor for the torsional mass in further analysis. A low mass damping factor is also consistent with the commonly-used steel masses in real power systems.

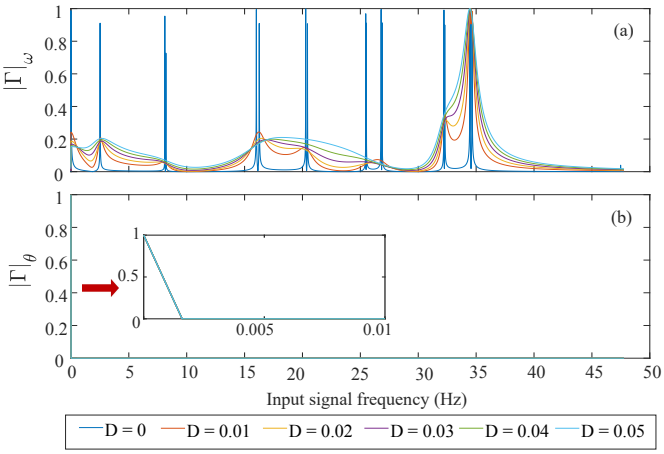

Fig. 3. Transfer Function Magnitude Curves of Gen 1.

The values of the ratio $R_M(\omega_a)$ proposed in (32) are shown in Fig. 4 for Gen 1: where Fig. 4 (a) presents the

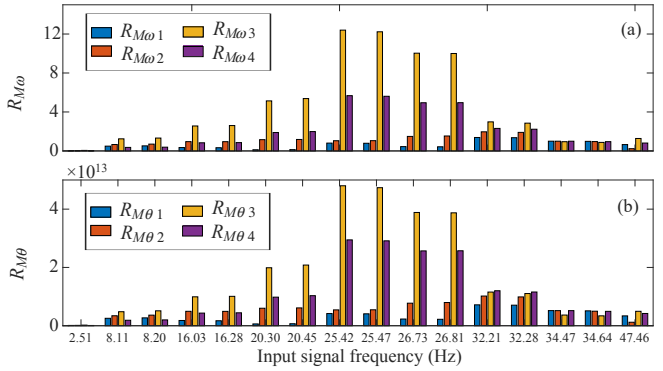

Fig. 4. R_M Values of Gen 1

magnitude ratio between the torsional speed difference and the terminal rotor speed, and Fig. 4 (b) illustrates the magnitude ratio between the torsional angle difference and the terminal rotor angel. The higher $R_M(\omega_a)$ value is, the more severe the oscillation of the torsional system will be compared to the generator terminal. Due to the low magnitudes of their transfer functions, the generator terminal variables stay closely to their steady-state values. The internal oscillation of the torsional system will thus be difficult to recognize. The system is also more vulnerable when exposed to the malicious input at frequency (ω_a).

In Fig. 5, the blue curves are the terminal speed and angle of Gen 1. The orange curves represent the speed and angel differences between the third and fourth mass, both connecting to shaft 34 of Gen 1.

As shown in Fig. 5(a), the $|\Gamma|_{\theta g1}$ values are close to 0 when the input signal frequency is above 0Hz, which explains

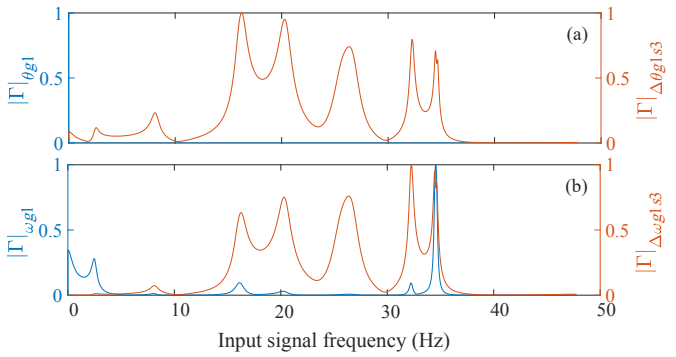

Fig. 5. Comparison of $|\Gamma|_{\omega}$, $|\Gamma|_{\theta}$ and $|\Gamma|_{\Delta\omega}$, $|\Gamma|_{\Delta\theta}$ of Gen 1

the reason why $R_{M\theta}$ values in Fig. 4(b) are significantly high. Therefore the the local maximums of $R_{M\theta}$ shown in 4(b) coincide with the local maximums of $|\Gamma|_{\Delta\theta}$ shown in 5(a). In Fig. 5(b), when the input signal frequency is close to 34.47Hz, both curves see a local maximum value. This local maximum is also the global maximum of $|\Gamma|_{\theta g1}$, meaning the oscillation at this frequency is usually damped by power system stabilizers, which are usually designed according to the speed and angle of the generator terminals. However, the oscillations corresponding to other local maximums often remain neglected from protective measures due to the lack of attention to the speed and angle of the torsional masses. The torsional system is therefore vulnerable to attack signals at these frequencies. Potential attacks can thus attack the system with injection of oscillatory signals at such frequencies with an energy storage device either remotely hacked or physically controlled by them. Considering the results shown in Fig. 3, the example system is at risk when input signal frequency lies within the range of 25.42-25.47Hz or 26.73-26.81Hz.

Note that the input signal frequency ranges depicted in Fig. 3-Fig. 5 are 0-50Hz, which is the typical frequency range of SSR. From 50 to 60Hz, the y-axis values in in Fig. 3-Fig. 5 approximate 0, and are left out for concision.

B. Time-Domain Analysis

Assuming the system is exposed to a square-wave input signal with magnitude $|\Delta L| = 1MW$ at Bus 3, we analyze the time-domain response of the output considering two attack frequencies: $f_{a1} = 25.42Hz$, and $f_{a2} = 26.81Hz$. The severity of an oscillation is measured by the amplitude of a signal's deviation from its steady-state value. We define $R_{\omega j} = \frac{max(|\Delta\omega_j - \Delta\omega_{j,0}|)}{max(|\omega_i - \Delta\omega_{i,0}|)}$, where the numerator is the deviation of the speed difference between mass j and mass $j+1$ from the initial steady-state difference. The denominator is the deviation of the terminal rotor speed from its initial state. Thus if the value of $R_{\omega j}$ is higher than 1, the oscillation inside the torsional system is more significant than that at the terminal rotor, and the significance increases with the rise of $R_{\omega j}$ value. The same definition and characteristic are applied to $R_{\theta j}$, thus is not repeated. Considering a 10s control horizon with a time step of $10^{-3}s$, an attack is issued at $t = 2s$, the values of $R_{\omega j}$ and $R_{\theta j}$ are presented in the following table.

TABLE II
R_{ω} AND R_{θ} VALUES UNDER DIFFERENT ATTACK FREQUENCIES

Item		$R_{\omega 1}$	$R_{\omega 2}$	$R_{\omega 3}$	$R_{\omega 4}$	$R_{\theta 1}$	$R_{\theta 2}$	$R_{\theta 3}$	$R_{\theta 4}$
f_{a1}	Gen 1	1.55	1.70	2.37	2.77	0.43	0.47	0.71	0.82
	Gen 2	1.56	1.60	2.45	**2.85**	0.57	0.65	1.01	**1.17**
	Gen 11	1.57	1.19	1.24	1.61	0.07	0.06	0.06	0.08
	Gen 12	1.69	1.30	1.64	2.07	0.08	0.07	0.10	0.11
f_{a2}	Gen 1	1.30	1.88	2.15	2.73	0.60	0.93	1.12	1.40
	Gen 2	1.16	1.91	2.33	**2.92**	0.60	1.11	1.39	**1.73**
	Gen 11	1.53	1.56	1.21	1.69	0.15	0.16	0.13	0.18
	Gen 12	1.37	1.66	1.44	1.95	0.16	0.21	0.20	0.26

The maximums of the $R_{\omega j}$ and $R_{\theta j}$ under each attack signal frequency are highlighted in bold in Table II. The time-domain responses of unit Gen 2 is further illustrated in Fig. 6, where Fig. 6(a) depicts output $\Delta\omega_{g2s4}$ and ω_{g2}, and Fig. 6(b) presents output $\Delta\theta_{g2s4}$ and θ_{g2}. The $R_{\omega j}$ and $R_{\theta j}$

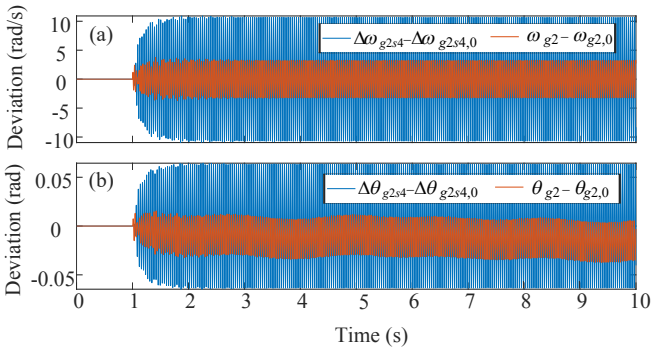

Fig. 6. Time-domain Response under Attack Frequency 26.81Hz

values in Table II higher than 1 indicate that the torsional system of the corresponding generators oscillate notably while the terminal measurements close to the initial steady-state values. Considering attack signal frequencies f_{a1} and f_{a2} are both below 60Hz, the vulnerability revealed here results in SSR of the generators. And we prove the existence of such vulnerability that leads to SSR when the system is exposed to the proposed cyber-physical attacks. This paper assumes access to a complete knowledge of system structure and data, which is difficult to achieve in practice. To explore the system vulnerability with limited access to the system information remains our future work.

V. COUNTERMEASURES

The cyber-physical attack discussed in this paper requires only a relatively low-power BESS that can be located at some distance from the targeted generators. The resulting SSR leads to metal fatigue of the generator shafts through small oscillations and that could ultimately cause a fatal mechanical

failure. Further work is needed to identify generators that might be particularly susceptible to this type of attack and to develop effective countermeasures. These countermeasures can be divided into four categories: prevention, detection, reaction and mitigation.

Prevention is the first line of defense. Using best cyber security practices, it aims to prevent attackers from taking control of power devices. Unfortunately, the attack surface is getting larger due to the increasing number of BESS and other controllable components.

Detecting this form of cyber-physical attack and locating their source are challenging issues. Because the malicious power injections are small, they are likely to be lost in the noise in conventional SCADA measurements, especially if the network is large and complex. More sensitive measurements at a higher time resolution are likely to be needed to be able to pinpoint the source of the attack, which may be in a remote part of the network.

Once an attack has been detected and its source identified, to ensure a quick reaction, procedures must be in place to disconnect it from the system. Alternatively, the targeted generators may need to be disconnected.

If prevention, detection and reaction are deemed insufficiently effective, mitigation may be required. Such measures could be similar to those that were developed to deal with naturally occurring sub-synchronous resonance. Reference [15] groups these countermeasures into four categories: system switching and generator tripping, generator and system modifications, relaying and detecting devices, and filtering and damping devices. While some of these measures have been shown to be effective, they may be harder to implement in an adversarial context because the attack may be aimed at any generator rather than at a particular generator identified as being susceptible to sub-synchronous resonance through careful system studies. Protecting all generators against attacks at any dangerous frequency may also be difficult or very costly

VI. Conclusion

This paper exposes a potential vulnerability of power systems to a cyber-physical attack where a malicious actor could trigger a SSR in the shaft of large generators by creating small oscillations in the active power injections of a battery energy storage system. These small mechanical oscillations between the various masses connected to the shaft would cause metal fatigue and ultimately lead to a catastrophic failure of the generator. Because this resonance takes place within the shaft, it does not create significant perturbations at the terminal of the generator and might therefore be difficult to detect. Gaining access to the control system of a relatively low power BESS would therefore give an attacker an opportunity to inflict physical damage on equipment of a considerably larger rating and importance to the reliable operation of the system. Our further work will explore detection, reaction and mitigation countermeasures.

Acknowledgment

The work described in this paper was carried out with funding from the US National Science Foundation under its CRISP - Critical Resilient Interdependent Infrastructure Systems and Processes program, grant number 1832287.

References

[1] J. Liu, Y. Gu, L. Zha, Y. Liu, and J. Cao, "Event-triggered h_∞ load frequency control for multiarea power systems under hybrid cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1665–1678, 2019.

[2] W. Chen, D. Ding, H. Dong, and G. Wei, "Distributed resilient filtering for power systems subject to denial-of-service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1688–1697, 2019.

[3] Q. Wang, W. Tai, Y. Tang, and M. Ni, "Review of the false data injection attack against the cyber-physical power system," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 2, pp. 101–107, 2019.

[4] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 4868–4877, 2018.

[5] L. Zheng, T. Gao, and X. Zhang, "Security protection and testing system for cyber-physical based smart power grid," in *Proceedings of PURPLE MOUNTAIN FORUM 2019-international forum on smart grid protection and control*. Springer, 2020, pp. 847–857.

[6] S. Mousavian, M. Erol-Kantarci, L. Wu, and T. Ortmeyer, "A risk-based optimization model for electric vehicle infrastructure response to cyber attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6160–6169, 2017.

[7] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, "Electric power grid resilience to cyber adversaries: State of the art," *IEEE Access*, vol. 8, pp. 87 592–87 608, 2020.

[8] M. Zeller, "Myth or reality—does the aurora vulnerability pose a risk to my generator?" in *2011 64th Annual Conference for Protective Relay Engineers*. IEEE, 2011, pp. 130–136.

[9] M. Assante *et al.*, "High-impact low-frequency event risk to the north american bulk power system," *North American Electric Reliability Corporation (NERC), Atlanta, GA, Tech. Rep*, 2010.

[10] D. A. Tejada-Arango, A. S. Siddiqui, S. Wogrin, and E. Centeno, "A review of energy storage system legislation in the us and the european union," *Current Sustainable/Renewable Energy Reports*, vol. 6, no. 1, pp. 22–28, 2019.

[11] C. Glenn, D. Sterbentz, and A. Wright, "Cyber threat and vulnerability analysis of the us electric sector," Idaho National Lab.(INL), Idaho Falls, ID (United States), Tech. Rep., 2016.

[12] IEEE SSR Working Group, "Proposed terms and definitions for subsynchronous resonance," in *IEEE Symposium on Countermeasures for Subsynchronous Resonance, IEEE Pub, 81TH0086-9-PWR*, 1981, pp. p92–97.

[13] P. M. Anderson, B. L. Agrawal, and J. E. Van Ness, *Subsynchronous resonance in power systems*. John Wiley & Sons, 1999, vol. 9.

[14] P. Kundur, "Power system stability," *Power system stability and control*, vol. 10, 2007.

[15] IEEE Subsynchronous Resonance Working Group, "Countermeasures to subsynchronous resonance problems," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-99, no. 5, pp. 1810–1818, 1980.