Forced Power Systems Oscillations Due to Cyberattacks: Threats, Detection and Partial Mitigation

Andrew G. Miles
Alaska Center For Energy and Power
University of Alaska Fairbanks
Fairbanks AK
Agmiles@alaska.edu

Rômulo G. Bainy
Center for Secure and Dependable Systems
University of Idaho
Moscow, ID
romulo@uidaho.edu

Kendall Bean
Department of Electrical and Computer Engineering
University of Idaho
Moscow, ID
bean1366@vandals.uidaho.edu

Brian K. Johnson
Department of Electrical and Computer Engineering
University of Idaho
Moscow, ID
bjohnson@uidaho.edu

Dakota Roberson
Department of Electrical and Computer Engineering
University of Idaho
Idaho Falls, ID
dakotar@uidaho.edu

Reynaldo Nuqui
Hitachi Energy
Raleigh, NC

2023 Resilience Week (RWS) | 979-8-3503-4747-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/RWS58133.2023.10284613

***Abstract*—Forced oscillations in power systems can be caused by misconfigured controllers at generator stations. They can also be caused by cyberattacks against the exciters or governors. This paper explores the effects of forced oscillations from cyberattacks on generator excitation and governor systems and the effectiveness of a novel control system for a static var compensator in mitigating those oscillations to enhance transmission system resilience. A brief overview of oscillations, especially forced oscillations, within power systems is presented, along with an overview of cyberattacks on power systems. This paper also examines and implements FACTS devices to partially mitigate the forced oscillations created by cyberattacks by reducing the magnitude of the oscillations caused by the attack. The proposed approach is more effective against attacks targeting exciters.**

Keywords—Cybersecurity, False Data Injection, Power Generation Components, Topology Attacks

I. Introduction

In power systems, the natural electromechanical modes are excited by sudden load variations or changes in generation. Outside the natural modes, additional unwanted oscillations, also known as forced oscillations, may be generated through external mechanisms such as cyclic loads or mechanical aspects from generators [1], [2]. If the frequencies of the forced oscillations coincide with the local modes of the system, i.e., 0.1-2.0 Hz, they can produce a dangerous effect. [3], [4]. More prominently, resonance can occur, leading to oscillations that are much larger than that of the source when an inter-area mode is poorly damped, and forced oscillations are injected at a frequency close to the system mode frequency at a location where the inter-area mode is participating [2]. A thorough review of forced oscillations in power systems with converter controlled resources is provided in [3]. Furthermore, the authors provide case studies to show options for mitigating forced oscillations. Forced oscillations are primarily due to configuration errors due to unanticipated interactions. There is also a risk of forced oscillations due to cyberattacks against controllers, whether in synchronous machines or other generation equipment. These forced oscillations impact the resilience of the transmission system.

Due to a combination of changing economic policies, there has been a shift to the increasing installation of inverter-based resources (IBR), which has accelerated as IBR's capital and operational costs have declined. As a result, many countries are investing in IBRs, and some have achieved penetration of up to 150% of this type of emerging technology [5]. Although this large deployment of IBRs is beneficial to meet societal needs, undesirable oscillations have been recorded in those power systems, resulting in over-voltages, over-currents, and oscillations [6]. Oscillations have occurred and been studied within the United States, Canada, Australia, and China [1], [7] as new technologies have been implemented. As these events are understood, new technologies and methodologies have been researched, such as damping controllers and flexible AC transmission systems (FACTS) devices to dampen the oscillations [7]. It is important to note that oscillatory behavior is not uniquely an IBR-related event. Furthermore, subsynchronous oscillations (SSO) have been observed in HVDC (High Voltage Direct Current) systems, FACTS devices, wind parks, and synchronous generators, as noted in [5]. Weak grids have historically been susceptible to oscillatory phenomena, although much of the effects are still poorly understood [5].

Along with this increased installation of IBRs, the infrastructure required to operate and monitor these devices also requires attention. As described in a Department of Energy (DOE) report in 2020 [8], infrastructure is expanding in the power grid and information and operational technologies. However, the risks associated with vulnerabilities differ

depending on the intruder's intentions and how they plan to achieve their intended result [8]. For example, an expert intruder could deliberately target specific measurements at carefully chosen measurement devices to augment the system's state used for many functions in a control center [9], an attack technique known as false data injection (FDI). These FDI attacks can also be used to augment the viewable topology of the system [10], [11], creating an issue for topology-based power flow and analysis. Furthering this, attacks to intercept data [1] and modify them to a specific malicious value could affect control operation through an attack technique known as a man-in-the-middle (MITM) or to block communications as a whole, known as a denial of service (DoS) attack [12].

The threat analysis performed in this research showed that attacks on excitation controls for generators could trigger oscillations in a power system. These scenarios looked at cases where the exciter or the measurement system was accessible through communication networks. The attacks of most interest are those targeting the voltage measurements or voltage references used for the exciter. Since the exciter control primarily impacts the reactive power output of a machine, a damping controller-based reactive compensator scheme such as a static VAR compensator (SVC) should be able to dampen oscillations, even the effects of driven oscillations.

A secondary threat vector examined attacks on power system stabilizers (PSS). It is known that poorly tuned PSS have been observed to create oscillations with neighboring generators. This can be exploited by an attacker who either modifies the exciter gains or modifies the measurements received by the exciter. Since the PSS control also primarily impacts the reactive power output of a machine, a reactive power compensation scheme such as one using an SVC should be effective in damping oscillations in this scenario. The third and last threat examined in this research was an attack on a machine governor, affecting either the measurements or the set point.

This paper is organized as follows: Section II presents cybersecurity risk and the attack vectors considered. Section III discusses the modified 12-bus system with a wind park and a SVC. Finally, Section IV studies the attack scenarios and the feasibility of the proposed damping scheme.

II. Attack Vectors Considered

As more digital monitoring devices are installed on power systems, the ability to monitor each device through utility-owned communication systems has become increasingly common. However, there are places where these networks have bridges to the open internet. These bridges open vulnerabilities for intruders to remotely manipulate or disrupt real-world processes and equipment, such as the operation of a wind turbine or a wind plant's interconnection to a power grid, circuit breakers, or bulk transmission switching devices. These events can cause disastrous effects ranging from oscillatory behavior from circuit breaker operations to sub-synchronous control interaction (SSCI) due to topology changes. Many of these network-facing features of industrial control systems are essential in modern control centers. However convenient, using network-based platforms to control and monitor physical processes considerably broadens the cybersecurity risk. Established cyber vulnerabilities, threats, and events involving the exploitation of power system equipment are split into three areas and discussed below.

1. Data Communication
2. Human Machine Interface (HMI)
3. Control Parameter Augmentation

A. Data communication

Supervisory Control and Data Acquisition (SCADA) communications are used to collect measurement data for system operations and to enable commands originating at the control center to go out to substations. Operators can open and close breakers, change generator operating points, and change power system topology through SCADA networks through switching orders. One of the main communication protocols used in North America for SCADA networks is the Distributed Network Protocol (DNP3). DNP3 can also send control signals back to the field equipment. In this section, attack vectors involving the DNP3 used for SCADA are considered.

1) Vulnerability A.1: DNP3 implementation errors

Devices used at the substation and/or the control center have had the control interface implemented incorrectly and insecurely by the manufacturer, allowing a threat agent to bypass DNP3 authentication and send malicious messages.

2) Vulnerability A.2: Use of outdated versions of DNP3 Secure Authentication (SA)

Devices used in operation are using an outdated version of DNP3 secure authentication. The use of outdated DNP3 SA is caused by legacy equipment no longer supported by its manufacturer, updating internal software/firmware is not possible, or a lack of proper patch management. A threat agent can potentially take advantage of the devices using outdated versions of DNP3 secure authentication by bypassing DNP3 SA and sending malicious messages.

3) Vulnerability A.3: Use of DNP3 without authentication or encryption

The control center and the converter substation are using DNP3 without any form of authentication or encryption. This might be by choice or because of the lack of bandwidth required for authentication and encryption. A threat agent that has gained access to the system can send malicious messages between the substation and the control center.

B. Human Machine Interface implementation errors

An HMI has been implemented for a SCADA system, allowing manufacturer observability. If the HMI is poorly secured, it creates a risk, enabling external users to control the equipment.

4) Vulnerability B.1: Use of HMI without authentication or encryption

A threat agent has gained access to the system through the HMI and can send malicious messages between the substation and the control center.

5) Vulnerability B.2: Unauthorized use of vendor terminal at an external interconnection such as a wind park

A threat agent that has gained access to a vendor terminal used for diagnostics, such as ones used at wind parks.

C. Control Parameter Augmentation

The settings for control devices are accessible via physical access to the equipment as well as through remote engineering access. The network vulnerability can include remote access for changing settings and remote firmware updates. Changes in the equipment settings may cause a de-tuning effect and oscillatory behavior.

6) Vulnerability C1: Control Parameter Augmentation of Inverter Based Resources

A threat agent has gained access to the vendor control panel at the resource location.

III. Power System Model

A. Test System

The power system model used in this research is the IEEE 12-bus system test system [13] shown in Fig. 1. The IEEE 12-bus system was developed as a platform for the study of dynamics and control for power systems with high penetration of power electronic coupled generation, FACTS devices, and HVDC transmission [13]. This IEEE test system is designed with the generation and loads separated by long transmission lines. Furthermore, the system may be split into three sub-areas for additional analysis. The 12-bus model was modeled on the Real Time Digital Simulator (RTDS) to thoroughly test the system on platform capable of simulating systems at the electromagnetic time scale.

These three areas are divided based on the overall system oscillation behavior and swing centers. The first area is predominantly a generation area, where generators connected at Bus 9 and Bus 10 are hydroelectric generators rated 800 MVA and 700 MVA, respectively. Area 3, shown in Fig. 1, is the main load center with some generation available. The generator connected to Bus 11 in this region is a 500 MVA hydroelectric generator. The main modifications to the IEEE 12-bus system are within Area 2 and Area 3. Area 2 is the transmission system between Area 1 and Area 3, with some hydro generation available at Bus 12 rated at 500MVA. The transmission line between buses 7 and 8 is series compensated to 70 % of the total impedance of the line (i.e., each capacitor bank is set to 35 %. In addition, a large wind farm is added at Bus 8, built to simulate 400 Type 3 turbines, and where each Type 3 turbine is rated for 1.67 MVA.

B. Damping Controller

To test the damping potential of FACTS devices in a scenario with high renewable energy source penetration, an SVC has been installed at Bus 3. A novel control system [14] is installed on the SVC utilizing a PMU to provide sufficiently high sample rate measurements. The controller allows the SVC to simultaneously regulate both reactive power and frequency through reactive power modulation. The block diagram of the SVC frequency control loop is shown in Fig. 2.

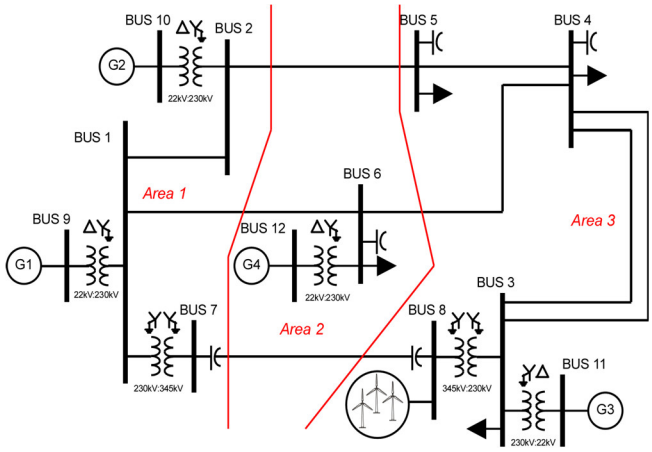

Fig. 1. Modified IEEE 12-Bus system with added wind park

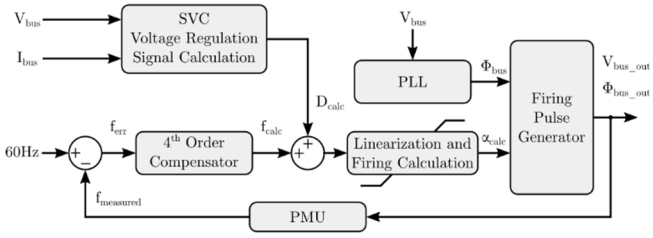

Fig. 2: Block diagram of the SVC's frequency control loop

The transfer function acts as a filter on the frequency error of measurements taken by the PMU, increasing control effort within the bandwidth constraints of the controller. This control increases SVC output modulation based on the magnitude of frequency deviation from nominal system frequency while maintaining existing control gain applied to the voltage measurement in isolation. The feedback signal path (i.e., return ratio) is $T(s) = C(s)P(s)H(s)$, where $C(s)$ is the control transfer function, $P(s)$ is the plant, and $H(s)$ is the PMU [15]. In this case, $P(s)$ is estimated using an averaged (i.e., Welch) periodogram over a range of the compensator function is:

$$C(s) = \frac{10(s+14)(s^2+1.5s+10)}{(s+20)(s+8)(s^2+1.8s+18)} \quad (1)$$

The cascaded poles and zeros in Eq. 1 maximize gain in the control signal path at frequency intervals of interest, constrained by the control bandwidth between the octaves of 2 to 8 Hz. The bandwidth constraint therefore minimizes control effort in bands associated with other natural disturbances found in power system operations and therefore have minimal impact on the voltage regulation functionality of the SVC under otherwise nominal operations.

In the simulation, regenerative oscillations are not detected, indicating sufficient phase margin. A more thorough stability analysis, including stability in the face of saturation nonlinearities, is reserved for future work. This is consistent with the minimal phase system assumption implied in the control design (i.e., no phase lag is outside of that found by the Bode Phase/Gain Relationship.) This controller was designed

and implemented in the RTDS and applied directly into the FACTS system for control.

IV. . Simulation Studies

The threat scenarios primarily focus on generator control components such as exciters, power system stabilizers, and governors coupled with communication abilities. Specifically, generation facilities connected to remote control centers or have automatic generation control capability. To explore the effect of the threat vectors discussed in Section II, a few specific scenarios are developed to showcase the damaging effects that measurement corruption can produce.

To relate the attack vectors presented in section II to simulations, these vectors may be split into two categories: augmentation of measurements and augmentation of control parameters. Augmentation of measurements may be defined as the corruption of measurements used for control action for the exciter or governor, such as voltage, current, and speed. An augmented control parameter may be described as the intentional change of control parameters such as the upper and lower excitation voltage and speed boundaries or proportional-integral-derivative (PID) feedback control gains.

In correlating the attack vectors to cyberattacks on the 12-bus, we begin by setting the scenario where the modeled system contains communication-assisted facilities. This not only provides enormous benefits, it also increases the paths of potential cyberattacks. As in Section II A, DNP3 is a widespread communication protocol that allows the user to monitor and send commands through the communication medium. In the first attack, the attacker targeted the control command of DMP3 and opened a breaker, resulting in a change of topology in the system. Specific changes to topology can have dangerous effects if the system's impedance changes drastically. The second attack consists of a measurement stream on the excitation system of a generator. The effective signal is spoofed with a malicious set. Lastly, in Section II C, the control parameters on the generation asset are subject to threat as actors may physically misconfigure devices on site. Here, the third simulated cyberattack targets the governor's reference signal for torque, where the control reference parameter has been spoofed.

A. Attack trigging sub-synchronous oscillations in wind farm

In this scenario, the attacker created a topology change in the system by causing the transformer relay between buses 3 and 8 to trip and lock out. As a result, in conditions where the wind park is radially connected to a series compensated transmission line. Attackers may potentially gain access to a transformer relay if it is connected to the network. Changes in basic settings (e.g., current transformer ratio) can trip the differential element, thus tripping the breakers surrounding the transformer.

The radial connection of the wind farm triggers SSCI, and the amplitude of the current from the wind park drastically increases, as shown in Fig 3. The magnitude of the current can damage the series capacitor banks (SCB) and/or the wind turbine (e.g., crowbar). The wind park will also likely disconnect from the power system, leading to an outage or even a blackout. The control system was removed from the wind park to show that the designed 12-bus model has the potential to encapsulate SSCI behavior.

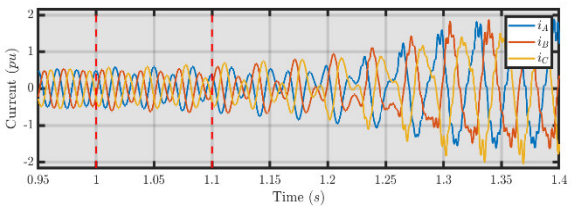

Fig. 3. Current injected by the wind park during SSCI triggered by an attack

B. Excitation system cyberattack

In the second set of cyberattack vectors, the attacker modifies the measured reference signals used by the excitation system. The specific vectors targeted were the generator field voltage and current signals. The reference signals are replaced with the designed cyberattack to create a transient emanating from the generators electrical torque. These tests have been conducted on the complete 12-bus system without generating power from the wind farm.

In implementing the cyberattack, a 10-second repeating vector was created to simulate oscillations on the power system. In each, the reference signal is spoofed by the cyberattack. In testing the exciter cyberattacks, spoofing the field current measurement did not show impactful results due to the exciter automatically adjusting its voltage; therefore, changing the exciter voltage reference was the most effective. In the following case, the reference signal was augmented by a scaling function between 0 - 200 %, as shown in (2). Where z_k is the original signal, C_k is a scaling factor as denoted by the user, and lastly, z_k^c is the corrupted signal after the augmentation.

$$z_k^c = z_k \cdot C_k \tag{2}$$

The first attack vector explored is on the generator field voltage measurement read by the exciter. This signal is intercepted and augmented by a defined time series data array. The magnitude of the attack is between -18% and +18% of the measured signal. This can be seen in Fig. 4, where the plot of the cyberattack signal was recorded and plotted for visualization. The exciter's control system response to the cyberattack is shown in Fig. 5, where the black trace denotes the per-unit excitation voltage. The resulting waveform is not square due to the exciter adjusting its voltage with respect to the voltage reference. The exciter primarily impacts reactive power output. However, since there is cross-coupling to the reactive power output of the machine, the attack triggers forced oscillations in real power and frequency.

Note that the system with the SVC enabled reduced the peaks caused by the cyberattack since the SVC impacts local voltage magnitude and, hence, reactive power.

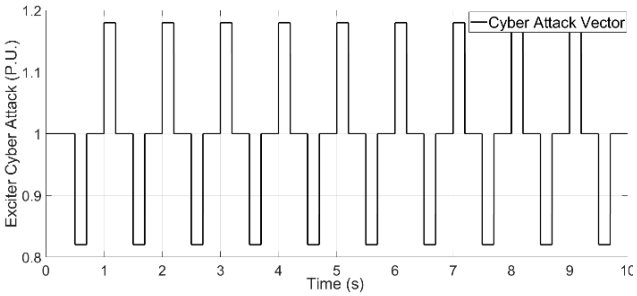

Fig. 4. Cyberattack vector on exciter voltage measurement

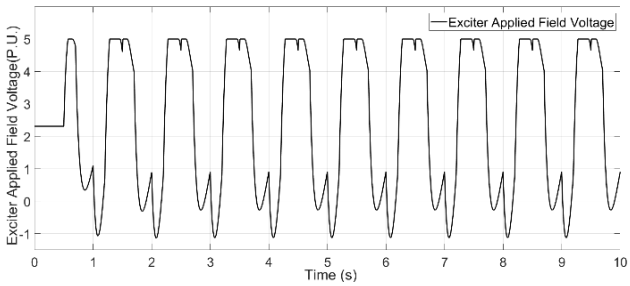

Fig. 5. Excitation Voltage Applied to Generator 6

Fig. 6 shows the frequency measured at Bus 6, where the generator under attack is connected. It can be noted that the oscillation mimics the waveform supplied by the exciter. Furthermore, it can be shown that the SVC damps the oscillation. The magnitude of the damping results from Bus 6 being physically far away from the SVC located at Bus 3. Fig. 7 shows the frequency recorded at Bus 3 in the original system (black trace) and with the SVC enabled (red trace). Here, the positive impact of the damping scheme of the SVC is shown in red. The SVC effectively reduces the amplitude of the forced oscillation in the system. But it does not drive them to zero.

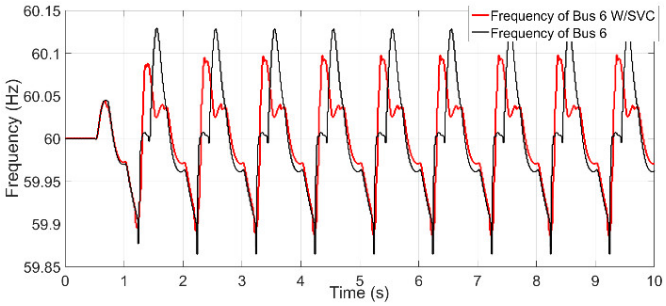

Fig. 6. Frequency measured on Bus 6 with and without the SVC

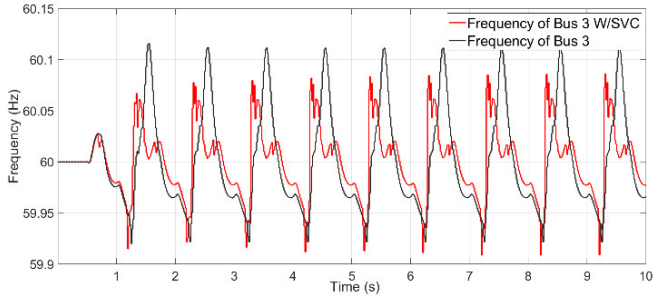

Fig. 7. Frequency measured at Bus 3 with and without the SVC

C. *Cyberattack on governor*

In the third series of cyberattacks, the governor was targeted, and its reference signals were spoofed. The resulting torque signal was intercepted and spoofed as well, resulting in an augmentation of the torque supplied to the generator, therefore affecting the power supplied by the generator. Similar to the excitation attack, the torque signal was intercepted and augmented by a 10-second cyberattack signal shown in Fig. 8. Note that the exciter was set to a constant excitation value to avoid any interference from the exciter itself.

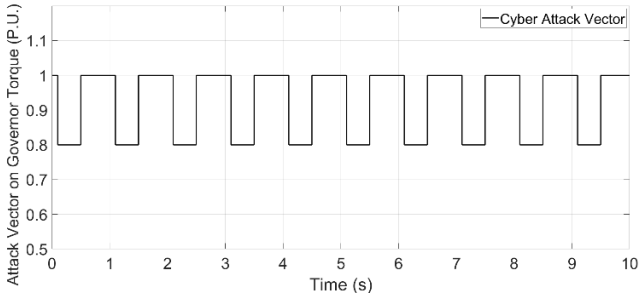

Fig. 8. Cyberattack vector targeting governor torque measurement

Fig. 9 shows the resulting torque supplied to Gen 6 through the duration of the cyberattack. Since the cyberattack affected the torque applied to the generator, the external SVC did not significantly impact the mechanical torque of the generator itself. Fig. 10 shows the frequency measured at Bus 3 without (black trace) and with (red trace) the SVC enabled. It can be observed that the SVC and its control scheme can provide a damp to reduce the oscillation at the bus. In comparing the two cyberattacks, it is noted that while the attacks both resulted in forced oscillations, the behavior of the oscillations was different. For the excitation attack, generator voltage fluctuated, indirectly causing a frequency change to the inherent coupling of active and reactive power.

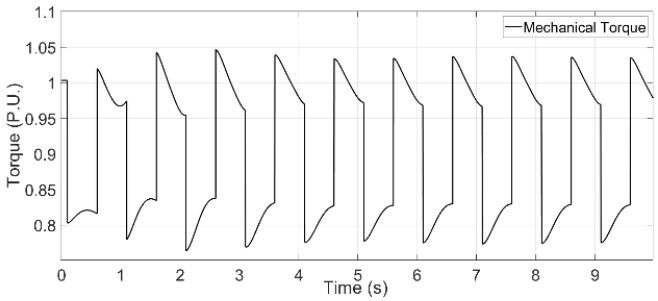

Fig. 9. Torque supplied to Generator 6

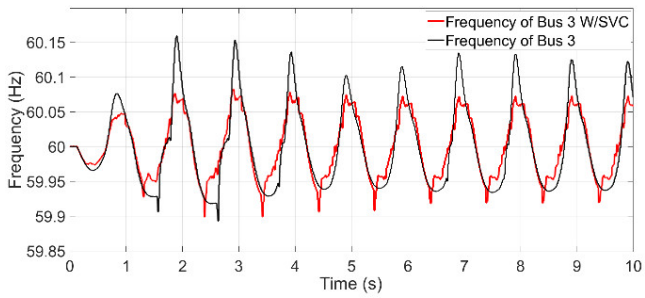

Fig. 10. Frequency at Bus 3

When analyzing the second cyberattack on the governor, since the torque into the generator fluctuates, the real power of the machine is impacted. An oscillation is apparent due to the changing injection of real power. In this case, the power oscillations are directly driven by the attack on the governor. Similar to a power system stabilizer, the SVC is able to provide indirect damping by modulating reactive power injection. The damping effect is weaker. Through these two attack vectors, the SVC may be evaluated for performance against forced oscillations stemming from real and reactive sources.

V. Conclusion

Through this research, forced oscillations induced by cyberattacks against generator controls were implemented and explored through excitation and governor signal spoofing attacks. Each attack was derived from communication-based access points, and the attack vector was regulated to signals which may be read from live data streams. During the excitation attack, a forced oscillation was induced in the system, creating a transient on the power system's frequency. Through the implementation of a reactive power-based frequency control scheme, damping was achieved on the power system to reduce the effects of the cyberattack on the oscillatory behavior of the power system. The SVC and its reactive power control capabilities applied to reduce frequency oscillations effectively mitigated this reactive power-based oscillation.

In the second scenario, attacks were conducted on the governor of the same generator, and similar but diminished results were obtained. The SVC dampened oscillations near its location but was not as effective as when the exciter was attacked. The frequency oscillations caused by the governor attack are being directly produced by the voltage angle changing and active power being altered; trying to dampen the oscillations through reactive power control is less effective. The coupling between the cause of the oscillation and the oscillations is much stronger with the governor attack than with the exciter attack. These results noted positive outcomes in the effectiveness of the damping scheme developed and implemented with SVCs. As this damping scheme was evaluated for forced oscillations, tests on other oscillatory behavior would be an area of future work.

In both cases, the SVC's response time was adequate to enact damping. Implementing a voltage source converter device such as a static synchronous compensator (STATCOM) will make it possible to enact faster responding damping. FACTS devices capable of directly interacting with real power injections, such as series compensators or STATCOMs with energy storage, provide added capabilities to improve resilience against forced oscillations.

Acknowledgment

This work is part of a U.S. Department of Energy project, under the Cooperative Agreement No. DE-OE0000897. Disclaimer: This paper was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

References

[1] T. Surinkaew, K. Emami, R. Shah, S. Islam and N. Mithulananthan, "Forced Oscillation in Power Systems With Converter Controlled-Based Resources–A Survey With Case Studies," in *IEEE Access*, vol. 9, pp. 150911-150924, 2021, doi: 10.1109/ACCESS.2021.3124246.*)*

[2] S. A. N. Sarmadi and V. Venkatasubramanian, "Inter-Area Resonance in Power Systems From Forced Oscillations," in IEEE Transactions on Power Systems, vol. 31, no. 1, pp. 378-386, Jan. 2016, doi: 10.1109/TPWRS.2015.2400133.

[3] M. A. Magdy and F. Coowar, "Frequency domain analysis of power sysem forced oscillations," IEEE Proc. Gener., Transm., Dostrob., vol. 137, no 4, pp. 261-268, Jul. 1990.

[4] C. D. Vournas, N. Krassas, and B. C. Panadias, "Analysis of forced oscillations is a multi-machine power system," in Proc. IET Int. Conf. Control '91, 1991, pp. 443-448.

[5] Y. Cheng *et al*., "Real-World Subsynchronous Oscillation Events in Power Grids with High Penetrations of Inverter-Based Resources," in *IEEE Transactions on Power Systems*, doi: 10.1109/TPWRS.2022.3161418.

[6] Joint NERC and WECC Staff Report, "(2020, November) San Fernando Disturbance, South California Event: July 7, 2020."

[7] IEEE PES Wind SSO Taskforce, "PES TR-80: Wind Energy Systems Subsynchronous Oscillations: Events and Modeling, 2020," https://resourcecenter.ieeepes.org/publications/technical-reports/PES TP TR80 AMPS WSSO 070920.html

[8] U.S Department of Energy Energy Efficiency and R. Energy Wind Energy Technologies Office, "Roadmap for Wind Cybersecurity," 2020.

[9] A. Sharma, "A combined survey on distribution system state estimation and false data injection in cyber - physical power distribution networks," no. October 2020, pp. 41–62, 2021, doi: 10.1049/cps2.12000.

[10] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber Risk Analysis of Combined Data Attacks Against Power System State Estimation," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3044–3056, May 2019, doi: 10.1109/TSG.2018.2817387.

[11] F. F. Wu and E. L. Wen-Hsiung, "Detection of topology errors by state estimation," *IEEE Transactions on Power Systems*, vol. 4, no. 1, pp. 176–183, 1989, doi: 10.1109/59.32475.

[12] H. Zhang, B. Liu, and H. Wu, "Smart Grid Cyber-Physical Attack and Defense: A Review," *IEEE Access*, vol. 9, no. December 2015, pp. 29641–29659, 2021, doi: 10.1109/ACCESS.2021.3058628.

[13] Shan Jiang, U. D. Annakkage, A. M. Gole, "A Platform for Validation of FACTS Models", IEEE Transactions on Power Delivery. Vol. 21, No.1, January 2006.

[14]] K. Bean, "Simultaneous Frequency and Voltage Regulation with Static Var Compensation." Master's Thesis, University of Idaho, 2022.

[15] D. Roberson and J. F. O'Brien, "Loop Shaping of a Wide-Area Damping Controller Using HVDC," in IEEE Transactions on Power Systems, vol. 32, no. 3, pp. 2354-2361, May 2017, doi: 10.1109/TPWRS.2016.2608356.