Journal of Future Internet
2019 Vol. 3, No. 1, pp. 12-19
ISSN(e): 2409-790X
ISSN(p): 2413-8401
DOI: 10.18488/journal.102.2019.31.12.19

ANALYSIS OF CYBER ATTACKS ON LOAD FREQUENCY CONTROL IN SMART GRID

Md Musabbir Hossain[1+]
Fatamatuz Ayasa Khan[2]

[1]*School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China.*
Email: musabbir@shu.edu.cn
[2]*Computer Science and Engineering, Islamic University, Kushtia-Jhenaidah, Bangladesh.*

(+ Corresponding author)

Article History
Received: 20 August 2019
Revised: 25 September 2019
Accepted: 28 October 2019
Published: 3 December 2019

Keywords
LFC
Smart grid security
Cyber attack
Smart grid
Power system stability.

ABSTRACT

Smart Grid has gained tremendous technology momentum over the past few years. The data and cyber security of the smart grid face severe challenges and has gained significant importance. This paper addresses the reliability of smart grid by examining their own importance and the effect of cyber-attack during sudden load changes in frequency disturbing aspects. Moreover, it also introduces a solution approach for stabilizing the system. Using the continuous power flow approach with static var compensator (SVC) and static synchronous compensator (STATCOM), maximum load ability of the load buses is determined. The stable limit of speed control for load frequency control (LFC) and integral controller gain for automatic generation control (AGC) is extracted from their characteristic equations to evaluate the effect of cyber-attack on power systems. Simulations are conducted to demonstrate the frequency variations and oscillations of the power system, depending on the nature of cyber-attack (positive biased or negative biased attack). Finally, to eliminate these oscillations, a feedback LFC block with a three-input shift is proposed.

Contribution/Originality: Cybersecurity of the modern power system is becoming a major concern throughout the design and implementation of smart grid applications and technology. Therefore, it is essential to study the impact of cyber attacks on the power system. This paper discusses cyberattacks that induce positive and negative biased attacks and their impact on transient stability. Cyber attacks are launched on measured data for a FACTS device (static var compensator - SVC). Therefore, a new procedure of analyzing power system frequency stability under cyber-attack by static var compensator (SVC) and static synchronous compensator (STATCOM).

1. INTRODUCTION

Electricity cannot be collected like wind energy from moving air or pumped like oil from the surface. It is produced by the use of natural gas, oil, or nuclear reactions from primary energy sources. So, it's considered a secondary power source. Today, with the rapid development of social economy, science and technology, the demand for electricity is greater than ever before. Due to the excessive exploitation and use of these primary energy sources, energy reserve shortages have been widely recognized. Therefore, finding a sustainable and effective way to tackle energy issues in the long term is urgently needed. Renewable energy sources like wind and solar energy tend to be a better candidate for future generation of electricity in terms of safety, cleanliness and sustainability over the past few years. Renewable energy advantages are now widely recognized and the use of renewable energy is now on a fast track. The amount of wind and solar photovoltaic generating capacity added in 2015 amounted to 118GW, well above the next highest annual estimate, the 94GW of 2014 [1].

Flexible AC transmission system, also known as FACTS, is not only capable of providing a solution to improve power system transmission efficiency with great flexibility but is also helpful in enhancing the reliability of the power system. The dynamic stability of the power system can be defined as the stability of small signals and transient stability [2]. Small-signal stability determines the power systems' ability to recover from minor fluctuations without losing synchronism to their original steady state. Small disturbances caused by random fluctuations in certain system parameters can stimulate power system oscillations in normal power system operations; these oscillations are also known as low frequency oscillations as their frequencies (0.1Hz~2.0Hz) are relatively low compared to the basic AC system frequency (50/60Hz) [3]. One of the main causes of small-signal instability is insufficient damping of low-frequency oscillations; and even for a stable system, it is also important to ensure that the system has sufficient damping to minimize the settling time of the decaying oscillations based on certain system operating requirements.

Increased load on the interconnected grid system makes the system day by day heavily loaded. In addition, operational deregulation is causing a dramatic shift to modern electrical systems. All these make it unstable and less stable to the power system. At the same time, because of the increase in electronic charges, the quality of power supply has become a critical issue [4]. In view of all these things, there is now an increasing trend to switch from a centralized power grid system to a local energy grid with a control capability called micro grid in the event of an emergency or power shortage in the main grid [5].

Micro grid can separate and operate autonomously from the conventional grid. In addition, small-scale power stations are required to enlighten remote areas in order to set up where grid extension for power supply is expensive and difficult. The availability of power supply in many cases becomes the primary concern for medical treatment, scientific study, manufacturing, transport, etc. For all these cases, it is necessary to set up a special generating station [6] to ensure continuous power supply. The main power sources for these devices are renewable energies such as photovoltaic cells (PV), fuel cells, wind power, etc. in conjunction with diesel generators. For these small power generating networks, decentralized and autonomous control of generation is necessary. At substation or customer loads, they are normally connected to the grid. The power generated by PV, fuel cells are in the form of direct current, whereas the power generated by wind generators, micro turbines are in the form of alternating current at a frequency other than the 50 Hz required. Therefore, the system containing these sources requires a power electronic interface [7-11].

Since small-scale isolated power systems can help improve energy quality and flexibility in power supply, power utility companies are also gaining attention. We can not only be used to provide spinning reserve, but also to reduce the cost of transmission and distribution. Also, during the event of an outage in the primary substation they can be used to feed the customers [12]. Modern micro grid can provide energy that can switch from insulated mode to grid-connected mode. It should ensure the reliability of the power supply, which includes a smart regulation of the power station. To do this, it is necessary to adopt advanced control system with communication interface. To ensure smooth power supply, system reliability should be properly maintained [13].

In order to stabilize the system's output variable, its pre-assigned value should be kept constant in general by voltage and frequency. Due to any disruption of these output quantities, the entire system could collapse. Due to any interruption of these output quantities, the entire system can collapse. Cyber risk on an insulated power station is considered as being fitted with a smart control system to be a powerful means of disruption that can cause the device to become seriously unstable. The system may lose its stability or cause poorly damped oscillations when a disruption occurs in the system such as generation/load imbalance or any fault caused by cyber-attack. To enhance system performance, the research aims are as follows:

1. Analyzing the frequency deviations and oscillations of an insulated power station on its cyber vulnerable parts, such as load frequency control (LFC) and automatic generation control (AGC), throughout the cyber-attack. Therefore, it is important to determine how to eliminate frequency deviations and oscillations.

2. Electrical test systems are studied using PSAT (Power System Analysis Toolbox) in MATLAB to improve system stability and reduce the possibility of voltage failure. An analysis of the voltage stability of the WSCC 9-bus test system is conducted with STATCOM and SVC. The findings show a higher voltage stability margin for a STATCOM than for an SVC.

2. FREQUENCY STABILITY IMPROVEMENT DURING CYBER ATTACK

The alternator frequency varies with a power station's load switch. The frequency sensor detects the system frequency and the LFC sets the primary mover speed to compensate for the system frequency according to the signal from the frequency sensor. In this study, the vulnerable quantity is known as speed regulation. Because of cyber-attack, malfunctioning of the governor speed regulator makes the prime mover's speed out of reach and results for unstable device rate.

Appropriate selection of integral controller gain (KI) is essential for the proper functioning of AGC. Improper choice of the KI value results in a governor failure in setting the correct point to restore the frequency of the device. This research describes KI as the other weak cyber-attack quantity. Any KI change due to unauthorized access to the AGC loop may cause system frequency oscillation that disturbs the stability of the system. Cyber-attack is divided into two forms in this work, one is positively biased, and the other is negatively biased, depending on the affected value of speed regulation (R) and integral controller gain (KI). First, the control system is believed not to be targeted by unauthorized individuals. In this condition, if a sudden change under load (increase in load) occurs, the device frequency will drop for a brief instant below the nominal frequency. The frequency sensor detects the device frequency drop and for proper speed control sends signals to the LFC. The LFC sets the governor speed control to compensate for the prime mover speed and regulate the system frequency according to the signals from the frequency sensor. It will only be necessary for the governor speed limit to be properly set. Due to cyber-attack, LFC may not be able to set the regulation properly and if this occurs then the system frequency will oscillate and make the system unstable. Similar to Hassan [14] the stable speed limit (R) can be obtained from the characteristic equation of the LFC loop using Routh-Hurwitz series as follows:

$$\frac{\Delta\Omega(s)}{\Delta P_L(s)} = \frac{(1+\tau_g s)(1+\tau_T s)}{(2Hs+D)(1+\tau_g s)(1+\tau_T s)+\frac{1}{R}}$$

This study considers an insulated power plant with the following parameters at a nominal frequency of 50Hz with 250MW turbine output power and a sudden change in load of 50MW [15]. From the above formula, the stability limit of speed control is obtained as R > 0.0133 using the power system parameters of the Table 5.1and Routh-Hurwitz set. From Figure 1(a) If R=0.05, the frequency variance of the device is stable. Therefore, the fixed value of R should be 0.05 for the balanced operation of this power station. Any deviation from this fixed value results in the unstable variance of the device frequency. The uncertainty of system frequency deviation renders the governor unable to account for the difference in frequency i.e. In the case of a sudden change in load, the device frequency will not be restored. The deviation from the defined value of speed regulation is due to the cyber-attack on LFC (Unauthorized access to LFC control).

Based on the governor speed control, a shift in the system load can result in a steady state frequency variance with the primary LFC loop. The primary LFC loop takes a considerable amount of time to restore unallowable device frequency. A modification is needed to LFC to reduce the frequency deviation to zero. Through adding an integral controller to operate on the load reference setting to adjust the speed setting level, the adjustment can be accomplished. The integral controller increases the type of system through 1 which forces the final deviation of frequency to zero. The LFC system is the Automatic Generation Control (AGC) with the addition of a secondary circuit (integral controller). It is important to change the integral controller gain KI for a satisfactory transient response. Adding integral controller in parallel with LFC enables the governor to set acceptable points to increase

turbine speed in the event of a sudden increase in load and to restore the system frequency faster than the primary LFC circuit.

Appropriate KI value is determined using the equation of AGC loop characteristics from which the function of the closed-loop transfer is obtained [14].

$$\frac{\Delta\Omega(s)}{-\Delta P_L(s)} = \frac{(1+\tau_g s)(1+\tau_T s)}{(2Hs+D)(1+\tau_g s)(1+\tau_T s)+K_1+\frac{5}{R}}$$

Unauthorized access to AGC control can result in deviation of the system frequency and sometimes render the deviation in nature oscillating. If the system frequency deviation is unpredictable, the system frequency will not be restored by the president. Moreover, the attack on AGC may cause unwanted delay to restore system frequency. The frequency difference oscillation contributes to system frequency instability. Because of this oscillation, the governor will not set the right point to restore the frequency of the device. The oscillation deviation in the green curve is higher, suggesting a serious attack on AGC and the governor will no longer be able to restore the frequency of the system. The more the positive biased attack occurs, the greater the effect on the intensity of the program would appear. The frequency of the AGC attack depends on the type of attack. Negative biased attack means that the value of KI decreases from the set value due to unauthorized access to the AGC system. This attack may be counter to the objectives of using integral controller with primary LFC loop to obtain AGC system to reduce to zero the frequency deviation. To increasing the frequency deviation to zero, the primary LFC control loop is adjusted to form AGC. It is clear that frequency is deviated from nominal frequency due to negative biased attack, which leads to unwanted delay in restoring the frequency of the system. Negative biased attack on AGC is not as severe as it is positive because it does not oscillate in essence the frequency deviation.

3. MITIGATION OF FREQUENCY DISTURBANCE

When an alternator's load is adjusted, the prime mover's speed also adjusts in accordance with Lenz's rule. When the load increases, the prime mover's rate decreases and vice versa. The relationship between speed and frequency is related to the following formula [14]:

$$f = \frac{NP}{120}$$

Where, f = generator electrical frequency, P= generator pole number, N= prime mover speed in rev/min. When the load of a generating station increases suddenly, the generators need to supply more power to load and so the speed of the prime mover drops causing a drop-in frequency as well.

But this frequency fall is not allowed to preserve the stability of the system. This rise or fall in frequency is not allowed to preserve the stability of the system. The unexpected amplitude variability should be recovered as quickly as possible. The environment of the governor performs this function. If the frequency deviation is constant (sudden rising or falling), the governor is able to restore the system frequency by increasing or decreasing the fuel supply. However, if the variation in frequency is not constant (in fact oscillating), then the governor would fail. The frequency disturbance caused by cyber-attack may collapse the whole system stability. By connecting a three-input switch in the LFC block feedback direction, a solution is proposed [14] to reduce the oscillating frequency deviation. The switch's mathematical description is shown below.

$$S.P = \begin{cases} U1, & U2 \geq Threshold \\ U3 & else \end{cases}$$

Where, $S.P$ = Terminal shift, $U1$ = Terminal 1, $U2$ = Terminal 2, $U3$ = Terminal 3 data. The switch can mitigate the instability of cyber-attack-induced frequency deviation during sudden change of load.

4. RESULTS AND DISCUSSIONS

If the importance of speed control increases due to cyber-attack, a positive biased attack is triggered [14]. From Figure 1(a), it is obvious that the system frequency can be restored in the event of a positive bias without disrupting the system frequency stability. But too much system frequency variation may cause the governor to take longer to set the desired system frequency to restore location. Thanks to cyber-attack, the decline in the price of speed control is called negative biased terrorism. Because of the attack, if the speed control value falls below the stable condition (R>0.0133), the frequency deviation is oscillating in nature and the governor does not restore the frequency of the device as shown in Figure 1(b). Therefore, negative biased cyber-attack is the major challenge for engineers to keep the system frequency in stable condition during the system's sudden change in load. Simulation curves are built depending on the nature of cyber-attack (positive biased attack or negative biased attack) and a solution approach is proposed to stabilize the system. For negative biased attack, if the speed control value falls below the stable condition, the frequency deviation is oscillating in nature and the governor does not restore the frequency of the system as shown in Figure 2(a). Through their output curves, the disparity between the primary LFC loop and AGC can be easily determined. The same premises used in the LFC process are used to draw the output curves in Figure 2(b). In the Figure 3(a), the effect of a positive biased attack on AGC is displayed and the red curve is the set value under unaffected condition. The yellow curve means that there is a slight frequency deviation from the set condition (Red curve). This leads to unwanted delays to restore the system frequency. The blue curve indicates that the frequency deviation is slightly oscillating in nature. Out of the Figure 3(b), as the R value decreases from 0.05(1/R=1/.05=20), the frequency variance shifts to instability. That is why the threshold value for injecting the set value after cyber-attack is selected as (1/R=1/.04) 25. The attack can occur due to unauthorized access to the control system and also due to bad data being inserted into the system. If the input terminal 2 value is greater than the threshold value, which means that R is less than 0.04, then the system tends to become unstable.

The switch enables the output terminal 1 at this moment to insert the set value forcedly in order to achieve system stability. If the input value at terminal 2 is below the threshold, the system appears to be stable and the switch allows input 3. When a generating station's load increases suddenly, the generators need to provide more power to load, so the prime mover's speed drops causing frequency drop as well. But this frequency fall is not allowed to preserve the stability of the system. The frequency change with the load change is shown in Figure 4(a). Finally, Figure 4(b) clearly indicates the deviation of the cyber-attack frequency before and after the switch. As the load rises abruptly, the frequency deviates during the attack without any change. Whereas the deviation of frequency can be greatly reduced using the suggested shift.

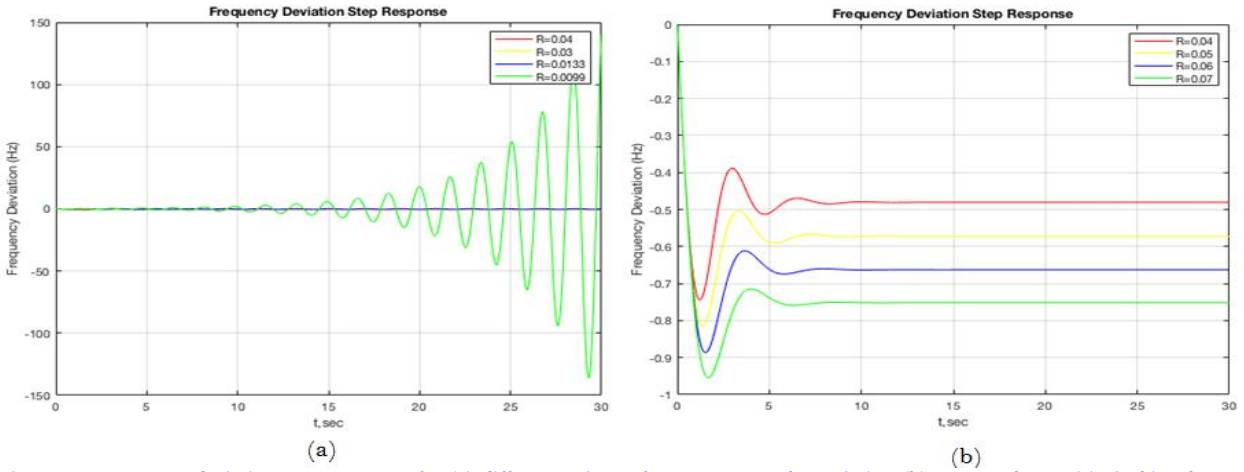

Figure-1. Frequency deviation step response for (a) different values of governor speed regulation (b) LFC under positively biased attack condition.

Source: Hassan [14].

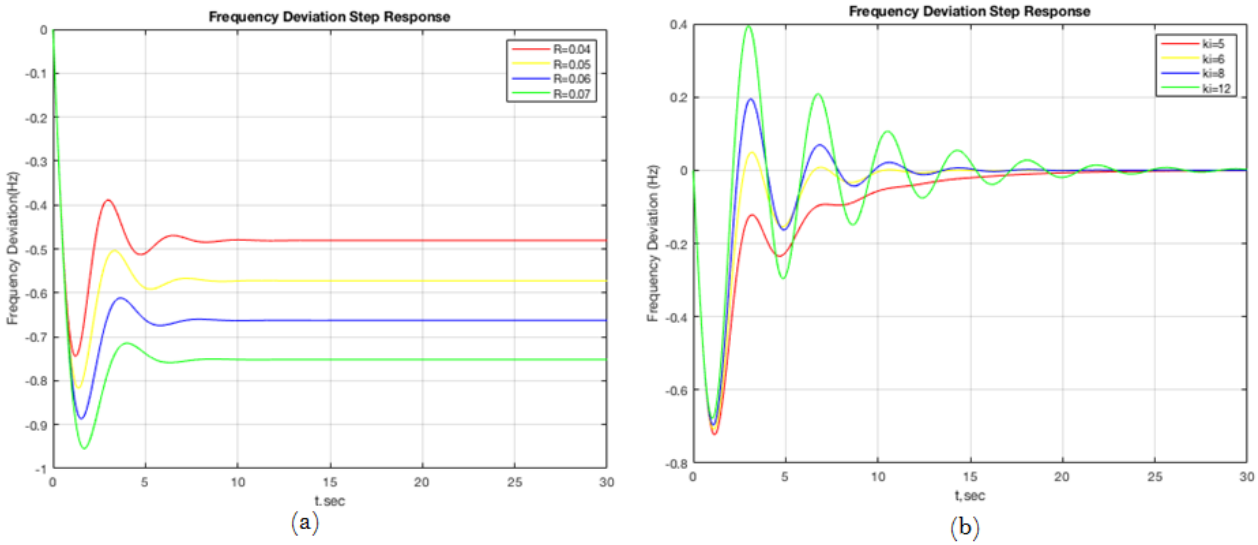

Figure-2. Frequency deviation step response for (a) LFC under negatively biased attack condition (b) determining frequency deviation step response for AGC.

Source: Hassan [14].

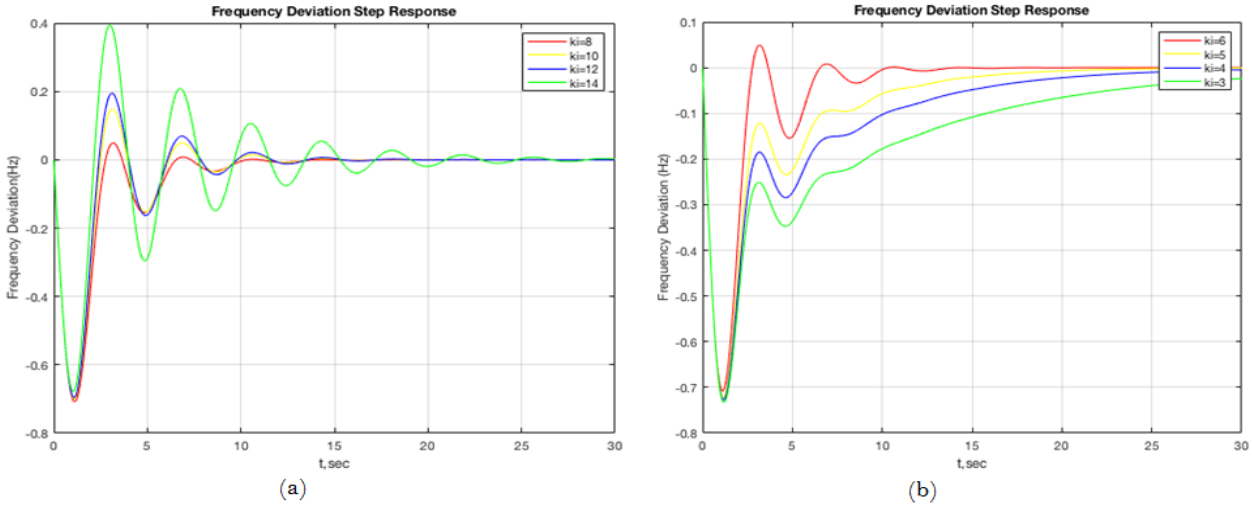

Figure-3. Frequency deviation step response for determining (a) frequency deviation for AGC under positively biased attack condition (b) frequency deviation for AGC under negatively biased attack condition.

Source: Hassan [14].

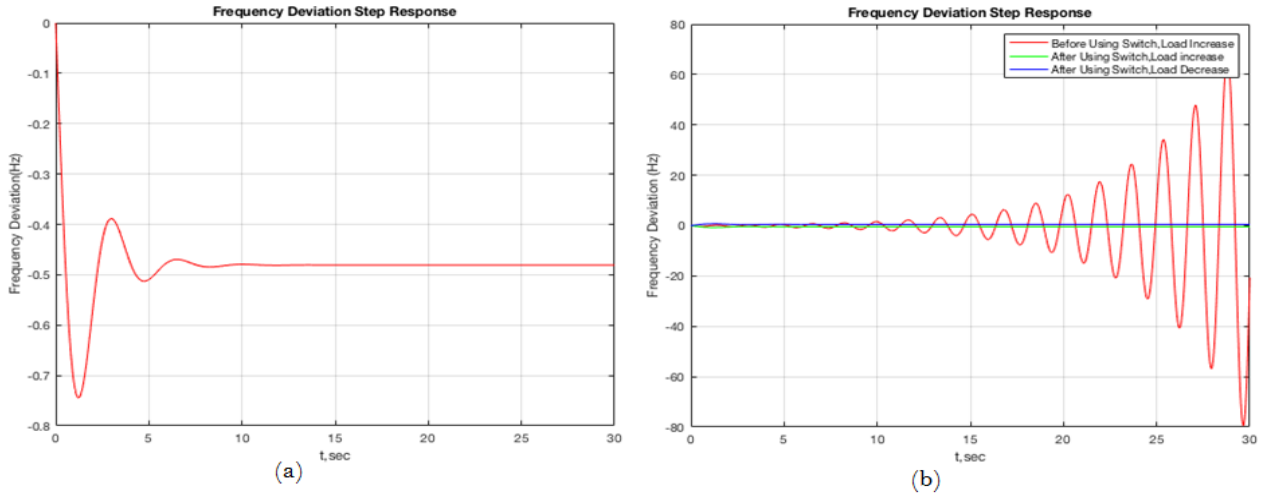

Figure-4. Frequency deviation step response for determining (a) frequency deviation step response under sudden load increase (b) frequency deviation step response using switch in LFC loop under sudden load change.

Source: Hassan [14].

5. CONCLUSION

On LFC and AGC, the impact of cyber-attack is analyzed by considering their individual set value or stable limit parameter which can be an appropriate means of cyber-attack.

Positive biased attack on LFC causes the frequency of the system to fall but quickly reaches stable condition. While it develops severe frequency oscillation on AGC that prevents the governor from setting the appropriate point to restore the frequency of the system.

For AGC, negative biased attack is not as serious as positive attack, but with little oscillation in LFC, frequency deviates greatly. Proper connection of a three-input switch in the LFC feedback loop and sufficient threshold assumption can effectively minimize cyber hazard frequency disturbance.

Funding: This study received no specific financial support.
Competing Interests: The authors declare that they have no competing interests.
Acknowledgement: Both authors contributed equally to the conception and design of the study.

REFERENCES

[1] UN News, "Major milestones reached on renewable energy investments, UN reports, UN News, 25-Mar-2016. [Online]. Retrieved: https://news.un.org/en/story/2016/03/525392-major-milestones-reached-renewable-energy-investments-un-reports. [Accessed 15-Nov-2019]," 1994.

[2] N. G. Hingorani, "Flexible AC transmission," *IEEE Spectrum*, vol. 30, pp. 40-45, 1993.

[3] K. Prasertwong, N. Mithulananthan, and D. Thakur, "Understanding low-frequency oscillation in power systems," *International Journal of Electrical Engineering Education*, vol. 47, pp. 248-262, 2010.

[4] D. E. Olivares, A. Mehrizi-Sani, A. H. Etemadi, C. A. Cañizares, R. Iravani, M. Kazerani, A. H. Hajimiragha, O. Gomis-Bellmunt, M. Saeedifard, and R. Palma-Behnke, "Trends in microgrid control," *IEEE Transactions on Smart Grid*, vol. 5, pp. 1905-1919, 2014.

[5] M. K. Jalboub, A. M. Ihbal, H. S. Rajamtani, and R. A. Abd-Alhameed, "Determination of static voltage stability margin of the power system prior to voltage collapse," presented at the In Eighth International Multi-Conference on Systems, Signals & Devices. IEEE, 2011.

[6] R. Claudia and F. P. Maciel Barbosa, "Indicators for voltage collapse margin," presented at the Asia- Pacific Power and Energy Engineering Conference, 2010.

[7] A. Atputharajah and T. K. Saha, "Power system blackouts - literature review," presented at the International Conference on Industrial and Information Systems, 2009.

[8] L. Baozhu and L. Bolong, "A novel static voltage stability index based on equilibrium solution region of branch power flow," in *In 2008 Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies*, 2008, pp. 809 – 814.

[9] J. Zhao, Y. Wang, and P. Xu, "A comprehensive online voltage stability assessment method based on continuation power flow," in *In Proceeding IEEE International Conference SUPERGEN, China*, 2009, pp. 1-5.

[10] C. Sharma and M. G. Ganness, "Determination of the applicability of using modal analysis for the prediction of voltage stability," in *In Proceedings IEEE International Conference Transmission Distribution, Chicago*, 2008, pp. 1-7.

[11] Y.-H. Moon, H.-S. Ryu, J.-G. Lee, and B. Kim, "Uniqueness of static voltage stability analysis in power systems," in *In Power Engineering Society Summer Meeting*, 2001, pp. 1536-1541.

[12] L.-J. Cai and I. Erlich, "Power system static voltage stability analysis considering all active and reactive power controls-singular value approach," in *2007 IEEE Lausanne Power Tech*, 2007, pp. 367-373.

[13] M. Mirzaei, J. Jasni, H. Hizam, N. I. A. Wahab, and E. Moazami, "Static voltage stability analysis using generalized regression neural network," in *In 2013 IEEE 7th International Power Engineering and Optimization Conference (PEOCO). IEEE*, 2013, pp. 391-396.

[14] M. Hassan, "Damping performance enhancement of a power system by STATCOM and its frequency stability consideration," Diss. Khulna University of Engineering & Technology (KUET), Khulna, Banglades, 2016.

[15] J. Lakkireddy, R. Rastgoufard, I. Leevongwat, and P. Rastgoufard, "Steady state voltage stability enhancement using shunt and series FACTS devices," presented at the In 2015 Clemson University Power Systems Conference (PSC). IEEE, 2015.