EE582-Assignment 3

Linli Jia 011683418

(Q1) Prepare a short report about your view on

a) "2019 March Venezuela Power Outage" and allegations made by Venezuelan President Nicolas Maduro accusing USA for cyber-attack.

Event[1]:

The first widespread blackout occurred on 7 March 2019 at 4:56 pm local time, and power was not restored for most of the country until 14 March. It was the largest outage in the history of Venezuela, causing serious damage to the society, and at least 43 deaths resulted. Around 15 of Venezuela's 23 states went through outage from 25 to 28 March. Another blackout started in the evening of 29 March, followed by another 24 hours later. During March, big scale outage spread in Venezuela for at least 10 days in all.

Causes:

There are two statements of the cause of the event. One cause is the vegetation fire in the Guri. Satellite images show that the fire stated one day before the blackout. Most of Venezuela's largest cities are powered by the hydroelectric power plant at the Guri Dam. The fire overheated the transmission lines, triggering load rejection mechanisms, and then causing the turbines to increase their speed, which leads to an overload on electrical systems. When safety control systems in Guri were activated to reduce the increased energy input, however the system fail to operate and Guri has to be disconnected. This results in overload of other power plants and frequency fluctuations that exacerbated the power grid and contributed to continued blackouts. The direct cause of this event is underfunding and mismanagement. According to survey, the vegetation near power lines had not been pruned since 2019, and soldiers instead of electricians were deployed. A fault affected three large cables from the Simon Bolivar Hydroelectric Plant, which supply 80% of Venezuela's power.

Another cause exacerbates the event maybe US sabotage but without enough evidence. Guri dam had been restarted which destabilized the grid further, but this is not scheduled. And none of the backup plants powered by diesel or natural gas functioned during the outage. It is reported by New York Times that the supply of fuel required to run thermal power plants has been affected by US sanctions.

However Venezuelan energy experts rejected the theory that blackout was caused by sabotage, saying the design of the hydroelectric plant system does not allow cyber-attacks.

There's not enough evidence to prove that the blackout is caused or acerbated by cyber-attack, the weakness of the Venezuela physical power grid is the direct reason of the large-scale outage, since most of loads are supplied from the same source, they cannot be transferred efficiently when event happens to Simon Bolivar Hydroelectric Plant. However, we can see the possibility that the status of switches in crucial backup power plants or substations are controlled or influenced by cyber-attack. This could lead to serious social events, leaving large area of the country in black and paralysis. So besides strengthen the physical power grid, nowadays we should also pay much attention to the security of cyber system, which maybe even more vulnerable to attacks.

b) ENTSO-E cyber intrusion and impacts.

Event: The European Network of Transmission System Operators for Electricity (ENTSO-E) reported that on 9 March a cyber intrusion successfully attacked their office network. ENTSO-E represents 42 electricity Transmission System Operators (TSOs) across Europe. The office network is not connected to any operational TSO system. There's no indication that the attack has affected the IT systems[2]. Fingrid reported the incident impacted file exchange policies between the organization and ENTSO-E, which results in delays in issuing energy identification codes to electricity suppliers and producers.

Although this cyber attack didn't cause terrible consequences for the power grid, it reminds us that cyber-attack may not only target power system equipment, but also critical electricity organizations. The attack of such organization may influence multiple power grids at the same time. This attack shows the potential for adversaries to target such organizations to further attack objectives on the electric utilities and various ICS entities. In addition, it is also possible that sensitive information about supported entities may be stolen by attackers in a single intrusion. What's more, during this Covid-19 crisis, a shortage of people to spot the intrusions, also highlights the need for more automated methods to identify malicious and unauthorized attacks quickly.

(Q2) Develop data exchange between “Tiny Power System, that you developed in Assignment 1” and “the cyber system developed in Assignment 2”. Analyze impact of selected cyber events on performance of the power system. Describe your model and cyber-event in a 2-page report. Real time interface is preferred but not necessary as long as interdependence analysis can be done.

In homework1, the physical model of the tiny power system was already built. Here a three-phase fault is assumed occurs between line1-2, as shown in Fig.1, and then breakers on both sides of line 1-2 should be triggered to disconnect line1-2.

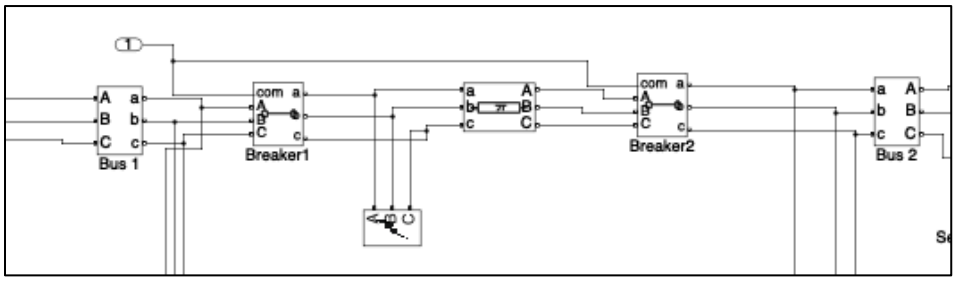
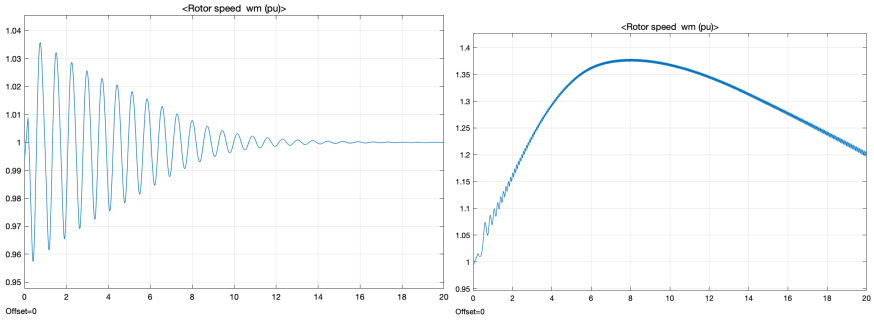


Fig.1 Three-Phase Fault position

Here we tested the critical clearing time of this case, and find that if the breakers cannot operate before 15/60 sec after the fault happens, the power grid would loss stability.



switch time =10/60s switch time =15/60

Fig.2 Critical Clearing Time

In homework 2, a cyber-attack of ‘unauthorized access to control assets’ was assumed, this may cause the latency of control signal of breaker1 and breaker2. If the latency is higher than the acceptable threshold, which is the critical clearing time

here, then breaker1 and breaker 2 cannot be operated in time, and results in instability event of the power grid.

Here the ICT of each station is modeled as a queuing system[3], the cyber-attack assumed would cause all of the servers occupied, and the waiting time of control information packet of breaker 1 and 2 could be longer than the threshold.

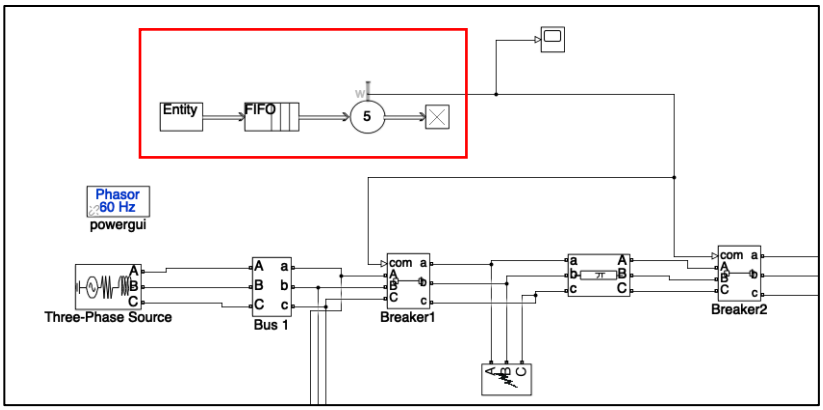


Fig.3 ICT as Queuing System

Suppose the average waiting time is 1 sec because of the cyber-attack, from the simulation we can see it successfully stop the operation of breaker1 and breaker2, and finally results in instability of the power system.

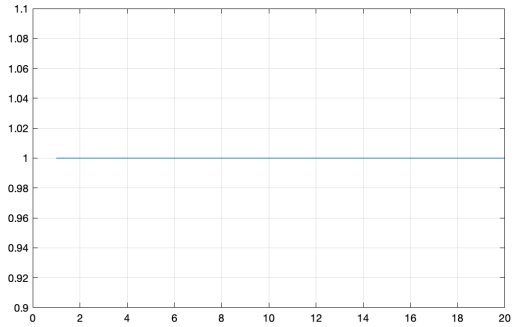


Fig. 4 Average Waiting Time in Server

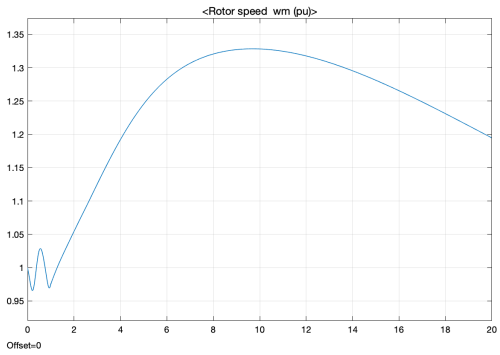


Fig.5 Generator angle influenced by cyber-attack

Reference

[1] https://en.wikipedia.org/wiki/2019_Venezuelan_blackouts

[2] https://www.welivesecurity.com/2020/03/12/european-power-grid-organization-entsoe-cyberattack/

[3] Stefanov A, Liu C C, Govindarasu M, et al. SCADA modeling for performance and vulnerability assessment of integrated cyber–physical systems[J]. International Transactions on Electrical Energy Systems, 2015, 25(3): 498-519.