Concordia University

INSE 6640 – Smart Grids and Control System Security

Assignment -1

Submitted to:

Professor Jun Yan, PhD

Submitted By:

Student Name	Student ID
Nithish Reddy Yalaka	40164619

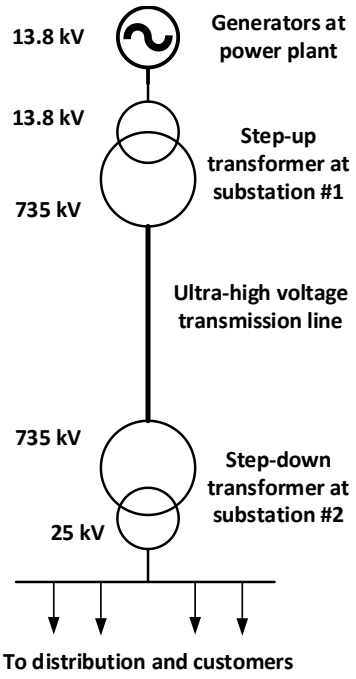
Assignment #1 (**100 points**): Due 11:59 pm, Sunday, February 13, 2022

1. (**20 points**) Security is a fast-evolving area where professionals shall stay tuned for information from an array of credible sources. To answer this question, use an email of yours to subscribe to a total of five feeds from security agencies, organizations, firms, and/or researchers, all of which shall be related to topics in this course. Report your subscriptions in the table below (no need to submit proof of subscription). Make sure you subscribe to at least one newsletter from the industry and one researcher/government agencies not in the industry. Feel free to add more lines in MS Word if needed.

Your email used for subscription	nithishreddy.yalaka@mail.concordia.ca		
Category	**Publisher**	**Publisher type**	**Starting date**
Subscription #1	Jun Yan	Researcher on Google Scholar	2022-02-10
Brief reason	Instructor of the course and researcher on cyber-physical security in the smart grid.		
Subscription #2	ICS-CERT alerts	Newsletter of a U.S. government agency	2022-02-10
Brief reason	Provides timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks.		
Category	**Publisher**	**Publisher type**	**Starting date**
Subscription #3	CERT-EU	Email Alerts for the EU Institutions, Bodies and Agencies	2022-02-10
Brief reason	Provides timely alerts on various product vulnerabilities, threats, and hacking methodologies in the market used by the adversaries.		
Subscription #4	CSL-FIU	Provided newsletters on the latest cyber threats and alerts	2022-02-10
Brief reason	CSL-FIU reports on news and events impacting latest technology and security.		
Subscription #5	NIST	Smart Grid and Cyber-Physical Systems Newsletter	2022-02-10
Brief reason	Provides updates on NIST Framework and roadmap for smart grid Interoperability		
Subscription #6	Azzam Mourad	Google Scholar Security Researcher and prof at Lebanese American University & New York University	2022-02-10
Brief reason	Researcher on cyber security, IOT Security, Federated ML, and Cloud Computing		
Subscription #7	Sara Ayoubi	Google Scholar Cloud and ML Security Researcher	2022-02-10
Brief reason	Researcher on Network Security, Data Center, Cloud and ML security		

Subscribed to **#1, #2, #6**, and **#7** using the email provided above

2. (**15 points**) The figure on the right shows an abstract model of power transmission grids in Quebec, where the ultra-high voltage transmission line has a rated voltage of 735 kilovolts (kV). The Ohm's law states that the active power consumption at the end of the line is $P = UI$ and the active power loss along the line $P_{loss} = I^2R$, where U, I, and R are the rated voltage, line current, and line resistance, respectively. Assume that the active power consumption at substation #2 is $P = 1{,}000\ MW$.
   a. If the 735-kV line is 100 kilometers long with a resistance of 0.5Ω per kilometer, what is the active power loss along the line according to the Ohm's law? Show your result in megawatts (MW).
   b. If the rated voltage of this line is reduced from 735 kV to 315 kV while the length and resistance remain the same, what is the active power loss along the 315-kV line?
   c. According to recent data, the average power consumption of a household in Quebec is 1.9 kilowatts (kW); the average charging demand of an all-electric vehicle over a common 120 V outlet is 1.4 kW. When increasing the rated voltage from 315 kV to 735 kV, the saved active power loss can power up how many households in Quebec? How many all-electric vehicles?



Answer:

a.

Given values are,
U=735 KV, where KV, when converted the value U= 735*1000 = 735000 MW, where 1 MW = 1000 Kv*A.

According to Ohm's law: P=UI, where U =Rated Voltage, I= LineCurrent, R= Line Resistance.

Power Consumption in Megawatts: P= 1000 MW.Ohm's law can write as: I=P/U.

I= (1000 x 10^6)/735000 = 1360.544.

Resistance: 0.5 Ω per km this can be further write as 0.5 * 100 = 50 Ω.

Active power loss $P_{loss} = I^2R$,

$(1360.54)^2 * 50$ = 92553998.8 W (1W = 0.000001MW)

$\boldsymbol{P_{loss}}$ **= 92.55 MW.**

b. Given that, rated voltage is changed from 735 kV to 315 kV

U =315 KV
Resistance = 0.5 Ω per kilometer
=>0.5*100 = 50 Ω

We know that P = UI
I = P/U, (10 * 10^6)/315000 = 3174.6 A
Resistance(R): 0.5 Ω per km this can be further write as 0.5 * 100 = 50 Ω.

And the active power loss across the line $P_{loss} = I^2R$

$P_{loss} = I^2R$

= 3174.6 * 3174.6 * 50 = 503904265.8W = **503.9MW** (1 MW = 0.000001 MW).

c. Given, the average power consumption of a household in Quebec is 1.9 kW.

The average charging demand of an all-electric vehicle over a common 120 V outlet is 1.4 kW.

For voltage is 735 KV, U = 735 kV, active power loss across the line, $P_{loss} = 92.55\ MW$
For voltage is 315 KV, U = 315 kV, active power loss across the line, $P_{loss} = 503.9\ MW$

So, Saved active power loss = (503.9-92.55) MW

= 411.35 MW

= 411350 KW

Number of households in Quebec that can be powered by saved active power loss

= 411350 / 1.9

= 216500 households

Number of electric vehicles = 411350 / 1.4 = > 293821.43

Saved active power loss can power up to ~ **293821** Electric vehicles

3. (**15 points**) The peak load of a power grid refers to the highest load demand seen during a certain period. The table below shows the weekly peak load in a regional power grid, in terms of the percentage with respect to the peak load of the entire year: for example, the peak load observed in Week 1 is 86.2% of the peak load observed over the entire year. Weeks 1-8 and 44-52 are in the winter, weeks 9-17 are in the spring, weeks 18-30 are in the summer, and weeks 31-43 are in the fall. Answer the following questions.

Week	Peak load (%)	Week	Peak load (%)	Week	Peak load (%)	Week	Peak load (%)
1	86.2	14	75.0	27	75.5	40	72.4
2	90.0	15	72.1	28	81.6	41	74.3
3	87.8	16	80.0	29	80.1	42	74.4
4	83.4	17	75.4	30	88.0	43	80.0
5	88.0	18	83.7	31	72.2	44	88.1
6	84.1	19	87.0	32	77.6	45	88.5
7	83.2	20	88.0	33	80.0	46	90.9
8	80.6	21	85.6	34	72.9	47	94.0
9	74.0	22	81.1	35	72.6	48	89.0
10	73.7	23	90.0	36	70.5	49	94.2
11	71.5	24	88.7	37	78.0	50	97.0
12	72.7	25	89.6	38	69.5	51	100.0
13	70.4	26	86.1	39	72.4	52	95.2

(Reference: IEEE Reliability Test System (RTS) - 1996)

a. Which weeks have the highest and lowest peak load of the year?
b. If the annual peak load is 2,850 MW, what are the average peak loads (in MW) of the winter weeks and the summer weeks, respectively?
c. If the annual peak load is 2,850 MW and we have two power plants whose capacities (maximal generation power) are 1,500 MW and 1,000 MW, respectively. During the week with the highest peak load, how much extra power generation capacity (in MW) do we need to meet the peak load of the year? During the week with the lowest peak load, at least how much power generation capacity (in MW) would be in idle?

Answer:

a.

Week 51 has the highest peak load of the year with **100%**.
Week 38 has the lowest peak load of the year with **69.5%.**

b. Annual Peak Load: 2850 MW, the average peak loads of the winter weeks:

Week	Peak Load of Winter Weeks	
1	86.2	2456.70 MW
2	90	2565 MW
3	87.8	2502.3 MW
4	83.4	2376.90 MW
5	88	2508.00 MW
6	84.1	2396.85 MW
7	83.2	2371.20 MW
8	80.6	2297.10 MW
44	88.1	2510.85 MW
45	88.5	2522.25MW
46	90.9	2590.65MW
47	94	2679.00 MW
48	89	2536.50 MW
49	94.2	2684.70 MW
50	97	2764.50 MW
51	100	2850.00 MW
52	95.2	2713.30 MW
17 Weeks	Sum	**43325.8**
	Average = Sum/No of winter weeks	**43325.8 /17 = 2548.5 MW**

the average peak loads of the summer weeks:

Week	Peak Load of Summer Weeks	
18	83.7	2385.45 MW
19	87	2479.5 MW
20	88	2508 MW
21	85.6	2439.6 MW
22	81.1	2311.3 MW
23	90	2565 MW
24	88.7	2527.95 MW
25	89.6	2553.6 MW
26	86.1	2453.8 MW
27	75.5	2151.7 MW
28	81.6	2325.6 MW
29	80.1	2282 MW
30	88	2508 MW
	Sum	31491.5
	Average = Sum/No of Summer weeks	31491/13 = 2422.3 MW

c. Given that, Annual Peak Load is 2850 MW

Week 51 has the highest peak load of the year with 100%.
= > 100% of 2850 MW
= 2850 MW

Week 38 has the lowest peak load of the year with 69.5%.
= > 69.5% of 2850 MW
= 1980.75 MW

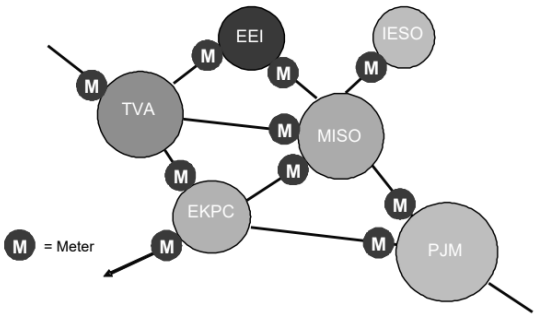
Maximum power generation capacities of two power plants are 1500 and 1000, respectively.
Total power generation by two power plants = 1500 + 1000
= 2500 MW

Extra power generation capacity required to meet the highest peak load of the year during week 51 is = (2850-2500) MW
= 350 MW

Idle power generation capacity required during the week 38 with lowest peak load
= (2500-1980.75) MW
= > **519.25 MW**

4. (**20 points**) The diagram shows some of the interconnected balancing authorities (Bas) in North America, where the grid frequency is 60 Hz. Recall that the area control error (ACE) is calculated by:

$$ACE = (NI_a - NI_s) - \beta(f_a - f_s) - \epsilon$$



In practice, the power flowing into a grid (generation P_{gen} and purchase P_{import}) is often assigned a negative sign, and that out of a network (consumption P_{load} and sales P_{export}) is assigned a positive sign. With this notion, we shall rewrite the power balance equitation as:

$$P_{gen} + P_{load} + P_{import} + P_{export} = 0.$$

Note that this is slightly different from our lecture notes, where $P_{gen} + P_{import} = P_{load} + P_{export}$.

Assume the active power generated or flowing into a BA is negative, and the active power consumed or flowing out of a BA is positive. Assume that the frequency bias β of **IESO** is -500 MW/Hz, and that the meter is error free ($\epsilon = 0$).

Answer the following questions:

RTO/ISOs:

- **IESO**: Independent Electricity System Operator (Ontario)
- **MISO**: Midcontinent Independent System Operator (Manitoba and multiple mid-west and southern states in the US)
- **PJM**: Pennsylvania-New Jersey-Maryland Interconnection LLC (13 eastern states/districts in the US)

Local Utilities:

- **TVA**: Tennessee Valley Authority (7 southeastern states in the US)
- **EEI**: Electric Energy, Inc (Illinois)
- **EKPC**: East Kentucky Power Cooperative, Inc. (Kentucky)

Source: "Balancing and Frequency Control" by the NERC Resources Subcommittee

a. Assume that IESO has NOT scheduled to purchase any electricity from MISO. According to the tie line meter, the actual NI between MISO and IESO is zero; the actual frequency of IESO is 60.01 Hz. Find the ACE of IESO. How shall we adjust the generation according to ACE?

b. Assume that IESO has scheduled to purchase 100 MW from MISO. According to the tie line meter, the actual NI between MISO and IESO is -110 MW; the actual frequency is 60.01 Hz. Find the ACE of IESO. How shall we adjust the generation according to ACE?

c. Assume an attacker plans to manipulate the ACE, which can be done by injecting an error ΔNI to NI_a or injecting an error Δf to f_a. Find the expression of injected error to the ACE (Δx) using an equation with ΔNI, Δf, and β.

d. Consider the operation scenario in Question 1.b and the attack model in Question 1.c above. If an attacker only manipulated the actual NI by adding an NI error of $+20$ MW and the actual frequency 60.01 Hz was reported accurately, what is the perceived ACE after manipulation? If an attacker caused an ACE error of -1 MW by only manipulating the actual frequency, what was the frequency error added by the attacker?

Answer:

a. Given, the frequency of the grid is 60 Hz. Also, according to the question,

The power flowing into a grid is $P_{gen} + P_{import}$ = -Ve Sign
The power flowing out of a network is $P_{load} + P_{export}$ = +Ve Sign

$Pgen + Pload + Pimport + Pexport = 0$

according to the tie line meter, the actual NI between MISO and IESO is zero
Then,
$NIa = 0$
$NI_s = 0$

Frequency Bias, β = -500 MW/HZ

Meter is error free, so ϵ = 0

Frequency of IESO, f_{IESO} = 60.01 HZ

ACE of IESO = > $ACE = (NI_a - NI_s) - \beta(f_a - f_s) - \epsilon$

= > (0 – 0) – (-500) (60.01 – 60) – 0
= > 500 (0.01)
= 5 MW

We generate **5 MW** to adjust the ACE (less generation)

b. Given, IESO has scheduled to purchase 100 MW from MISO and the actual NI between MISO and IESO is −110 MW = > NI_s = 100 MW & NI_a = -110 MW

The actual frequency, f_a = 60.01 Hz & f_s = 60 Hz

ACE of IESO = > $ACE = (NI_a - NI_s) - \beta(f_a - f_s) - \epsilon$
= > (-110 – 100) – (-500) (60.01 – 60) – 0
= > -210 + 500 (0.01)
=> **- 205**

We can adjust more generation as per the generated ACE.

c. Given that,

If an attacker plans to manipulate the ACE, which can be done by injecting an error ΔNI to NI_a or injecting an error Δf to f_a.

the expression of injected error to the ACE (Δx) using an equation with ΔNI, Δf, and β. Is:

ACE (Δx) = ΔNI - β (Δf) – ϵ

d. Given that,

If an attacker only manipulated the actual NI by adding an NI error of +20 MW and the actual frequency 60.01 Hz was reported accurately which implies ΔNI = +20 MW

NI_a = - 110 MW + 20 MW (error) => - 90 MW

NI_s = 100MW
f_a = 60.01 HZ
f_s = 60.0 Hz
Frequency Bias, β = -500 MW/HZ

ϵ= 0

ACE = $(NI_a - NI_s) - \beta\,(f_a - f_s) - \epsilon$
= (-90 – 100) – (-500) (60.01 – 60) – 0
= **-185**

Frequency error added by the attacker by only manipulating the actual frequency of an ACE error of -1 MW intending to -1 is

-1 = (-110 – 100) – (-500) (f_a – 60) – 0
-1 = -210 +500f_a + 30000 – 0
500 f_a = 30209
f_a = 30209/500 = **60.42 Hz**

5. (**10 points**) Answer the following questions:

   a) List the two major interconnections and three minor interconnections in North America.

   b) In addition to Dragos and Nozomi Networks, the two examples listed in our slides, identify three more industrial control system (ICS) security solution providers in the world. Show the names of the companies and the links to their home page in your answer.

   c) Create an account on Shodan.io, then follow the Explore => Industrial Control Systems => Protocols to identify which **port number** was used by this search engine to identify Internet-connected ICS devices communicating over the following protocols, respectively:
   1) Modbus; 2) DNP3; 3) IEC 60870-5-104 4) S7 (S7 Communication)

Answer:

a. The two major interconnections in North America are:
   1. Western Interconnection
   2. Eastern Interconnection

   The three minor interconnections in North America are:
   1. Alaska Interconnection
   2. Quebec Interconnection
   3. Texas Interconnection

b. Industrial control systems (ICS) help industry strengthens the cybersecurity of its computer-controlled systems. In addition to Dragos and Nozomi Networks, the other ICS security solution providers in the world are:

1. Bayshore Networks (https://bayshorenetworks.com/)
2. CyberX (https://cyberx-labs.com/)
3. FORTINET (https://www.fortinet.com/)
4. CYBERARK (https://www.cyberark.com/solutions/audit-compliance/)
5. Veracity (https://veracity.io/)

c.

1. Modbus uses the Port Number – 502
2. DNP3 uses Port Number – 20000
3. IEC 60870-5-104 uses Port Number – 2404
4. S7 (S7 Communication) uses Port Number – 102

6. (**20 points**) Choose one ICS cyber security incidence from the following list, search for details via the links provided and from other online sources you can find, then formulate the attack model by summarize the details in the table below. (*Note*: Think about this as your personal note of what is going on While there is no "correct answer" here, you shall provide accurate, informative details, while keeping your answer as brief as possible. If any information was not given nor found, simply put "unspecified" in the corresponding blanks.)

- **Compromise of U.S. Water Treatment Facility**
  https://us-cert.cisa.gov/ncas/alerts/aa21-042a
  https://www.cyberscoop.com/florida-water-facility-hack-password/
- **Cyber incident occurring at the Bowman Avenue Dam near Rye, NY**
  https://www.nbcnews.com/news/us-news/iranian-hackers-claim-cyber-attack-new-york-dam-n484611
  https://ics.sans.org/media/SANSICS_DUC4_Analysis_of_Attacks_on_US_Infrastructure_V1.1.pdf
- **Cyber Attack on the Ukrainian Power Grid**
  https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
  https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
- **Hackers Remotely Kill a Jeep on the Highway**
  https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
  http://illmatics.com/Remote%20Car%20Hacking.pdf
- **Stuxnet targeting the Iran's nuclear-fuel enrichment program**
  https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
  https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf

Compromise of U.S. Water Treatment Facility

Incidence	Compromise of U.S. Water Facility
Attacker/hacker	Unspecified
Attack date/year	February 5, 2021
Motive	There was no exact motive behind this attack as the adversaries never revealed anything. Assumptions are public health damage as the attackers increased the quantity of Sodium Hydroxide, also some assumptions are monetary blackmail.
Target	Target was the water treatment process in Water facility. Attackers targeted and exploited desktop sharing software "TeamViewer" and computer networks running operating systems with end-of-life status to gain unauthorized access to SCADA systems.
Vulnerability	There were several vulnerabilities that cause this attack such as Outdated Windows Operating System (32-bit version of Windows 7), No firewall was implemented, Poor password security as most of the pc's shared the same passwords for remote access, on System level, and Remote access software, TeamViewer, was installed on numerous computers to check the status and alarms that arose throughout the water treatment process, and it was used to control the SCADA system at the water treatment plant.
Tool	The main reason of this successful attack is because of the poor configuration of Remote access tool TeamViewer which in turn gained the access to the system for attacker. Improper RDP accesses leads to several attacks. Also, Phishing campaigns and several social engineering tactics on the water facility employees.
Method	Adversaries used the TeamViewer tool to gain the unauthorised access to the Supervisory Control and data Acquisition (SCADA) systems which gave the remote control and injecting several harmful files such as viruses like trojans. Upon gaining the access, the attacker increased the sodium hydroxide to more than 100 times than its supposed measure.
Impact	The attacker's intent was to raise the chemical content in the water may be to harm the public health, but SCADA system detected the changes in the concentration and alarmed due to this unauthorised change and the employees were alerted and fortunately it was stopped before putting the public at risk.