Case Study with Supporting Media and Simulation Exercise

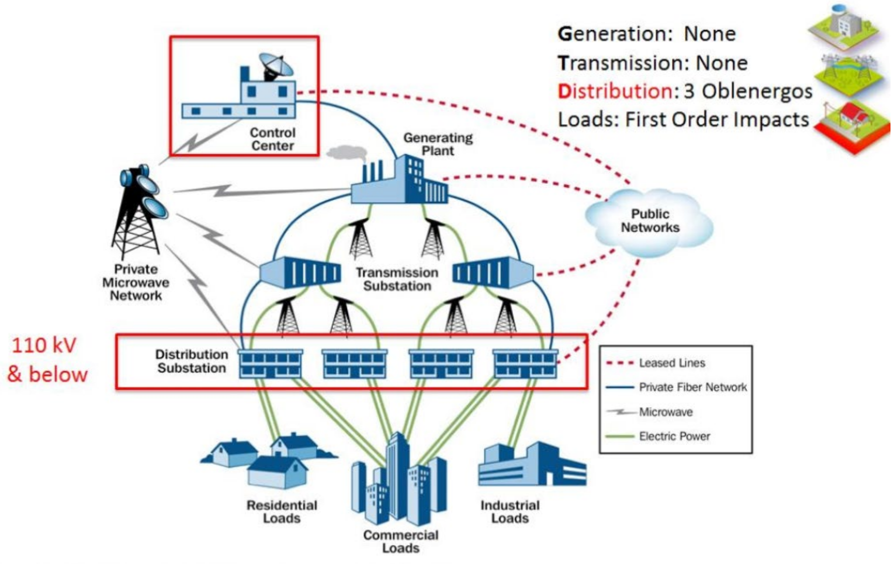
Title: The Role of Circuit Breakers in the 2015 Electric Grid Attack in Ukraine

Real World Inspiration

The real-world inspiration for this case study is the cyber-attack on the Ukraine power grid in 2015. Cyber attackers gained remote access to the operating system of three regional electrical power distribution centers and disconnected approximately 225,000 customers from power [1]. It is believed that this attack was perpetrated by cyber actors on behalf of the Russian nation-state to disrupt Ukraine's critical infrastructure and undermine its sociopolitical status [2].

(a) Background: Electric Grid Structure

Power grids, as illustrated in Figure 1, are comprised of three major layers: generation, transmission, and distribution. Electricity is generated by using resources like natural gas, coal, or renewable energy. Then, it is transmitted from power plants to cities and residential areas to power homes and offices. Electricity is transmitted at a high voltage to reduce power losses and so it can be transmitted over long distances. As the electricity is moved, substations across the country process and distribute energy throughout each region of the grid. As the electricity travels, the voltages must be gradually stepped down to lower voltages to be used in homes and offices safely. Tampering with the distribution at substations can cause blackouts regionally, directly impacting customers.

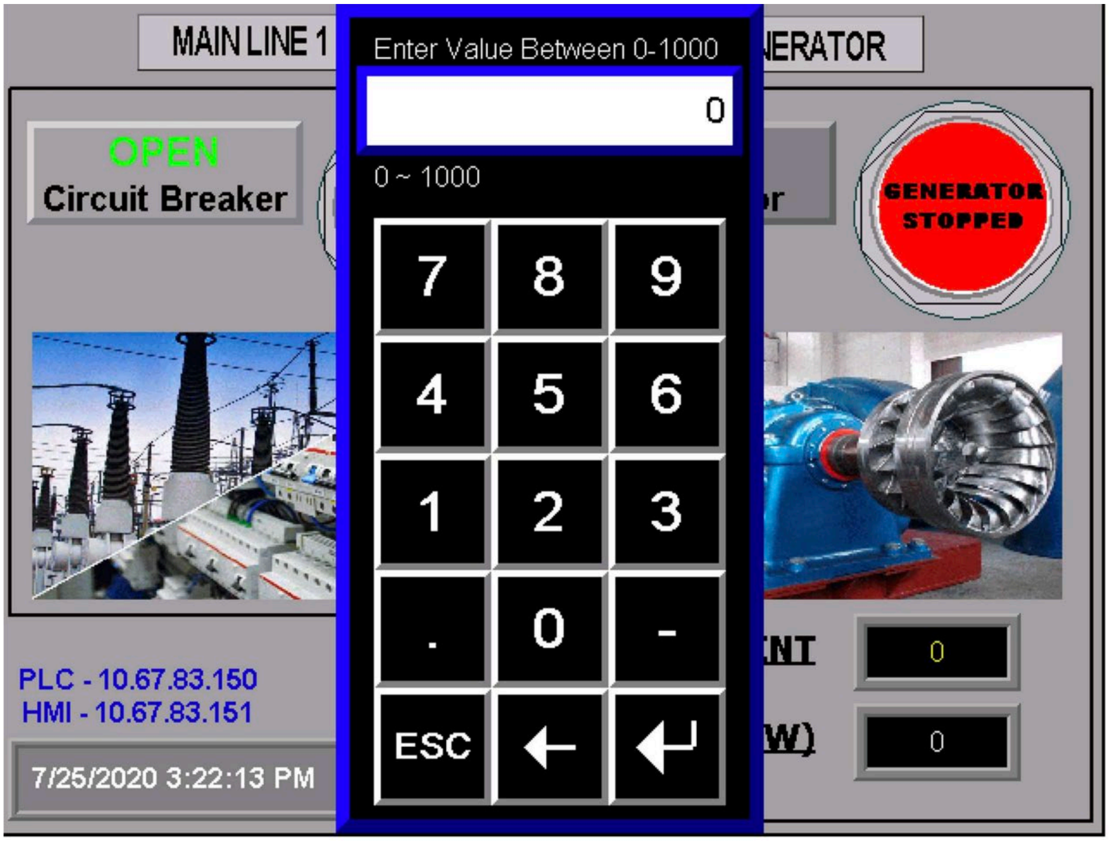


Source: Modification to the DHS Energy Sector-Specific Plan 2010

Figure 1: A simplified graphic of electric grid topography [1]

(b) Attack Details and Circuit Breakers

In this specific attack on Ukraine, cyber attackers completed a series of strategical steps over a year before the attack was orchestrated to infiltrate the distribution centers' operation systems. The attackers started by gathering publicly available data about operating systems, personnel, and network. Then, they initiated a phishing email campaign to the networks of the electricity distributors, through which they delivered malicious Microsoft Word documents containing malware. After establishing access to the organizations' internal servers, they were able to obtain valid credentials, enabling them to expand access into the control environment. Finally, they used these credentials to gain remote access to the controls at the substation via Human-Machine Interface (HMI) workstations. HMI workstations, as shown using a simplified lab version in Figure 2, provide a user interface for operators to remotely control devices within the control environment.



Enter Value Between 0-1000

0

0 ~ 1000

PLC - 10.67.83.150
HMI - 10.67.83.151

7/25/2020 3:22:13 PM

Figure 2: An example of the HMI in the operating system [INL CyberStrike Lab 2: HMI Control]
YouTube: https://youtu.be/NJ-sC_QCOPY

Figure 3 shows a full diagram of the cyber activity in the 2015 Ukraine Grid Attack, where the HMI is highlighted in blue in the context of the entire attack process. The HMI, as shown in Figure 2, is the digital control system which attackers were able to physically manipulate physical systems. After gaining control of the HMI, attackers were able to open the substation circuit breakers, shown in the purple box on Figure 3, disconnecting the distribution substations from the rest of the electrical grid [2]. This resulted in regional blackouts, meaning that customers in the affected substation provider network could not access power.

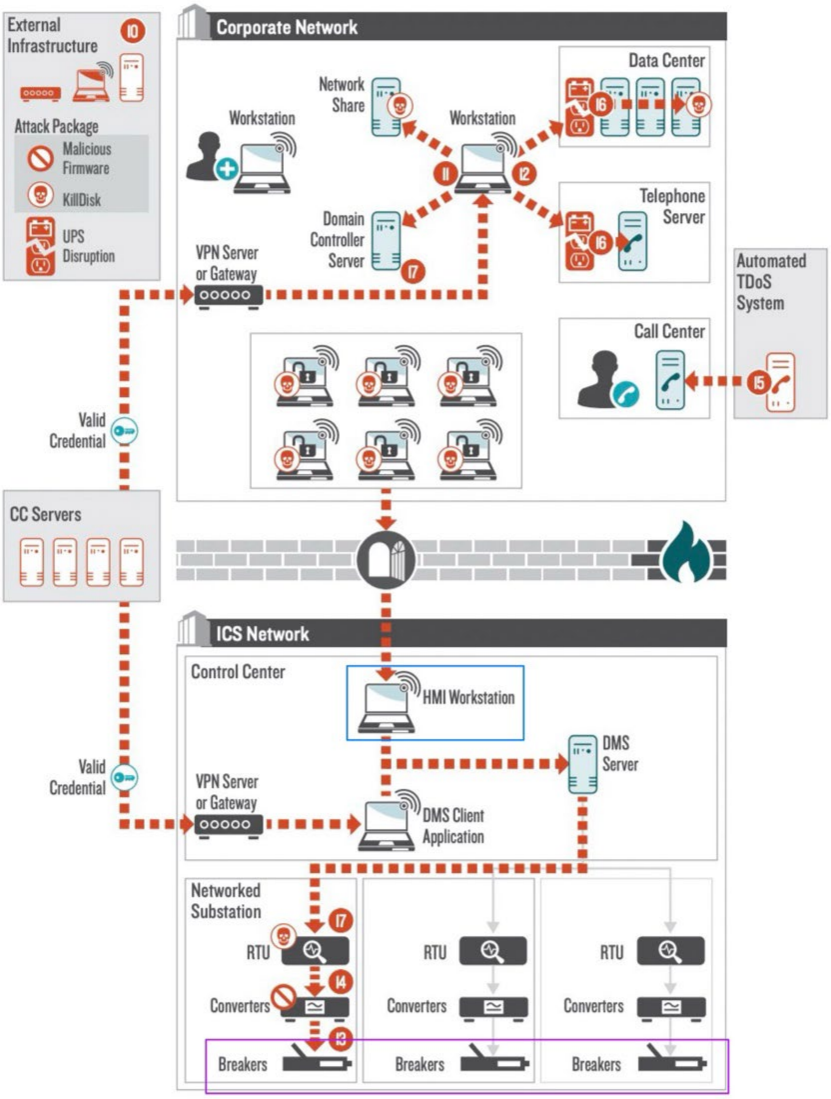


Figure 3: A diagram of cyber actor activity in the 2015 Ukraine Grid Attack [2]

This attack is known as a Substation Circuit Breaker Takeover attack [3]. A circuit breaker is an electrical component that is used to protect an electrical circuit from excessively high currents. These devices appear in homes, typically aggregated together in one electrical panel in a basement. When there is an overload, too many things are plugged in requiring too much power, or there is a short circuit, an unintended connection is made in the circuit, the circuit breaker will ‘trip’, opening the circuit and restricting power flow. In a home, these devices are small, and the circuit can be reconnected to restore power with the flip of the breaker. Larger circuit breakers are also used in the electric grid. These are high voltage circuit breakers that are much bigger than the ones in homes, as shown in Figure 4, and utilize electromechanical actuators, like springs, to open the circuit as needed which makes it harder to reclose the breakers and restore power.

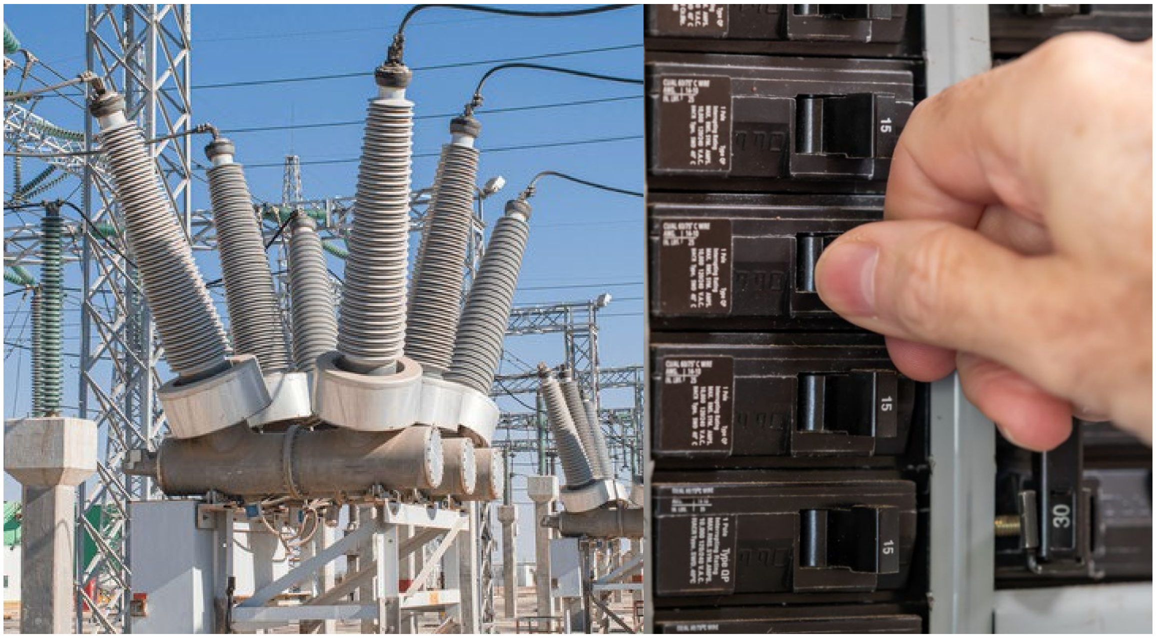


Figure 4: A high voltage circuit breaker (left) versus a residential circuit breaker (right) [shutterstock.com]

(c) Applicable CIE principles

Cyber-Informed Engineering (CIE) is an engineering approach that integrates cybersecurity considerations into the conception, design, build, and operation of any physical system that has digital connectivity, sensors, monitoring, or control [4]. A cyber-physical system is an engineered systems that is built from and depends upon the seamless integration of computation and physical components. As cyber-physical power systems evolve and threat of cyber intrusions to the U.S. power grid grows, CIE principles and countermeasures with these in mind are a necessary component of the design and deployment processes of critical infrastructure [5]. Because many power system control devices in the electric power grid are connected to the internet, the risk of cyber intrusions is high. Remote access to large operational components of the grid like circuit breakers, through internet-connected devices such as the HMI, arise through network attacks, which lead to power system security challenges [5]. Coordinated, complex attacks on the U.S. power grids that lead to cascading failures and regional blackouts must be mitigated with countermeasures that address the intertwining threats in the cyber and physical aspects of the power grid. CIE principles inform early design decisions so that engineering decisions reduce and mitigate the consequences of a cyber-attack [4].

A broad approach to ensuring a secure power grid requires understanding that a perfect technical solution to an engineering problem may not be effectively implemented or scaled to work within an organization's existing culture. Culture, as defined in the Idaho National Lab's Cyber-Informed Engineering Implementation Guide, is the "sum total of the organization's behaviors, practices, and choices that expose the organization's values and priorities" [4]. Before technical approaches can be leveraged to mitigate the possibility of attack and address the consequences if an attack is successful, an organization must have security at the forefront of their practices. **CIE Principle 12, Organizational Culture**, involves ensuring that everyone's behavior aligns with the security goals of an organization [4]. The strongest countermeasure is fostering a strong cyber security culture in the leadership, and having these values step down throughout the organization. Having a strong cyber security culture involves consistent cyber security training for all users of the system, and having organizational policies that empower the users of the system to report security threats or suspicions without fear of repercussions. Implementing strong security measures at every level of electrical grid operations from the top-down includes strong, overarching regulatory policies to consistent training and security policies at the internal organizational level.

Another countermeasure involves **CIE Principle 3, Secure Information Architecture**. Preventing undesired manipulation of important data can be accomplished by only allowing control of the system in a specific place, for example the control room in the substation, or having good authentication protocols, like two factor authentication, to help ensure the person trying to access the system is legitimate. An additional countermeasure is to reduce attack surfaces and remove vulnerabilities like a remotely accessible control interface (HMI) from the system entirely.

CIE Principle 2, Engineered Controls is about selecting and implementing controls to minimize avenues for attack or the damage that could result. The Engineered Controls principle asks questions like, "What key functional controls of the system will be dependent on digital technologies?" and "What risk will this dependency introduce?" [4]. The 2015 Ukraine attack incident is a clear example of how critical parts of the power system, the circuit breakers, were connected to and able to be controlled by digital technologies, and how the risk this introduces is the complete shutdown and disconnection to power via remote access of the digital controls. A simple countermeasure is to eliminate this digitally introduced vulnerability. Another question that is relevant to **Engineered Controls** is, "Can failure modes be eliminated or mitigated by adding mechanical, non-digital, or non-networked equipment?" [4]. One countermeasure is to protect circuit breakers and substations from physical attacks by padlocking control rooms and adding protective covers to electrical panels.

Overall, cybersecurity in cyber-physical power systems is strengthened by a layered defense. **CIE Principle 5, Layered Defenses**, involves reducing the opportunity of one failure to result in cascading failures or loss of critical functioning [4]. Protective measures at the Industrial Control Systems (ICS) network level include disabling remote access into an organization's ICS network wherever possible, the restriction of user accounts with remote access privileges to the minimum necessary and requiring two-factor authentication for all VPN connections [1]. These defensive mechanisms contribute to a layered defense by protecting the critical functioning of the circuit breakers and preventing one from accessing any point of possible exploitation at the HMI level. Additionally, they address the interconnectedness of the HMI workstation and the circuit breakers in the Ukraine attack and restrict remote access. Moreover, practicing incident response scenarios to understand how to disrupt remote connectivity and manually operate ICS equipment to bring operations back to a safe state in the event of an HMI breach is layered defense at the circuit breaker level [1]. Layered defenses consider the subsystems and connections in cyber-physical power systems and critical components that exist at each level and ensures that these levels are isolated enough from each other such that even if a VPN network or HMI control system is compromised, this will not lead to further control of critical control systems.

Media Feature for the General Audience

For a custom media clip designed by faculty and students of the University of Pittsburgh, please click on the video file found here: Team Anaconda Media Feature

Educational videos, like those produced in this project, are a valuable tool in higher education. According to the National Library of Medicine, "Effective use of video is enhanced when instructors consider cognitive load, student engagement, and active learning" [6]. The first element to observe, cognitive load, has produced theories that give rise to several educational video recommendations, including using signaling to highlight essential information, segmenting to chunk messages, speaking in a conversational tone, and creating narrated animations. [6] These are all strategies that were implemented in this project's video to minimize extraneous cognitive load, optimize germane cognitive load, and manage intrinsic cognitive lead. When promoting student engagement through educational videos, it is essential to keep videos short, speak relatively quickly and with enthusiasm, and to create them for the environment in which they will be used [6]. These approaches were kept in mind when planning the video above, especially to create a feature that thrives in the new environment of CIE. Finally, to enhance active learning for students, educational videos are said to be most effective when paired with guiding questions or associated homework assignments [6].

Future Policy Implications

The future policy implications for the cybersecurity of the electrical grid and other critical infrastructure are complex and far-reaching. One broad but useful approach is to examine the existing policy through an external and internal dynamic. Externally, one must be aware of the intricate policy environment that relates to critical electrical infrastructure. Internally, one must be aware of an organization's culture and its implications for implementing and strengthening cybersecurity measures. Therefore, in accordance with CIE, it is vital to place policy and organizational considerations within every step of the technical process, rather than having it remaining as an afterthought to the technical solution.

After meeting with a local vendor that specializes in software and security solutions and a tour of a local circuit breaker company, two policy-related roadblocks were highlighted: the supply chain and the patchwork of government agencies and organizations. For example, the circuit breaker company places a particular emphasis on physical protection, which may be something as simple as a padlock on an electrical pane or a barbed wire fence. As product suppliers, they largely leave cybersecurity responsibilities to their customers or asset owners, such as a local power utility. For example, the product supplier will carve a space for a Schweitzer protective relay, a device used in power systems that monitors for short-circuits or abnormalities. Nevertheless, it remains the asset owner's responsibility to program the relay at the breaker level. Therefore, this creates the difficult challenge of making sure that the key parties that make up the patchwork of the electric grid, from regulatory government agencies to product suppliers to power utilities, are on the same page in terms of prioritizing cybersecurity. Specifically, Ukraine, due to not being a member of the European Union, relies on a myriad of different American, Russian, and German equipment, all made under different regulations for that region which may foster susceptibility to cyberattacks. Furthermore, this illustrates a larger pattern of how open-source information's availability, including detailed lists of infrastructure such as Remote Terminal Units (RTU) vendors are posted by Industrial Control Systems (ICS) vendors [2]. As a result, the availability of this information further increases the surface area for a potential cyberattack. Therefore, one may ask how this may be mitigated within the larger external policy environment.

The North American Electric Reliability Corporation (NERC) is a regulatory body that looks to assure effective reliability and reduce risks related to the security of the grid. NERC is subject to oversight by the Federal Energy Regulatory Commission (FERC), an independent agency that provides stipulations regarding the transmission of interstate electricity, natural gas, and oil. Consequently, NERC and FERC have worked together to develop Critical Infrastructure Protection (CIP) standards, which are mandatory security regulations aimed to secure the Bulk Electric System (BES). As a result, electric utilities, regional transmission organizations, and independent system operators are subject to CIP enforcement by FERC. Specifically, CIP-011 and CIP-0-113 oversee the protection and security of BES cyber system information and the supply chain. In addition, through a focus on supply chain security, one will be able to home in on the security of software, hardware, and services used or acquired through grid operations. Therefore, NERC, FERC, and CIP provide the foundation for cybersecurity regulations for critical infrastructure bodies.

The most ambitious way to approach this challenge is to think externally, specifically in terms of national policy. The U.S. has a nascent overarching national cyber security policy. However, the SAFETY Act, which is part of the Homeland Security Act of 2002, Public Law 107-196, has been the foundation of infrastructure security. Under this act, the Department of Homeland Security examines critical infrastructure vendors by looking at secure development processes, lingering vulnerabilities, third-party penetration work, and perhaps most importantly, create a point of contact between federal agencies and the respective vendor so that, in the event of an attack, they may work together and coordinate a proper and effective response. The SAFETY Act may be contrasted with the European Union's impending Cyber Resilience Act (CRA), an overarching and wide-reaching cybersecurity-specific act, that looks to bolster standards, increase incident reports, and enhance general cyber resiliency. Going forward, it is vital to think about how existing policy, specifically the SAFETY Act, can be enhanced to bridge these agencies and lessen compartmentalization that may invite attacks, rather than creating a national policy from scratch.

The other pivotal facet of power grid security is internal organizational culture (CIE Principle 12). An organization's security culture must be strong enough to support and scale any potential technical engineering developments. McKinsey & Company characterizes an organization's culture as, "The outcome of the vision or mission that drives a company, the values that guide the behavior of its people, and the management practices, working norms, and mindsets that characterize how work actually gets done". An internal approach that emphasizes strong values and management should be scaled to organizations across grid operations. A broad internal approach should be centered on defense-in-depth strategies. Through these strategies, an organization may prohibit a single-point failure, raise the likelihood of network detection, and increase the adversary's cost of conducting an attack [1]. Thinking internally, a specific area to focus on is Privileged Access Management (PAM), a type of identity management and cyber defense mechanism that plays a critical role in defense-in-depth strategies and enabling zero trust. To apply this framework, particularly reducing privileges, to the operational processes in the substations to ensure that control of the utility is contained to trusted individuals with high clearances. Therefore, going forward, PAM should be utilized in substations and used to foster a stronger security culture within operational facilities, specifically where important controls are located. Nevertheless, it is important to recognize these privileged individuals within an organization are perhaps more prone to targeted attacks, thus it remains crucial to monitor their operations and connections.

(a) Future Policy Implication Discussion Questions

1. How would one go about strengthening organizational culture in a way that transforms cybersecurity from being "an imposition to an inherent quality [4]?"

2. With the SAFETY Act and the European Union's CRA in mind, what are the benefits for critical infrastructure, specifically electrical grids, for the United States to have an overarching security policy?

3. What internal security policies regarding monitoring, authentication, and security zones and boundaries could be made to ensure a Secure Information Architecture?

Expand Your Understanding with a Laboratory Exercise

(a) Use Case

Attacks on critical infrastructure such as the power grid are often leveraged for terroristic purposes, typically by extremist groups to further their sociopolitical goals by destabilizing society. The United States has become a target of increased malicious cyber activity in the past decade following the Russian-Ukraine conflict. These attacks can have cascading societal and industrial impacts [7]. According to the Department of Homeland Security, “Critical infrastructure provides the goods and services that are the backbone of [the United States’] national and economic security and the well-being of all Americans” [7]. This use case aims to provide an example of electric grid generator instability resulting from the opening and closing of a circuit breaker in a distribution substation connected to the larger regional grid. The simulation simplifies the mechanical design and operations of a circuit breaker.

Keeping the circuit breaker open and allowing the generator to keep spinning will affect the rotor angle stability of the generator. The rotor of the generator is the part that spins to generate electrical power. The user should observe the normal generator behavior as shown by a graph of the rotor angle deviation of the generator. Then, they will observe the result of the rotor stability angle measurement when the breaker is opened, and the power being generated is not equal to the power being used since the load of the system is disconnected.

The learning objective of this lab is to demonstrate another possible consequence of an attack like the substation circuit breaker takeover attack in Ukraine that is beyond the black out itself. Users will gain an enhanced understanding of CIE Principle 1, **Consequence-Focused Design**, that asks the key question “How do I understand what critical functions my system must ensure and the undesired consequences it must prevent” [4]. This is a key concept for any attack on critical infrastructure, and directly relates to the electric grid attack discussed in this document. Consider both the critical functions of the electric grid and the potential consequence while going through the lab.

Simulation Set-Up

The simulation for this use case will be in Simulink, a MATLAB-based graphical programming environment, to simulate a real-world generator. Please make sure that you add Simscape and Simscape Electrical Simulink libraries from Matlab. The Simulink file, Team-4-Electric_Grid-1-Week-8_Code.slx, is included in the materials for this case study. When the file is opened in Simulink, there will be two windows that open. The main window should look like the screenshot in Figure 5 which contains the synchronous machine block that represents a real generator, several green blocks that are scopes to open the graphical representation of the outputs of the synchronous machine after the simulation is run, and the Subsystem block that contains the details of the load the generator is powering. In this case, the subsystem is an infinite bus.

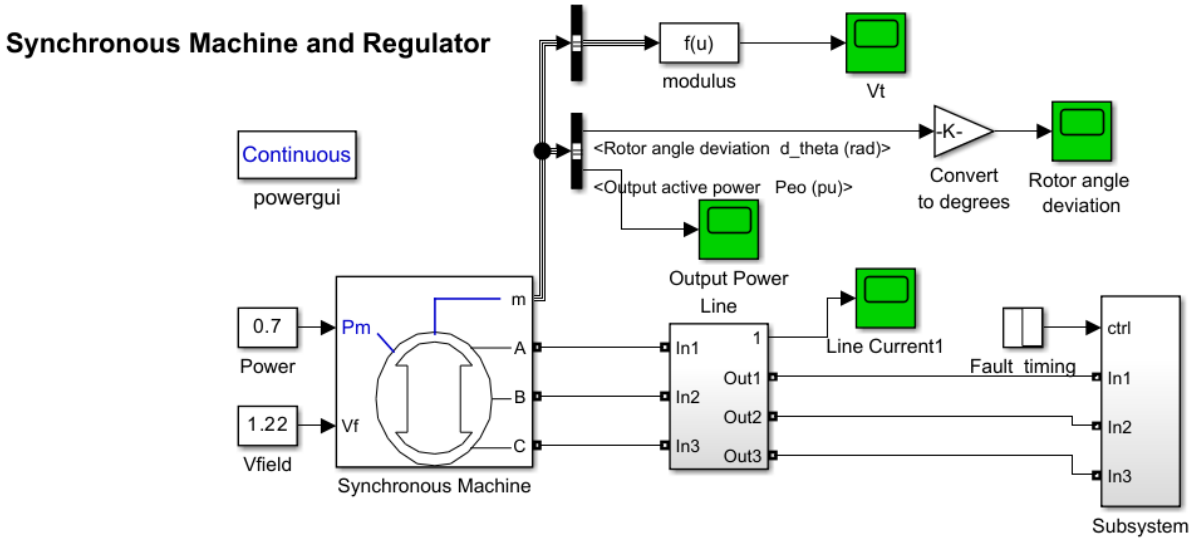


Figure 5: Screenshot of the Simulink simulation file containing the generator

The second window, shown in Figure 6, will show the detailed diagram of the subsystem block from the main simulation. This diagram is the representation of an infinite bus, which is an ideal component used in electric simulations that will maintain a constant voltage regardless of what happens in the rest of the system. The infinite bus is used in this simulation to isolate the generator behavior for analysis. The second window in Figure 6 also shows the switches that act as the circuit breaker in this simulation. The behavior of these switches will be controlled by the Fault Timing block in the main simulation window, and this is the part of the simulation that will be changed in each task to observe the resulting behavior of the generator.

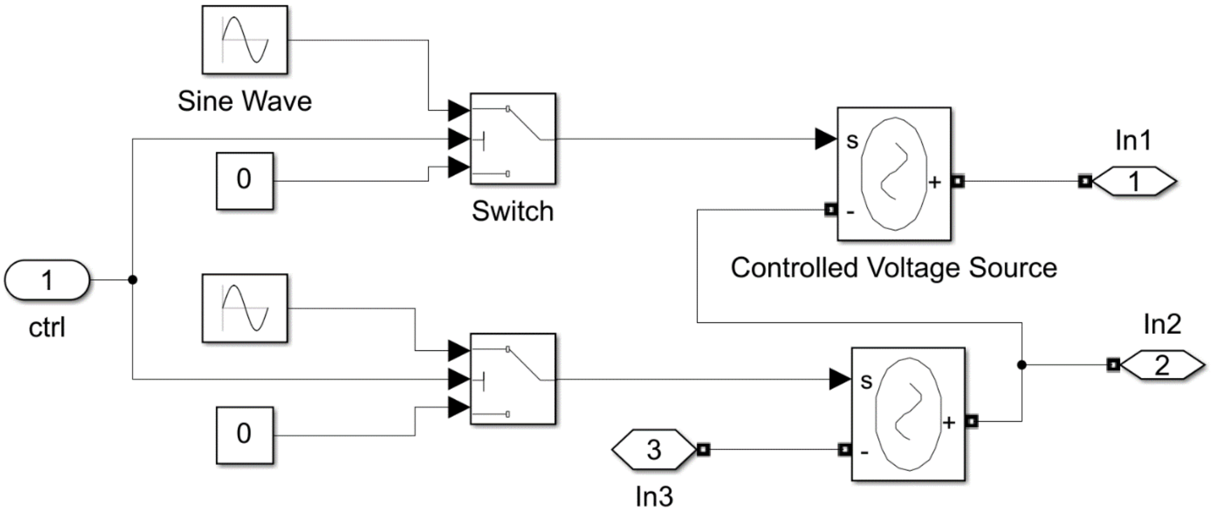


Figure 6: Screenshot of the window showing the details of the Subsystem representing the infinite bus

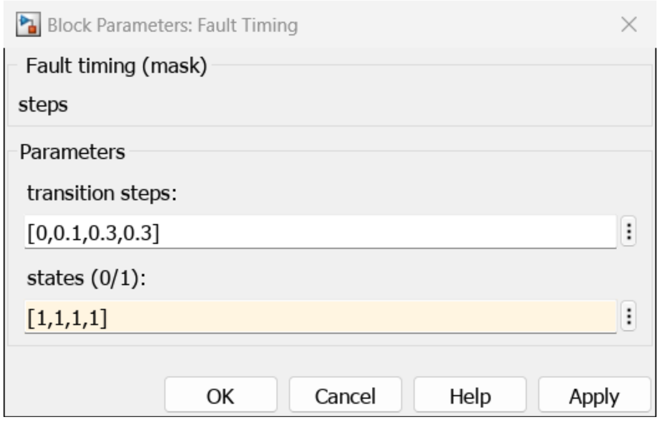
For a deeper explanation of the blocks used in the simulation and the parameter set on each of them, please click on the video file found here: **https://youtu.be/6YHAIyXP7x8**

(b) Tasks of this Exercise

Task 1: Observing The Normal Generator Behavior

The goal of this first task is to observe the behavior of the generator without opening the circuit breaker at all.

1. Double click the Fault Timing block to open the block parameters pop-up.
2. Set the states of the block to all be 1 as seen in Figure 7 and click Apply. The transition steps can be left as is. An output of state of 1 corresponds to the breaker being closed, so these settings will keep the breaker closed for the entire simulation run.



Block Parameters: Fault Timing

Fault timing (mask)

steps

Parameters

transition steps:

[0,0.1,0.3,0.3]

states (0/1):

[1,1,1,1]

Figure 7: Screenshot of what the states parameter of the Fault Timer should be for Task 1

3. Ensure the Stop Time of the simulation is set to 2 seconds and press Run.
4. Double click the Rotor angle deviation scope to pull up the output graph of the rotor angle. Select the Scale X & Y Axes Limits from the toolbar of the graph pop-up as shown in Figure 8.

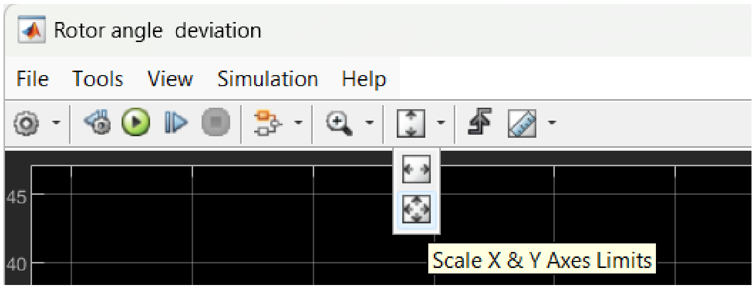


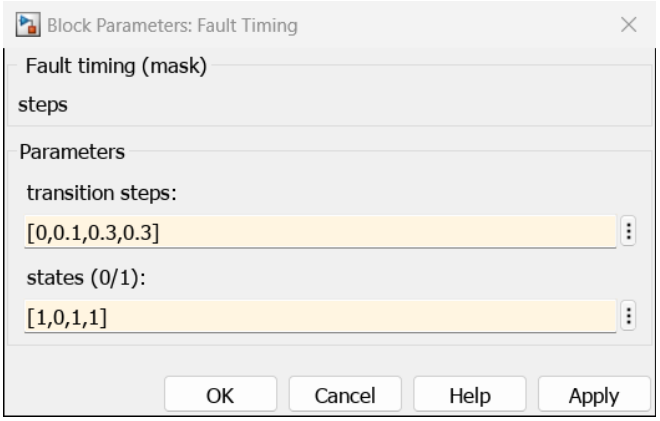
Figure 8: Scale X & Y Axes location on the graph toolbar

5. Note the graph behavior as the generator is started with no interruptions. Pay attention to the scale of the output on the Y axis.

Task 2: Opening and Closing the Circuit Breaker

For the next lab task, the circuit breaker connected to the generator is going to be opened and then re-closed for a short period of time to observe the effects on the generator.

1. Double click the Fault Timing block to reopen the block parameters pop-up.
2. Change the parameters of the block to match Figure 9 so that the transition steps are [0,0.1,0.3,0.3] and the states are [1,0,1,1], click apply. These configurations will set the output of the block to 0 when the simulation time is 0.1, opening the circuit breaker, and then set it back to one at 0.3 seconds reclosing the circuit breaker for the rest of the simulation run.



Fault timing (mask)

steps

Parameters

transition steps: [0,0.1,0.3,0.3]

states (0/1): [1,0,1,1]

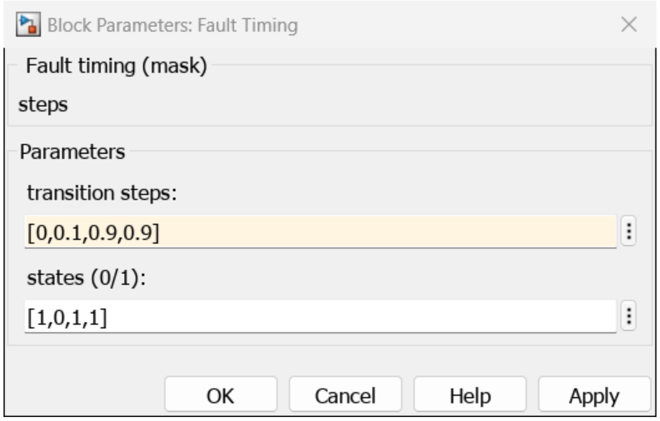
Figure 9: Screenshot of what the parameters of the Fault Timer should be for Task 2

3. Press Run.
4. Once the simulation has finished running, open the Rotor angle deviation graph again, and select the option to scale the X & Y axes again.
5. Note the graph behavior as the generator starts and then has the circuit breaker between it at the load opened briefly. Again, pay attention to the scale of the output on the Y axis.

Task 3: Opening the Circuit Breaker for A Longer Period of Time

For the final lab task, the circuit breaker will be left open for a slightly longer period of time. It is worth noting that the time the circuit breaker will open for is still less than 1 second, proving how incredibly precise the timing of opening or closing circuit breakers at this scale must be.

1. Double click the Fault Timing block to reopen the block parameters pop-up.
2. Change the parameters of the block to match Figure 10 so that the transition steps are [0,0.1,0.9,0.9] and leave the states as [1,0,1,1], click apply. These open the simulation when the simulation time is 0.1 second just like in Task 2 but will not reclose the circuit breaker until the simulation time is 0.9 seconds.



Fault timing (mask)

steps

Parameters

transition steps: [0,0.1,0.9,0.9]

states (0/1): [1,0,1,1]

Figure 10: Screenshot of what the parameters of the Fault Timer should be for Task 3

3. Press Run.
4. Once the simulation has finished running, open the Rotor angle deviation graph again, and select the option to scale the X & Y axes again.

5. Note the graph behavior as the generator starts when the circuit breaker is open slightly longer than before, and the affect it has on the Y axis of the graph compared to Task 1 and Task 2.

(c) Conceptual Question

1. What potential consequences could result to the generator based on the rotor angle behavior shown in the graph from task 3, as opposed to the behavior in the graphs from tasks 1 and 2?
2. What are some other consequences that could result from an attack like the one in Ukraine that results in a black out? These could be specific to the grid or wider social consequences.
3. CIE principle 4 is **Design Simplification**, which emphasizes only having features that are absolutely necessary to achieve the critical functions, since unnecessary applications and latent capabilities of a system can be leveraged by attackers [4]. What are some functions of a normal computer that should **not** be a feature of an HMI that controls critical infrastructure like the electric grid with design simplification in mind?
4. CIE principle 10, **Planned Resilience**, emphasizes the necessity for a plan or set of plans in place that assumes normal operation or safe failure after a cyber-attack. How can a power system operate or deliver power to customers under circuit breaker takeover conditions?

Further Reading and Useful Public Video Links

For further reading, the following references would be suitable to explore at your convenience.

[1] “Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case,” 2016. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

[2] J. Styczynski and N. Beach-Westmoreland, “When The Lights Went Out,” BoozAllen.com, Sep. 2016. https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

[3] B. Singer et al., “Shedding Light on Inconsistencies in Grid Cybersecurity: Disconnects and Recommendations,” 2023. Available: https://users.ece.cmu.edu/~lbauer/papers/2023/sp23-grid.pdf

[4] V. L. Wright et. al., "Cyber-Informed Engineering Implementation Guide," United States, 2023. Available: https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf

[5] R. V. Yohanandhan et. al., "A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid – Part – I: Background on CPPS and necessity of CPPS testbeds," International Journal of Electrical Power & Energy Systems, vol. 136, 2022, Art. no. 107718. [Online]. Available: https://doi.org/10.1016/j.ijepes.2021.107718.

[6] C. J. Brame, “Effective Educational Videos: Principles and Guidelines for Maximizing Student Learning from Video Content,” CBE—Life Sciences Education, vol. 15, no. 4, Dec. 2016, doi: https://doi.org/10.1187/cbe.16-03-0125.

[7] Department of Homeland Security, “Homeland threat assessment,” 2023. Available: https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf

[8] J Duncan Glover, T. J. Overbye, and M. S. Sarma, Power System Analysis & Design. Boston, Ma: Cengage Learning, 2017.

Authors

Erin Clark is a rising junior studying Communication Rhetoric, along with a minor in Spanish Language and a certificate in Television and Broadcast Arts. She has previous experience in the world of media, including work with anchoring, reporting, producing, interviewing, and hard-news broadcasting.

Abby Magistro is a rising senior computer engineering major. She has experience with cyber-security and simulations from her coursework, and plans to learn more about cyber-security, cyber-physical systems, and software development throughout her senior year to help her pursue a career in one of those fields.

James Ross is a rising senior studying History and Political Science and pursuing a certificate in Public and Professional Writing. He plans on pursuing graduate study in public policy and international affairs.

Amy Zhang is a rising junior majoring in Information Science and Digital Narrative and Interactive Design, with a minor in Computer Science. She has experience in journalism and storytelling through digital interface and is interested in the implications of increased digitalization of physical systems.