

## Case Study with Supporting Media and Simulation Exercise

### Title: The Role of Human Machine Interface and Remote Terminal Units in the 2015 Ukraine Power Grid Attack

#### Real World Inspiration

The real-world inspiration for this project was the Ukraine power grid attack of 2015. This grid attack featured Russian hackers gaining access to the Ukraine power grid distribution systems by utilizing phishing emails that accessed their computers which then allowed remote access to other machines in the power grid system. The access in the power station, as seen in Figure 1, had a cascading effect across the country. This attack caused power outages around the western Ukraine area. Around 225,000 customers were affected for about 1 to 6 hours [1]. The attackers were likely the Sandworm Group, whose motives remained unclear but seemed intent on causing significant infrastructure damage, aiming to disrupt the power grid for an extended period [2]. They were able to perform this attack because the power grid system used in Ukraine was of Russian architecture. Many pieces of detailed information will be explored to understand how this attack happened and what vulnerabilities lie within the system.

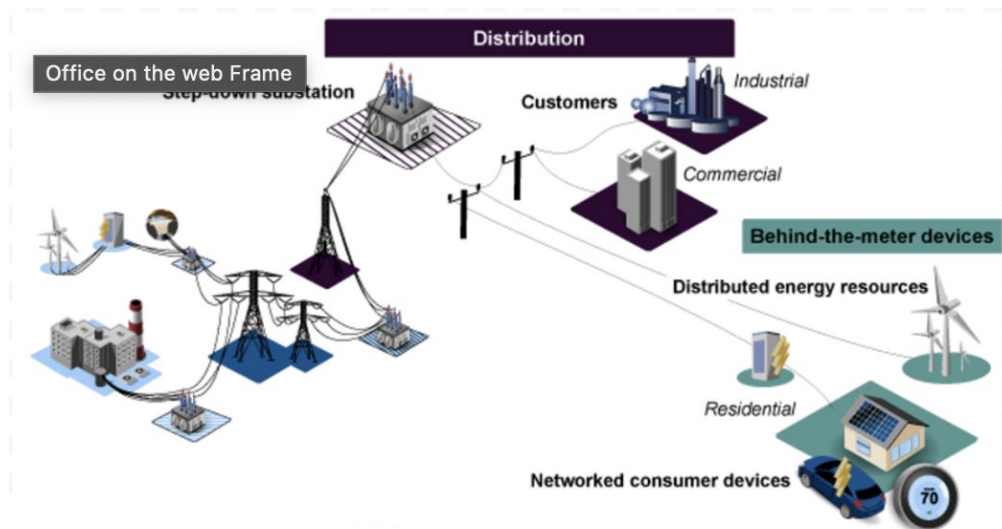
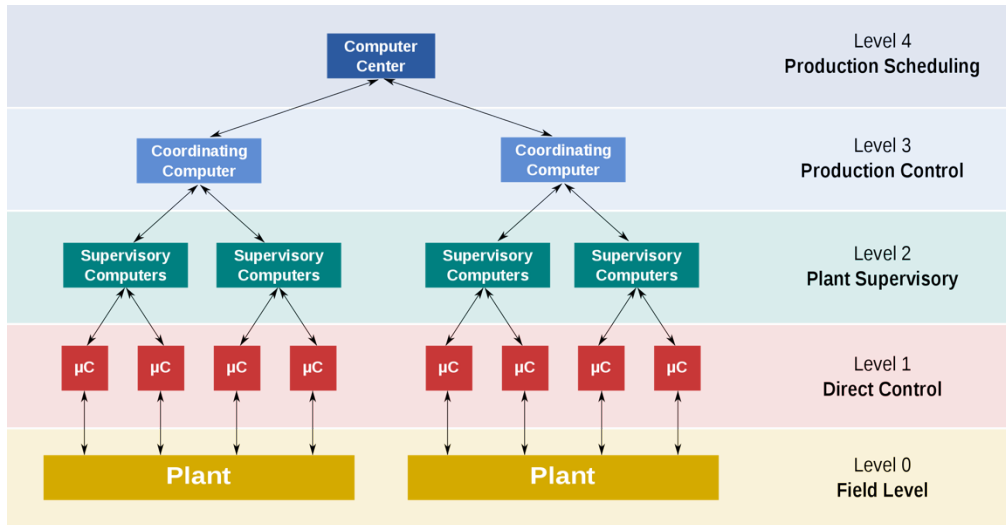


Figure 1: Distribution of Power System [3]

Mentioned previously, the architecture of this system was of Russian descent which allowed the attackers to understand the system further. This system utilized Supervisory Control and Data Acquisition (SCADA) architecture, which is a standardized control system for industrial systems such as power grids. One key aspect of this attack was accessing the Human Machine Interface (HMI) remotely, controlling the Remote Terminal Units (RTUs), and those units accessing the circuit breakers. The supervisory computers were on level 2 of the SCADA architecture, which connected to the RTUs on level 1, as seen in Figure 2. These layers contain distinct levels of control within the entire system which is why the attackers entered on a higher level and used the internal resources to reach the lower levels.



**Figure 2: Levels of SCADA System Architecture [4]**

These circuit breakers are switches that open and close the electrical circuit which connects to the power generators, keeping them stable. The generators need these breakers to remain stable, so the power load and output are balanced. The attackers opened the circuits which caused the generators to become unstable resulting in the power outage. These HMIs were able to be accessed via phishing emails. These emails contained the KillDisk malware which caused corruption to the Windows-based computers [5]. Another part of the cyber-attack was accessing remote control software on the HMIs and enabling control on the RTUs. These generators failed due to the attackers gaining control and disrupting their balance. Some adaptors were used between the HMIs and RTUs called serial-to-ethernet adaptors. The remote connections allowed the attackers to upload corrupted firmware to these adaptors which caused another failure in this grid system. The specific adaptors used were 'Moxa UC 7408-LX-Plus' and 'IRZ-RUH2 3G' [6]. Additionally, the attackers used Telephone Denial of Service (TDoS) attacks to disrupt internal communications between the substations and customer reports of their power outages.

**a) Risks Associated with Attack**

Several risks arise from this attack due to the damage caused by the attackers. Many internal devices were damaged such as the computers affected by malware, firmware corruption on the serial-to-ethernet adaptors, and generation damages due to unbalanced loads. The networks in this system can be compromised as in this use case scenario. All these machines and devices cost a significant amount of money to maintain and repair. Some external risks include conductors being overloaded and causing damage to nearby objects due to arcing electricity. These risks are focused on the power grid and its systems, but external entities are affected too. Businesses that rely on this power as well as customers are affected by these types of attacks. This specific power grid system is responsible for power generation but with generator instability, those generators could cause damage to the power grid infrastructure or any other plants/subsystems.

**b) Possible Countermeasures**

Countermeasures of this cyber-attack include many options. Back-up RTUs would allow these systems to resume operation when the primary units become compromised. There would be automatic sensors in place to detect if the primary units are not performing optimally and the backup units would activate and disable the primary ones until maintenance is performed. Some other countermeasures include having upgraded serial-to-Ethernet adapters that do not allow remote firmware updates from the supervisory computers [7]. These adapters would have centralized servers that would push the updates directly to the devices without external communication to the overall network. The primary vulnerability of this cyber-attack was the supervisory computer operators opening the phishing emails which allowed access to the overall system. Policies would need to be enforced to teach the operators about misleading emails and only allow trusted emails through. Ideally, these supervisory computers would not have access to emails outside of their internal network to prevent the phishing emails from entering.

As discussed, internal organizational policies need to be implemented and enforced to ensure operators receive the proper cyber-security education and training for their day-to-day role. Baseline organizational policies employee training and encryption should be consistent. It is recommended to implement dual factor authentication for logins, regular system wide security checks and risk assessments, password updates every six months, regular cyber training, reporting policies, and much more. Human error is one of the largest vulnerabilities to cyber security right now, especially as phishing is so prevalent. Consistent education and backup plans, if that education fails, are important to ensure cyber security practices remain consistent. Additionally, as company policy expands, such as using personal devices that may not have the same encryption as company devices, cloud systems in industrial control systems, and virtual machine technologies [8], it is important for companies to update and follow their cyber security practices.


### c) Relevant CIE Principles

Utilizing CIE (Cyber-Informed Engineering) principles would need to be implemented to secure the overall power grid system from any potential future attacks. **CIE Principle 7: Interdependency Evaluation** is the principle of evaluating how systems and subsystems impact each other. We can also consider setting what entities need to be independent of each other to prevent any unnecessary communication or connection. Applying this to the network would help ensure the internal devices connected to the networks are secure. The networks using this principle will help secure the overall network by disabling any open ports that would prevent access to applications not in use by the network. **CIE Principle 2: Engineered Controls** is another principle that can be used as its primary purpose is to have restrictions in place so that if an issue arises, the entities in question can only perform so far out of their designed range. This means that the functionality of these entities can be compromised, but they are designed in a way that only allows a certain range of nonfunctional operations. Some devices that can utilize this principle could be breakers that implement a delayed disconnect. This delay-disconnect would ensure that the breakers only open or close within a given time frame, which prevents opening and closing them continuously. Upgrading the firmware of the serial-to-Ethernet adapters is another engineered control as there would be a centralized server that is hardwired to only push updates to the devices while being disconnected from the rest of the network. **CIE Principle 6: Active Defense** protects the given system from attacks. Credential monitoring would be an active defense measure that can be implemented to only allow authorized users access to the system. Application whitelisting would only allow a certain list of authorized applications to be accessible within the protected system [8]. **CIE Principle 1: Consequence-Focused Design** ensures the critical functions of a given system remain operable even when under attack or suffering from issues. The critical function of the power grid system would be to deliver power whether the

system is damaged or not. This means that the entire power grid system needs to remain active under any circumstances.

Furthermore, **CIE Principle 8: Digital Asset Awareness**, ensures that there is awareness and understanding of digital access and its functions. This would allow for understanding of how programs such as Microsoft runs on different devices, and what operations and maintenance is needed to maintain these systems. **CIE Principle 9: Cyber-Secure Supply Chain** ensures security throughout the supply chain. This considers how different organizations, sectors, or regions provide different services and their cyber-security responsibilities. **CIE Principle 10: Planned Resilience**, turning potential “what ifs” into manageable “even ifs”. This looks at the people, materials, and equipment needed in the event of an event that impacts the power grid, and the systems and functions which need to withstand such an event. **CIE Principle 11: Engineering Informational Control**, manages and protects knowledge about the system to keep it secure. This considers what is sensitive information, how it is identified and collected throughout the lifetime of the system, what is shared internally and externally, and who has access to various levels of the system. Lastly **CIE Principle 12: Organizational Culture** ensures that employee behavior and decisions align with security goals. This principle considers the organization's stated and real priorities and their tradeoff between efficiency and security.

### 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: <https://youtu.be/-SOcSP1w8WI>

Our video includes interactive elements to enhance engagement. Our anchors successfully explain the use case in its simplest form, helping the audience understand the case we are addressing. The video features interviews with students sharing their perspectives on the use case, including how they learned about it, what interesting observations they made, and how they applied CIE principles to address the problem.

We present a mini package where students demonstrate how to run the simulation we built, explaining each step in simple terms. This helps viewers understand how the simulation works and why it is an effective tool for preventing cyber-attacks. Additionally, we include another mini-interview that covers the rules and regulations related to the simulation. This segment addresses how these regulations impact the implementation of our student-created simulation and explores the legal considerations involved.

Throughout the interview, we address questions about how policy and national laws influence the rollout of our simulation. By highlighting these aspects, we aim to show viewers the significance of our student-made simulation and the regulatory framework that supports it. Understanding these rules and regulations will provide viewers with insight into how we plan to bring our simulation to the world and its role in preventing future attacks.

### Future Policy Implications

Policy surrounding the energy grid within the United States dates back decades, with the most recent infrastructure advancements stemming from events such as the 2003 Northeast Blackout, Superstorm Sandy and the Ukraine Power Grid cyberattack. Following the 2003 Northeast Blackout, the United States Congress codified its Energy Policy Act of 2005, creating mandatory standards for utilities and implementing fines for failures in reliability. Decades later, national policies and recommendations have been levied to include cybersecurity when updating mandatory standards. Many of the physical aspects of the energy grid are aging, with 70 percent of transmission lines nearing 30 years old and 60 percent of the circuit breakers nearing 35 years old [3]. It is recommended to invest in and upgrade these aspects to prevent potential energy disasters. Additionally, in recent years there has been a national push to include renewable energy in the power grid, which is also largely unprotected from cyber issues. As the energy grid

is updated, both physically and electronically, it is important to ensure that there are a wide variety of protections and regulations implemented to protect our nation's energy in both the private and public sectors. CIE principles should be implemented as these systems are updated, instead of after the fact, to ensure the most comprehensive cyber-security implementation. Dual collaboration, efforts, and investments are recommended to create the largest opportunity for effective defense for our power grid in both a top-down and bottom-up approach. A top-down approach, as seen in Figure 3, for a public private collaboration allows for proper risk strategy, as each tier informs the next. A bottom-up approach covers risk evaluation, each tier informing the one above in a similar manner.



**Figure 3: Tiers of Cyber-Security Integration [9]**

While efforts to develop an overarching national cyber security policy are recent, there are minimum federal regulations that the United States Government monitors. The North American Electric Reliability Corporation (NERC) created the Critical Infrastructure Protection (CIP) standards as mandatory regulations and guidelines to protect the Bulk Electric System from cyber threats [10]. These standards were also created in an effort by the United States Federal Energy Regulatory Commission (FERC), to ensure the reliability of the North American power grid. The NERC CIP standards include 14 categories and are mandatory for all entities that own or operate bulk power systems within the United States. Compliance with the standards is enforced by FERC, which has the authority to impose penalties [11]. Beyond the current regulations, the Department of Energy has also backed a new set of energy distribution cyber security baselines for anyone who participated in the nationwide grid transition. These baselines are for the electric distribution systems and distributed energy resources (DER), creating minimum voluntary standards that DER operators, utilities and other electric distribution systems should meet [12]. This begins the top-down approach of Risk Strategy, as referenced earlier. Having consistent standards across all companies helps to provide reliability in security for all parties. The DER providers can use these baselines and prepare strategies to meet them. It is recommended that organizations implement these new standards as soon as possible and follow the current regulations already in place.

In addition to federal policy and regulations, the legal system and governmental relationships can and should be used to further cybersecurity in Tier 1. When a foreign agent attacks the United States via a cyber-attack, it is particularly difficult to apprehend these individuals. Depending on the relationship with the country of residence depends on if the individual will be extradited to the United States. In cases where the agent is not extradited, an indictment may still be brought upon them much as it was for the 2015 Ukraine Cyber Attack. Cybersecurity is not consistent nationally, never mind internationally, however the United States

can help develop better international standards that can positively impact us. The legal system's role can be strategically used to be non-combative and develop relationships with foreign countries, with what tools we have.

As discussed, policy informs risk security management by helping to create standard practices across sectors. Not all organizations have the same policies, such as a dedicated manager or employee who is working to improve and implement cyber security practices. Minimum standard internal practices are just as important as minimum federal regulations. This considers the CIE principle 8: Digital Asset Awareness and 9: Cyber-Secure Supply Chain. Platforms, such as the Electric Grid Cybersecurity Alliance, help to provide organizations ways to identify organizational gaps in standard practices and begin to develop a plan to implement them. Actionable policy and procedure can be implemented here, in addition to guidance constraints [9].

These standard practices translate into our third and final tier, where companies can implement better and more consistent cyber security practices, which follows CIE principles 11: Engineering Informational Control and 12: Organizational Culture. As discussed above in our Countermeasures, implementing policies such as dual-factor authentication is necessary. In addition to security checks, companies should also be performing simulations and exercises across the grid to identify potential vulnerabilities and respond to attacks [13]. This follows the CIE principle 10: Planned Resilience.

Each of these recommendations can be reversed engineered to provide risk evaluation. Employees should have a straightforward way to provide feedback on policies and updates about vulnerabilities they may come across to management and be provided with updates about the results of monitoring. As management is made aware of these updates and feedback, informing policy makers of vulnerabilities they see to create more comprehensive updates to these policies which can allow other organizations to implement the necessary security updates.

## Expand Your Understanding with a Laboratory Exercise

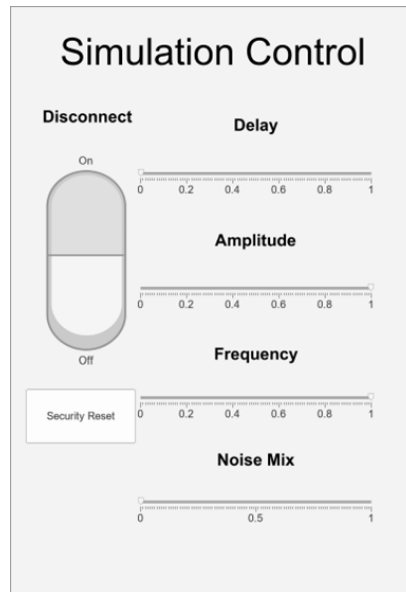
### (a) Use Case

The Use Case example for this project is a cyber-attack on the energy grid. Shadowbyte Collective decided to target Andorra Electric and Woodmont Electric, which supplied energy to thousands of customers. Their goal was to disrupt the energy supply to these customers, by sending phishing emails to the employees of the energy companies. These emails contained PDFs, that were embedded with malicious code. When opened, this code went onto the servers of Andorra and Woodmont Electric, which was then used to remotely disrupt the energy supply to its customers.

The malicious code was used to access the HMI remotely, controlling the RTUs, with the goal of those units opening the circuit breakers. Due to the cyber-security preventive measures that Andorra and Woodmont Electric had implemented; the admin dashboard, a secured HMI, locked the hackers out of the system and prevented the attack from continuing.

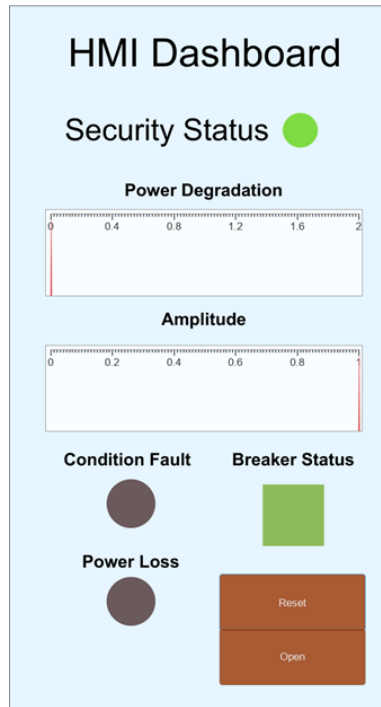
### (b) **Simulation Set-Up**

The MATLAB simulation features 3 main interactive dashboards and one subsystem that houses the innerworkings of the system. The interactive dashboards are the simulation control, HMI dashboard, and the admin dashboard. The simulation control dashboard allows for control on the main simulated generator that creates a sine wave which represents the alternating current output. It allows for the user to control the delay of the sine wave output, the amplitude (height) of the sine wave, the frequency (or repetition) of the sine wave, and the noise, which is any interference to the power output, as seen in Figure 4. There is a disconnect button which cuts the power from the circuit and a reset security button which resets the security status of the system. The security system will be explained when the functionality of the HMI and Admin dashboards are introduced.



**Figure 4: Screenshot of Simulation Control Dashboard**

The HMI dashboard is the main dashboard that a user/operator would access and control the circuit breaker, as seen in Figure 5. There are a couple of User Interface (UI) elements and buttons which inform the user and allow control over the circuit breaker system. The security status light is used to show if the security mechanism has been activated. The light is green when the system is functioning normally and red when the lockout has been activated. The security system is activated when the HMI “Reset” and “Open” buttons are activated too quickly within a given time frame (alternate reset and open indicates a suspicious behavior in this experiment). The power degradation gauge shows the difference in sine waves being produced by the generator and an ideal sine wave that is the expected output. The amplitude gauge shows the height of the sine wave being generated. The condition fault light is shown when the sine waves do not match the internal, or ideal, sine wave. If all the sliders delay is greater than zero, noise mix greater than zero, amplitude less than one, or frequency less than one in the Simulation Control panel this would cause the condition fault. The power loss light is on when the generator is disconnected, or off, or if the amplitude or frequency is zero. The breaker status light is shown to represent the current state of the circuit breaker being opened or closed. The reset button closes the breaker, and the open button opens it.



**Figure 5: Screenshot of HMI Dashboard**

The admin dashboard is a higher privileged panel that has the highest authority over the HMI dashboard, as seen in Figure 6. Ideally, this panel would be accessed by a higher authority employee who has the clearance necessary to access the panel and use it to override the HMI dashboard when a problem arises. This panel shows a couple more gauges with information and a master switch which disables the HMI dashboard. There are two new gauges added that show the raw input coming out of the generator and into the circuit breaker and the power output which shows the power leaving the circuit breaker and into the rest of the system. Another addition is the master switch which disables or enables the HMI dashboard panel. The main reason for this master control switch is to disable the HMI dashboard if/when something goes wrong, such as unauthorized use of the HMI.



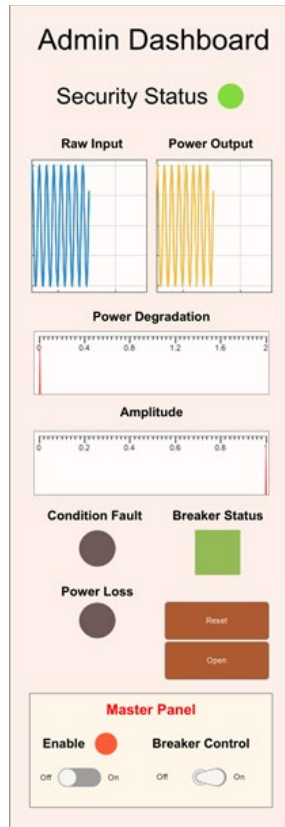


Figure 6: Screenshot of Admin Dashboard

The simulation has a couple of standardized components from the Schweitzer Engineering Laboratories data sheet (SEL-2407 and SEL-751 ) [14]. As seen in Figure 7, the SEL-2407 is the GPS clock component in blue on the left most side of the system. This houses the GPS clock which is the global clock connected to the entire simulation for power generation and analysis. SEL-735 is the blue component on top of SEL-751 which allows for the monitoring of the power quality within the system for the user to identify any potential issues [15]. The SEL-751 is the relay protection component which protects the circuit by implementing limits to power draw [16]. SEL-3350 is the main component that acts as the RTU/PLC in the system. This is what records events and processes the inputs and outputs of the other components.

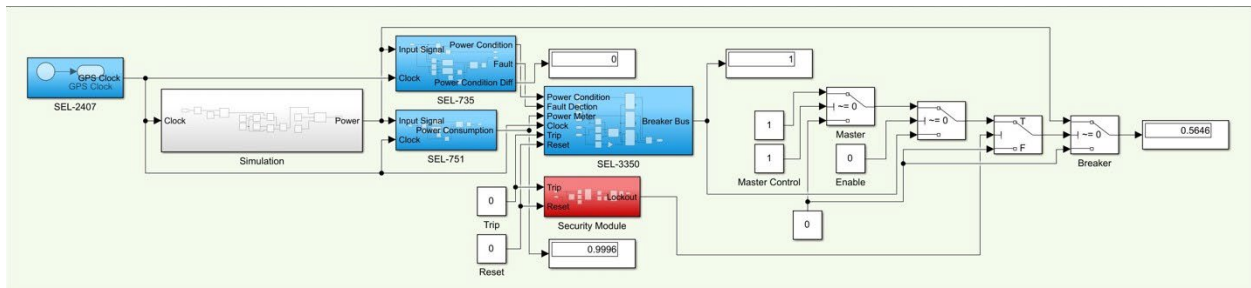


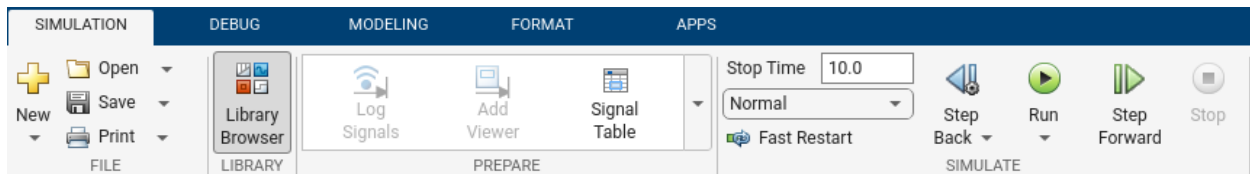
Figure 7: Screenshot of the Matlab Simulation Internals.

*This simulation features a few CIE principles such as Engineered Controls, Active Defense, and Interdependency Evaluation. The primary CIE principle was Engineered Controls as the security system currently implemented blocks the user at the hardware level. Active defense applies because the security system actively defends the system through a lockout when detecting an insufficient delay between opening and closing the breaker. Interdependency evaluation applies because of the distinct levels of privilege between the HMI and admin dashboards.*

### (c) Tasks of this Exercise

#### Task 1: Setting up Simulink and Monitoring its values for Lab Preparation

To start, launch the model by opening a Matlab installation that includes Simulink (version R2024a), type “Simulink” and press enter. This should bring up a Simulink window, as seen in Figure 7. From there open the simulation .slx file. When you press the green 'run' button, as seen in Figure 8 at the top of the window, the simulation will begin.



**Figure 8: Screenshot of Simulink Header Bar**

Then, you can press the reset button on the HMI panel to close the breaker and restore power to the system. After that try adjusting one of the simulation parameters. Changing any of the sliders will trigger a fault due to the comparison of an ideal sine wave and the one being currently generated. The Schweitzer system will automatically trip the breaker and it will need to be manually reset after the fault is cleared. This can be monitored on the HMI or admin panel, as seen in Figures 5 and 6.

#### Task 2: Admin Dashboard overrides HMI Dashboard

This next task will have you use the admin panel shown in Figure 6. To test the override functionality of the admin panel, flip the master switch 'enable' button located on the bottom of the panel to ON. This overrides all the other breaker controls except the security module. With this master switch enabled, the HMI dashboard panel will be completely disabled from accessing or controlling the overall system.

#### Task 3: Cycling the Breaker

This task will be testing the lockout mechanism of the security module. There are two lights that indicate the current status of the security system, green and red. The green light means that the lockout is inactive, and the dashboards have control over the system. The red light means the security module has been activated and the system is locked out of any user inputs. Figures 9 and 10 show what the light indicators look like. This lockout will only occur when opening and resetting/closing the circuit rapidly on the HMI dashboard panel. The lack of delay between opening and closing the breaker causes this lockout. The admin panel does not have this feature implemented as it has a higher privilege of control than the standard user/operator of the HMI dashboard. In order to reset the security lockout, you need to click the reset button located on the simulation control panel.

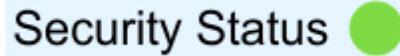
A screenshot of a 'Security Status' indicator. The text 'Security Status' is in a blue font. To its right is a solid green circle. The entire indicator is enclosed in a thin black border.

Figure 9: Screenshot of Security Status: Inactive

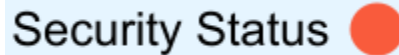

A screenshot of a 'Security Status' indicator. The text 'Security Status' is in a blue font. To its right is a solid red circle. The entire indicator is enclosed in a thin black border.

Figure 10: Screenshot of Security Status: Active

#### Task 4: Creating the Security Module

This task will have you create the security module that gets inputs from the Trip and Reset blocks as shown in the overall simulation above (Figure 7). This module's output will connect to a latch near the end of the simulation block, also shown in the overall simulation. There are multiple ways to implement this module. An ideal way would be to take the inputs and use 2 S/R latches with comparison blocks to create the lockout mechanism. Another component that should be used is a transport delay that connects to one of the S/R latches. Figure 7 shows how this block will be connected to the overall system, but you will not be provided with the red security module itself. Overall, you can choose 2 S/R latches, 1 transport delay, and comparison components to make the entire lockout mechanism and connect it to its required components.

#### Further Reading and Useful Public Video Links

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

- [1] “Cyber-Attack Against Ukrainian Critical Infrastructure,” Cybersecurity and Infrastructure Security Agency CISA, <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>.
- [2] “Power grid cyberattack in Ukraine (2015),” International cyber law, [https://cyberlaw.ccdcoe.org/wiki/Power\\_grid\\_cyberattack\\_in\\_Ukraine\\_\(2015\)](https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015)).
- [3] C. Brooks, “3 alarming threats to the U.S. Energy Grid – Cyber, physical, and existential events,” Forbes, <https://www.forbes.com/sites/chuckbrooks/2023/02/15/3-alarming-threats-to-the-us-energy-grid--cyber-physical-and-existential-events/>.
- [4] D. Pugliesi, “English: Functional levels of a Distributed Control System,” *Wikimedia Commons*, Mar. 09, 2014” Wikimedia Commons, [https://commons.wikimedia.org/wiki/File:Functional\\_levels\\_of\\_a\\_Distributed\\_Control\\_System.svg](https://commons.wikimedia.org/wiki/File:Functional_levels_of_a_Distributed_Control_System.svg).
- [5] “Ongoing Sophisticated Malware Campaign Compromising ICS (Update E),” Cybersecurity and Infrastructure Security Agency CISA, <https://www.cisa.gov/news-events/ics-alerts/ics-alert-14-281-01e>.
- [6] “IR-ALERT-H-16-043-01AP CYBER-ATTACK AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE,” Homeland Security, [https://legacy-assets.eenews.net/open\\_files/assets/2016/07/19/document\\_ew\\_02.pdf](https://legacy-assets.eenews.net/open_files/assets/2016/07/19/document_ew_02.pdf).
- [7] Petra, “What is a data diode?,” Advenica, <https://advenica.com/learning-center/know-how/what-is-a-data-diode/>.
- [8] “Seven Steps to Effectively Defend Industrial Control Systems,” Homeland Security, [https://www.cisa.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems\\_S508C.pdf](https://www.cisa.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf) Steps to Effectively Defend Industrial Control Systems\_S508C.pdf.
- [9] Industrial Control Systems Cyber Emergency Response Team, “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,”

- Homeland Security,  
[https://www.cisa.gov/sites/default/files/recommended\\_practices/NCCIC\\_ICS-CERT\\_Defense\\_in\\_Depth\\_2016\\_S508C.pdf](https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf).
- [10] J. Livingston, "NERC CIP Standards: Safeguarding North America's Power Grid," Verve Industrial, [https://verveindustrial.com/resources/blog/what-are-the-nerc-cip-standards-in-ics-security/?trk=article-ssr-frontend-pulse\\_little-text-block](https://verveindustrial.com/resources/blog/what-are-the-nerc-cip-standards-in-ics-security/?trk=article-ssr-frontend-pulse_little-text-block).
- [11] "CERTREC's NERC Penalties Directory," Certrec, <https://www.certrec.com/resources/nerc-primer/certrec-nerc-penalties-directory/>.
- [12] "New DoE-funded initiative outlines proposed cybersecurity baselines for Electric Distribution Systems and distributed energy resources | Department of Energy," Department of Energy, <https://www.energy.gov/ceser/articles/new-doe-funded-initiative-outlines-proposed-cybersecurity-baselines-electric>.
- [13] C. E. C. Directors, "13 years after: The northeast blackout of 2003 changed grid industry, still causes fear for future," POWERGRID International, <https://www.power-grid.com/executive-insight/13-years-after-the-northeast-black-of-2003-changed-grid-industry-still-causes-fear-for-future/#gref>.
- [14] "SEL-3350-1 automation controller," Schweitzer Engineering Laboratories, <https://selinc.com/api/download/133033/>.
- [15] "SEL-735 Power Quality and Revenue Meter," Schweitzer Engineering Laboratories, Inc., <https://selinc.com/products/735/>.
- [16] "SEL-751 Feeder Protection Relay," Schweitzer Engineering Laboratories, Inc., <https://selinc.com/products/751/>.

## Authors

Ethan Crosby is a rising junior majoring in Computer Science. His background also includes work in electrical engineering.

Michael Estocin is majoring in Film and Communications with a certificate in TV broadcasting.

Katie Fitzpatrick is a rising senior pursuing a degree in Political Science and Psychology. She has a background in human interaction and behavior in the political landscape and application to policy.

Aidan Gresko is a rising senior majoring in computer engineering pursuing a Bachelor's degree. He thrives on gaining knowledge about technology and has a background in coding, circuits, and digital design work.