PREPRINT
INL/CON-17-42143

Publisher IEEE: https://doi.org/10.1109/RWEEK.2017.8088647

Using simulators to assess knowledge and behavior of "novice" operators of critical infrastructure under cyberattack events

Resilience Week

A. Rege, S. Biswas, L. Bai and E. Parker
Temple University

T.R. McJunkin
Idaho National Laboratory

2017

Using Simulators to Assess Knowledge and Behavior of "Novice" Operators of Critical Infrastructure under Cyberattack Events

Aunshul Rege[1], Saroj Biswas[2], Li Bai[2],
Edward Parker[1]
[1] Criminal Justice, [2] Electrical Engineering
Temple University
Philadelphia, PA
rege@temple.edu

Timothy R. McJunkin
Power and Energy Systems Department
Idaho National Laboratory
Idaho Falls, Idaho
Timothy.McJunkin@inl.gov

***Abstract*—The transition from the traditional power grid to the smart grid improves reliability, performance, and management, while simultaneously increasing its susceptibility to cyberattacks. One of the biggest weaknesses in grid security is the human agent responsible for its maintenance and operations. As such, it is crucial to embed hands-on understanding of grid operations and security, especially for students in the Electrical and Computer Engineering (ECE) fields. This paper presents a case study where ECE students from Temple University used an interactive microgrid simulator, "Grid Game", a program developed by Idaho National Laboratory. This case study offers insights into the ECE students' understanding of key engineering principles (microgrid stability, generation control system, generator inertia, energy storage, and grid security) gained by using the simulator program. Furthermore, the human behavior (strategies to prepare for and respond to cyberattacks, and cooperation and conflict in decision-making) of defenders/ECE students as they experience cyberattacks are also discussed. The paper then offers some limitations and possible suggestions for future research.**

Keywords— multidisciplinary operations; hands-on simulation training; critical infrastructure; cybersecurity; gamification; power systems; control systems; human-in-the-loop

I. INTRODUCTION

The U.S. power grid is a complex networked system that serves more than 300 million people, comprises more than 200,000 miles of transmission lines, and is valued at over $ 1 trillion [22]. The transition from the traditional power grid to the smart grid improves reliability, performance, and management by creating bi-directional communications to operate, monitor, and control the flow of power distribution and observational techniques. However, the implementation of the smart grid communication networks brings with it security vulnerabilities and challenges [21, 22]. The grid is considered to be "target number one" for cyberattacks and cyberterrorism as power disruptions can impact other dependent infrastructures and have significant economic ramifications and industry downtime costs [14, 16, 20, 22]. There have been many incidents of cyberattacks on the power grid all over the world, three notable ones being the denial-of-service attack on a German power utility in 2012 that shut down the load power supply for five days, the sniper attack on a California substation that damaged 17 large power transformers, and the 2015 Ukranian grid cyberattacks. A recent study [19] shows that loss of only 9 substations out of over 55,000 substations in the US could lead to widespread of power outage lasting over 18 months. Not surprisingly, the increased threat to power grid security has amassed a lot of attention from the government, the energy industry, and consumers. With the advances in technology and connectivity, security of the power grid has shifted from just prevention of physical attacks against power plants and distribution centers to include prevention of cyberattacks against the software and hardware that keeps the smart grid stable and operational. Unfortunately, the power sector is not prepared for cyberattacks [14, 18, 23, 24].

One of the biggest culprits in security breaches are the workers themselves. Employees should not only be knowledgeable about basic gird operations and functionality, but they should also be trained to recognize potential threat agents, effectively manage technical and social engineering attack vectors, efficiently respond to cyberattacks and mitigate impacts, and think proactively about cybersecurity. This paper offers findings from a unique and innovative multidisciplinary joint course project between Temple University's Electrical and Computer Engineering (ECE) department, Criminal Justice (CJ) department, and Idaho National Laboratory (INL) in Fall 2015. The project is the first of its kind that bridges disciplines to train the future workforce via hands-on training via a simulated power grid (Grid Game) not only on understanding engineering and power grid concepts, but also on how to prepare and respond to cyberattacks by making dynamic decisions in groups.

This paper is structured as follows. The Section II provides a brief research review on power grid security. Section III summarizes the microgrid simulator, GridGame, which was used in the joint course project. Section IV provides the design and implementation of the project. Section V and VI provide information on the learning outcomes of ECE students on (i) engineering principles, such as microgrid stability and generation control system, generator inertia and energy storage, and grid security, and (ii) human behavior and dynamics, such as grid operations, cybersecurity preparedness, cyberattack

response, cooperation and conflict, and overall performance improvement (if any). The paper then provides some limitations and possible improvements for the grid game software, ECE course project, and methodology, in Section VII. Section VIII offers some future directions that the researchers plan to undertake.

II. Power Grid Security

Security requirements for power grid are substantially different from that of typical business enterprises primarily because of the fact that a power generator cannot be immediately taken off-line if its controller is compromised since restarting the generator may take several hours. Nevertheless, the power grid is equipped with appropriate protection systems that that keep the system operational as long as there are no current or voltage overloads. Thus, in addition to timely detection and application of countermeasures against all cyber threats, a fundamental requirement of power system security is to design its control system that makes the system resilient to cyberattacks.

Security of power grids can be modeled as a three layer process: infrastructure security, information security, and control system security [8]. Infrastructure security deals with the protection of physical and cyber assets of the grid, such as SCADA systems, RTU's, various sensors, and computers etc., which is achieved by firewalls, authentication processes, and various other methods. Information security pertains to the protection of information by encryption, digital signature, authentication codes, etc. Control system security is the application layer of power grid protection usually based on mathematical and control theoretic tools for robust intrusion tolerant algorithms.

Considerable research has been devoted recently to detection of data attacks on power grids and their impacts on SCADA control systems. One of the approaches to detection of data attacks is based on state estimation of the power system [9, 10]. Sridhar [11] classifies SCADA attacks into *intelligent attacks* and *brute-force attacks* based on the expertise and resources available to the attacker, and modeled the attacks as changes in sensor data to their maximum or minimum values. Replay attacks have been considered [12] in which the attacker simply alters sensor data to certain prerecorded values. The effects of data attacks on system observability and state estimation are the subject matter considered in [9, 13]. Intelligent data attacks that alter the mean and/or variance of sensor data have also been reported in the literature. While these methods are mathematically rigorous, the attacker's actions are usually expressed in terms of a random process of known statistics. In reality, whether or not human decisions can be formally expressed in terms of a mathematical formalism remains questionable. As such, a better architecture for understanding power grid security can be described in the cyber-physical-human system shown in Fig. 1., which clearly depicts interactions between the four entities involved: cyber system: SCADA control system and related protocols, physical system: power grid infrastructure, the offender: cybercriminals and state agents, and the defender: system operators and engineers.

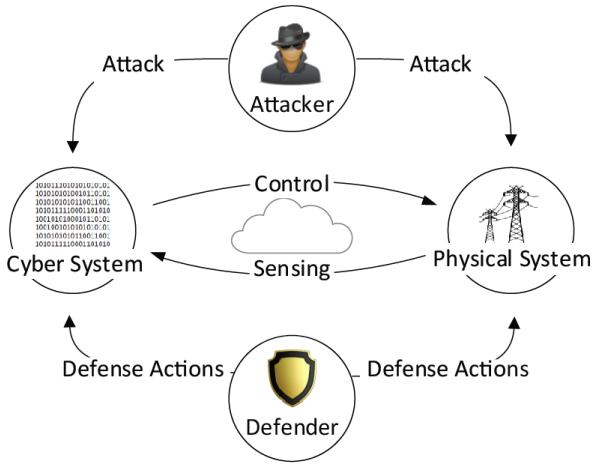

Fig. 1: Cyber-Physical Attack & Defense Diagram

This paper pertains to security of generator control loop. It is known that power generators must operate at a constant speed so as to maintain a constant grid frequency, which is 60 Hz. The rotational speed of the generator is controlled by a closed loop system using feedback of bus frequency signal. Changes in the speed could occur due to several reasons, which could be both natural or a cyberattack. Normally frequency change can occur due to variations in customer load or prime mover inputs, which are easily controlled by the closed loop control system. On the other hand, a cyberattack on frequency sensor or SCADA system could also lead to an apparent imbalance between input and output of the generator leading to variations in frequency.

A. Generator Control Loop

The Swing equation [2] of a generator provides an avenue to develop an understanding of cyberattacks and some of the possible impacts to the power grid. The swing equation is given by

$$\frac{2H}{\omega_{syn}} \frac{d^2\delta}{dt^2} = P_m - P_e \qquad (1)$$

where H is defined as the inertia of the generator, ω_{syn} is the synchronous speed in terms of electrical radians, P_m is the mechanical input power to the generator in per-unit, P_e is the electrical output of the generator in per-unit, and δ is the rotor angle associated with the generator voltage. In steady state conditions, (prior to any attacks or faults), $P_m = P_e$, i.e., there are no fluctuations in power, the generator frequency ω will be constant.

A cyberattack could cause a number of things to go awry, such as tripping of a circuit breaker, or shutting down the generator. A cyber attacker could inject falsified data into the feedback loop causing an imbalance between prime mover input and generation for which the generator then has to compensate. This leads the controller to either increase power output to compensate for the lack of power generation or to slow down due to a drop in demand. Both of these situations can cause the generator harm because of the innate sensitivity of a synchronous generator's operating speed.

B. Power Grid Attack and Defense

There are a number of cyberattacks that can affect the power grid which include, but are not limited to: denial of service (DoS), virus, worm, phishing and spoofing attacks. The intent and impact of the DoS attack is to prevent the use of network resources by flooding the network with a large amount of packets against the target [3]. An example of this could be blocking communications to the power provider during an outage so that the consumer cannot relay that the power is out, thus extending the duration and increasing the costs of the outage. Both viruses and worms are forms of malware that could easily be introduced into a system via a phishing attack. Phishing is a social engineering attack that tricks users or workers at the power grid to unintentionally download and install malware onto the system. It is typically done through email using a link or attachment. Once downloaded, it is very easy for the malware to travel to more sensitive portions of the network where it can execute its espionage or destructive code. The most recent example of this was the attack against the Ukrainian electric power industry on December 23, 2015. The malware known as Blackenergy was used by cybercriminals to shut down the power for a few hours while making the targeted hardware unbootable [4]. The spoofing attack is when an adversary tricks the operator into believing everything is status quo with falsified data while there is really an attack going on. Phishing is a form of spoofing attacks. A different example would be acquiring network access, intercepting data going back to the control system, and then altering the data to fool the operator or control system there is a problem or everything is okay.

There are a variety of ways to protect the power grid from cyberattacks. Ensuring the anti-virus and malware protection on computers is up-to-date is a simple first step. Intrusion Detection Systems (IDS) are typically employed to monitor network traffic. When unusual activity is discovered, the IDS sends an alert to the operator to warn of a potential breach in security. An example alert may be "Suspicious traffic volume from Network-printer-A." when malware is performing an nmap scan. There are a variety of these systems on the market and more are being developed specifically for Industrial Control System (ICS) SCADA networks.

III. GRID GAME

The GridGame is an interactive microgrid simulator with multiple participant capabilities that was originally developed for a multi-disciplinary course in Resilient Control Systems [5]. The goal of the game is to maintain a constant grid frequency on your own microgrid through the implementation of a control system. Whilst maintaining the microgrid, the player must purchase more power generation sources as well as garner more customers to maximize their score/revenue. The players undergo a series of random attacks throughout the duration of the gameplay, much like a real power grid. The players must make an effort to fortify their defenses to the best of their abilities or else they will be shutdown resulting in a loss for that particular game session.

The physics of the game are based on the Swing equation relating the change in speed/frequency of the spinning synchronous machines powering the grid to the power balance of generation versus load, described in Section 2. A one year period of five-minute interval data for the residential loads and hydroelectric and wind generation from Idaho Falls Power [6] drives realistic variations into the game. The data is played back at 3000 times the actual variations to make the dynamics of daily and seasonal changes more interesting for game play. A storage device representing a battery or pumped hydro was added to the game to provide an element of feedback control whereby the player can balance the generation and load by injecting or absorbing power from the microgrid. Automatic feedback control, using a proportional-integral-differential (PID) control gains to choose magnitude of power transfer to and from the storage source based on measured comparison of grid frequency to frequency set point (60Hz), shown in Fig. 2., provides students with an intuitive concept of the effects of the gains on the stability and dynamics of the system. If the frequency varies beyond +/- 2Hz, a blackout is caused and the player penalized with downtime and loss of customers. The players earn points based on the amount of energy they provide to their customers and the quality of power provided as measured by frequency and phase errors as well as other tertiary factors. The players are given the option to recruit customers, add more wind and hydro generation by expending some of their points as an investment towards higher point totals in the future. Players also use points to purchase more assets or protection or remedies against cyberattacks.

A market for exchanging power for points between players is provided by an external server, which also serves as the home of a game scoreboard [7] and game master controls. Game masters have the capability to send cyberattacks to the players or send information or taunting messages. The cyberattacks range from score deducting financial attacks to cyber-physical attacks that alter the control system and/or the integrity of the data displayed to the player on the control panel.

In the early stages of the game, it is imperative that the grid engineer (player) gathers as many customers as possible to maximize revenue. To offset the newly acquired load demands, the player must balance the demand by both purchasing new power generation units (Wind or Hydro). To help aid the counterbalance in power generation/consumption, it is wise for the player to also increase the amount of energy storage capabilities to create a large reservoir of backup power. Once the game has progressed enough, the player should begin researching possible preventative actions from Table I to combat the future cyberattacks that have yet to occur.

There are currently five cyberattacks that exist in the GridGame: the Little Guy Virus (LGV), the Big Guy Virus (BGV), DDoS, Gluxnet, and Blue Frog (BF). The LGV and BGV are the same virus but the BGV is a more severe version. These viruses attack the score/revenue of the grid operator. The analog of this in a real power grid is any sort of malware attack that causes some minor damage or inconvenience to the grid/operator. The DDoS attack affects the power market place making it difficult to communicate with customers. The real world analog is like the example provided previously of blocking communication during an outage. Gluxnet is a more sophisticated piece of malware that attacks the control system gains. This makes the operation of the control system

suboptimal increasing cost to the grid, stress on the machinery, and potential damage to the system. An analog to this attack could be Stuxnet as its name suggests. Finally, there is the BF which disables the automatic control system and forces the manual operation of the grid. Manual operation of the grid is challenging and it adjusts control values. Thus, even if the player/operator is successful in stabilizing the system, once the automatic control is restored it can throw the frequency off and cause a blackout. A real world analog is the recent Ukranian attack described above where the Blackenergy malware disabled the electric power grid.

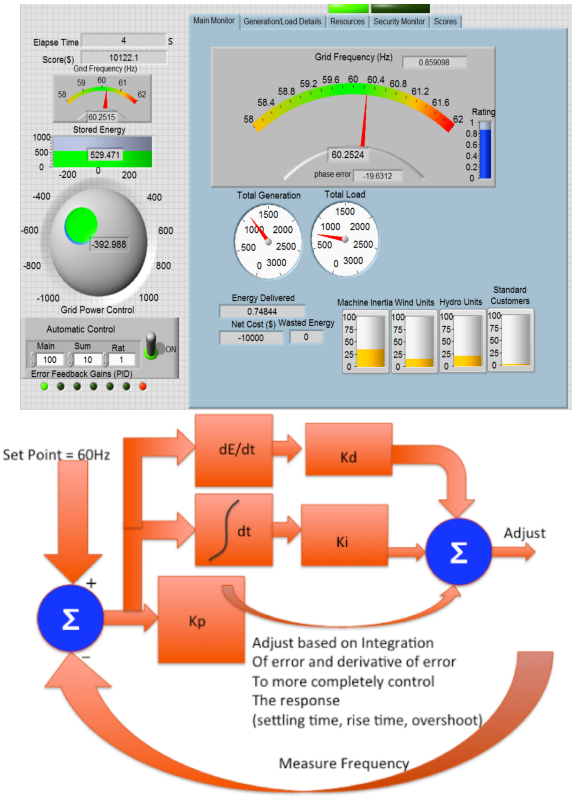

Fig. 2: GridGame Control System Illustration

The GridGame supplies cyber defense mechanisms the operator can employ against cyberattacks. There are six preventative measures to take and their characteristics are described in Table 1. The player has either purchased the protection from the attack and is immune or is immediately infected by the attack. A successful attack persists until the player applies a sufficient remedy.

IV. Case Study: Joint Course Project

The GridGame exercise was scheduled in November 2015 and had 23 Electrical and Computer Engineering students from the ECE 4712 course, who were assembled in a single classroom. The students had already downloaded the GridGame software on their laptops from the game website. The students worked in eight groups of three to four members, where they played the role of electric utility administrators responsible for managing consumer loads minute by minute while trading energy with each other, earning profits and fending off waves of malicious cyberattacks trying to bring the grid down. Each group was responsible for maintaining its grid while an INL researcher and Temple ECE graduate students played the role of cyberattackers. The exercise lasted for 2.5 hours and was divided into three rounds of 30 minutes each. Each round itself was structured to have 15 minutes of buildup time and 15 minutes to manage an assortment of cyberattacks launched against them. Furthermore, different teams were randomly subjected to different attacks throughout the three different rounds. At the end of each round, students restarted the GridGame and start afresh. Thus, Round 1 served as warm-up, and during Rounds 2 & 3 students were more comfortable with their tasks. Each team was observed and interviewed by Criminal Justice students as it progressed through the three rounds. This class project was approved by Temple University's Internal Review Board. All students were informed of the study's purpose and signed the informed consent forms.

Table I: GridGame Countermeasures

Types of Security	Cost ($)	Description & Time to Apply (s)
BasicAnti-virus	2000	Removes and prevents "little guy" class viruses (10)
Firewall	4000	Protects communications and stops DoS attacks (10)
Advance Anti-virus	9000	Eliminates and blocks all up to "big guy" class viruses (20)
Security suite	11000	Provides a firewall and advance virus protection (30)
ACME security service	25000	Hires a team of computer experts that find/fix the problem for all attacks except the zero day (50)
Wipe Operating System	0	Removes all infections, returns system to normal and removes all previously installed cyber protection (120)

V. Student Learning Objectives and Outcomes

The ECE students experienced the impacts of real time cyberattacks on the power grid, from stability of the grid to power quality evaluation to power markets. Following the GridGame exercise, the students were asked to share their thought process, in several areas listed below, as they made engineering decisions along the way.

A. Microgrid Stability and Generation Control System

The microgrid stability component tested students' understanding of grid stability based on analysis of swing equation under various scenarios due to cyberattacks, such as loss of a generator, loss of the generator controller, remedial actions of stabilizing the grid. The generator control system component assessed students' understanding of closed loop proportional-integral-derivative (PID) control in the generator control loop, and effects of changes in various gains.

All teams gained a strong understanding of frequency stability of the grid, and how it can be controlled using the PID

controller. Students' project reports showed that they were able to explain grid stability using the swing equation, in general, from energy conservation point of view.

B. Generator Inertia and Energy Storage

The generator inertia component tested students' understanding of the effects of generator inertia on system stability, and on whether the generator inertia can play any role in maintaining stability in the event of a cyberattack. The energy storage component evaluated students' understanding of the spinning reserve and its use for maintaining stability and power balance in the events of cyberattacks. There was a subtle relation between generator inertia and stability with stored energy reserve which is not so apparent in the swing equation.

On effects of generator inertia, Team 3 explains "by using hydro power the inertia of the system increases, which diminishes the effects on the frequency regulation of the power supplied (i.e., it reduces frequency drift)." At the same time the team was also concerned that "hydro plants causes large environmental impacts around the dam areas." Members of Team 4 on the other hand gained only superficial understanding of effects of generator inertia on frequency stability. Team 7 had the best understanding of effects of inertia on grid stability which can be seen from its report: "The more and bigger the machines, the more the inertia. Hydro generators have large spinning machines. More inertia slows down the change in frequency with power imbalance."

On energy reserve, Team 3 members had a clear view as it explained that "if a supply interruption takes place in the microgrid, the storage energy will provide the power necessary to keep on supplying the critical load." They also understood that having excessive reserve is also a poor business decision "as the generation and the load consumption are not matched, … production is not very efficient or Optimum". Team 4 stated that there will be high generation cost during peak periods due to lack of adequate reserve energy. It also realized that if there is not enough reserve, a real life microgrid might have to be shut down in case there are outages. Team 7 observed that adding distributed renewable generation is a good idea for microgrid as the stored energy can be used during outages of conventional generation due to a cyberattack. They also suggested the concept of encouraging customers for shifting demand in case there is not enough storage.

C. Grid Security

The grid security component assessed students' understanding of the general concept of grid security, and decision making process of grid owners. All teams received a strong understanding of grid security and the need for grid protection. The teams used various tools available at their disposal, such as a) purchasing antivirus, b) increasing stored reserve energy, c) manually tuning the generator control system, and d) increasing generation inertia. During cyberattack events, however, the teams reacted differently based on their own preference. These decisions were more based on human behavior than on engineering principles since defending the grid costs money and affects their decisions on energy trading. The following section reviews the human behavior of some defender teams.

VI. Assessing Human Behavior of Defenders

There were a total of eight teams of students who participated in the GridGame exercise. The students were observed and interviewed to understand how they behaved when playing the game and managing their grids when under cyberattacks. While providing a minute-by-minute assessment of their behavior is impossible in this paper, observations from a few teams are offered.

A. Grid Operations

All teams had specific approaches to making money and effectively maintaining operations. For instance, Team 3 stated that it wanted to balance out what it bought and how many customers it got with regards to storage. Members did not want to overload in any one specific area, such as buying so many customers that it crashed their storage. Team 4's approach was to store energy and maintain frequency at 60Hz. One member stated that the best way to maintain grid operations was to focus most of the team's efforts on keeping the stored energy at mid-range on the grid as this would give them more time and allow them to react to any changes in the grid with greater efficiency. Team 7 knew how to create, buy, and sell contracts, and generate revenue successfully. Overall, this team was confident with its knowledge of the system and how to generate and increase their revenue. Team members discussed the best amount of loads and walked through each input, step, and action.

B. Cybersecurity Preparations

Team 3 had not thought out its defense strategy effectively. When asked if it had any preemptive steps to defend against attacks, one member stated: "Good question, I did not think about that. We will probably buy it later, but I am not really sure about this." Influenced by their own response, Team 3 members bought the basic Anti-Virus protection measure, which remained a constant approach across all three rounds; the team never progressed to buying any further defenses.

During the first round, Team 4 did not focus much on preparing for security. Learning from the first round, however, the team members then did focus on security. As one member stated: "at this moment we don't need any [security measures], but we should get at least basic security because we never know when an attack will take place. We want to build up. These are investments in our infrastructure so we want to make sure we are buying what we can afford at the time of the purchase".

In the first and second rounds Team 7 members were novices with regards to their strategy for purchasing and using cybersecurity defenses. For instance, the team had no idea about the number and types of attacks, and as such believed that the best course of action was to buy the advanced anti-virus, which it assumed would protect it against most attacks in general.

C. Response to Cyberattacks

Team 3 managed cyberattacks against its grid poorly. When the attacks started, the team members did not know what any of the cybersecurity measures did (except for the basic Anti-Virus) or that there were even multiple options available

for defense. On occasion, the team did not even realize that it was under attack.

Team 4 essentially ignored the attack aspect of the game in the first round. For the most part this team's approach was to react: "We implemented some security measures… it's just that we didn't use them properly… So this round we [need more] time to recognize those attacks".

When Team 7 experienced the Blue Frog attack, and its system went into manual mode, the team members were unable to effectively manage the grid. Members were unaware that they could survive this attack by either operating their grid in manual mode or by wiping out their operating system. As one member shockingly stated: "I did not know we could run on manual mode or that wiping the OS – we had never tried that!".

D. Cooperation and Conflict

Team 3 members were very cohesive and cooperated with each other; however, one member was more engaged than the other. Overall, the team was relaxed, never became frustrated even when they were under attack and lost.

Team 4 members experienced some conflict as there was dissatisfaction with one member's operation during the first round. After losing the first round, the team members had an argument about the main purpose of the game. While one member stated that "the purpose of the game was to make money" another member argued that there should be a greater focus on security and stated "You don't know what attack you are seeing. You don't know how the hackers are manipulating the data you see". These conflicts remained throughout the three rounds.

Members of Team 7 were very cohesive with constant communication throughout each input, step and action. They continuously discussed strategy, what they wanted to improve on, and what approach they wanted to take in the subsequent rounds.

E. Improvement across Three Rounds

Overall, it appeared that all three teams learned from each round. They were more prepared and better understood the systems as they progressed through the exercises. Team 7 seemed to have the best approach in that it had a continuous feedback performance loop both during and between each round; the team continuously tried to improve itself. It is difficult to gauge Team 4's improvement as only one member was thoroughly engaged in the game. However, Team 4 experienced the most conflict, which impacted its overall operations and performance.

F. Measuring Human Behavior

This paper discusses observations from a single course project where ECE students used the Grid Game. Furthermore, the primary purpose of the course project was to allow ECE students to understand grid operations and the need to defend against cyberattacks. Understanding human behavior was a secondary purpose of the study. As such, only a preliminary assessment of human behavior was possible through observations. Two basic ranking mechanisms were used to assess each of the above-mentioned human behaviors. Regarding performance, teams were ranked on a three-point scale of Poor (P), Average (A), and Good (G). Conflict and cooperation were ranked on a three-point scale of Low (L), Medium (M) and High (H). Thus, Team 3 ranked average (A) in terms of basic grid operations, poor (P) in terms of preparing for cyberattacks, responded poorly (P) to cyberattacks, exhibited poor (P) progress through the three rounds, and exhibited low (L) cooperation and low (L) conflict. The measurements for Teams 3, 4 and 7 using these two ranking mechanisms are summarized in Table 2 below:

Table II: Measuring Human Behavior of Defenders

Human Behavior Elements	T3	T4	T7
Basic Grid Operations	A	A	G
Cybersecurity Preparations	P	A	P
Response to Cybersecurity attacks	P	P	P
Cooperation/Cohesion	A	L	H
Conflict	L	H	L
Improvement Across Three Rounds	P	P	A

1: P: poor; A: average; G: good
2: L: low; M: medium; H: high

VII. Limitations and Possible Improvements

There were three categories of limitations (and corresponding improvements): grid game software, engineering, and methodology, each of which are discussed next.

A. Grid Game Software

There are numerous possibilities for improvements to the Grid Game. With respect to cybersecurity, two of these include (i) More realistic attack and defense mechanics and more realism to resources needed an system configuration and defense. (ii) Attacker interface needs to be constructed such that the Red Team members are not just omnipotent game masters but become players that must manage resources and risk to accomplish their nefarious aims. Additions would allow multi-player team to delineate primary responsibilitie between security and control of the system.

B. Engineering

Two main lessons can be learned on the engineering front. First, given that all teams struggled with the concepts of generator inertia and energy storage, it is imperative to focus more on these concepts prior to the game events in future iterations of the course. Second, the overall performance with regards to understanding grid security, maintaining operations when under attack, and implementing cybersecurity measures effectively was poor. As such, these aspects of grid security need to be further stressed in future offerings of this course. The Grid Game could be incorporated further and more hands-on simulated course projects could be done to improve student learning.

C. Methodology

This study had three main methodological limitations. First, the technical logging that is built into the current game were not available at the time. This would have helped understand student performance in general and over the course of the three rounds to see if there was any improvement in strategy. Second, the three rounds were condensed into a single 2.5 hour

class. These rounds should have been spread out over more classes, so that students became more well-versed with the software, which may impact their performance in the future. Furthermore, this would have allowed for richer interview and observation data. Third, better measurement of human behavior and its various components, such as basic operations, cybersecurity preparedness, cyberattack response, cooperation, conflict, and overall improvement, is essential. The ranking scheme identified here is a rudimentary assessment based on observations conducted in a compressed 2.5 hour class project. More research is needed and a metrics system that better captures the various components of human behavior needs to be developed.

VIII. Future Directions

While the Grid Game cyberattacks are not representative of actual breaches on the US power grid, it nonetheless allowed ECE students to play the role of simulated microgrid administrators and experience real time cyberattacks. The students had to concisely formulate and justify their decisions with regards to grid functionality and cybersecurity measures. In doing so, the students improved on their analytical ability, verbalized their thought process, and defended their decisions (even if on occasion they made errors).

Temple plans on repeating this exercise in future semesters and will work with INL to design specific cyberattack scenarios to better assess how students manage their grids. Temple is also working with INL to capture information on students' actions and decisions through technical logs, which will allow for a more thorough measurement of the student performance, evaluation of GridGame's current functionality, and improvements for both the game and course project.

While the author recognize the attack and defense mechanisms are superficial, the experience of adressing security while operating the system provides an appreciation for the connected facets of the system as a whole.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. 1446574 and Grant No. 1453040. Mr. McJunkin's thanks the Resilient Controls and Instrumentation Systems (ReCIS) and support of Idaho National Laboratory and Center for Advanced Energy Studies. The authors, also, thank Idaho Regional Optical Networks for providing servers for GridGame communication support.

References

[1] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," *in Proc. SoutheastCon,* Apr. 2015*,* pp. 1–6.

[2] J. Clerk Maxwell, *A Treatise on Electricity and Magnetism, 3rd ed.,* vol. 2. Oxford: Clarendon, 1892, pp.68–73. N. Mohan, Electric Power Systems: a First Course, John Wiley & Sons, 2012

[3] X. Chen, S. Li, J. Ma, and J. Li, "Quantitative Threat Assessment of Denial of Service Attacks on Service Availability", in *Proc. Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on, Jun. 2011*, pp. 220-224.

[4] A. Lipovsky and A. Cherepanov "BlackEnergy Trojan strikes again: Attacks Ukranian electric power industry*,"* Retrieved January 27, 2016. Online at http//www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry.

[5] T.R. McJunkin, C. Rieger, B.K. Johnson, et al, "Interdisciplinary Education through "Edu-tainment": Electric Grid Resilient Control Systems Course," in *2015 ASEE Annual Conference and Exposition*, Seattle, Washington, 2015.

[6] "Idaho Falls Power", *Wind-for-schools.caesenergy.org*, 2017. [Online]. Available:http://wind-for-schools.caesenergy.org/wind-for-schools/IF_Power.html. [Accessed: 22- May- 2017].

[7] "Grid Game Scoreboard", *Gridgame.ironforidaho.net*, 2017. [Online]. Available: http://gridgame.ironforidaho.net/scoreboard.php. [Accessed: 22- May- 2017].

[8] G. Manimaran , "Cyber-Physical System Security of Smart Grid," presentation at *NSF-ECEDHA Energy and Power Summer Program*, Georgia Tech, Atlanta, July 2011.

[9] Y. Liu, P. Ning , and M. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids," ACM Trans on Information and System Security, Vol. 14, May 2011.

[10] A. Teixeira G. Dan, H. Sandberg, and K. Johansson, "Cyber Security Study of a SCADA Energy Management System: Stealthy Deception Attacks on the State Estimator," in *IFAC World Congress*, Milan, Italy, 2011.

[11] S. Sridhar and G. Manimaran , "Data Integrity Attacks and their Impacts on SCADA Control System," *in IEEE Power and Energy Society General Meeting*, July 2010.

[12] R. Chabukswar, Y. Mo, and B. Sinopoli , "Detecting Data Integrity Attacks on SCADA Systems," in *18th IFAC World Congress*, Milano, Aug 2011.

[13] A. Giani , E. Bitar, M. Garcia, M. McQueen , P. Khargonekar, and K. Poola , "Smart Grid Data Integrity Attacks," IEEE Trans on Smart Grid, Vol. 1, pp. 1-11, 2012.

[14] B. Wingfield, B. . "Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months*,"* Retrieved November 28, 2012. Online at http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html

[15] McAfee. . "In the Crossfire: Critical Infrastructure in the Age of Cyber War" 2017. [Online]. Available: http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf. [Accessed: 22- May- 2017].

[16] R. Rantala. "Cybercrimes Against Businesses, 2005. Bureau of Justice Statistics," Retrieved February 19, 2009, from http://www.ojp.usdoj.gov/bjs/pub/pdf/cb05.pdf

[17] GAO (General Accounting Office).. *Critical Infrastructure Protection: Challenges in Securing Control Systems*. Retrieved March 20, 2010. Online at http://www.gao.gov/new.items/d04140t.pdf

[18] R. Nicholson. "Critical Infrastructure Cybersecurity: Survey Findings and Analysis," in *Energy Insights*, November 2008.

[19] Wall Street Journal, *"*U.S. Risks National Blackout From Small-Scale Attack", March 12, 2014.

[20] S. Baker, S. Waterman and G. Ivanov, *In the Cross re: Critical Infrastructure in the Age of Cyber War*, McAfee, Santa Clara, California, 2009.

[21] A. Rege, "Cybercrimes against critical infrastructures: A study of online criminal organizations and techniques," *Criminal Justice Studies*, vol. 22(3), pp. 261-271, 2009.

[22] Staff of Congressmen Edward J. Markey (D-MA) and Henry A. Waxman (D-CA), Electric Grid Vulnerability: Industry Responses Reveal Security Gaps, U.S. House of Representatives, Washington, DC, 2013.

[23] L. Tinnel, O. Saydjari and D. Farrell, "Cyberwar strategy and tactics: An analysis of cyber goals, strategies, tactics and techniques," in *Proceedings of the IEEE SMC Workshop on Information Assurance*, pp. 228-234, 2002.

[24] U.S. Government Accountability O ce, Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities and Remaining Challenges, Report No. GAO-05-327, Washington, DC, 2005.