1-1-2016

Multidisciplinary Game-Based Approach for Generating Student Enthusiasm for Addressing Critical Infrastructure Challenges

John F. Gardner
Boise State University

New Orleans JAZZED about Engineering Education

Paper ID #15948

Multidisciplinary Game-based Approach for Generating Student Enthusiasm for Addressing Critical Infrastructure Challenges

Mr. Timothy R McJunkin, Idaho National Laboratory

Timothy R. McJunkin is a Senior Research Engineer at Idaho National Laboratory in the Energy and Environment Science and Technology Division, since 1999. He has also served as an adjunct instructor at Idaho State University, teaching control systems and resilient controls systems. Prior to joining INL, he was a design engineer at Compaq Computer Corporation in Houston Texas. Mr. McJunkin is the principal architect of the Grid Game developed for the Resilient Control Systems class.

Dr. Craig G Rieger, Idaho National Laboratory

Craig Rieger, PhD, PE, is the Chief Control Systems Research Engineer at the Idaho National Laboratory (INL), pioneering multidisciplinary research in the area of next-generation resilient control systems.

In addition, he has organized and chaired eight Institute of Electrical and Electronics Engineers (IEEE) technically co-sponsored symposia and one National Science Foundation workshop in this new research area, and authored more than 40 peer-reviewed publications.

Craig received B.S. and M.S. degrees in Chemical Engineering from Montana State University in 1983 and 1985, respectively, and a PhD in Engineering and Applied Science from Idaho State University in 2008. Craig's PhD coursework and dissertation focused on measurements and control, with specific application to intelligent, supervisory ventilation controls for critical infrastructure.

Craig is a senior member of IEEE, and has 20 years of software and hardware design experience for process control system upgrades and new installations. Craig has also been a supervisor and technical lead for control systems engineering groups having design, configuration management, and security responsibilities for several INL nuclear facilities and various control system architectures.

Dr. Aunshul Rege, Temple University

Dr. Rege is an Assistant Professor with the Department of Criminal Justice at Temple University. Her main areas of research include critical infrastructure resilience and protection, cyber and cyber-physical security, infrastructure planning and policy, and global security and international affairs.

Dr. Saroj K Biswas, Temple University

Saroj Biswas is a Professor of Electrical and Computer Engineering at Temple University specializing in electrical machines and power systems, multimedia tutoring, and control and optimization of dynamic systems. He has been the principle investigator of a project for the development of an intelligent tutoring shell that allows instructors create their own web-based tutoring system. His current research focuses on security of cyber-physical systems based on multiagent framework with applications to the power grid, and the integration of an intelligent virtual laboratory environment in curriculum. He is an associate editor of Dynamics of Continuous, Discrete and Impulsive Systems: Series B, and is a member of IEEE, ASEE, and Sigma Xi.

Dr. Michael Haney, University of Idaho
Dr. Michael John Santora, University of Idaho

Dr. MIchael Santora is a Clinical Assistant Professor at University of Idaho since Fall of 2013. He has worked in industry as a R&D Controls Engineer creating OEM machinary. He specializes in controls, embedded systems and automation.

Dr. Brian K. Johnson, University of Idaho, Moscow

Brian K. Johnson received his Ph.D. in electrical engineering from the University of Wisconsin-Madison in 1992. Currently, he is a Professor and the Schweitzer Engineering Laboratories Chair in Power Engineering in the Department of Electrical and Computer Engineering at the University of Idaho (Moscow,

Idaho). His interests include power systems applications of power electronics, power systems protection and relaying, resilient operation of power systems, applied superconductivity, and power systems transients. Dr. Johnson is a registered professional engineer in the state of Idaho.

Dr. Ronald Laurids Boring
Dr. D. Subbaram Naidu P.E., University of Minnesota Duluth

Dr. D. Subbaram Naidu did his graduate (M.S. & Ph.D.) work in Electrical Engineering with an emphasis in Control Systems at the Indian Institute of Technology (IIT). Professor Naidu held various positions with IIT, the Guidance and Control Division at NASA Langley Research Center, Old Dominion University, the Center of Excellence for Control Theory at the United States Air Force Research Laboratory (AFRL), the Center of Excellence for Ships and Ocean Structures (CESOS), Measurement and Control Laboratory at Swiss Federal Institute of Technology, the Universities of Western (at Perth) and Southern (Adelaide) Australia, and East China Normal University. Professor Naidu was most recently with Idaho State University (ISU) during 1990-2014. Professor Naidu joined the University of Minnesota, Duluth on August 25, 2014 as Minnesota Power Jack Rowe Endowed Chair for Energy and Controls, and as Professor in Electrical Engineering.

Dr. John F. Gardner, Boise State University

Gardner is Director of the CAES Energy Efficiency Research Institute (CEERI) and professor of mechanical and biomedical engineering at Boise State University, where he has been a faculty member since 2000. Through CEERI he leads research, outreach, and educational efforts to promote the efficient and effective use of energy. He received his Bachelor's degree from Cleveland State University in 1981, and his M.S. and Ph.D. (all in Mechanical Engineering) from Ohio State in 1983 and 1987, respectively. He has published more than 60 peer-reviewed research papers, 2 textbooks and has been awarded 3 US Patents. He is a registered professional engineer in the state of Idaho and a Fellow of the American Society of Mechanical Engineers.

Multidisciplinary Game Based Approach for Generating Student Enthusiasm in Addressing Critical Infrastructure Challenges

Introduction

Building upon experiences from past course offering,[1] several universities across the United States (U.S) have incorporated a critical infrastructure educational game platform as a unifying platform to integrate different disciplines to a common goal. The critical infrastructure backbones of the world provide the delivery mechanisms for energy and other utilities that provide the lifestyle we have come to expect in our society. As these critical infrastructure systems have evolved, the complexity of their integration has generated numerous challenges as a side effect of increased automation that are more pronounced as the infrastructure ages. Although still a modern technological wonder, the power grid needs a workforce that understands the complex, interdependent facets of the current grid as it evolves to a smarter grid and is pushed closer to its limits through improvements in automated measurement and control. The next generation of technology developers and operators will require an interdisciplinary understanding to reliably and securely integrate advanced communication and control technologies into the infrastructure and create systems to address the new demands of increased renewable and distributed generation, complex markets, and resilience to damaging storms and cyber attacks. Educational institutions need to accept the challenge of weaving the great diversity of contributing disciplines into the common fabric which allows specialties to effectively work together.

To energize the multidisciplinary studies challenge, Idaho's public universities, the University of Minnesota-Duluth, Colorado State University and Temple University, in cooperation with U.S. Department of Energy's Idaho National Laboratory, developed undergraduate and graduate courses targeted at the critical infrastructure challenge using a game based approach. The Grid Game provides realistic and entertaining motivation in science, technology, engineering and mathematics, through inclusion of the physics of power systems, cyber-physical vulnerabilities, energy markets, and control systems. The game provides the mechanism for understanding the impact on stability of a small electric grid due to factors ranging from computer security, balanced growth of customer base and power generation assets, energy markets, and the balance of automation and human operator decisions. The human decision-making process of grid operators and cyber criminals supply a basis for the consideration of other social components including criminology studies. The methodology and outcomes of two sets of courses at the universities will be discussed in this paper.

Findings from a special topics course in resilient systems co-taught by Electrical and Computer Engineering, Mechanical Engineering, Computer Science professors and professionals in disciplines of control systems and cognitive psychology offered through University of Idaho, Idaho State University, and Boise State University will be discussed. The outcomes of mentor guided projects addressing resilience challenges in multi-agent decision controls, human factors, computer security, and power systems will be assessed. Projects range from notional resilience improvement to integration of distributed electric grid simulation to hardware in the loop.

One anticipated engagement assessment method was the percentage of students that continue projects beyond the one semester course is reported. Student projects were measured based on completeness of understanding of resilient control systems topics as applied to critical infrastructure. We will also discuss findings from an integrative grid game course project between the Electrical and Computer Engineering and Criminal Justice departments at Temple University. Specifically, we will share lessons learned in three areas: (i) approaches to promote discipline-specific student research capabilities and enhancing experiential learning, (ii) fusing social sciences and engineering to foster multidisciplinary experiential learning and gain a holistic approach about grid resilience, and (iii) using this multidisciplinary course project to further improve the Grid Game's functionality.

Course Methods/Design using the Grid Game

A course in Resilient Control Systems (ResCS) was taught for the third time as a special topics class jointly across multiple universities. And a likely "first of it's kind" joint class in Electrical and Computer Engineering and Criminal Justice was introduced at Temple University. The Grid Game, with the user interface shown in Figure 1, has been used as a device to add to both the interactive entertainment and experiential factors of the student experience in both of these classes. The game contains realistic simulation with a multifaceted interactive control interface of a microgrid. The Grid Game also includes a market for players to exchange energy to expand the game to multiple players by allowing cooperative and competitive strategies between the individual players or teams. Players are also allowed to choose to spend earned points to purchase resources to defend against or react to cyberattacks that can be administered by the game masters/Red Team. Additional details of the Grid Game have been previously reported at ASEE2015.[1]

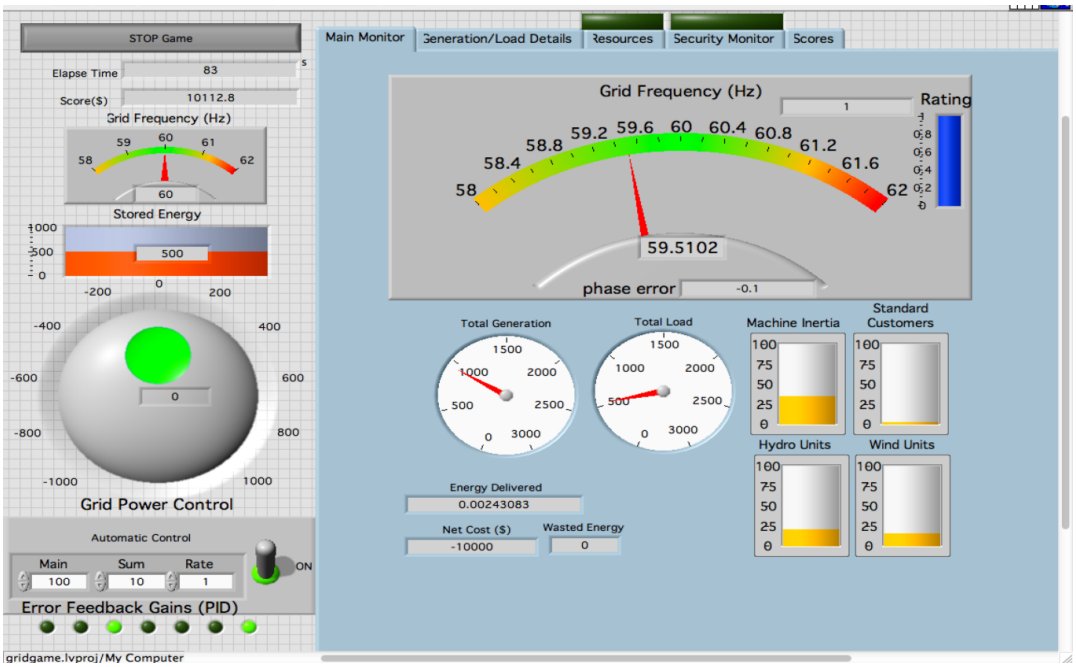

Figure 1. Grid Game Screen Capture: Main Screen

Resilient Control Systems (ResCS)

Resilient control systems is a relatively new research area used in the control of complex systems with interdependencies between control algorithms; human operators, stakeholders, and consumers; and computer systems and networks that connect the components. Critical infrastructures such as the electric grid are examples of such complex systems. The quality of design of a more resilient system is measured in terms of the reduction in the severity of the effects of a natural or manmade disturbance and the reduction in the time to recover to full performance of the system. The ResCS course was created to establish a perspective for college students on the unique challenges of automation in our society. This is the third consecutive year that the ResCS course has been taught and the second year that the GridGame was used as the focal point for the class. In 2015, students at two universities enrolled for credit in a special topics course.

The objective of the class were:

i. Establish a perspective for college students on the unique challenges of automation in our society.
ii. Provide insight on how a power control system works and how it can fail--including threats from cyber security, human error and complex interdependencies.
iii. Teach introduction to promising concepts that are being investigated to make these control systems more resilient to these threats.
iv. Leave students with the appreciation of the interdisciplinary nature of critical infrastructures and the beginning of skills required to converse in the "languages" of some of those disciplines.
v. Mentor students into projects that engage in the areas of ResCS as demonstrated through project papers and presentations.

The semester course was structured as a weekly lecture with subject experts from the universities and the national laboratory to provide introductions to resilience, power systems, control systems, cognitive psychology, and computer security. Additionally, interactive lectures were given specifically to discuss challenges in the disciplines that might lend themselves to class projects. Each university with enrolled students provided additional contact time with the students in different ways. One of the two provided weekly meetings focused on the project topic and coordination of the two person team. The other university provided a weekly meeting of the entire class to participate in game sessions and project idea discussions. Students also completed assignments associated with the topical areas in the lectures to solidify their understanding of the weekly lecture topics. The course concluded with mentor-guided projects that allowed students to creatively enhance resilience to a power grid by designing their own enhancements concepts to the Grid Game or through other methods of demonstrating the concepts of resilience. Grading of students emphasized comprehension and understanding of the introductory material to ResCS as demonstrated in the project concept description (30%), report(30%), and presentation(30%), with weekly assignments given a weight of the remaining 10 percent.

The first weeks of the course focused on introduction to ResCS and power systems to provide a basis for entry into the interdisciplinary domains of ResCS. The expectation for students was that

they had a technical background in mathematics and some coursework completed in engineering, computer science or cognitive psychology. A class session on the Grid Game architecture provided to background necessary to utilize the game as part of their projects.

The ResCS overview lecture for the class described the analysis, design, and implementation of resilient systems. The process includes implementing the design through the architectures and system components to achieve this result where disturbances caused by natural or malicious causes are adapted to mitigate or minimized in terms of magnitude and duration. ResCS holistically considers the benefits and possible problems with automation, including integrating humans into the loop in ways that increase resilience rather than increase brittleness. ResCS is designed with the understanding that anticipated and unanticipated disturbances will happen (e.g. components will fail or degrade, people will make mistakes, nature will intervene, and mischief makers will make their mischief).

Power systems were discussed to provide a basic overview of electric grid architecture, steady-state operation and dynamic response to events ranging from load changes to faults along with an overview of common simulation techniques were discussed at a level that provided introduction or review of basic concepts depending on the level and discipline emphasis of the students. The swing equation was derived and demonstrated through simple examples to illustrate one of the underlying aspects of the Grid Game. An exercise was assigned that provided the student an opportunity to consider what aspects of the game were realistic as compared to a real power system, and in this context, how grid stability is affected by different types of disturbance.

An overview of **control systems** and their application to the stability of critical infrastructure was given. Students were assessed based on basic understanding of the application to the electric grid, serving as a focal point for some projects. This lecture was structured to provide a basic review or introduction to control systems including history, types of control systems, overview of theory, and insights to the control of the electric grid considering the impact of energy storage and demand response, which are two areas the game explores. An assignment was given for students to consider and write short summaries on control system performance and means to correct to disturbance conditions. Additionally, students were provided with a lecture on the overview of industrial control systems, including the types of devices and programming environments used to implement distributed control systems (DCS) and supervisory control and data acquisition systems (SCADA). The types of architectures, human machine interfaces and diagnostic tools available in typical systems were discussed. Students were challenged to consider different types of control schemes that could be developed for a microgrid and the Grid Game. In particular, students were provided background on Multi-level agent control systems as a potentially powerful architecture for ResCS[2-3].

Class sessions on **cognitive psychology/human factors** focused on the impact that human operators have on critical infrastructure systems. The process of analysis, design and validation of human-machine interfaces was discussed. Initial analyses center on understanding the users and contexts of the system; design includes applying standards for usability and good visualization; and, validation entails assessing operator-in-the-loop performance to determine the optimal design. Simple simulations called microworlds[4-5] afford the opportunity to test users of a system cost effectively. By simplifying the process and controlling extraneous considerations,

microworld environments allow quick training to proficiency, thereby making it possible to test system human-interfaces with student/novice operators instead of experienced operators. Thus, microworlds provide the ideal platform for student based investigation of process control technologies. Microworlds, such as the Grid Game, provide a high degree of experimental control. Simple tools are accessible to students and affordably made available for training and academic research. Students were challenged with exploring improvements to the human engagement with systems with emphasis on maintaining the operator's situational awareness.[6] An assignment was given to summarize the topic through a short writeup of their perceptions of how degrees of automation allow for human interaction and the impact of human factors on overall system performance and usability.

With regards to the **cybersecurity** elements of grid management, students were given two primary assignments. The first involved becoming familiar with the North American Electricity Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards. After a lecture to provide an overview and brief synopsis of the standards promulgated by NERC and Federal Energy Regulatory Commission (FERC) for grid operators, students were assigned the task of navigating to the standards, selecting one of interest, and writing a summary of the standard's requirements. A second assignment required students to perform a greater level of critical thinking. They were asked to describe a scenario in which an attack on the electric grid takes place and the likely results of such an attack.

During the resilient controls course, one of two class days per week involved **laboratory sessions**. During the laboratory sessions, playing the Grid Game was highlighted. The first session was learning the game and then how to play interactively with other students. During the course the students learned the important concepts of the game, for instance, learning about power systems, controls, security and resilience. A session to learn the interactive aspect of the game was followed by competitive matches where students teams acted as Blue (i.e., design team to maintain resilience against disturbance) and Red i.e., (students creating disturbances) teams active. The participants consisted of on-campus University of Idaho students as well as distance students in several locations, with the farthest located in Philadelphia. The matches lasted 30 minutes. During the matches students were excited to learn how to play and increase their knowledge of having a resilient system to be the microgrid that increased their profits the most. After every game the top three micro grid contenders would describe to the rest of the class how they were able to make such a resilient and profitable microgrid compared to the rest, using their winning the round as a learning tool.

In some weeks the second contact day included recitation sessions where students discussed the concepts from the lecture session, with input from the local instructors to help them relate their previous course backgrounds to resilience control system. A few lab sessions were spent in the University of Idaho power systems lab where students were able to see commercial protection and control equipment operated on a scale model power system. In addition there were a few lab sessions where students learned to apply programmable logic controllers.

Finally, students were required to complete projects to further develop and demonstrate their understanding of the course material. The students were encouraged to incorporate the topics of ResCS into these projects. Projects could establish new concepts for the Grid Game or otherwise explore resilience through other means, such as using other simulation environments to develop

and test control system methods to improve resilience. These enhancements will either add additional realism in emulating the current grid, or improved human interaction and system operation. This paradigm enables students to understand how their skills can be used to address the real world challenges of complex systems design and operations (e.g. the power grid) that *require* coordination within an interdisciplinary team.

Electrical and Computer Engineering and Criminal Justice Joint Project Using Grid Game

The Electrical and Computer Engineering Department (ECE) and the Criminal Justice (CJ) Department at Temple University received an **NSF CPS** grant that focused on a multidisciplinary approach in better understanding power grid cybersecurity. Staying true to the theme of multidisciplinary work, the Temple University team worked in partnership with INL to create a joint course project on smart grid security. In the Fall 2015 semester, the Grid Game software was used for a class project in two upper division courses: *ECE4712: Modern Power System Engineering* in the Department of Electrical and Computer Engineering, and *CJ 4007: Computer Crime* in the Department of Criminal Justice, respectively. ECE4712 is similar to a standard upper-level course on power systems which is taught at most universities. In this course students learn power system modeling, simulation, dynamics and stability, and operational aspects of power systems. CJ 4007 is an upper-level Criminal Justice course that introduces students to an assortment of cybercrime, cybercriminal and cyberattack taxonomies. This course also focuses on critical infrastructure cybersecurity from a Criminological perspective.

The objective of using the Grid Game in this joint course project was to introduce real time security breach events on a simulated power grid, and expose human behavior component of cyberdefense.

The Grid Game exercise was scheduled in November and had 23 ECE students and 18 CJ students, who were assembled in a single classroom. The ECE students had already downloaded the Grid Game software on their laptop from the INL website. ECE students worked in groups of three to four, where they played the role of electric utility administrators responsible for managing consumer loads minute by minute while trading 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 INL engineers and Temple ECE graduate students played the role of cyberattackers. CJ students worked in groups of two to three. The CJ students observed and interviewed ECE students' decision-making with regards to security, group dynamics and divisions of labor. The exercise lasted for 2.5 hours and was divided into three rounds of 30 minutes each. At the end of each round, students could restart the Grid Game and start afresh. Thus, Round 1 served as warm-up, and during Rounds 2 & 3 both ECE and CJ students were more comfortable with their respective tasks.

The ECE class was a project based course on Power Systems. Students were required to do four projects during the semester for a total of 60% weight on the final grade, (and the remaining 40% on exams). Thus the GridGame project accounts for 15% of the students' final grade. The CJ course was a project based course that introduced Criminal Justice students to cybercrime and cybersecurity. Students were required to do this hands on project during the semester for a total of 50% of the final grade.

Results/Outcomes

The following are results and observations in regards to the two sets of classes using the Grid Game as a device to contribute to and motivate learning in interdisciplinary courses.

ResCS Course Outcomes

The ResCS course has in the past attracted a mixture of undergraduate and graduate engineering and computer science students. This year the student body was made up of 15 graduate level ECE, 1 control systems graduate student and 1 auditing cognitive psychology doctoral student. In addition, an architecture student began the course but stopped attending part way through the semester. The 16 students enrolled for credit divided into ten project teams. One course goal was to obtain a mixture of disciplines in the course. In that metric, the promotion of the course in areas outside of ECE can improve. The engagement of the one doctoral student in human factors was of particular benefit to the interdisciplinary discourse as the student provided one of the lectures and engaged with the other students in discussions after the lecture. The success in engaging students to tackle the cognitive psychology topic is quantified in the number of students addressing human factors in their projects, that is, two student team projects applied course subject matter in human factors in depth and three others considered the human in the loop in their concept. The topic of human factors is arguably furthest separated from the typical engineering course work, making this result noteworthy and is directly attributed to the participation of the cognitive science student.

The lack of class members with course work emphasis or background in computer security was evident from the lack of a project selected with depth in cybersecurity. Six of the projects did mention cybersecurity but only one did so in any amount of depth. Other observations come from the earlier mentioned assignments in cyber security. For the first class assignment in cybersecurity, students selected a wide range of different standards to summarize, showing a varied interest in what is required of grid operators for cybersecurity. Overall, completed assignments showed a respectable level of comprehension. However, on the second assignment, students achieved a lower-than-expected outcome in determining the possible vulnerabilities and possible adverse results of those vulnerabilities. Many were able to cite papers or publications that discussed the potential threat to various electric grid elements, but at a very abstract level. However, few showed the expected level of creativity in describing how grid operators may be duped, components may be compromised, etc. This assignment followed a lecture providing an overview of cybersecurity issues and common threats. However, it is likely that the students of this class did not have the prior knowledge or exposure to the subject matter the instructor expected. In future incarnations of the course, greater guidance and instruction, as well as example "plots" (e.g. targeted phishing attacks, distributed denial of service) will be given during the lecture period(s).

Other areas showed successes as well across the breadth of the ResCS topic areas. Fully functional prototypes either in additions to the Grid Game, real time data simulators, micro-controllers, etc. were completed in over half of the projects. Given only several weeks at the end of the semester to focus on projects, this is considered a notable result. Most projects

Table I. A summary of student project accomplishments out of ten projects Full/Partial/Low mastery of expected outcomes.

Fully Satisfied	Partially Satisfied	Not Satisfied	Expected Outcome
10	0	0	Complete Development of Concept
6	4	0	Implemented Prototype
9	1	0	Conveyed Knowledge of Critical Infrastructure
0	5	5	Considered Cyber Security
2	3	5	Considered Human Factors
5	4	1	Included Other Resilient Concept in Depth
5	5	0	Clearly Conveyed Project in Presentation
7	3	0	Clearly Described Project in Paper

conveyed an understanding of electric grid or other critical infrastructure. For example, one project topic was advanced protection (i.e., algorithms and hardware necessary to disconnect portions of the grid from that are experiencing problems). This project demonstrated an advanced algorithm to increase reliability and robustness. The project lacked a holistic resilient approach that considered cybersecurity or human grid interaction, but showed promise as an architecture that could include those. A summary of the assessments of the student projects with respect to topics covered in the class is shown in Table I.

As a general observation from the ResCS course, laboratory sessions engaging the students with game play was made: “The students were very receptive to learning with the Grid Game and teaching each other what they have learned.” Three project teams have inquired about possibility of continuing the project. One student will participate in a related internship at INL in the summer of 2016.

Students from the most recent offering of the class were surveyed through standard course evaluations at the University of Idaho and an additional course survey. The course evaluation was completed by 10 of 15 students. The course and the instructors were rated on a 0 to 4 scale with 4 as the most favorable rating. The survey included a ranking of the value to career or academic pursuits, perceived difficulty, enjoyment of the class and opportunity to comment on the relevancy of the course to their field. Two students from 2014 completed the survey and 4 from 2015. Students provided values of 0 (least favorable) to 5 (most favorable) on the questions of value, difficulty, and enjoyment. Results of the numeric ratings are given in Table II.

Four students provided written comments on the course evaluation. All respondents to the survey provided written comments. Comments ranged from enthusiastic on the diversity and ability of the topics to hold the students attention for the 75 minute class period to concerns on the effectiveness of the teleconference delivery method. The students for the most part enjoyed the variety of instructors and game play. One student commented that more time on the attack aspects of the game was needed. Multiple students suggested more coverage of National Instrument’s LabView language would have allowed projects to go further towards implementation.

Table II. Numerical ratings provided by ResCS students through course survey and course evaluations.

Year	Metric	Course Survey 0 to 5			Course Evaluation 0 to 4	
		Value	Difficulty	Enjoyable	Course Rating	Instructor Rating
2015	Mean	3.75	2.375	4.25	3.8	3.6
	Range	3 to 5	1 to 3.5	4 to 5	3 to 4	2 to 4
2014	Mean	3	1.25	3.25	N/A	N/A
	Range	3	1 to 1.5	3 to 3.5	N/A	N/A

An additional positive outcome to the ResCS course is the acceptance of concepts from this course into a new course titled, Grid: Resiliency, Efficiency and Technology at University of Minnesota Duluth (UMD) first taught in Spring 2016.

ECE/CJ Course Outcomes

The joint exercises at Temple University focused on the nexus of *multidisciplinary* experiential learning in power grid cybersecurity. Experiential learning is defined as learning through action, experience, and discovery and exploration.[7] This joint ECE/CJ exercise offered valuable experiential learning experiences for both students in two important ways:

1. Discipline-Specific Experiential Learning

ECE students experienced the impacts of real time cyberattacks on the power grid, from stability of the grid to power quality evaluation to power market. ECE students were asked to share their thought process as they made engineering decisions along the way. Students were asked to write their project on few broad areas:

i. Microgrid stability in the event of a cyberattack: Here stability of the generator should be discussed using swing equation under various scenarios due to cyberattack, such as loss of a generator, loss of the generator controller, remedial actions of stabilizing the grid.
ii. Grid security: Here students were asked to discuss their experience of an attack, and defense actions following the attack. Students were also asked to write why they had chosen the particular defense actions.
iii. Generator control system: In this part students were asked to discuss the effects of a proportional-integral-derivative (PID) controller in the generator control loop, and how they reconfigured the controller on the fly in the event of a cyberattack.
iv. Energy source: In this part students were asked to discuss 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. Students considered hydro, conventional fossil, and wind generators as their energy source.

v. Energy storage: Students had the option to purchase battery storage as one of the ways of maintaining stability of the grid, and were asked to discuss effects of energy storage, if any, on stability in the event of a loss of generator due to an attack.

vi. Energy trading: In this part, students looked into how cyberattacks impacted their microgrid business.

CJ students got a snapshot of what cyberattacks against power grids might look like and an intuitive experience of attackers and defenders 'in action'. CJ students observed ECE students' decision-making with regards to security (purchasing defenses such as firewalls, antiviruses, tuning generation control gains, etc), group dynamics and division of labor. Collectively, these experiences simply cannot be obtained by reading about cyberattacks through traditional coursework.[7] Furthermore, CJ students could improve their hands-on research skills by conducting interviews and observations. Students were asked to write their reports on the following areas:

i. Team dynamics: This component examined how ECE students, who played the role of power grid administrators, worked in groups. It addressed any divisions of labor with regards to maintaining grid operations, decisions on purchasing cybersecurity products, and any conflicts between members (and how these were resolved).

ii. Team strategy: This component examined whether ECE students had a particular strategy to ensure they were successful at maintaining their microgrids, generating revenue, and successfully fending off (or minimizing the impact of) cyberattacks.

iii. Team preparedness: This aspect focused on whether ECE students were prepared, knew the various elements of the Grid Game, and understood what different cyberattacks did to their systems.

iv. Methodological issues: This section asked CJ students how they felt about doing hands-on research, any difficulties they experienced in observing and interviewing ECE students, and also reflections on what they could have asked or observed.

2. Multidisciplinary Experiential Learning

ECE students and CJ students rarely get to work on joint course projects. In fact, to the best of our knowledge, we are not aware of these two disciplines working together in the context of educational settings. Here, ECE and CJ students worked together in two ways. First, once the CJ students designed the interview questions, they practiced these questions on ECE graduate students to become more familiar with how the grid worked, whether their questions made sense, and used any feedback to revise their question set. Second, during the joint exercise, CJ and ECE students had conversations about strategies for securing the grid and maintaining operations. CJ students understood the ECE (plant operator) mindset; ECE students had to concisely formulate and justify their decisions with regards to grid functionality and cybersecurity measures. In doing so, ECE students improved on their analytical ability, verbalized their thought process, and defended their decisions (even if on occasion they made errors).

Thus, the joint exercise had multiple benefits, such as breaking down disciplinary stereotypes and barriers, fostering dialog across ECE and CJ disciplines, and ultimately understanding and appreciating that cybercrime and cybersecurity could (and should) be researched via multiple

lenses. Thus, this exercise encouraged multidisciplinary dialog between the two groups of students, which is reflective of the real world where joint approaches to infrastructure security are needed.

Conclusions/Future Plans

Conclusions

The instructors for both the ResCon and ECE/CJ courses have drawn conclusions with some common themes. The Grid Game was shown to be device with high utility in exploring many disciplines in an intuitive manner while providing the students with opportunities to expand and improved concepts of resilient controls through the game.

ResCS: As in past years, the students indicated that they enjoyed the class as a unique opportunity to look at systems with a holistic perspective. The game play added to the enjoyment and enthusiasm of the students. The course projects once again add to the list of interesting concepts that would make good additions to the current game platform. Unfortunately, the compactness of a study of the large area of ResCS into one semester did not leave sufficient time for full implementation. Several teams have expressed interest in continuing the development of their concepts with one student accepting an internship on a related project at INL. Student feedback has been sought and in general supports the conclusion that the course has value but can be improved through continued improvement in connecting the interdisciplinary topics and the possible creation of a reference textbook to formalize the curriculum. Though the diversity of the subject areas is challenging to the students, in general the students classified the course as easy, suggesting the that level of rigor could be increased somewhat without losing engagement of the class.

ECE/CJ: While the Grid Game cyberattacks are not representative of actual cybersecurity breaches on the US power grid, it nonetheless allowed ECE students to play the role of administrator of electric utilities of a simulated microgrid, provided an opportunity for both ECE and CJ students to experience in real time of what might happen in a real life cyberattack on the power grid, and allowed CJ students to do hands-on research in an otherwise technically dominated area of cybersecurity. Thus, this joint Grid Game exercise at Temple University promoted multidisciplinary experiential learning, innovative research, dismantled disciplinary boundaries, and enhanced student experiences.

Future Plans

The ECE and CJ students are repeating this joint exercise in the Spring 2016 semester and will work with INL to design specific cyberattack scenarios to better assess how ECE students manage their grids and how this might impact CJ students' interview and observation tactics. Temple University is also working with INL to capture information on ECE students' performance through technical logs, which will allow for a more thorough measurement of ECE student performance, evaluation of Grid Game's current functionality, and improvements in terms of the software program and joint project.

In the RecCS course, a better mix of student disciplines is desired. Future iterations of the class will focus on this. The ResCS instructors plan to attempt to augment the participation from the

disciplines outside ECE by incorporating short modules in core classes of the subject areas of human factors, cybersecurity, and other relevant disciplines to introduce the concept or ResCS and encourage participation in the ResCS course. To provide more in depth exploration and completeness of projects the ResCS course will have an optional second semester structured as an undergraduate capstone or graduate thesis support to encourage completion of concepts into implemented designs. The team seeks to disseminate the successes of the course and the Grid Game to other universities and continue to encourage related disciplines at universities to participate in this interdisciplinary endeavor.

Both the ResCS and ECE/CJ courses have identified the Red Team aspect of the Grid Game as in need of improvement to reduce the omnipotence of the game master making a more realistic attack frequency with potential for the Red Team to be "caught" or otherwise temporarily thwarted. As future work, the Grid Game will be augmented with a "Red Team" interface to program capabilities for cyberattacks to affect opponents' grid operations. These attacks will be available based on a point system in which attackers solve puzzles or implement various system attacks, requiring additional time and ingenuity to carry out.

Acknowledgement

Research of Saroj Biswas and Aunshul Rege was supported in part by the National Science Foundation under grant CNS-1446574. Research of Aunshul Rege was also partially supported by NSF CAREER grant CNS-1453040.

This effort performed as an outreach of the Resilient Controls and Instrumentation Systems (ReCIS) research team at Idaho National Laboratory and Center for Advanced Energy Studies.

The authors thank Idaho Regional Optical Networks for providing servers for Grid Game communication support as well as the Canvas website to support online materials for the Resilient Control Systems course.

References

1. T.R. McJunkin, C. Rieger, B.K. Johnson, et al, "Interdisciplinary Education through "Edu-tainment": Electric Grid Resilient Control Systems Course," 2015 ASEE Annual Conference and Exposition, Seattle, Washington, 2015.
2. C. G. Rieger, K. L. Moore, and T. L. Baldwin, "Resilient control systems: A multi-agent dynamic systems perspective," *IEEE International Conference on Electro-Information Technology , EIT 2013*, 2013.
3. A. Bidram, F. L. Lewis, and A. Davoudi, "Distributed Control Systems for Small-Scale Power Networks: Using Multiagent Cooperative Control Theory," *IEEE Control Systems IEEE Control Syst.*, vol. 34, no. 6, pp. 56–77, 2014.
4. Dyre, B. P., Adamic, E. J., Werner, S., Lew, R., Gertman, D. I., & Boring, R. L. (2013, September). A Microworld Simulator for Process Control Research and Training. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Vol. 57, No. 1, pp. 1367-1371.

5. Boring, R. L. , Kelly, D. , Smidts, C. , Mosleh, A. & Dyre, B.P. (2012) . Microworlds, simulators, and simulation: Framework for a benchmark of human reliability data sources. In R. Virolainen ed., Proceedings of International Joint Conference PSAM'11/ESREL'12
6. K. L. L. Blanc and J. H. Oxstrand, "Initiators and Triggering Conditions for Adaptive Automation in Advanced Small Modular Reactors," *ASME 2014 Small Modular Reactors Symposium*, 2014.
7. Rege, A. (2015). Multidisciplinary Experiential Learning for Holistic Cybersecurity Education, Research and Evaluation. Proceedings of the 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education. (3GSE 15).