IGEM17-001

Security Management of Cyber Physical Control Systems
July 1, 2018 thru December 31, 2018
Final Mid-Year Report

University of Idaho
College of Engineering

Higher Education Research Council
Idaho Global Entrepreneurial Mission Program
Mid-Year Report

Grant Number IGEM17-001

Security Management of Cyber Physical Control Systems

January 15, 2019
The third and final mid-year report of a three-year project, July 2016-June 2019

University of Idaho, College of Engineering

Project Director and PI: Larry Stauffer, Dean

Co-PI's: Fredrick Sheldon, Professor, Computer Science
Brian Johnson, SEL Endowed Chair, Electrical & Computer Engineering
Michael Haney, Assistant Professor, Computer Science
Daniel Conte de Leon, Assistant Professor, Computer Science

Executive Summary

Cyber-attacks and intrusions are nearly impossible to reliably prevent given the openness of today's networks and the growing sophistication of advanced threats. Knowing the vulnerabilities is not adequate, as the evolving threat is advancing faster than traditional cyber solutions can counteract. Accordingly, the practice of cyber security should focus on ensuring that intrusion and compromise do not result in business damage or loss through more resilient solutions. We are creating a platform to facilitate and build complementary and multidisciplinary R&D capabilities to address these pressing problems. Our platform will incubate innovative products and services for safeguarding cyber physical control systems (CPCSs) that are ubiquitous and underpin key sectors of our economy. Early participation of industry will aid in vetting promising technologies. Better methods for assessment combined with more resilient systems design will safeguard against potentially immense economic impact currently being faced by Idahoan stakeholders.

Idaho SBOE Contact:

Cathleen McHugh, PhD
Chief Research Officer
cathleen.mchugh@osbe.idaho.gov
Tel: (208) 332-1572

1 Summary of Project Accomplishments and Plans

This report presents the activities, accomplishments, and current status of the project titled "Security Management of Cyber Physical Control Systems." They are presented under the *four objectives* listed in our original project plan. We are mid-way through the third and final year (July 1, 2018 - December 31, 2018) of this three-year project.

1.1 Objective 1: Strengthen our capacity by adding key faculty and enhancing laboratories

In this third year of the project we have been able to add two new faculty members to the two we hired in year one. The hiring took longer than originally planned due to a very competitive job market for cyber security faculty. We have made substantial progress especially on deploying the new video technology infrastructure, continued laboratory enhancement projects, additional industry collaborations, producing research results, and planning for the post-grant period. A summary is as follows:

1.1.1 Faculty Searches

Our work plan called for the hiring of four faculty members to work in the area of cyber physical systems, two in electrical engineering and two in computer science. We planned to hire three in year one and one in year two of the project. We had a failed search for one of the positions last year but now all four positions are filled.

Our first hire was Yacine Chakhchoukh, a new assistant professor in Electrical and Computer Engineering is an expert in signal processing with experience in power systems cyber security operations. He earned a PhD in 2010 from Paris-Sud XI University/Superior School of Electricity, Supélec (Paris, France) with highest honors. Prior to joining the UI he was an assistant professor at the Tokyo Institute of Technology. He is located in Moscow.

Our second hire was Dakota Roberson. Dr. Roberson earned a PhD in Electrical Engineering from the University of Wyoming in 2017. During his studies, he was also a half-time intern for Sandia National Laboratories. Being located in our program in Idaho Falls is an excellent fit for his national laboratory background and is already helping us in our work with the Idaho National Laboratory. His area of expertise is in wide-area damping control to impact the effects of asymmetric time delay in geographically disparate locations, impact on coupling due to sensor/output collocation issues and forced oscillations in the wide-area damping control environment. These situations matter because grid operators consider all these limitations as they develop control systems to be implemented in their jurisdiction. However, sensor/output collocation disparities may limit their ability to ever implement the control.

As a result of a national search we made our third hire for the project, Jia Song. Dr. Song's research focuses on cybersecurity, high assurance computing systems, and security policy design. She was a member of team CSDS, for the DARPA Cyber Grand Challenge, an international competition in automated binary vulnerability analysis and repair. Building all the tools from scratch, the team was able to qualify as one of the seven finalist teams for the August 2016 competition. As security is a concern in many different areas, Dr. Song is collaborating with researchers in other fields, such as cyber physical systems, and sociology, to provide her knowledge of cybersecurity into multidisciplinary research. She is supporting an NSF research project on securing smart power grids under data measurement cyber threats. Dr. Song was also involved in an NSA project to develop a collection of cybersecurity learning modules which include teaching materials and student laboratory exercises. This curriculum is being shared among universities and government agencies to provide education on cybersecurity.

Continuing last year's failed search, we have recently hired Constantinos Kolias for Computer Science in Idaho Falls. Dr. Kolias was most recently an Assistant Research Professor in the CS Department at George Mason University in Virginia, which he joined in 2014. His main research interest revolves around security and privacy for the Internet of Things (IoT). He is also active in the design of intelligent Intrusion Detection Systems (IDS) with a special interest in privacy preserving distributed IDS. In 2015 he created and released the first wireless dataset specifically intended for research in

wireless security, namely the AWID dataset. Today AWID has been downloaded and used as a benchmark by hundreds of organizations and universities. Currently, he is developing non-intrusive, remote malware detection tools and techniques for IoT systems, based on involuntary side-channel emanations (e.g., electromagnetic emissions from the CPU and power consumption of the device) and is investigating the applicability of blockchain-based authentication methods in the IoT realm.

1.1.2 Graduate Students

Four graduate students worked as research assistants under the project: Ananth A. Jillepalli, Ibukun Oyewumi, Andrew Miles, and Maadhavi Sathu. We briefly describe the research work performed by each of these students below. Subsections 1.3.3 and 1.3.4 list the publications that have resulted from the research performed by these graduate students and faculty in the project.

1. Graduate student Ananth Jillepalli is pursuing a doctorate in Computer Science. Jillepalli is completing the development of the High-level and Extensible System for Training and Infrastructure risk Assessment (HESTIA) for Cyber-Physical Control Systems (CPCS). Identifying vulnerabilities in a critical infrastructure can be challenging without a high-level security policy specification. Yet knowing the security policy specification is not enough to eliminate vulnerabilities. Knowledge of possible attacks and respective defense measures are also needed to secure critical infrastructure. HESTIA is a holistic systems and behavioral modeling process and tool-set. A primary approach of HESTIA is to enable Cyber-physical Control System (CPS) engineers to model their system, behaviors, and security capabilities, or lack thereof, using an adversarial-based approach. The goal of HESTIA is enabling scalable and incremental system modeling for cybersecurity risk assessment and optimal system and device hardening strategy determination.

2. Graduate student Ibukun Oyewumi is pursuing a Master's degree in Computer Science. He is co-advised by Yacine Chakhchoukh and Daniel Conte de Leon. During the Fall 2018 semester Oyewumi worked on the design and development of the control system and cyber portions of the Power Laboratory component of the ISAAC ICS Testbed and also the network interconnection between the ICS Testbed laboratories.

3. Graduate student Andrew Miles is pursuing a Doctorate in Electrical Engineering. Miles is working on research toward the implementation of robust state estimators for power systems this past semester. Robust estimators provide resistance against cyber-attacks. He began the semester by continuing his education on data analytics and estimation theory. He has also worked in parallel in software programs such as MATLAB and Python to test new algorithms. The new algorithms learned (GM/MM/S/Tau) estimators are being further implemented in a power system software OpenDSS to show feasibility studies for real world applications. The power systems Lab equipped with the RTDS is very useful for the real-time evaluation of the developed algorithms.

4. Graduate student Maadhavi Sathu is pursuing a Master's degree in Electrical Engineering. Sathu is working on a Power Swing Blocking Scheme for Power System Disturbances with the Integration of Renewables. Power systems operate close to their nominal frequency under steady state conditions. During the power system disturbances like faults, line switching, loss of load, generator disconnection results in sudden change to electrical power, whereas the input mechanical power to generator remains constant. These disturbances cause oscillations in machine rotor angles which results in severe power flow swings. Based on the severity of the power system disturbance, system can remain stable and return to equilibrium state which is referred as stable power swing, on the other hand if there are severe system disturbances there will be a large separation of generator rotor angles, large power swings, large fluctuations of voltage and currents and results in loss of synchronization between generators which is referred as unstable power swing. Large power swings either stable or unstable causes unwanted relay operations at different locations which can cause major power outages or power blackouts. In modern digital relays, power swing blocking (PSB) function is available in distance relays to prevent unwanted distance relay element operation during power swings by differentiating between faults and power swings. Most PSB elements are based on traditional methods which monitors the rate of change of positive sequence impedance such as Conventional Blinder Schemes. The required settings for PSB scheme are difficult to calculate in many applications, particularly those where fast swings can be expected. One such application is integration of renewables such as Wind Generation, Photo-Voltaic Generation with the existing power system models where fast swings are expected which can't be detected with the existing methods. A new method has to be developed in order to detect the fast swings which could prevent unwanted relay operation. Application of these methods will be demonstrated using power system modeled on a Real Time Digital Simulator (RTDS).

1.1.3 Laboratory Enhancements

In our proposal we projected to enhance equipment and make capability and facility improvements. In the original proposal we planned to use the existing space dedicated to the Power Laboratory (PowerLab) and just enhance the equipment in it. But we took advantage of an opportunity presented by the Murdock Foundation to invest an additional $285,000 of their funding plus an additional $200,000 of other funding invested in Coeur d'Alene to create a distributed Industrial Control Systems (ICS) Testbed with locations in Moscow, Idaho Falls, and Coeur d'Alene. Below we briefly describe the purpose and the progress on designing, installing, or upgrading each of the components of the ICS Testbed.

The Testbed will enable research and development of novel and secure techniques and algorithms for securing today and tomorrow's Power Grid (PG) along with other types of Industrial Control Systems (ICS). Its major advantage is that it will enable researchers and engineers to perform and collaborate on ICS-specific cybersecurity research, development, and testing on a system that closely resembles current distributed critical infrastructure cyber-physical control systems. It will expose hardware-in-the-loop simulation, enable the capture and use of real operational data, integrate current and future components of the power grid and other industrial control systems, and enable realistic attack-defend scenarios for research, evaluation, and testing. The Testbed includes a Real Time Digital Simulator (RTDS) for enhanced power system transmission and distribution system simulation capabilities. We are evaluating options for making the Testbed available from non-UI locations such as BSU. This capability will significantly enhance our ability to demonstrate (in-situ) advanced Power Grid and Industrial Control Systems cybersecurity technology to Idaho industry partners.

The Testbed is planned to connect the following five laboratories to create a distributed cybersecurity control systems and smart grid testbed unique in the Northwest.

A: The Power Laboratory in Moscow, Idaho.

B: The RADICL-Moscow Cybersecurity laboratory in Moscow, Idaho.

C: The SCANVILLE Analytics and Visualization Laboratory in Moscow, Idaho.

D: The RADICL-Idaho Falls Cybersecurity laboratory in Idaho Falls, Idaho.

E: The Industrial Control Laboratory in Coeur d'Alene, Idaho.

Enhancements to laboratories A, B, and C are well under way and will be completed soon. Equipment for the laboratories in Coeur d'Alene and Idaho Falls will be installed in February 2019.

A: ICS Testbed: PowerLab

The most significant accomplishment with respect to laboratory enhancements is the expansion of the Power Applications Laboratory (PowerLab) in Moscow. This laboratory underwent a major expansion from about 1,500 sq.ft. to 2,200 sq.ft. (Figure 1). The increased scope and capability of this change has come with a cost, in that the enhancements have taken about a year longer than we originally anticipated. However, this is a justified price to pay for the benefit we are gaining.

The space for the PowerLab section of the ICS Testbed was remodeled and completed the end of November, two months behind schedule because of asbestos abatement in the new space. We have worked with the Schweitzer Engineering Laboratory (SEL) Engineering Services Division to design this portion of the ICS Testbed for performing research on cybersecurity of power and industrial control systems. A contract was given to Schweitzer Engineering Laboratories for the industrial control equipment and RTDS upgrade. The equipment started to arrive in December 2018, as shown in Figure 2. The existing RTDS and associated amplifiers were moved to the PowerLab and test equipment was connected to the RTDS as shown in Figures 3-6. The upgraded RTDS equipment is shown in Figure 7, with the new RTDS NovaCor rack at the left. The existing rack was supplemented with additional processor cards donated by Schweitzer Engineering Laboratories.

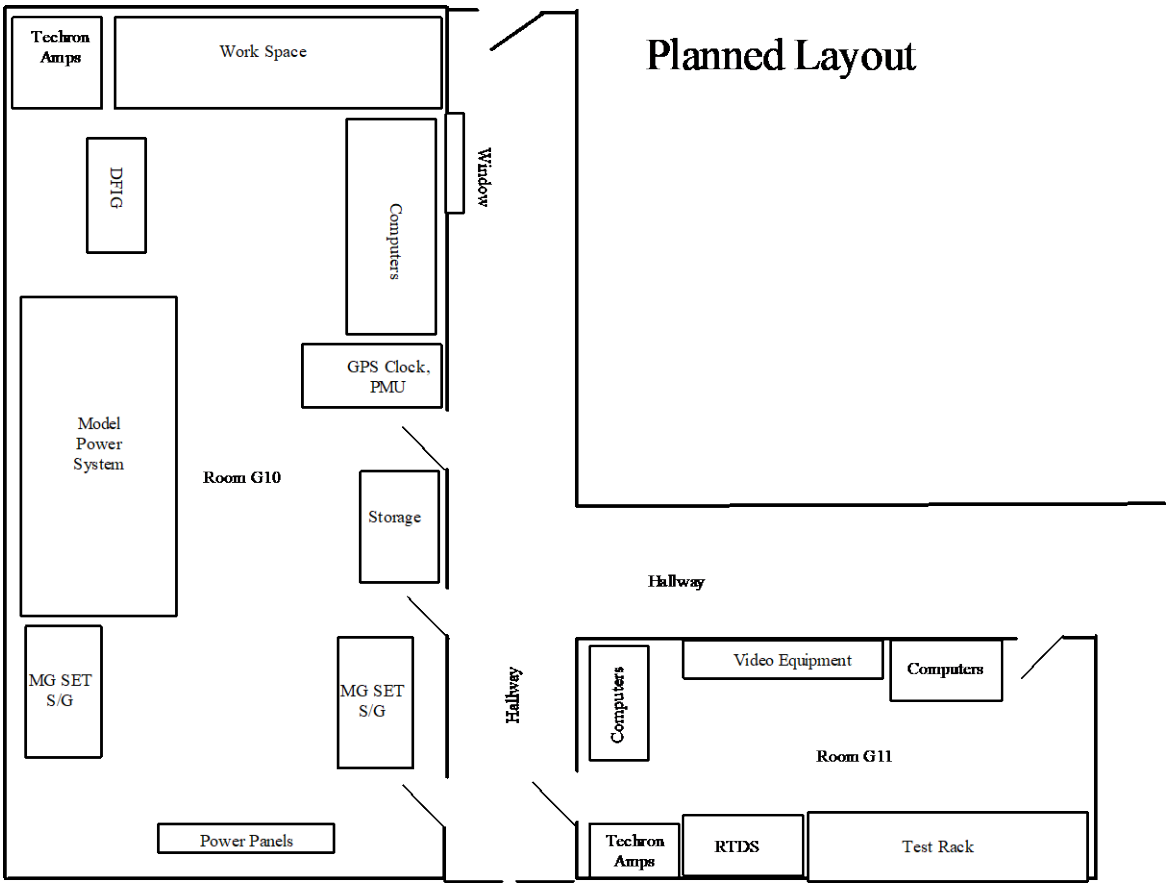

Figure 1: Illustration of the Power Systems Laboratory (PowerLab) Expansion.

Figure 2: Amplifiers moved and installed in the new PowerLab space.

Figure 3: Some of the test equipment for the expanded PowerLab along with new equipment racks.

Figure 4: Some of the test equipment for the expanded PowerLab along with new equipment racks.

Figure 5: RTDS, some of the test equipment racks and power amplifiers in the remodeled PowerLab space

Figure 6: Some of the test equipment for the expanded PowerLab along with new equipment racks (each rack will simulate a complete power substation's control).

Figure 7: PowerLab Component of the ICS Testbed with the addition of the new RTDS NovaCor rack (to the left).

B: ICS Testbed: RADICL Cybersecurity Lab:

The RADICL cybersecurity laboratory is the Reconfigurable Attack-Defend research and Instructional Computing Laboratory. This laboratory enables students and researchers to perform cybersecurity experiments in a controlled and isolated environment. Under the planned laboratory enhancements, we are enhancing the cybersecurity, computing, and analysis capabilities of this laboratory and integrating them into the ISAAC industrial control systems cybersecurity testbed.

Figure 8: Students working in the RADICL Cybersecurity laboratory before its renovation under this project.

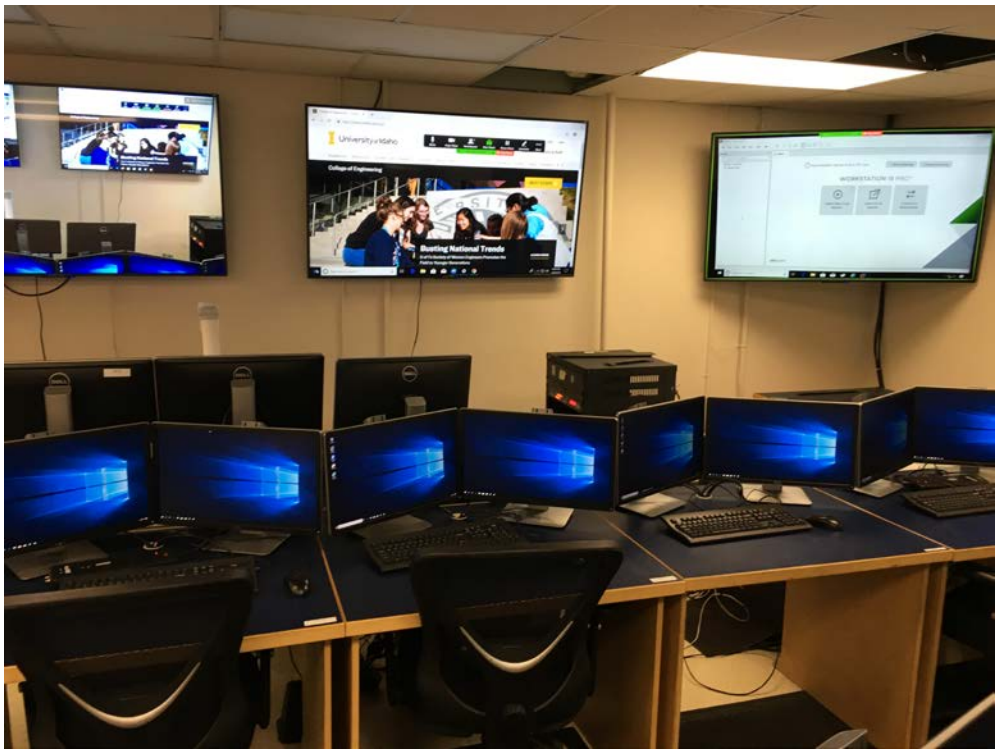

Figure 9: The RADICL Cybersecurity laboratory after its renovation during the Fall of 2018.

C: ICS Testbed: SCANVILLE Lab:

SCANVILLE: Securing Cyberphysical systems ANalytics, Visualization, IoT, and machine Learning Laboratory of Enquiry - A new component if the ICS Testbed.

This laboratory will be used to perform research on the architecture, design, implementation, and evaluation of systems for improving the cybersecurity of cyber-physical control systems, information technology (IT) and operational technology (OT) network and software systems, and Internet of Things (IoT) systems. This research includes, among other related activities, the architecture, design, implementation, testing and evaluation of software and combined hardware and software systems for analysis, machine learning, visualization, intrusion detection and avoidance, integration and testing including attack-defend scenarios, of networked digital systems with the purpose of improving the cybersecurity of said or related systems. This laboratory will also be connected to the Idaho Cybersecurity testbed through a dedicated high-speed fiber network.

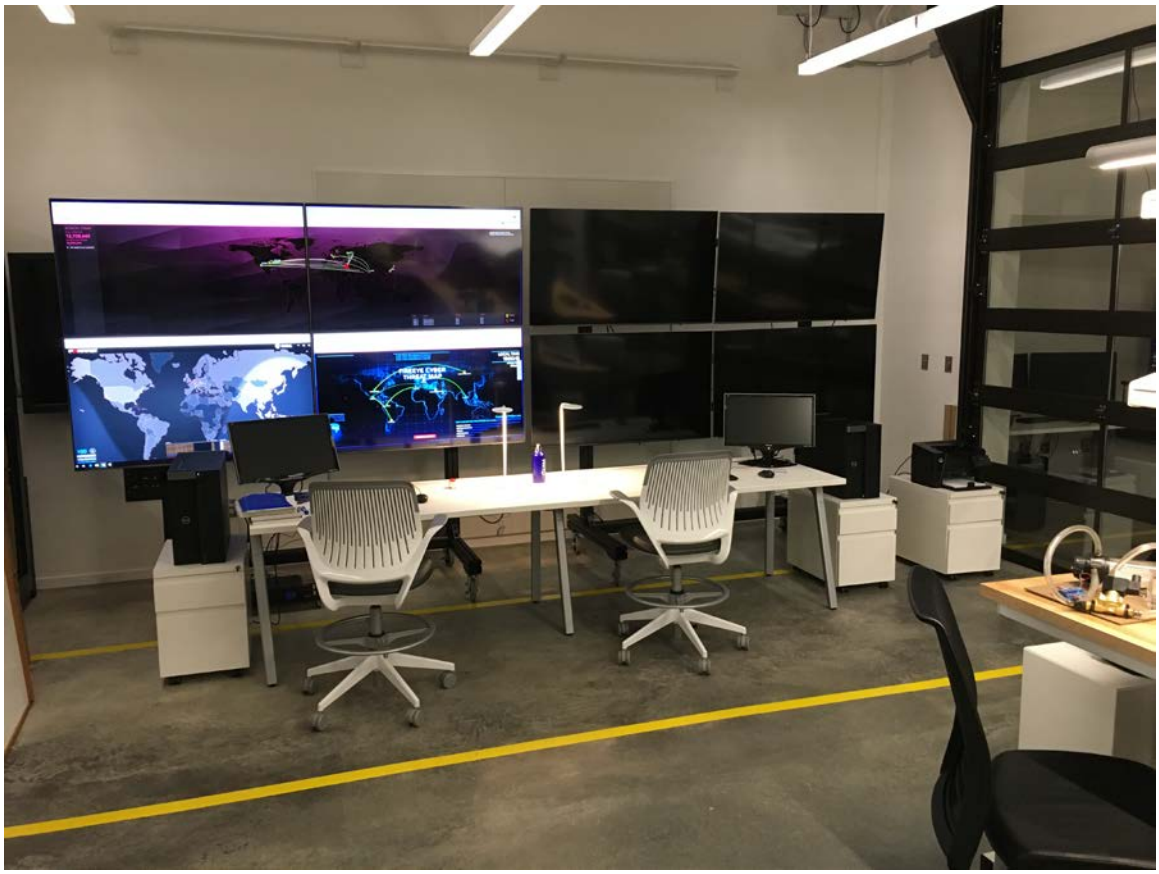

Figure 10: The SCANVILLE Screen Wall (each screen is a 55 inch 4K high definition TV).

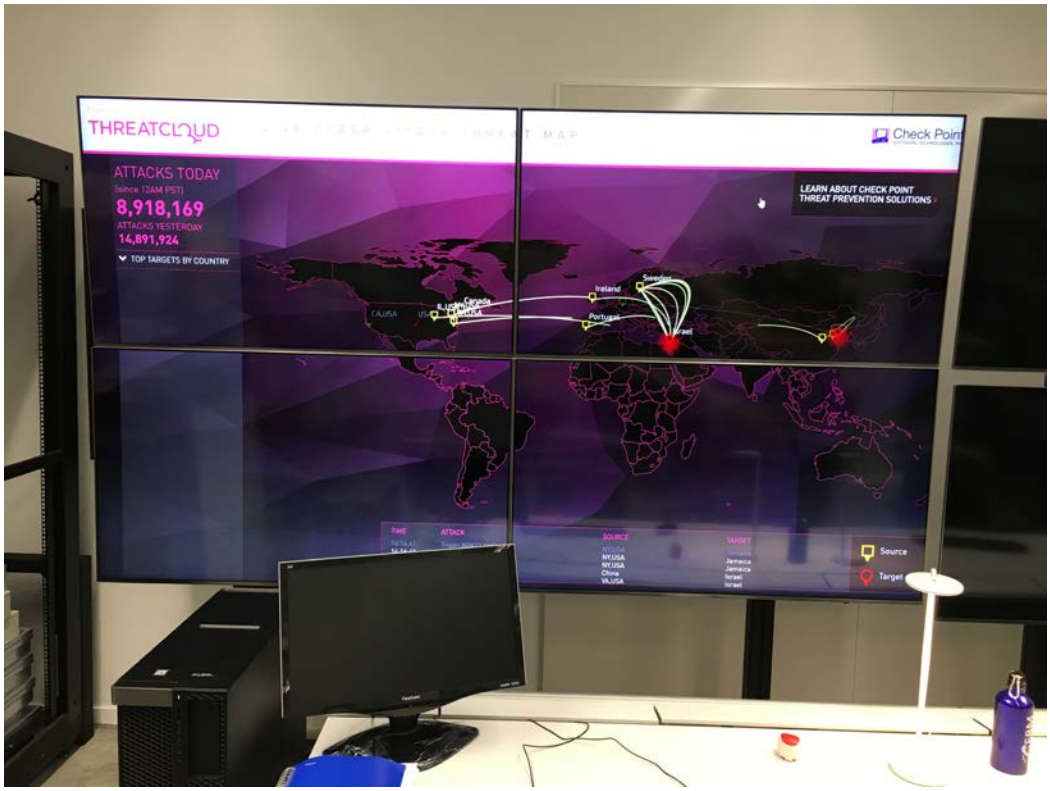

Figure 11: The SCANVILLE Screen Wall - Close Up.

Figure 12: The SCANVILLE Workstations.

D-E: ICS Testbed: Industrial Control and HMI Labs (Coeur d'Alene and Idaho Falls):

We are currently developing the nodes in Idaho Falls and Coeur d'Alene through a contract with Ameresco Inc. Each installation will have an identical Human Machine Interface (HMI) and control system. These are specified as:

1. Single Wonderware HMI running windows OS PC using a virtual machine.
2. (3) PLC supporting Modbus and DNP3 Ethernet protocols from HMI to PLC
    a. AB 1400 PLC- DNP3.0
    b. Automation Direct Dumore BRX PLC- Modbus
    c. Productivity 1000 PLC includes IO simulator
3. Small OIT terminal to read and write variables to PLC's.
4. Network switches and video hubs to extend application to a training video monitor touch screen.
5. Power hub for Ethernet
6. BOX PC with hosted virtual MS OS for Wonderware SCADA HMI
7. All programing development software to be included on BOX PC
8. Kobalt workbench for above stated equipment to be mounted- with caster wheels

The assets that are controlled by this system will be different in both locations. In Idaho Falls the security asset to be controlled will be related to a nuclear reactor. In Coeur d'Alene the security asset to be controlled will be a robotic manufacturing system. In both cases the plan is to integrate these devices into the IDC cybersecurity testbed.

Figure 9 shows a similar system currently being assembled at the vendor facility. Installation is scheduled for late-September. One of the benefits of this system is the flexibility it provides with the Wonderware software platform. Wonderware is the current industry standard.

Figure 13: Kobalt workbench with HMI and PLC for Asset.

1.2 Objective 2: Strengthen collaboration with Idaho industry and Idaho Universities

Our team had numerous on-going and one-time collaborations with industry and other universities. Some of these collaborations are listed below.

1. Brian Johnson has had weekly meetings with Craig Rieger and Tim McJunkin from the INL related resilient control of critical infrastructure. Efforts included:

(a) Ongoing research project as part of DOE Grid Modernization Lab project related to resilience metrics for power distribution systems, which ended September 2018.

(b) Collaboration on an ongoing LDRD proposal related to cybersecurity for industrial control systems, with collaboration from Virginia Commonwealth University. UI funding for year three was increased by $31,000 over the original budget.

(c) Collaboration course ECE 469/569: Resilient Control of Critical Infrastructure with collaboration between UI, ISU, WSU, UNR, and INL along with some interaction with Naval Post Graduate School, Weber State University, and Boise State University. Yacine Chakhchoukh coordinated the class from the UI this year.

(d) Helped organize a Resilient Controls track for the IEEE Industrial Electronics Society Annual Meeting (IECON), October 21-23, 2018 in Washington DC. Brian arranged for Scott Manson from Schweitzer Engineering Laboratories to be an invited keynote speaker for the track.

2. Brian Johnson and Dakota Roberson had monthly meetings with engineers from ABB Corporation Corporate Research, University of Illinois, Argonne National Lab and Bonneville Power Administration as part of a project addressing cybersecurity for HVDC transmission systems. They also participated in the DOE Cybersecurity for Energy Delivery Systems (CEDS) Peer Review meeting in Washington DC in November 2018 as part of this project.

3. Dakota Roberson and Brian Johnson coordinated an article titled “Improving Grid Resilience Using HVDC” which had contributors for Argonne National Laboratory, University of Illinois Urbana-Champaign and support from ABB. The article was an invited contribution a special issue of IEEE Power and Energy Magazine.

4. Brian Johnson and Yacine Chakhchoukh have been investigators on a project with Avista Corporation looking at non-wire solutions that use sensors and controls to alleviate the need for new transmission lines to improve reliability of power systems at a lower cost. That project ended in August 2018.

5. Yacine Chakhchoukh, Daniel Conte de Leon, and Brian Johnson have been investigators of a project with Avista Corporation looking at developing a secure framework for transactive energy trading at the power distribution level.

6. Brian Johnson was invited to participate in a US DOE Peer Review on the “Future State of Protective Relaying,” July 18-19, Oak Ridge National Lab.

7. Brian Johnson and Maadhavi Sathu had weekly meetings with researcher from INL, Oregon State University and industry advisors as part of a project to develop a white paper for the US DOE setting research needs related protective relaying systems.

8. Brian Johnson was advisor for four industry sponsored senior design teams in the fall semester, one sponsored by Avista, one by Schweitzer Engineering Laboratories and two related to developing power lab capabilities related to this grant.

9. Daniel Conte de Leon was advisor for one senior design team during the Fall 2018 semester. This team is working on developing 3D visualization techniques with the objective of visualizing complex industrial control systems.

10. Daniel Conte de Leon was customer for a student building a Faraday Cage to enable research and instruction on wireless IoT and control system devices.

11. Jia Song attended the research and collaboration meeting with SEL to discuss possible collaborations on computer science and security related research topics. (Nov 29, 2018)

12. Michael Haney was selected for a fourth consecutive year to hold a Joint Appointment with the Idaho National Laboratory, maintaining a strong working relationship with the Cybercore Integration Center under the National & Homeland Security division.

13. Michael Haney and Dakota Roberson were selected to support the INL’s Cybercore Integration Center strategic planning meeting, representing UI along with Janet Nelson, VPR, Brad Ritts,

Associate VPR, and John Russell, UI's Associate Director of the Center for Advanced Energy Studies (CAES).

14. Michael Haney, Dakota Roberson, and Frederick Sheldon were each selected to receive a Summer Faculty award by the Center for Advanced Energy Studies (CAES) in July and August of 2018 in Idaho Falls.

15. Michael Haney was selected to serve on ISU's search committee for their new cluster hires in cybersecurity, data science, and electrical engineering for the ISU Polytechnic in Idaho Falls.

16. Michael Haney continues to serve on the Advisory Board member, Energy Systems Cyber-Physical Security program, Energy Systems Technology and Education Center (ESTEC), Idaho State University.

17. Michael Haney was invited to speak at the first BSides Idaho Falls cybersecurity conference and presented his work on developing open sourced threat intelligence in September 2018. He has now joined the BSides Idaho Falls advisory board to plan the second and future open security conferences in eastern Idaho.

18. Michael Haney was invited to speak at the Tulsa Cyber Summit, sponsored by the University of Tulsa and the George Kaiser Family Foundation to be held in March 2019 in Tulsa, Oklahoma. There he will present his ongoing research in the methods for preserving privacy in pervasive networking monitoring and large-scale surveillance.

19. Michael Haney was recently invited to join an $(ISC)^2$ task force for updating the Common Body of Knowledge and the exam for the Certified Information Systems Security Professional (CISSP) exam.

20. Michael Haney continues to direct the Nuclear Cybersecurity Working Group within CAES, cultivating university and industry connections across the state of Idaho, across the nation's nuclear sector, as well as with the International Atomic Energy Agency (IAEA).

1.3 Objective 3: Foster technology transfer and commercialization through technology incubation

During the first half of this third year we have had several proposals funded and others submitted for research in this area:

1.3.1 Funded Project Proposals

B.K. Johnson, "Supplement to Resilient Scalable Cyber State Awareness of Industrial Control System Networks to Threat: Power System Design and Testing," Idaho National Laboratory, January 2019 - September 30, 2019, $31,000.

B.K. Johnson and J. Alves-Foss, "REU Supplement for: Small: Securing Smart Power Grids Under Data Measurement Cyber Threats", Syracuse University (subcontract of NSF funding). January 1, 2019 - June 30, 2019, $7,999.

A.Zadeghol, H. Lei and B.K. Johnson, "Air-core Reactor Inter-turn Fault Detection, using Magnetic Field Sensors" Schweitzer Engineering Laboratories, $139,221.94.

B.K. Johnson, "Protective Relay Study," Idaho National Laboratory, August 1, 2018-November 30, 2018, $10,000.

Y. Chakhchoukh, D. C. De Leon, H. Hess, B. Johnson, H. Lei and A. Daffin, "Designing and Evaluating an Energy Trading System for Prosumers", Avista Corporation, August 1, 2018 - September 1, 2019, $89,771

Smart Grid Resiliency Seed Funding from Center for Advanced Energy Studies (CAES) at Idaho National Laboratory to provide UI CS/ECE support to engage INL, BSU, ISU and Univ. Wyoming in Larger Scale Extramural Bid, Submitted Feb. 13, 2018 to CASE, provides $30,000 (six months) to the UI Computer Science (CS). PI F.T. Sheldon, Co-PIs: Michael Haney, Yacine Chakhchoukh, Zouheir Rezki, Paul Titus [INL] and John Stubban [BSU] and Others; Purpose: Develop larger scale proposal to DOE/NSF during CY 2018 (see DE-FOA-0001897 Building EPSCOR-State/National Laboratory Partnerships)

1.3.2 Funding Proposals Submitted and Under Review

B.K. Johnson, "Tool for auto-generation of dynamic zone selection logic for busbar protection," Schweitzer Engineering Laboratories, January 2019-December 2018, $98,187.

J. Song, "CRII: SaTC: Automating Fuzzing Based on Grammar Detected from User Input", National Science Foundation, May 2019 – May 2021, $174,999.

J. Alves-Foss, J. Song, "Automated Vulnerability Detection and Repair", DHS, May 2019-April 2022, $910,484.80.

M. Haney, "GenCyber: Bringing the GenCyber Experience to Eastern Idaho," National Security Agency, May – September 2019, $99,870.

R. Christensen, M. Haney, et al. "2019 NEUP Infrastructure: Developing a NuScale Simulator for Multi-Institutional Research of Small Modular Reactors", Department of Energy Nuclear Engineering University Program, October 2019, $285,763.01.

M. Haney, et al, "2019 NEUP NE-1: Analysis and Design of Future Digital Instrumentation and Control in Gen IV Nuclear Power Plant Control Rooms", October 2019, $798,700.

1.3.3 Publications: Published or Accepted

J.M. Sotelo, J. Guitierrez, B.K. Johnson, P. Moreno, A. Guzman "Time Domain Parameter Identification of Transient Electromechanical Oscillations," Accepted for publication in COMPEL: The International Journal for Computation and Mathematics in Electrical and Computer Engineering.

H. Esponda-Hernandez, E. Vasquez, M.A. Andade, B.Johnson, "A Setting-Free Differential Protection for Power Transformers Based on Second Central Moment," IEEE Transactions on Power Delivery. Available Early Access. Digital Object Identifier: 10.1109/TPWRD.2018.2889471.

N. Fischer, B.K. Johnson, A.G. Miles, J.D. Law, "Induction Motor Modeling for Development of a Secure In-Phase Motor Bus Transfer Scheme," IEEE Transactions on Industry Applications. Vol. 55, No. 1, January/February 2019, pp. 203-2012. DOI: 10.1109/TIA.2018.2868763.

M. Abuagreb, M. Allehyani and B.K. Johnson, "Design and Test of a Combined PV and Battery System Under Multiple Load and Irradiation Conditions," Accepted for 2019 IEEE PES Innovative Smart Grid Technologies Conference North America." February 17-20, 2019, Washington DC.

A.Momen, B.K. Johnson and Y. Chakhchoukh "Parameters Estimation for Very Short Line Using The Least Trimmed Squares (LTS)," *Accepted for 2019 IEEE PES Innovative Smart Grid Technologies Conference North America."* February 17-20, 2019, Washington DC.

K. Eshghi, B.K. Johnson, C.G. Rieger, "Resilient Agent for Power Systems Operation and Protection," *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*. Washington DC, October 21-23, 2018.

H.S. Samkari and B.K. Johnson, "Multi-Agent Protection Scheme for Resilient Microgrid Systems with Aggregated Electronically Coupled Distributed Energy Resources," *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*. Washington DC, October 21-13, 2018.

P. Khaledian, B.K Johnson, and S. Hemati, "Power Grid Resiliency Improvement Through Remedial Action Schemes," *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*. Washington DC, October 21-23, 2018.

A.Corredor, H. Beleed, B.K. Johnson, H.L. Hess, "D-FACTS for Improving Reliability of the Transmission System During Contingencies," *Proceedings of the 2018 North American Power Symposium*, Fargo, North Dakota, September 9-11, 2018.

H.S. Samkari, H.L. Hess and B.K. Johnson, "Developing a Microgrid Energy Management Scheme for a Pacific Northwest City," *Proceedings of the 2018 North American Power Symposium*, Fargo, North Dakota, September 9-11, 2018

P. Khaledian, B.K Johnson, and S. Hemati, "Harmonic Mitigation and a Practical Study of Torque Harmonics in Induction Motor Startup," *2018 IEEE Power and Energy Society General Meeting (PESGM)*, Portland, August 2018.

S.R. Sathu, N. Fischer, B.K. Johnson, "New Protection Scheme for Type 4 Wind Turbines," *71st Annual Conference for Protective Relay Engineers (CPRE).* College Station, Texas, March 2018.

Ibukun A. Oyewumi, Ananth A. Jillepalli, Philip Richardson, Mohammad Ashrafuzzaman, Brian K. Johnson, Yacine Chakhchoukh, Michael A. Haney, Frederick T. Sheldon, and Daniel Conte de Leon. "ISAAC: The Idaho CPS Smart Grid Cybersecurity Testbed." To appear in: Proceedings of the IEEE Texas Power and Energy Conference 2019 (IEEE-TPEC-2019), February 7-8, 2019, College Station, Texas, USA.

Ibukun A. Oyewumi, Ananth A. Jillepalli, Philip Richardson, Mohammad Ashrafuzzaman, Brian K. Johnson, Yacine Chakhchoukh, Michael A. Haney, Frederick T. Sheldon, and Daniel Conte de Leon. "Attack Scenario-based Validation of the Idaho ICS Smart Grid Cybersecurity Testbed (ISAAC)." To appear in: Proceedings of the IEEE Texas Power and Energy Conference 2019 (IEEE-TPEC-2019), February 7-8, 2019, College Station, Texas, USA.

Ananth A. Jillepalli, Daniel Conte de Leon, Ibukun A. Oyewumi, Jim Alves-Foss, Brian K. Johnson, Clinton L. Jeffery, Yacine Chakhchoukh, Michael A. Haney, and Frederick T. Sheldon. "Formalizing the HESTIA Process: Checking Consistency and Conflicts." To appear in: Proceedings of the IEEE Texas Power and Energy Conference 2019 (IEEE-TPEC-2019), February 7-8, 2019, College Station, Texas, USA.

Abercrombie, R.K., Ollis, B., Abercrombie, T., Jillepalli, A. and Sheldon, F.T., "Microgrid Disaster Resiliency Analysis: Reducing Costs in Continuity of Operations (COOP) Planning," To appear in Proceedings of the Hawaii International Conference on System Sciences (HICSS-52) January 7-11, 2019, Hawaii, USA.

Sheldon was invited to give a talk by Adolfy Hoisie (Brookhaven National Laboratory) and Behrooz Shirazi (National Science Foundation): Title of the talk: Analysis of COOP Planning Scenarios for a Microgrid to Enhance Sustainability and Resiliency," Sixth Symposium on Sustainable Energy and Computing (SSEC), Jan. 8-11 2019 at HICSS52 Maui, HI.

Y. Chakhchoukh and H. Ishii, Cyber security for power system state estimation, in J. Stoustrup, A. Annaswamy, A. Chakrabortty, and Z. Qu (editors), Smart Grid Control: Overview and Research Opportunities, Springer, pp. 241-256, 2019.

H. Lei, Y. Chakhchoukh and Ch. Singh, "Framework of a benchmark testbed for power system cyber-physical reliability studies," International transactions on electrical energy systems. August 2018. Wiley Online Library.

M. Ashrafuzzaman, H. M. Jamil, Y. Chakhchoukh and F. T. Sheldon, “A Best-Effort Damage Mitigation Model for Cyber-Attacks on Smart Grids,” 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, July 23-27, 2018.

M. Ashrafuzzaman, Y. Chakhchoukh, A. A. Jillepalli, P. T. Tosic, D. C. de Leon, F. T. Sheldon, B. K. Johnson, "Detecting Stealthy False Data Injection Attacks in Power Grids Using Deep Learning," 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, 2018, pp. 219-225.

M. McGregor and M. Haney, "Quantum Key Exchange Simulator," *22nd Colloquium for Information Systems Security Education* (CISSE 2018), June, 2018, New Orleans, LA.

M. McGregor and M. Haney, “Quantum Key Exchange Simulator,” In *Journal of the Colloquium for Information Systems Security Education*, Edition 6, Issue 1, September, 2018.

R. E. Hiromoto, M. Haney, A. Vakanski, and B. Shareef, “Towards a Secure IoT Architecture,” Elsevier Publishing, 2019.

1.3.4 Publications: Submitted and Under Review

Yacine Chakhchoukh, H. Lei, B.K. Johnson, “Diagnosis of Outliers and Cyber Attacks in Dynamic PMU-based Power State Estimation,” *Submitted to IEEE Transactions on Power Systems.* December 2018.

H. Lei, J. Geng, B. Johnson, “Influence of Superconducting Fault Current Limiters on Travelling Wave Based Protection,” *Submitted to IEEE Transactions on Applied Superconductivity.* November 2018.

A. Aljebrine, H. Lei, H. Hess, B. Johnson, J. Geng, “Superconducting Fault Current Limiter Application for Induction Motor Starting Current Reduction,” *Submitted to IEEE Transactions on Applied Superconductivity.* November 2018.

A. Momen, Y. Chakhchoukh, B.K. Johnson, “Series Compensated Line Parameters Estimation Using Synchrophasor Measurements,” *Submitted to IEEE Transactions on Power Delivery.* August 2018.

J. Hatton, B.K. Johnson, D. Roberson, and R. Nuqui, “Increased Grid Resilience Via Cyber-Secure VSC Multiterminal HVDC Systems,” *Submitted to the 2019 IEEE PES General Meeting.* Atlanta, Georgia, August 2019.

J. Song, J. Alves-Foss, “A Fuzzing Tool Based on Automated Grammar Detection”, Computers & Security, Dec 2018.

J. Alves-Foss, J. Song, “Revisiting Function Boundary Detection”, USENIX Security Symposium 2019, Dec 2018.

John Peterson, R.A. Borrelli, and Michael Haney, “An overview of the methodologies for cyber security vulnerability assessments conducted in nuclear power plants,” Journal of Nuclear Engineering and Design.

M. Haney, J. Benjamin, and R. A. Borrelli, “Cyberweapon Non-proliferation and Safeguards: an Approach from the Lessons Learned in the Nuclear Sector”, American Nuclear Society Conference on Safeguards, June, 2019.

T. McLean, R. A. Borrelli, and M. Haney, “Cyber Security Modeling of Non-Critical Nuclear Power Plant Instrumentation ,” International Conference on Infrastructure Protection, SRI International, March 11 – 13, 2019, Arlington, VA.

M. Haney, “Advances in Deceptive Systems and Honeypots for Threat Intelligence and Active Defenses in Critical Infrastructures,” International Conference on Infrastructure Protection, SRI International, March 11 – 13, 2019, Arlington, VA.

1.3.5 Presentations

November 2018: Speaker: Krishnanjan Gubba Ravikumar, Schweitzer Engineering Laboratories, Title: Experience with Remedial Action Schemes.

November 2018: Speaker: Dwight Anderson, Schweitzer Engineering Laboratories, Title: Cybersecurity for Power Protection.

December 2018: Speaker: Sudeep Pasricha. Department of Electrical and Computer Engineering at the Walter Scott Jr. College of Engineering in Colorado State University, Title: Smart Software for the Internet of Future Things.

1.4 Objective 4: Strengthen and expand the workforce

During the Summer of 2018 at least 9 students conducted internships focused on cybersecurity. Organizations were these students participated were: US Department of Defense, Idaho National Laboratory, Pacific Northwest National Laboratory, and US Department of Homeland Security.

Also during the Summer of 2019, Michael Haney developed and hosted the 2nd Cybercore Summer Camp held in Idaho Falls, receiving support from the College of Eastern Idaho and Idaho National Lab's Cybercore Integration Center. The tuition-free day camp hosted high school students from across eastern Idaho for three days of hands-on learning projects and "hacking" activities to introduce students to advanced computing and cyber-physical systems programming. Plans are in place and a grant application has been submitted to expand future camps for beginners and advanced students as well as area high school teachers.

As a follow-up to the successful summer camp, Haney has worked with the College of Eastern Idaho and Compass Academy to develop and host after-school programs supporting cyber-physical control systems and embedded device programming and cybersecurity activities for local high school students, which we believe will greatly strengthen the future workforce by fostering interest and skills at an early age.

2 Summary of Budget Expenditures

This summary is an estimate only as final mid-point expenditures have not all posted.

Salaries	$245,000
Fringe	$70,000
Travel	$4,000
Operating	$55,000
Tuition	$22,400
Total	**$396,400**

3 Demonstration of Economic Development and Impact

3.1 Patents, copyrights, plant protection certificates received or pending

There are none at this time. We are developing a strategy to raise the bar of awareness concerning patents and copyrights (including software and intellectual property) and engage with industry to identify opportunities.

3.2 Technology licenses signed, start-up businesses created, and industry involvement

Karen Stevenson who is our College of Engineering licensing associate at the UI Office of Technology Transfer (OTT) spoke to the Department about the UI Strategic Plan as it relates to Faculty, Research and Sponsored projects and Invention disclosures. We are planning to engage the OTT in the future to increase awareness pertaining to UI's Strategic Planning and Program Prioritization Process and the Commercialization of our research outcomes including public/private entrepreneurial partnerships. All told, we want to increase our enrollments/retention in both our Undergraduate and Graduate programs to meet the needs of Idaho's industry; bring viable technologies to market as well as creating high-value jobs while increasing our research capacity, especially as it pertains to the IGEM objectives and overarching theme: Security Management of Cyber Physical Control Systems.

These discussions are planned as Colloquium Topics and for Departmental Faculty Staff meetings.

3.3 Private sector engagement

See Section III (c) above for a list of formal engagements per our Computer Science Colloquium Series. Also, refer to the section on "Strengthening and Expanding the Workforce" at Section III (4) above regarding Industry/Government engagements.

The IGEM team of Co-PIs engaged with the Murdock Charitable Trust (as described above) to leverage (match) IGEM funding that was earmarked for laboratory equipment upgrades that are designed to improve our capabilities in Cyber Security Data Analytics and Visualization.

3.4 Jobs created

None for the reporting period other than the new faculty hires.

3.5 External funding

Nearly a million dollars of funding beyond the IGEM grant has been secured to help meet the objectives of this project. Of this amount, $795,000 came from external sources and $202,000 of college of engineering funding was redirected. A significant factor was the funding provided by the Murdock Charitable Trust to enhance power security laboratory as described above.

4 Numbers of Faculty and Student Participation as a Result of Funding

Seven faculty and four graduate students were the primary participants on this project. In addition, numerous other faculty and staff assisted in the activities such as supporting the faculty search process and expanding the laboratories and improved audio/video connections around the state as outlined in the original project plan.

Primary Faculty	Primary Students
Larry Stauffer	Hari Challa
Rick Sheldon	Krishna Koganti
Brian Johnson	Mohammad Ashrafuzzaman
Michael Haney	Ananth Jillepauli
Daniel Conte de Leon	Maadhavi Saathu
Yacine Chakhchoukh	Andrew Miles
Jia Song	Ibukun Oyewumi
Constantinos Kolias	
Dakota Roberson	

5 Description of Future Project Plans

Plans for the future are to accomplish the deliverables of the four objectives as stated in our original proposal. Specifically, for the final semester we plan to:

- Continue our research work on developing tools and techniques for securing critical infrastructure systems.
- Expand use of the UI Cybersecurity Training and Operations Center in Coeur d'Alene (including security assessments)
- Expand activities to initiate a Resilience Research Incubation Center in Moscow.
- Conduct assessments with willing industry partners to better understand the threats and potential impacts of compromises associated with CPCSs.
- Increase our capacities to deliver education course work (both for credit and non-credit professional development) and research.

Perhaps the most impactful outcome of this IGEM project this quarter is that we started to prepare a proposal for the first BS and MS degree programs in Cybersecurity in Idaho. In November 2018 the Computing and Accreditation Commission of ABET introduced the first program-specific criteria for cybersecurity. Given the ABET process, these students will be educated according to the new nationally accepted standards. Through this program we project to be delivering hundreds of cybersecurity engineers to the workforce over the next several years. We plan to educate students in Moscow, Coeur d'Alene, and Idaho Falls and will explore on-line delivery options as well. This program will deliver the talent needed by industry to help secure their data and infrastructure and grow Idaho's economy.