IGEM17-001

Security Management of Cyber Physical Control Systems
July 1, 2018 thru June 30, 2019
Final Report

University of Idaho
College of Engineering

Higher Education Research Council
Idaho Global Entrepreneurial Mission
Program Final Annual Report

Grant Number IGEM17-001

Security Management of Cyber Physical Control

Systems August 30, 2019
The third and final annual 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.go
vTel: (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 at the end of the final year (July 1, 2018 - June 30, 2019) 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 had all four new faculty working. We have made substantial progress especially on deploying the new video technology infrastructure, continuing laboratory enhancement projects, forming additional industry collaborations, producing research results, and planning for the post-grant period.

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 finished the hiring in year two of the project and this past year was the first that we were fully staffed. Our newly hired faculty have made an accomplished addition to our capacity in this area.

1.1.2 Graduate Students

Four graduate students worked as research assistants under the project during the reporting period: 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 2018-2019 academic year 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 Power Laboratory and the SCANVILLE Lab, both part of the ISAAC ICS Testbed being built as part of this project. In addition, in January Mr. Oyewumi joined a project funded by Idaho National Laboratory for the development of machine learning algorithms for the detection of attacks in power control systems. This project is being performed using the recently built ISAAC testbed.

3. Graduate student Andrew Miles is pursuing a Doctorate in Electrical Engineering. During the fall 2018 semester Mr. Miles worked on research toward the implementation of robust state estimators for power systems. 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 the power system software tool OpenDSS to show feasibility studies for real world applications. The Power

Laboratory now equipped with two RTDSs (Real-Time Digital Simulator(s)) is very useful for the real-time evaluation of the developed algorithms. Also, starting January 2019 Mr. Miles joined a project funded by Avista Utilities Corporation to develop an operationally secure and cyber secure transactive energy trading platform. Avista Utilities is an electric power and natural gas utility with more than 600,000 customers across 30,000 square miles in Eastern Washington, Northern Idaho, and parts of Oregon.

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 high penetration of the Integration of Renewables. Power systems operate close to their nominal frequency under steady state conditions. During the power system disturbances like three phase faults on heavily loaded lines, line switching, loss of large loads, large generator disconnection results in sudden change to electrical power, whereas the input mechanical power inputs to the remaining generators remain constant. These disturbances cause oscillations in machine rotor angles which result in severe power flow swings. Based on the severity of the power system disturbance, system can remain stable and return to a stable equilibrium state in what is referred as stable power swing. On the other hand if the disturbance is too severe there will be a large separation of generator rotor angles, large power swings that continue to grow, resulting in a loss of synchronization between generators, which is referred as unstable power swing. Large power stable swings can cause unwanted protective relay operations at different locations which can cause lead to major power outages or power blackouts. In modern digital relays, a 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. Integration of large numbers of renewable generation sources such as wind generation, photovoltaic generation decreases the inertia of the power grid which can't be detected with the existing power swing blocking 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). An RTDS Real-Time Digital Simulator is a hardware-firmware-software device that enables real-time simulation of power transmission and distribution systems. This IGEM project increased the research capacity of this laboratory by adding a second RTDS.

1.1.3 Laboratory Enhancements

In our proposal we projected enhancing laboratory equipment and make research 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. However, we took advantage of an opportunity presented by the M.J. Murdock Charitable Trust to invest an additional $285,000 of their funding plus an additional $200,000 of College of Engineering funding 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 ISAAC: The IdahoICS Cybersecurity Testbed.

The ISAAC testbed is enabling 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) and Industrial Internet of Things (IIoT). Its major advantage is that it enables 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 exposes commercial and prototype equipment to hardware-in- the-loop simulation, enabling the capture and use of real operational data, integrate current and future components of the power grid and other industrial control systems, and enables realistic attack-defend scenarios for research and development, evaluation and testing, and education and training. The ISAAC 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 significantly enhances our ability to demonstrate (in-situ) advanced Power Grid and Industrial Control Systems cybersecurity technology to Idaho industry partners.

The ISAAC Testbed connects 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 laboratory A: Power Laboratory (Moscow), have been completed. Enhancements to laboratories B: RADICL-Moscow and C:SCANVILLE, Moscow are also complete. The isolated network connection within the three laboratories on the Moscow, Idaho campus is complete and operational.

ISAAC testbed equipment for the laboratories in Coeur d'Alene (E) and Idaho Falls (D) have been purchased and are connected to the testbed isolated network system. Networking cabling and equipment in for the RADICL Idaho Falls laboratory have been installed. The virtually isolated network connection between the laboratories in Moscow and the ones in Coeur d'Alene and Idaho Falls will be provided by IRON (The Idaho Regional Optical Network) and are expected to be complete later this summer. These connections are expected to use MacSec encrypted network packets over an MPLS (Multi-Protocol Label Switching) network to ensure the safety and security of the testbed and prevent accidental leakage of testbed data into other systems. During a visit to the University of Idaho campus in Moscow, Idaho this May 2019, Idaho Governor Mr. Brad Little made a tour of the three laboratories (A, B, C above) that are part of the ISAAC Testbed. Figure 1 shows a picture taken during this visit.

Figure 1: Idaho Governor Mr. Brad Little (second from left), University of Idaho past President Dr. Chuck Staben (first from left), UI Distinguished Professors Dr. Jim Alves-Foss (speaking) and Dr. Brian Johnson (center of view), plus University of Idaho Faculty, Staff, and Students in the University of Idaho Power Laboratory During a Governor Visit in May 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 2). 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.

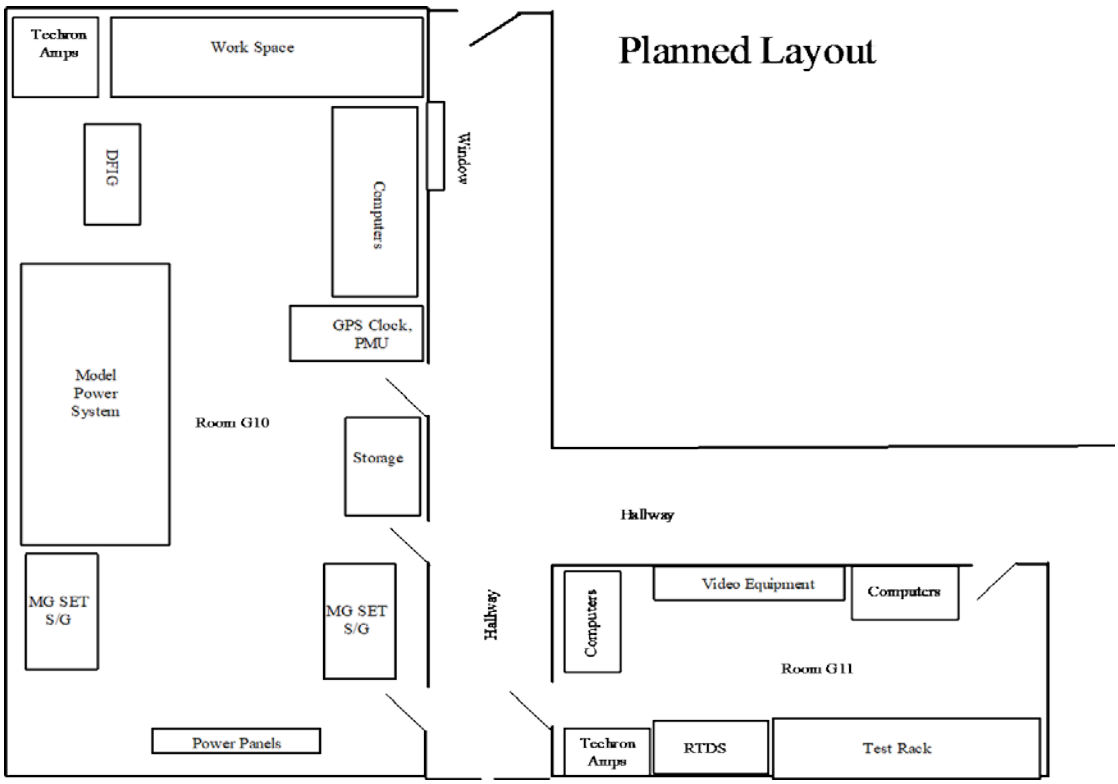

Figure 2: Illustration of the Power Systems Laboratory (PowerLab) Expansion.

The space for the PowerLab section of the ISAAC testbed was remodeled and completed the end of November 2018, 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 ISAACtestbed 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 existing RTDS and associated amplifiers were moved to the PowerLab and test equipment was connected to the RTDS as shown in Figures 3-5. Audio/video equipment used to communicate between labs is shown in Figure 6. In addition, the existing RTDS was upgraded with additional processor cards donated by Schweitzer Engineering Laboratories.

Figure 3: 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 4: PowerLab Component of the ICS Testbed with the addition of the new RTDS NovaCor rack (to the left).

Figure 5: Completed and Operational PowerLab Components of the ISAAC Testbed. Four SEL power control equipment racks (left) and new RTDS NovaCor (right). Each SEL equipment rack contains equipment roughly equivalent to a power substation.

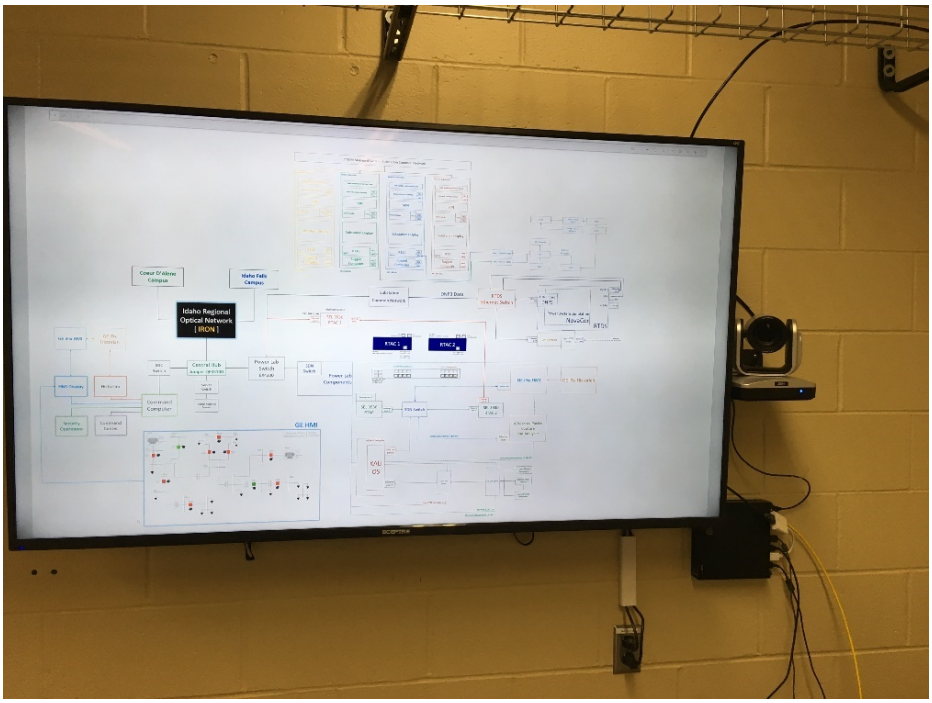

Figure 6: The audio/video equipment in the PowerLab.

B: ISAAC Testbed: RADICL-Moscow 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 (Figures 7 and 8). Under the planned laboratory enhancements, we enhanced the cybersecurity, computing, and analysis capabilities of this laboratory and integrated it into the ISAAC industrial control systems cybersecurity testbed. We also added audio/video connections to the other lab spaces.

Figure 7: Students working in the RADICL Cybersecurity laboratory before its renovation under this project.

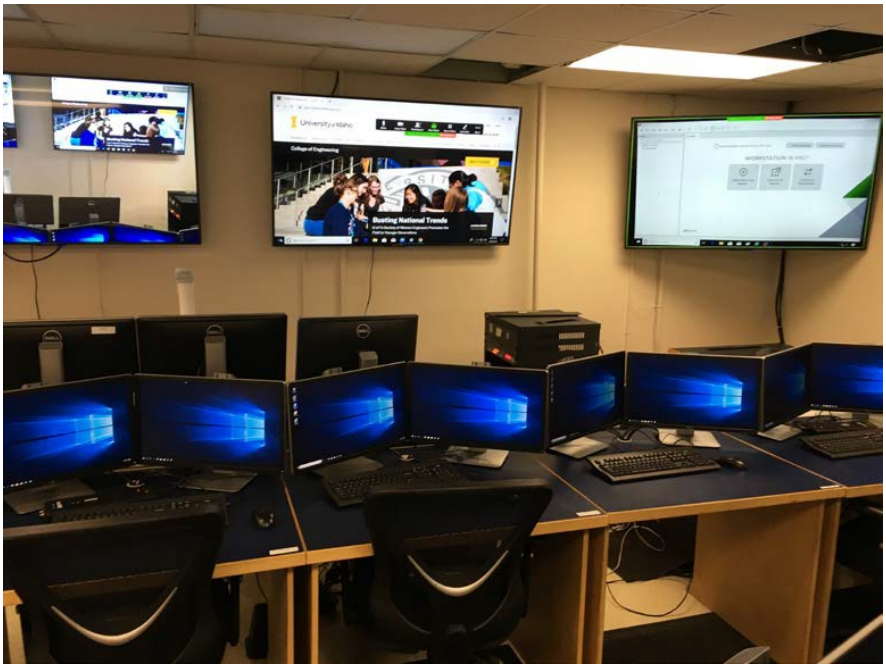

Figure 8: The RADICL Cybersecurity laboratory after its renovation during the Fall of 2018.

As part of this project and supported by additional funds secured from other sources we added audio/video capabilities to the RADICL-Moscow laboratory (Figure 9). We also built and added a small Faraday cage (Figure 10). This cage allows us to perform wireless networking research and education experiments and tutorials in a safe and secure manner. Wireless networking cybersecurity experiments and tutorials should not be performed outside of a Faraday cage.

Figure 9: The Video/Audio connection equipment in the RADICL-Moscow Cybersecurity laboratory. This system enables working collaborative for lectures, labs, and research with other researchers and educators in Idaho Falls and Coeur d'Alene.

Figure 10: The RADICL-Moscow Cybersecurity laboratory Small Faraday Cage.

C: ISAAC Testbed: SCANVILLE Lab:

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

This laboratory was designed, built, and is being 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 (Figures 11 and 12). 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 voidance, 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 ISAAC testbed through a dedicated high-speed fiber network.

The SCANVILLE laboratory is placed in a dedicated room in the new Integrated Research and Innovation Center (IRIC) at the Moscow campus. This is a significant improvement over our originally proposed plans. This improvement has enabled us to add laboratory space without additional project costs.

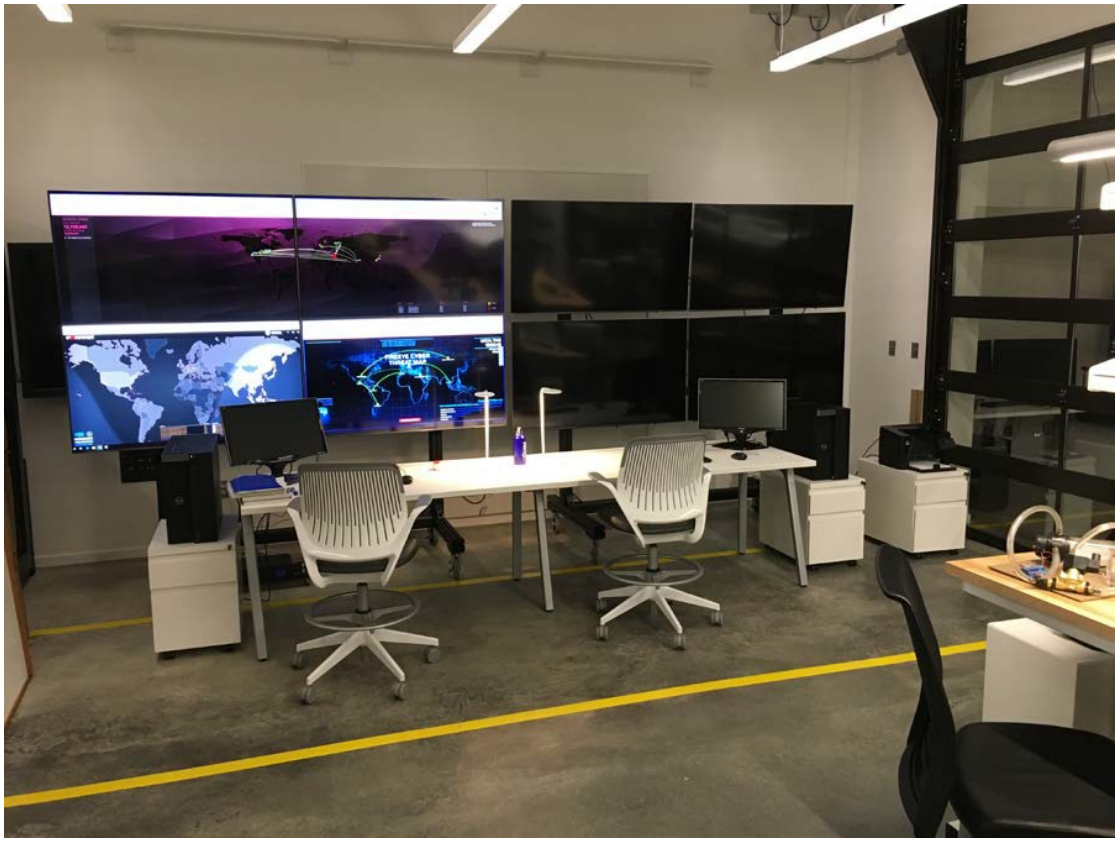

Figure 11: The SCANVILLE Screen Wall (each screen is a 55 inch 4K high definition TV).

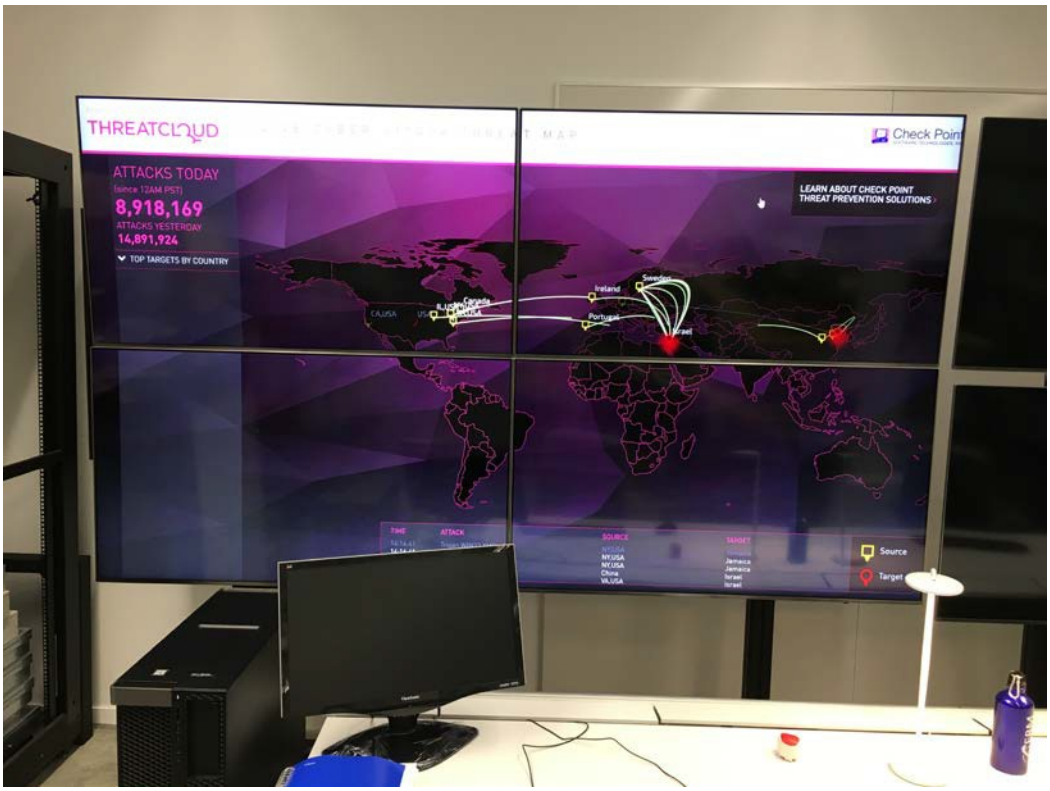

Figure 12: The SCANVILLE Screen Wall - Close Up.

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

We developed 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 industrial process assets controlled by these system will be different in each location. In Idaho Falls the security asset to be controlled will be related to nuclear reactors. 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 13 shows a similar system being assembled at the vendor facility. Installation isscheduled for late-September. One of the benefits of this system is the flexibility it provides with the Wonderware software platform. Wonderware is currently a de-facto 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. Participated in a DOE research project to identify future DOE R&D directions to ensure cyber-security of protective relaying systems during the fall 2018 semester.
    e. 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.

f. A new LDRD research project recently started that explores using dynamic predictive reliability analysis to identify cyber, physical attacks, or combined attacks as well as formulating operational responses to improve power system resilience. The team includes researchers from Ohio State University and INL.

g. A new project funded by the DOE solar energy technology office is starting that explores use of distributed photovoltaic generation to enhance the resilience of the power supply for city. The UI part of the project will collaborate with INL and VCU. The larger team includes the University of Utah and Washington State University.

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 and will participate in a final demonstration at a Bonneville Power Administration facility in fall.
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 appeared in the May/June issue of IEEE Power and Energy Magazine.
4. The authors of the “Improving Grid Resilience Using HVDC” article will be delivering a webinar on their article through the IEEE Power and Energy Society.
5. 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.
6. 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. This project was extended for a second year of research starting August 2019.
7. Brian Johnson was invited to participate in a US DOE Peer Review on the “Future State of Protective Relaying,” July 18-19, 2018 hosted Oak Ridge National Lab.
8. 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.
9. 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.
10. Daniel Conte de Leon was advisor for one senior design team during the Fall 2018 and Spring 2019 semesters. This team is working on developing 3D visualization techniques with the objective of visualizing complex industrial control systems.
11. Daniel Conte de Leon directed the design and implementation of student- built Faraday Cage to enable research and instruction on wireless IoT and control system devices. This Faraday cage has been incorporated into the ISAAC testbed.
12. 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)
13. 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.
14. 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.

15. 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.
16. 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.
17. 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.
18. 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.
19. 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).
20. 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.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).
21. A first meeting was conducted in May 2019 between Computer Science and Electrical and Computer Engineering faculty and department chairs for both, the University of Idaho and Boise State University to develop opportunities for sharing educational and research infrastructure and developing collaborative research and instruction. It was agreed to try to implement cross-University instruction by sharing CS and ECE courses across both campuses.

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

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.

B.K. Johnson, Y. Chakhchoukh, H.L. Hess, H. Lei, "Solar-Assisted State-Aware and ResilienT infrastructure System (SolarSTARTS) Physical Health Assessment and Prototype Support," Idaho National Lab (sub-award of DOE Solar Energy Technology Office Award to University of Utah), Sept 1, 2019-Aug. 31, 2022, $73,205.

B.K. Johnson, Y. Chakhchoukh, HL. Hess, and H. Lei, "Risk and Resilience Assessment of Cyberattacks on Electric Grids: Informing Risk Characterization using Dynamic Probabilistic Risk Assessment," Idaho National Laboratory, June 2, 2019-Septermber 30, 2021, $369,984

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

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 (supplement to previous award).

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

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, 2019 - September 1, 2020, $96,164

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

A Real-Time Optimum Control Scheme for PV System Fleets to Improve Power System Resilience,” Submitted to DOE EPSCoR with University of Nevada-Reno as lead, UI Budget: $329,978 over 2 years, renewable for 2 years. Other partners are Kansas State University, University of Nevada-Las Vegas and North Dakota State University.

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.

1.3.3 Publications: Published or Accepted

H. Lei, J. Geng, B. Johnson, “Influence of Superconducting Fault Current Limiters on Travelling Wave Based Protection,” *IEEE Transactions on Applied Superconductivity.* Vol. 29, No. 5, August 2019

A. Aljebrine, H. Lei, H. Hess, B. Johnson, J. Geng, “Superconducting Fault Current Limiter Application for Induction Motor Starting Current Reduction,” *IEEE Transactions on Applied Superconductivity.* Vol. 29, No. 5, August 2019

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

C. Enang and B.K. Johnson, “Enhanced Modular Multilevel Converter Based STATCOM with Hybrid Energy Storage,” *Accepted for the 2019 IEEE PES General Meeting.* Atlanta, Georgia, August 2019.

A. Momen, Y. Chakhchoukh, B.K. Johnson, “Series Compensated Line Parameters Estimation Using Synchrophasor Measurements,” IEEE early access, *IEEE Transactions on Power Delivery, June* 2019.

M. McGregor, Z. Lontz, D. Conte de Leon, and M. Haney, “Network Air Locks, Not Air Gaps, to Preserve LAN Security,” 23rd Colloquium for Information Systems Security Education (CISSE 2019), 10-12 June 2019, Las Vegas, NV.

D. Roberson, H.C. Kim, B. Chen, C. Page, R. Nuqui, A. Vales, R, Macwan, B.K. Johnson, "Improving Grid Resilience Using High Voltage dc," *IEEE Power and Energy Magazine.* Vo. 17, No. 3, May/June 2019, pp. 38-47 (Invited)

B.K. Johnson, "New Trends for HVdc: An Evolution of Applications Since 2007 [Guest Editorial]," *IEEE Power and Energy Magazine.* Vo. 17, No. 3, May/June 2019 (invited)

A. Momen, Y. Chakhchoukh, B.K. Johnson, "Series Compensated Line Parameters Estimation Using Synchrophasor Measurements," *IEEE Transactions on Power Delivery.* Early Access, May 2019

J. Peterson, R.A. Borrelli, and M. Haney, "An overview of the methodologies for cyber security vulnerability assessments conducted in nuclear power plants," Journal of Nuclear Engineering and Design. Volume 346, May 2019, 75-84.

H. Esponda-Hernandez, E. Vasquez, M.A. Andrade, D. Guillen, B.K. Johnson, "Extended Second Central Moment Approach to Detect Turn-to-Turn Faults in Power Transformers" *IET Electric Power Applications.* Vol. 13, No. 6, 2019, pp. 773-782

J.M. Sotelo, J. Guitierrez, B.K. Johnson, P. Moreno, A. Guzman "Time Domain Parameter Identification of Transient Electromechanical Oscillations," COMPEL: The International Journal for Computation and Mathematics in Electrical and Computer Engineering, 2019, https://doi.org/10.1108/COMPEL-11-2017-0475.

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. . Vol. 34, No, 2, April 2019, pp. 750-559,. Digital Object Identifier: 10.1109/TPWRD.2018.2889471.

Haney, Michael A., "Advances in Cyber-Physical System Honeypots to Enhance Threat Intelligence", Thirteenth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, SRI International, Arlington, Virginia, USA, March 11-13, 2019.

MacLean, Trevor, Michael A. Haney, and R.A. Borrelli, "Cyber Security Modeling of Non-Critical Nuclear Power Plant Digital Instrumentation," Thirteenth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, SRI International, Arlington, Virginia, USA, March 11-13, 2019.

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

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." Proceedings of the IEEE Texas Power and Energy Conference 2019 (IEEE-TPEC-2019), February 7-8, 2019, College Station, Texas, USA. 2nd Runner-up Best Paper/Pres

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)." Proceedings of the IEEE Texas Power and Energy Conference 2019 (IEEE-TPEC-2019), February 7-8, 2019, College Station, Texas, USA.

A.A. Jillepalli, D. Conte de Leon, I.A. Oyewumi, J. Alves-Foss, B.K. Johnson, C.L. Jeffrey, Y. Chakhchoukh, M.A. Haney, F.T. Sheldon, "Formalizing and Automated, Adversary-aware Rick Assessment Process for Critical Infrastructure," *2019 Texas Power and Energy Conference.* February 7-8, 2019, College Station Texas.

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.

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.

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

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.

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.

Thurston, Karen H.*; Conte de Leon, Daniel, "The Healthcare IoT Ecosystem: Advantages of Computing Near the Edge," Proceedings of the Third IEEE/ACM Conference on Connected Health: Applications, Systems, and Technologies (CHASE-2018), Washington, D.C., USA. 26-28 September 2018. ISBN: 978-1-5386-72068. 06 pages. ACM/IEEE: https://ieeexplore.ieee.org/document/8648669

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.

Jillepalli, Ananth A.; Conte de Leon, Daniel; Chakhchoukh, Yacine; Ashrafuzzaman, Mohammad; Johnson, Brian K.; Sheldon, Frederick T.; Alves-Foss, Jim; Tosic, Predrag T.; Haney, Michael A. "An architecture for HESTIA: High-level and Extensible System for Training and Infrastructure Risk Assessment," International Journal of Internet of Things and Cyber-Assurance, InderSience, 2018.

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.

1.3.4 Publications: Submitted and Under Review

R. Bainy, K. Melo, S. Lotfifard, A. Guzman and B.K. Johnson, "Dynamic Zone Selection for Busbar Protection Based on Graph Theory and Boolean Algebra," *Submitted to IEEE Transactions on Power Delivery.*

Y. Chakhchoukh, A. Miles, K. Dogancay, A. M. Zoubir, B. K. Johnson, "Robust S-based Unscented Kalman filter for Dynamic Power State Estimation," *Submitted to IEEE Transactions on Power Systems.* March 2019.

E. Balti and B.K. Johnson, "Tractable Approach to MmWaves Cellular Analysis with FSO Backhauling underFeedback Delay and Hardware Limitations," *Submitted to IEEE Transactions on Wireless Communications.*

Y. 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.

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.

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 Winter Conference, November, 2019.

1.3.5 Presentations

May 2019: Speaker: Yacine Chakhchoukh, RTDS Technologies Applications & Technology Conference, Denver, Title: Experiences Setting Up and Using a Cybersecurity Testbed.

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.

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.

January 8-11, 2019: Speaker Rick Sheldon, 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 HICSS 52 Maui, HI. (COOP means Continuity of Operations. A former colleague from ORNL had to make the actual presentation due to a personal issue with Dr. Sheldon.

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.

During the Summer of 2019, Michael Haney developed and hosted the 3rd Cybercore

Summer Camp held in Idaho Falls, receiving support from the College of Eastern Idaho and Idaho National Lab's Cybercore Integration Center. The two day camps (basic and advanced) will host high school students as well as several teachers from across eastern Idaho for five 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 and teachers to be sustained for years to come.

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	$512,116
Fringe	$117,030
Travel	$ 9,997
Operating – includes equipment	$ 27,207
Tuition	$ 33,650
Total	**$700,000**

3 Demonstration of Economic Development and Impact

3.1 Patents, copyrights, plant protection certificates received or pending

There were none during this time.

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.

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	Mohammad Ashrafuzzaman
Rick Sheldon	Ananth Jillepauli
Brian Johnson	Maadhavi Saathu
Michael Haney	Andrew Miles
Daniel Conte de Leon	Ibukun Oyewumi
Yacine Chakhchoukh	
Jia Song	
Constantinos Kolias	
Dakota Roberson	

Perhaps the most impactful outcome of student participation for this IGEM project is that we are submitting a proposal for the first BS, MS, and PhD degree programs in Cybersecurity in Idaho. In November 2018 the Computing and Accreditation Commission of ABET introduced program-specific criteria for cybersecurity. Given the ABET process, these students will be educated according to the new nationally accepted standards. Through these degree programs we project to be delivering hundreds of cybersecurity engineers to the workforce over the next several years. We will educate students in Moscow, and are making preparations to also educate students in Coeur d’Alene and Idaho Falls. This initiative will deliver talent needed by industry to help secure their data and infrastructure and grow Idaho’s economy.

5 Final Expenditure Report

A. FACULTY AND STAFF		
Name/Title	$ Amount Requested	Actual $ Spent
Larry Stauffer, Dean of the College of Engineering and Project Lead PI	$ 23,034	$21,462.18
Jia Song, Assistant Professor in Computer Science Department	$ 95,000	$101,946.60
Michael Haney, Assistant Professor in Computer Science and Project Co-PI	$ 14,176	0.00
Yacine Chakhchoukh, Assistant Professor in Electrical and Computer Engineering	$ 95,254	$105,023.20
Dakota Roberson, Assistant Professor in Electrical and Computer Engineering	$ 96,424	$90,720.07
Konstantinos Kolias, Assistant Professor in Computer Science Department, Idaho Falls	$100,000	$100,011.60
Konstantinos Kolias, Assistant Professor in Computer Science Department, Idaho Falls – moving allocation		$9,972.20
Jim Alves-Foss, Professor in Computer Science and Director of Center for Secure and Dependable Systems		$7,389.06
Frederick Sheldon, Professor in Computer Science and Project Co-PI		$1,338.88
Brian K. Johnson, Distinguished Professor in Electrical and Computer Engineering		$2,566.50
B. VISITING PROFESSORS		
Name/Title - None	$ Amount Requested	Actual $ Spent
C. POST DOCTORAL ASSOCIATES/OTHER PROFESSIONALS		
Name/Title - None	$ Amount Requested	Actual $ Spent
D. GRADUATE/UNDERGRADUATE STUDENTS		
Name/Title	$ Amount Requested	Actual $ Spent
	$ 49,471	
Mohammad Ashrafuzzaman, Student Temporary Help		$5,440.00
Tristan Clawson, Student Temporary Help		$3,225.75
Ananth Jillepalli, Grad Student Research Assistant		$22,179.60
Andrew Miles, Grad Student Research Assistant		$9,762.40
Ibukun Oyewumi, Grad Student Research Assistant		$11,860.70
Maadhavi Sathu, Grad Student Research Assistant		$19,217.40
Total Student Expense	$49,471	$71,685.85
E. FRINGE BENEFITS		
Rate of Fringe (%)	$ Amount Requested	Actual $ Spent
Fringe Benefits	$132,157	$117,029.89
Graduate Student Tuition and Fees	$ 23,500	$33,650.00
PERSONNEL SUBTOTAL:	**$629,016**	**$662,796.03**
F. EQUIPMENT: (List each item with a cost in excess of $1000)		
Item/Description	$ Amount Requested	Actual $ Spent
Technology Equipment from Right Systems, Inc		$5,652.05
EQUIPMENT SUBTOTAL:		**$5,652.05**
G. TRAVEL		
Description	$ Amount Requested	Actual $ Spent
1. Transportation/airfare	$ 10,000	$5,513.30
2. Lodging/per diem		$4,483.59
TRAVEL SUBTOTAL:	**$10,000**	**$9,996.89**
H. PARTICIPANT SUPPORT COSTS:		
Description	$ Amount Requested	Actual $ Spent
PARTICIPANT SUPPORT COSTS SUBTOTAL:		

F. OTHER DIRECT COSTS:			
Description		$ Amount Requested	Actual $ Spent
Operating Expenses – Includes conferences/registration; supplies; repairs/maintenance; technology infrastructure; software/applications; and other expenses		$ 60,984	$21,555.03
OTHER DIRECT COSTS SUBTOTAL:		**$60,984**	**$21,555.03**
TOTAL COSTS (Add Subtotals):		**$700,000**	**$700,000.00**
TOTAL AMOUNT REQUESTED:			**$700,000.00**
TOTAL AMOUNT SPENT:			**$700,000.00**