IGEM17-001

Security Management of Cyber Physical Control Systems
Computer Science
July 1, 2017 thru June 30, 2018
Annual Report

University of Idaho
College of Engineering

Higher Education Research Council
Idaho Global Entrepreneurial Mission Program
Year End Report

Grant Number IGEM17-001

Security Management of Cyber Physical Control Systems
Year 2 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, Chair and 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:
Caron Howell
(208) 332-1563
Carson.howell@osbe.idaho.gov

Table of Contents

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 concluding the second year (July 1, 2017-June 30, 2018) of this three-year project. As we are just initiating the project most of the effort has been towards planning and building capabilities of cyber physical control systems (CPCS).

1.1 Strengthen our capacity by adding key faculty and enhancing laboratories.

In this second 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. To compensate we assigned an additional portion of time for three faculty and the PI to keep schedule for meeting project objectives. We have made substantial progress especially on deploying the new video technology infrastructure, continued laboratory enhancement projects, built additional industry collaborations, and producing research results. A summary is as follows:

1.1.1 Faculty Searches

Our work plan calls 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 of 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 of 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, two in PhD programs and two in Master's programs, worked as research assistants under the project--Mohammad Ashrafuzzaman, Ananth A. Jillepalli, Hari Challa and Ibukun Oyewumi.

Mohammad was assisting Krishna Koganti (who graduated in summer 2017) with his work on the VMWare based Industrial Control Systems (ICS) Testbed project. Mohammad authored a paper based on this work that was accepted for the MALCON2017 conference. For his own research under this project, Mohammad is working on detecting and preventing stealthy cyber-attacks on cyber-physical power systems using deep learning techniques and cybernomics. He has started applying deep learning algorithms to detect false data injection attacks in power systems. The data-sets he is using are being generated by a MATLAB simulation by Dr. Yacine Chakhchoukh. Mohammad has presented the idea as a poster in the Pacific Northwest Industry Workshop and is now writing a paper for submission in a journal.

Ananth Jillepalli is developing a High-level and Extensible System for Training and Infrastructure risk Assessment (HESTIA) for cyber physical control systems (CPCS) infrastructure. Identifying vulnerabilities in a CPCS infrastructure can be challenging without a high-level security policy specification. Yet knowing the security policy specification is not sufficient to eliminate vulnerabilities. Knowledge of possible attacks and respective defense measures are also needed to secure CPCS infrastructure. Ananth has also assisted Krishna Koganti in testing Krishna's

Matlab-based ICS testbed. During his tenure as a research assistant in fall 2017 semester, Ananth has worked on several publications, a poster, and a lightning talk.

Hari Challa worked under the direction of Brian Johnson to develop a real time hardware-in-the-loop simulation of a small power system implemented using part of the new testbed. The simulated system included networked communication between the simulation and commercial communication and control devices using the DNP-3 protocol. The testing included remote access for UI researchers from Idaho Falls to launch cyberattacks on the network and researchers from Virginia Commonwealth University who performed data analytics on the results. Hari Challa also aided in the development of the overall testbed capabilities

Ibukun Oyewumi is working on Master's degree in Computer Science. He is co-advised by Daniel Conte de Leon. He is working on the development of the visualization and VPN aspects of the cyber-physical testbed.

1.1.3 Laboratory Enhancements

In our proposal we projected to enhance equipment and make capability and facility improvements.

The most significant accomplishment with respect to laboratory enhancements is the expansion of the Power Applications Laboratory in Moscow. It underwent a major expansion from about 1,500 sq.ft. to 2,200 sq.ft. (Figure 1). In the original proposal we planned to use the existing space 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 invested in the laboratory with an additional $200,000 of other funding invested in Coeur d'Alene to create a distributed testbed with locations in Moscow, Idaho Falls, and Coeur d'Alene. We have worked with the Schweitzer Engineering Laboratory (SEL) Engineering Services Division to design this testbed for performing research on cybersecurity of power and industrial control systems. This 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). The major advantage of this testbed 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. The testbed 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. It will integrate with the current Real Time Digital Simulator (RTDS) and be accessible from the other UI locations as well as BSU. This capability will significantly enhance our ability to demonstrate (in-situ) advanced PG/ICS technology to Idaho industry partners.

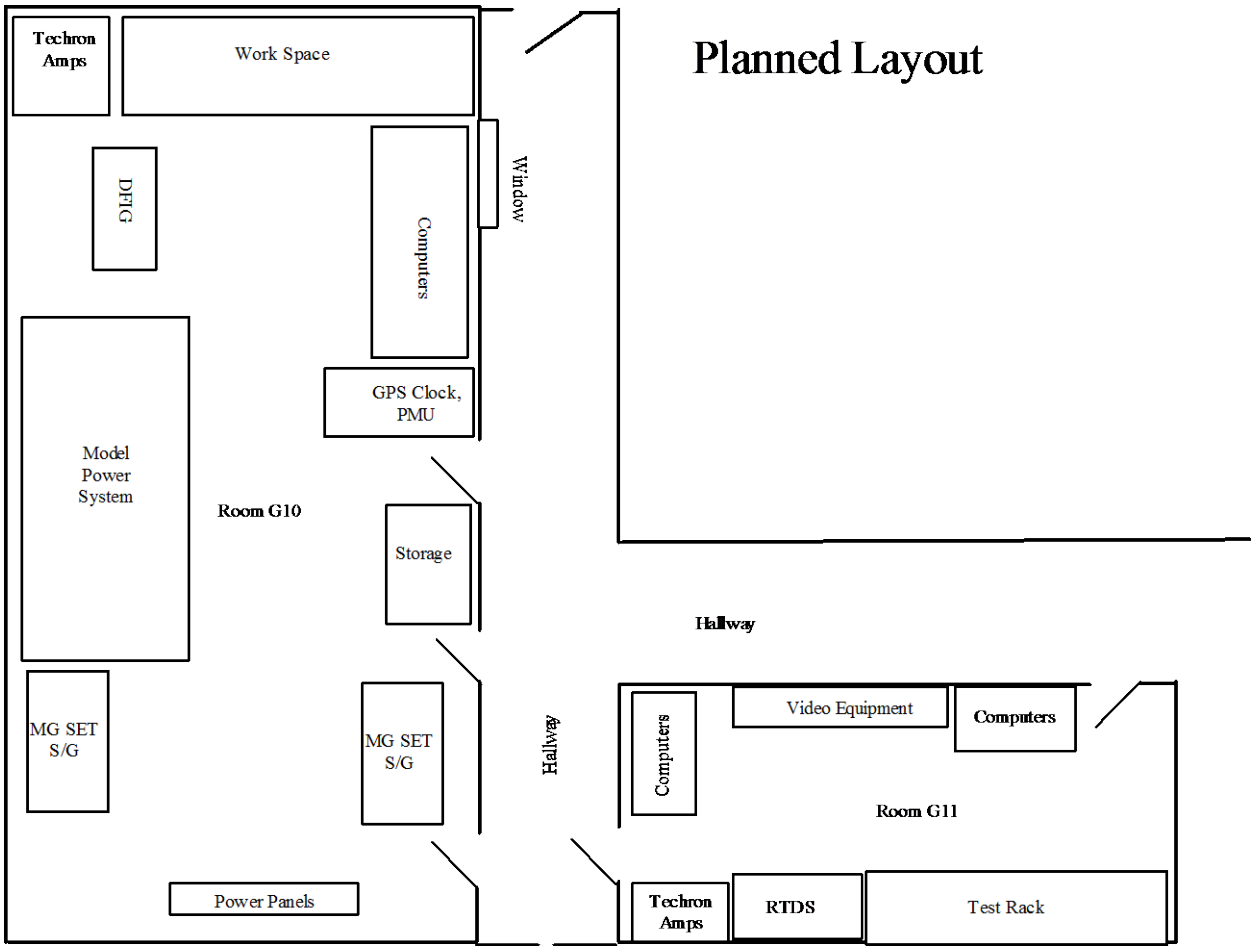

Figure 3: Illustration of Power Systems Laboratory Expansion.

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 test bed was remodeled and completed the end of November, two months behind schedule because of asbestos abatement in the new space. A contract was given to Schweitzer Engineering Laboratories for the industrial control equipment and RTDS upgrade. The equipment started to arrive in December, as shown in Figure 2. The existing RTDS and associated amplifiers were moved to the lab 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. The power lab has a secure connection to the RADICL lab, shown in Figure 8.

Figure 2: Some of the test equipment for the expanded power lab along with new equipment racks

Figure 3: Amplifiers moved and installed in the new space.

Figure 4: Some of the test equipment for the expanded power lab along with new equipment racks

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

Figure 6: Some of the test equipment for the expanded power lab along with new equipment racks

Figure 7: Testbed with the addition of the new RTDS NovaCor rack.

Figure 8: Students working in the RADICL lab.

The research team has recently received approval to set up a Cybersecurity Analytics and IoT Lab in the UI IRIC building. This lab will have secure connections to the power systems lab and to the RADICL lab, in addition to secure connections to the labs under development in Idaho Falls and Coeur d'Alene. Set up of this lab will take place in fall 2018.

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 they will be connected with the power security laboratory in Moscow through a VPN.

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 9. Kobalt workbench with HMI and PLC for Asset

1.2 Strengthen collaboration with Idaho industry and Idaho Universities

1.2.1 Industry and University Collaborations

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

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

(1) Ongoing research project as part of DOE Grid Modernization Lab project related to resilience metrics for power distribution systems.

(2) Collaboration on an ongoing LDRD proposal related to cybersecurity for industrial control systems, with collaboration from Virginia Commonwealth University.

(3) Collaboration course ECE 469/569: Resilient Control of Critical Infrastructure with collaboration between UI, BSU, and INL along with some interaction with Naval Post Graduate School, Weber State University, and Idaho State University.

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.

Brian Johnson and Yacine Chakhchoukh have been part of 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.

Brian Johnson was advisor for three industry sponsored senior design teams, one sponsored by Avista and one by Schweitzer Engineering Laboratories.

Yacine Chakhchoukh is having regular meetings with professors at Virginia Tech (Lamine Mili, Michael von Spakovsky, and Konstantinos Triantis). The team is writing a joint proposal with other professors at other universities to submit in March 2018 to the NSF. The title is: "Enhancing the resilience of interdependent power systems and emergency services via micro-grids" targeted starting date August 2018. For this project the cyber-security test-bed will be used in the research conducted at the University of Idaho. Collaboration will be started with AVISTA Corporation on this project.

Date: September 18, 2017: Visit and presentation: **Visitor/Speaker:** Dr. Svitlana Volkova, Senior Research Scientist, Data Sciences and Analytics Group, National Security Directorate, Pacific Northwest National Laboratory (PNNL). **Title:** Topic: Predicting the Future with Deep Learning and Signals from Social Media. Also, Dr. Volkova and a research and recruiting team from PNNL visited the University of Idaho and met with students and faculty.

Date: October 09, 2017: Visit and presentation: **Visitor/Speaker:** Ginger Wright, Program Manager for Domestic Nuclear Cybersecurity at Idaho National Laboratory (INL). CS Colloquium presentation, **Title:** Cyber Informed Engineering. Ms. Wright also met with College of Engineering faculty and students.

Date: November 27, 2017: Visit and presentation: **Visitor/Speaker:** Dr. Glenn A. Fink, Senior Cyber Security Researcher, Pacific Northwest National Laboratory (PNNL). CS Colloquium presentation, **Title:** Security and Privacy Grand Challenges for the Internet of Things. Dr. Fink also met with College of Engineering faculty and students.

Date: November 27, 2017: Presentation: **Visitor/Speaker:** Jason Dearien, Senior Application Engineer, Schweitzer Engineering Laboratories (SEL), **Title:** Requirements and Challenges of Building Software for Critical Infrastructure. Mr. Dearien also met with College of Engineering faculty and students after the presentation.

Date: Fall, 2017: Live Table Top Exercise: **Visitor/Speaker:** Dr. Jessica Smith, Cybersecurity Researcher, Pacific Northwest National Laboratory (PNNL), helped organize and participated in a critical infrastructure cybersecurity event tabletop exercise for University of Idaho students.

Date: Fall, 2017: Engineering Capstone Design Projects. **Customer:** Dr. Jessica Smith, Cybersecurity Researcher, Pacific Northwest National Laboratory (PNNL), is sponsoring two College of Engineering Capstone Design projects focused on cybersecurity of the Power Grid and Industrial Control Systems.

1.3 Foster technology transfer and commercialization through technology incubation

During this second year we have had several proposals accepted and submitted for research in this area:

1.3.1 Proposals

ACCEPTED

B.K. Johnson, H. Lei, Student Support for the 2018 International Conference on Probabilistic Methods Applied to Power Systems, National Science Foundation, $12,750

Y. Chakhchoukh, D. Conte de Leon, B.K. Johnson, H.L. Hess, H. Lei, "Designing and Evaluating an Energy Trading System for Prosumers," Avista Corporation, August 1, 2018—August 15, 2019, $89,771.

A. Ibrahim, T. Xing, J. Yuan, B.K. Johnson, "High Energy Efficient Aerogel-Glazing Coupled with Aerogel-Insulated Walls in Residential Buildings: Phase II," Avista Corporation, Aug. 1, 2018- August 15, 2019, $89,101.

H.L. Hess, B. Johnson, Y. Chakhchoukh, "Framework for Siting and Sizing Energy Storage for Enhanced Performance of the Avista System," Avista Corporation, August 15, 2017 - August 31, 2018, $83,712.89.

A. Ibrahim, B. Rezaie, B.K. Johnson, "Aerogel Insulation System: An Innovative Energy Efficient Thermal Wall," Avista Corporation, Sept. 1, 2017- August 30, 2018, $88,777.

B.K. Johnson, Y. Chakhchoukh and D. Conte de Leon, "Testbed for Power and Industrial Control Systems," Murdock Charitable Trust, May 18, 2017-August, 31, 2019, $284,500 (total project $872,407)

J. Alves-Foss, J. Song, "A Modular Approach to Cyber Security Learning: Enhanced with DARPA's DECREE for Cyber Security Laboratory Exercises", National Security Agency, Apr 2017- Apr 2018, $212,674

J. Song, "CRII: SaTC: Automatiing Fuzzing Based on Grammar Detected from User Input", National Science Foundation, Jan 2018 – Jan 2020, $173,782

J. Alves-Foss, J. Song, "Machine Learning and Path Finding: An Semi-supervised Approach to Vulnerability Analysis", Intel Corporate Research Council, Jan 2018 – Dec 2020, $299,724

J. Song, "Seed Grant: Automating Fuzzing Based on Grammar Detected from User Input", UI Office of Research and Economic Development, May 2018 – Aug 2019, $11,878

J. Song, J. Alves-Foss, “Automated Vulnerability Detection for Aerospace Systems”, Idaho NASA EPSCoR, May 2018 – Apr 2019, $44,982

SUBMITTED

J. Alves-Foss, J. Song, M. Haney, “JIMA: Assisting Developers via Semi-Automated Vulnerability Discovery and Repair”, DARPA, Nov 2018 – Apr 2022, $3,332,041

Craig Rieger and Tim McJunkin (INL), B.K. Johnson, Y. Chakhchoukh, H. Lei, R. Lew, and H.L. Hess (UI), “Real-time Sensing of Transient Occurrences through Resilient Design (ReSTORD),” INL LDRD, $900,000.

Y. Chakhchoukh (UI), L. Mili, M. von Spakovsky, and K. Triantis (Virginia Tech), CRISP “Type 2: Collaborative Research: Community Resilience via Micro-grids and Improved Emergency Services,” Submitted to NSF CRISP. $2,000,000 total budget.

D. Roberson, et. al, “Innovative AVR and Electronic Excitation Strategies for Synchronous Machines", $249,819, U.S.Department of Energy Office of Fossil Energy.

D. Roberson, et. al, ‘"Reconfigurable Feedback Control for Multiscale Structures Subject to Non-stationary Conditions", $416,737.40, U.S. Air Force Research Laboratory

D. Roberson (co-PI): “"CPS: Medium: Collaborative Research: An Integrated Sensor-Drone-Satellite Analyzer System to Enhance Soil-Crop Health", $824,138.95, National Science Foundation, USDA NIFA

D. Roberson (co-PI): “Integrated Front-End Control and Back-End Analytics for Solar PVs", $600,000, United States Department of Energy, SunShot SETO

D. Roberson (co-PI): "SaTC: EDU: Cyberphysical Systems Forensics and Reverse Engineering Lab and Curriculum Development", $298,684, National Science Foundation: Secure and Trustworthy Cyberspace

D. Roberson, H. Lei, Y. Chakhchoukh, “Smart Asset Health Management for Electric Power Systems,” Alfred P. Sloan Foundation, $241,342.20, 01/01/19-12/31/20

S. Sorour, M. Hefeida, Y. Chakhchoukh, “Fluid-Flow Electric Load Scheduling for Optimized Power Trading in Battery and Micorgid-enabled Smart Districts,” US-Egypt Joint Board on Scientific and Tech Coop, $199,617.50, 07/01/19-01/31/21

Haney, Michael; Computer Science, Roberson, Dakota; Electrical and Comp. Engineering, University of Idaho Idaho Falls
SaTC: EDU: Development of Reverse Engineering Laboratory and Curriculum; $ 300,000; October 1, 2018 to September 30, 2020 (2 years). NSF, Secure and Trustworthy Cyberspace, Education: SaTC:EDU.

Chakhchoukh, Yacine; Electrical and Computer Eng., Conte de Leon, Daniel; Computer Science, and Johnson, Brian K.; Electrical and Computer Eng. SaTC: CORE: Small: Cybersecurity Analysis of PMU-based State Estimation for the Smart Grid; $ 499,982; August 20, 2018 to August 19, 2021 (3 years). NSF, Secure and Trustworthy Cyberspace, SaTC, CORE Program.

1.3.2 Publications

PUBLISHED or ACCEPTED

Book Chapter: 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, to appear, 2018.

M. Ashrafuzzaman, H. M. Jamil, Y. Chakhchoukh and F. T. Sheldon, “A Best-Effort Damage Mitigation Model for Cyber-Attacks on Smart-Grids”, Proceedings of COMPSAC, Tokyo, July 23-27, 2018.

D. Roberson and J. F. O'Brien, "Loop-Shaping Methods for Multivariable Control Design for Stability Augmentation and Oscillation Rejection in Wide-Area Damping Using HVDC" in Elsevier Electric Power Systems Research

D. Roberson and J. F. O'Brien, "Variable Loop Gain using Excessive Regeneration Detector for a Delayed Wide-Area Control System" in IEEE Transactions on Smart Grids

D. Roberson and J. F. O'Brien, "A Feedback Perspective on Forced Oscillation/Small-Signal Stability Augmentation" in Proceedings of IEEE Power & Energy Society General Meeting

Y. Xia, B.K. Johnson, Y. Jiang, N. Fischer, and H. Xia, “A New Method Based on Artificial Neural Network, Wavelet Transform and Short Time Fourier Transform for Subsynchronous Resonance Detection,” *International Journal of Electrical Power and Energy Systems*, In Press.

A. A. Jillepalli, D. Conte de Leon, Y. Chackhchoukh, M. Ashrafuzzaman, B.K. Johnson, F.T. Sheldon, J. Alves-Foss, P.T. Tosic, M.A. Haney, “An Architecture for HESTIA: High-level and Extensible System for Training and Infrastructure Risk Assessment,” *Int. J.Internet of Things and Cyber Assurance,(IJITCA*), Volume: 01, Number: 02. PP 173-193. 21 pages. InderScience. June 2018.

Jillepalli, Ananth A.*; Conte de Leon, Daniel; Ashrafuzzaman, Mohammad+; Chakhchoukh, Yacine; Johnson, Brian K.; Sheldon, Frederick T.; Alves-Foss, Jim; Tosic, Predrag; Haney, Michael A., "HESTIA: Adversarial Modeling and Risk Assessment for CPCS," Proceedings of the 14th

IEEE International Wireless Communications and Mobile Computing Conference, (IWCMC-2018), 25-29 June 2018, Limassol, Cyprus, 08 pages. IEEE. June 2018.

Ashrafuzzaman, Mohammad+; Chakhchoukh, Yacine; Jillepalli, Ananth A.*; Tosic, Predrag T.; Conte de Leon, Daniel; Sheldon, Frederick T.; Johnson, Brian K.;, "Detecting Stealthy False Data Injection Attacks in Power Grids Using Deep Learning," Proceedings of the 14th IEEE International Wireless Communications and Mobile Computing Conference, (IWCMC-2018), 25-29 June 2018, Limassol, Cyprus, 08 pages. IEEE. June 2018.

A.I. Mohammad, T. Mort, J. Jeter, A. Hoth, J. Engund, B.K. Johnson, N. Fischer, K. Damron, "Turn-to-Turn Fault Protection for Dry-Type Shunt Reactors, *2018 IEEE Transmission and Distribution Conference and Exposition*, Denver, April 2018.

P. Khaledian, B.K Johnson, and S. Hemati, "Power Grid Security Improvement by Remedial Action Schemes Using Vulnerability Assessment Based on Fault Chains and Power Flow," *2018 Probabilistic Methods Applied to Power Systems (PMAPS)*, Boise, June 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.

Conte de Leon, Daniel; Stalick, Antonius Q.; Jillepalli, Ananth A.; Haney, Michael A.; Sheldon, Frederick T. (2017) "*Blockchain: Properties and Misconceptions*", Asia Pacific Journal of Innovation and Entrepreneurship, Volume: 11 Issue: 3, pp. 286-300, December 2017. https://doi.org/10.1108/APJIE-12-2017-034.

Conte de Leon, Daniel; Brown, Matthew G.; Jillepalli, Ananth A.; Stalick, Antonius Q.; Alves-Foss, Jim. *"High Level and Formal Router Policy Verification."* The Journal of Computing Sciences in Colleges, Volume 33, Number 1, pp. 118, October 2017. https://dl.acm.org/citation.cfm?id=3144631

Jillepalli, Ananth A.; Sheldon, Frederick T.; Conte de Leon, Daniel; Haney, Michael A.; Abercrombie, Robert K. "*Security Management of Cyber Physical Control Systems Using NIST SP 800-82r2*". In Proceedings of the 13th International Wireless Communications and Mobile Computing Conference (IWCMC), 26-30 June 2017, Valencia, Spain, IEEE. DOI: 10.1109/IWCMC.2017.7986568http://ieeexplore.ieee.org/document/7986568/

Conte de Leon, Daniel; Goes, Christopher; Jillepalli, Ananth A.; Haney, Michael A.; Krings, Axel. "*ADLES: Specifying, Deploying, and Sharing Hands-On Cyber-Exercises*", Journal of Computers and Security, To Appear, Elsevier 2018. https://www.journals.elsevier.com/computers-and-security

Jillepalli, Ananth A.; Conte de Leon, Daniel; Sheldon, Frederick T.; Haney, Michael A. "*Hardening the Client-side: A Guide to Enterprise-level Hardening of Web Browsers.*" In Proceedings of the 15th IEEE International Conference on Dependable, Autonomic and Secure Computing (IEEE DASC 2017). November 2017. IEEE.

Koganti, Venkata SreeKrishna; Ashrafuzzaman, Mohammad; Jillepalli, Ananth A.; Conte de Leon, Daniel; Sheldon, Frederick T.; *"A Virtual Testbed for Security Management of Industrial Control Systems."* In Proceedings of the 12th International Conference on Malicious and Unwanted Software (MALCON 2017). November 2017. IEEE.

S. Basumallik, S. Eftekharnejad, N. Davis, N. Nuthalapati, B.K. Johnson, "Cyber Security Considerations on PMU-base State Estimation," *Proceedings of the 2017 Cybersecurity Symposium.* Coeur d'Alene, Idaho, April 17-18, 2017

P. Penkey, H. Samkari, B.K. Johnson, H.L. Hess, "Voltage Control by Using Capacitor Banks and Tap Changing Transformers in a Renewable Microgrid," 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), April 23-26, 2017, Arlington Virginia

N. Fischer, B.K. Johnson, J.D. Law, A.G. Miles, "Induction Motor Modeling for Development of a Secure In-Phase Motor Bus Transfer Scheme," 2017 IEEE International Electric Machines and Drives Conference (IEMDC), Miami, FL May 22-25, 2017. Reviewed based on extended abstract)

N. Fischer, J.D. Law, A.G. Miles, B.K. Johnson, "Dynamic Modeling of an Improved In-Phase Motor Bus Transfer Scheme," *Proceedings of the International Conference on Power Systems Transients (IPST2017)*, Seoul, South Korea, June 26-29-18, 2017.

Anujan, B.K. Johnson, E.J. William, "Protection Studies of Geographically Dispersed Type 3 Wind Energy Systems," *Proceedings of the 2017 IEEE Power and Energy Society General Meeting*, Chicago, IL, July 2017

S. Chilukrui, M. Alla, B.K. Johnson, "Enhancing backup protection for thermal power generating stations using sampled values," *Proceedings of the 2017 North American Power Symposium*, Morganton, WV, September 17-19, 2017.

S. Basumallik, S. Eftekharnejad, N. Davis, B.K. Johnson, "Impact of false data injection attacks on PMU-based state estimation," *Proceedings of the 2017 North American Power Symposium*, Morganton, WV, September 17-19, 2017.

H. Beleed and B.K. Johnson, "Comparative study on IEEE12 bus system with D-FACTS devices in different simulation tools," *Proceedings of the 2017 North American Power Symposium*, Morganton, WV, September 17-19, 2017.

W. Parker, B.K. Johnson, C. Rieger, T. McJunkin, "Identifying critical resiliency of modern distribution systems with open source modeling," *Proceedings of Resilience Week 2017*. Wilmington DE, September 19-21, 2017

V. Koganti, M. Ashrafuzzaman, A. Jillepalli, F.T. Sheldon, B.K. Johnson, “A Virtual Testbed for Security Management of Industrial Control Systems,” MALCON 2017, Malware Conference, January 2018, San Juan, Puerto Rico (delayed due to hurricane damage)

N. Nagarjuna, J. Alves-Foss, J. Song. “Developing a Taxonomy of Cyber Attacks in WAMS”. In CyberSec ’18: Fifth Cybersecurity Symposium, Coeur d' Alene, ID, USA. April 2018, 6 pages.

X. Yang, Z. Yang, H. Y. Sun, Y. Fang, J. Y. Liu and J. Song, “Formal Verification for Ethereum Smart Contract Using Coq”, International journal of Information and Communication Engineering, 12(6), 2018.

SUBMITTED

Jillepalli, Ananth A.; Conte de Leon, Daniel; Sheldon, Frederick T.; Haney, Michael A. *"Enterprise-level Hardening of Web Browsers."* Submitted to Springer Security Informatics Journal. https://security-informatics.springeropen.com/

Steiner, Stuart; Jillepalli, Ananth A.; Conte de Leon, Daniel; *"Applying the Principle of Least Privilege to Harden Web Application Security."* Submitted to Springer Security Informatics Journal. https://security-informatics.springeropen.com/

Jillepalli, Ananth A.; Conte de Leon, Daniel; Sheldon, Frederick T.; Chakhchoukh, Yacine; Johnson, Brian K.; Haney, Michael A. *"An Architecture for HESTIA."* Submitted to 24th National Conference on Communications (NCC 2018). February 2018. Hyderabad, India.

Steiner, Stuart; Jillepalli, Ananth A.; Conte de Leon, Daniel; *"Hardening Web Applications Using a Least Privilege DBMS Access Model."* Submitted to 24th National Conference on Communications (NCC 2018). February 2018. Hyderabad, India.

IN PREPARATION

Jillepalli, Ananth A.; Conte de Leon, Daniel; Bhandari, Venkata A.; Steiner, Stuart; Alves-Foss, Jim *"Analysis of Web Browser Security Configuration Options."* To be submitted to IEEE Access Journal. http://ieeeaccess.ieee.org/

Ashrafuzzaman, Mohammad; Jillepalli, Ananth A.; Chakhchoukh, Yacine; Conte de Leon, Daniel; Sheldon, Frederick T.; "*Detecting Stealthy False Data Injection Attacks in Smart Grid Using Deep Learning"*. To be submitted to Future Generation Systems Journal

1.3.3 Presentations

. Title: Application of Protection Challenges for Connecting to a Microgrid
Place**:** Idaho Commons.
Co-sponsored by the IEEE Palouse Section and the University of Idaho.
Date&Time: September 14, 5:00pm
Speaker: John Kumm, P.E., POWER Engineers.

Title: Traveling Wave Technology for Accurate Fault Location and Ultra-High Speed Line Protection
Place: Schweitzer Engineering Laboratories Event Center.
Co-sponsored by the IEEE Palouse Section and the University of Idaho.
Date&Time: September 25, 6:00pm
Speaker: Venkat Mynam, Principal Research Engineer, Schweitzer Engineering Laboratories, Inc.

Title: Remedial Action Scheme Preventing Country-Wide Blackout
Place: Idaho Commons, University of Idaho.
Co-sponsored by the IEEE Palouse Section and the University of Idaho.
Date&Time: October 10, 6:00pm
Speaker: Brian Clarke, P.E., Automation Engineer, Schweitzer Engineering Laboratories, Inc.

Title: Smart Cities for Promoting Global Sustainability
Place: Washington State University.
Co-sponsored by the IEEE Palouse Section and the University of Idaho.
Date&Time: November 7, 11:00am
Speaker: Mohammad Shahidehpour, University Distinguished Professor, Bodine Chair Professor of Electrical and Computer Engineering, and Director of the Robert W. Galvin Center for Electricity Innovation at Illinois Institute of Technology (IIT)

1.4 Strengthen and expand the workforce

In our proposal we stated that accomplishments in this Objective would not occur until year 3. However, our team has already made some progress, namely

INL: Four Cybersecurity students participated in internships at Idaho National Laboratories during the summer of 2017. These students worked on projects related to the cybersecurity with a focus on industrial control systems and critical infrastructure protection.

PNNL: Three Cybersecurity students participated in internships at Pacific Northwest National Laboratory during the summer of 2017. These students worked on projects related to the cybersecurity of industrial control systems.

November, 10-11, 2017: NICCDC: NIATEC Collegiate Cyber Defense Competition, Pocatello, Idaho: Eight University of Idaho students (7 from Moscow and 1 from Idaho Falls) traveled and participated in this live cyber defense competition organized yearly by NIATEC at Idaho State University.

2 Summary of Budget Expenditures

Salaries	$460,715
Fringe	$128,732
Travel	$10,000
Operating	$78,153
Tuition	$22,400
Total	**$700,000**

3 Demonstration of Economic Development/Impact

1.1 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.

1.2 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.

1.3 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.

The IGEM team of Co-PIs engaged in discussions with Industry during the latter half of Spring 2017 Semester during both the CS and ECE Industrial Board meetings regarding many issues associated with building capacity here within the respective departments, understanding industry needs as they relate to curriculum requirements and student hands-on research experience. Some of the companies represented include PNL, INL, SEL, BPA, Avista, Itron, Clearwater Analytics, Cradle Point, Chief Architect, AHA, Micron, Google, Apple and Boeing. Not all of these companies are represented on our IABs. In the case of Google and Apple some of the PIs had separate meetings discussing industry needs and expectations. These meetings were conducted during the UI Career Fairs that are held in the early part of each (Fall and Spring) semester.

Additional opportunities to engage with the private sector include the Cybersecurity Symposium which was held in Coeur d'Alene Apr. 17-19, 2017 with the theme "Cybersecurity for a cyber and physical world." There were numerous paper and poster presentations over these three days (see: http://cybersecuritysymposium.com/schedule.html).

2018 IEEE PMAPS Conference; we presented and were a co-sponsor

1.4 Jobs created

None this past year.

1.5 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	
Yacine Chakhchoukh	
Jia Song	
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 year we plan to:

- Continue our research work,
- 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
- Leverage these activities with our industry and academic partnerships

6 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	$10,775	$31,529.41
Frederick Sheldon, Chair of Computer Science and Project Co-PI	$93,583	$108,738.56
Michael Haney, Assistant Professor in Computer Science and Project Co-PI	$48,906	$48,906.00
Yacine Chakhchoukh, Assistant Professor in Electrical and Computer Engineering	$93,850	$93,849.60
Dakota Roberson, Assistant Professor in Electrical and Computer Engineering	$95,000	$95,004.00
Jia Song, Assistant Professor in Computer Science Department		$60,308.10
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
Matchya Raju Alla, Graduate Research Assistant	$35,343	
Venkata SreeKrishna Koganti, Graduate Research Assistant		$1,920.00
Mohammed Allehyani, Research Assistant		$1,460.00
Mohammad Ashrafuzzaman, Student Temporary Help		$16,320.00
Ananth Jillepalli, Student Temporary Help		$16,240.00
Maadhavi Sathu, Student Temporary Help		$9,430.72
Ibukun Oyewumi, Student Temporary Help		$7,675.00
Chiranjeevi Chelluboina, Temporary Help		$4,620.00
Hari Prasad Challa, Graduate Assistant		$2,244.00
Total Student Expense	$35,343	$59,910
E. FRINGE BENEFITS		
Rate of Fringe (%)	$ Amount Requested	Actual $ Spent
Fringe Benefits	$128,732	$115,211.69
Graduate Student Tuition and Fees	$22,400	$23,658.00
PERSONNEL SUBTOTAL:		**$637,115.08**
F. EQUIPMENT: (List each item with a cost in excess of $1000)		
Item/Description	$ Amount Requested	Actual $ Spent
1. Test Bed		$19,663.13
EQUIPMENT SUBTOTAL:	**$52,600**	**$19,663.13**
G. TRAVEL		
Description	$ Amount Requested	Actual $ Spent
1. Transportation/Airfare		$2,965.47
2. Per diem		$7,162.46
TRAVEL SUBTOTAL:	$10,000	**$10,127.93**

H. PARTICIPANT SUPPORT COSTS:		
Description	$ Amount Requested	Actual $ Spent
PARTICIPANT SUPPORT COSTS SUBTOTAL:		

F. OTHER DIRECT COSTS:		
Description	$ Amount Requested	Actual $ Spent
1. Operating Expenses – Includes Conferences/Registration; advertising; meeting expenses; supplies; and other expenses		$33,093.86
OTHER DIRECT COSTS SUBTOTAL:	$25,000	**$33,093.86**
TOTAL COSTS (Add Subtotals):		**$700,000.00**
TOTAL AMOUNT REQUESTED:		**$700,000.00**
TOTAL AMOUNT SPENT:		**$700,000.00**