D. Itemized Project Budget

We propose implementing a Distributed Testbed for the Smart Grid and Industrial Control Systems Cybersecurity Research. This testbed will allow research and development of novel and secure techniques and algorithms for securing today and tomorrow's Power Grid 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 proposed testbed will expose hardware-in-the-loop, 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.

D.2 Introduction and Justification

Today’s economy and society depends on the stable, efficient, and secure operation of critical infrastructure systems such as the power grid. Likewise, modern manufacturing and production facilities depend on the stable, efficient, and secure operation of industrial control systems for maximum productivity and reduced overall costs. The number of cybersecurity threats and the success rate of cyber-attacks on current Information Technology and Operational Technology systems poses an immeasurable amount of risk to these critical infrastructures on which our society and economy depend. Recent high-profile cyber-attacks and data breaches attest to this risk. Hence, research, development, and testing of innovative techniques and algorithms for securing critical industrial control systems is imperative.

The special characteristics of most industrial control systems, such as, cyber-physical, real-time, diverse, and distributed, preclude us from directly applying cybersecurity techniques and algorithms used today within other cyber-domains. Many characteristics of the operation of industrial control systems and the smart grid can be simulated in software alone. However, while performing industrial control system cybersecurity evaluations using computer simulations provides preliminary insight, these simulations are not realistic enough to fully represent the complexity of today’s interconnected cyber-physical systems. This is especially true for the evolving power grid called the smart grid. Using operating control systems for research and testing is not possible because of the sensitivity of the researched topics and the potentially catastrophic consequences. This justifies the necessity for a specialized and distributed testbed to enable research and development of techniques and algorithms for cybersecurity and secure control of industrial control systems and the smart grid. Such techniques must be developed and tested using an environment that accurately emulates the behavior of today's control systems and also the physical system under control.

The proposed testbed will be centered at the University of Idaho's (UI) Moscow campus in two current laboratories leveraging existing computing hardware and infrastructure. In an attack-defend scenario, these may act as measurement and control and cyber analysis centers, respectively. In addition, it will have hardware and access endpoints at UI campuses in Coeur d’Alene and in Idaho Falls. Combined, these may act as distributed and geographically remote subsystems, such as, a power substation or field devices. The testbed will include new power control equipment, a dedicated network, and video/audio connectivity for four labs in separate locations: 1) the Power Systems Laboratory, 2) the Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL), the Industrial Control Systems and Cyber Security laboratories in 3) Coeur d’Alene and 4) Idaho Falls. UI has been rapidly expanding its faculty at these campuses. Six new faculty members with expertise in computing, cybersecurity, power, and control are being hired, four this year and two next year. The proposed testbed will be accessible to researchers and practitioners at UI and partner organizations. The testbed will enable a type of research on smart grid and industrial control systems cybersecurity not possible today at any educational institution in Idaho or the Pacific Northwest. It will enable the investigation, development, and testing of solutions that improve the resiliency and security of the smart grid and ICS. Innovative solutions will be developed by combining computer and digital control security and power system control and reliability approaches without compromising the real-time operational priorities of ICS systems. Developing solutions that improve the cybersecurity of control systems and the smart grid that can reliably operate within today’s and tomorrow’s complex control and power systems constitutes practical research very much needed by the power, manufacturing, and other modern industry sectors.

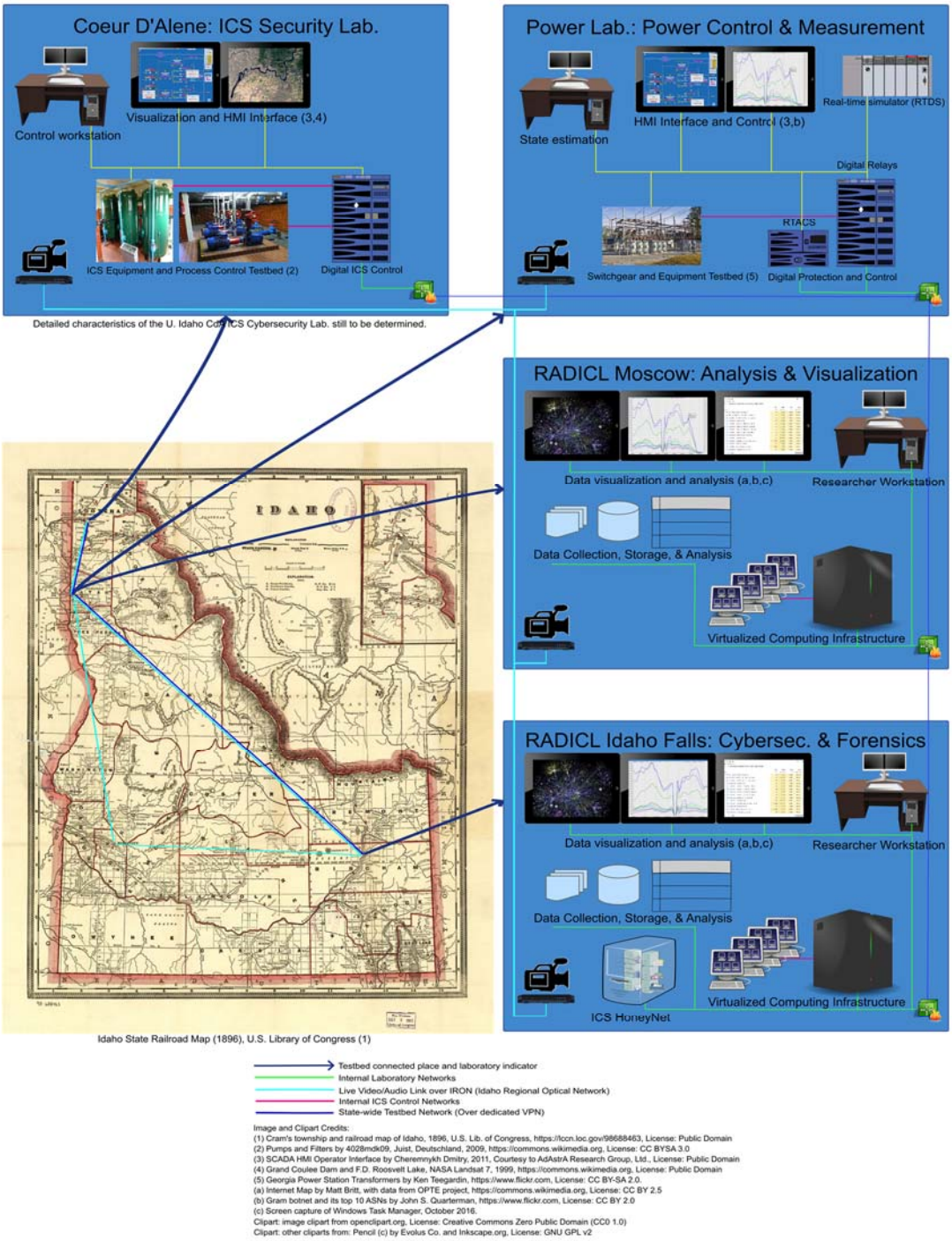

Figure 1. Idaho ICS Cybersecurity Testbed: Concept Drawing

Figure 1 above, is a concept drawing of the proposed testbed. In the figure, the testbed composition and connectivity is shown. The four laboratories are shown with their expected industrial control system cybersecurity focuses and their respective places within the State of Idaho. The intent is that these four laboratories will complement each other to offer different functionalities and capacity for research and instruction on the cybersecurity of smart grid and industrial control systems. Through this testbed, these laboratories will be connected through a dedicated computer network and a video/audio network. This will enable the creation of a distributed and hence more representative testing environment and also sharing of the testbed and other laboratory functionality across the State.

D.3 Why Is This Project Needed?

Power systems are evolving toward what is called the smart grid where improved communication and distributed control enable increased integration of renewable energy sources such as solar and wind with classical sources such as coal, nuclear, natural gas, and hydroelectric. The rapid development of energy storage technologies will aid this evolution. These trends will result in an electric grid which is more sustainable that will help address current environmental concerns [1,2]. Furthermore, allowing users to participate in generation and including them as active actors of the energy process is in accordance with the objectives of the future smart city [3]. Indeed, future power generation will be distributed through the use of rooftop photovoltaic (PV) panels and other types of local units. This implies that households and commercial and industrial users could be active players in both generation and consumption.

At the same time, integrating these components creates several challenges to grid management. Indeed, to allow efficient and reliable operation, communication and control networks must be integrated into power control systems making them more complex and potentially more vulnerable. Cyber-attacks could target the communication network, corrupt data, and impact different control and protection actions on the power grid [4-6]. These cyber-attacks could be generated by malicious individuals or organizations through the Internet connected to enterprise Information Technology (IT) or Operational Technology (OT) systems and could disrupt or alter the normal operation of the grid which could result in great losses [6].

Similar characteristics and current problems apply to other Industrial Control Systems (ICS) such as natural gas and oil pipelines and chemical and industrial process control.

Hence, it is necessary, and even urgent, to improve the cybersecurity of the Smart Grid [6,7] and Industrial Control Systems (ICS).

This testbed will enable types of ICS cybersecurity experiments not possible today at and educational institution in the Northwest. We intend to investigate and develop, among other topics, procedures and metrics to assess the cyber-vulnerabilities and their consequences on the power or smart grid and ICS, propose novel procedures to detect and isolate cyber-attacks, counter the impacts resulting from attacks, and take adequate correcting actions to ensure a reliable, efficient, and economical operation of the system. Research and development of these and other topics will be enabled by the proposed Smart Grid and ICS Cybersecurity Testbed.

The availability of this testbed will also increase collaborative research projects at the University of Idaho and across the State. As a result, cross-disciplinary research will be conducted more effectively by combining available expertise in computer science, cybersecurity, electrical engineering, and power systems operation and control. The testbed has the potential for greatly increasing collaborative work with local and regional power companies and Idaho National Laboratory (INL) for R&D, testing, technology transfer, and education and training. INL in Idaho Falls is a world leader in ICS cybersecurity.

In addition, the testbed will allow hands-on graduate and undergraduate training and research where the students and researchers could be both potential attackers and operators, i.e., defenders. A new hands-on course will be introduced in the curriculum with this goal. The new course will include the fundamentals and computing tools used for control of the smart grid and cybersecurity concepts and techniques. Cross-disciplinary instruction is needed for future power, industrial control, and cybersecurity engineers to be able to work seamlessly in industry.

G. Full Project Description

G.1 Advantages of the Testbed

If funded, the advantages of this testbed will be:

1) **Accurate Match with Real Systems:** The distributed nature of the testbed and the geographical distance between its components will enable us to more accurately simulate current large distributed industrial control systems such as the power grid. Communication systems latency and jitter are a major concern in real-time distributed systems. The proposed geographically distributed testbed will create a system with real network latency and jitter and avoid the drawbacks of needing to simulate these in

software.

2) **Increased Researcher Access:** The four locations within three separate University of Idaho campuses located in Northern and Southeastern Idaho will greatly increase access to the resources and functionality offered by the testbed. UI has been rapidly expanding its faculty at all these campuses with the support from the State of Idaho. Six new faculty members with expertise in computing, cybersecurity, power, and control, are being hired at UI, four this year and two next year. Four of these new faculty hires are within focus-area of cybersecurity of the smart grid and industrial control systems.

3) **Increased Third-Party Access and Partnerships:** The new networking and video/audio equipment will enable external practitioners and engineers to access the testbed facilities remotely and to collaborate with UI researchers in common projects. This will benefit utilities and other external partners as well as increase the opportunities for research partnerships. For example, faculty at UI have strong ties with Idaho National Laboratory (INL). INL is a Department of Energy R&D lab, runs the Dept. of Homeland Security ICS-CERT, and is a leader in ICS Cybersecurity.

4) **Adversarial Model and Competitions:** This testbed will enable researchers and practitioners to design and carry out power and industrial control systems attack-defend scenarios. These scenarios are extremely valuable for the training of engineers and practitioners in cybersecurity of ICS. They are also extremely valuable to the testing of new cyber-detection and cyber-defense techniques, or combinations of these techniques.

5) **Connected Complementary ICS Systems:** The four laboratories proposed to integrate this testbed offer complementary functionalities all focused on the power and smart grid, industrial control systems, and cybersecurity. This testbed will potentiate the shared use of these functions. In addition, the complementary functionality in these laboratories is expected to be further enhanced in the near future with additional hardware not part of this proposal.

5) **Potential Connection with Boise State ICS Cybersecurity Laboratory:** We have established contact with Boise State University to connect this testbed to their upcoming Industrial Control Systems cybersecurity laboratory funded by the State of Idaho. If this collaboration is crystallized and the connection is made, this will further increase the reach and usefulness of the testbed.

G.2 Detailed Description and Characteristics of the Testbed

The proposed testbed will be distributed and include new power control equipment, a dedicated network, and video/audio connectivity for four labs in four separate locations in three cities in Northern and Southeastern Idaho. The lab names and locations are: A) the Power Systems Laboratory, Moscow, B) the Reconfigurable Attack-Defend Instructional Computing Laboratory for cybersecurity (RADICL), Moscow, C) the Industrial Control Systems and Cybersecurity lab in Coeur d'Alene, and D) the ICS-RADICL Cybersecurity and Forensics Laboratory in Idaho Falls. The four laboratories included in this testbed offer complementary functionality and hardware assets and these functionalities will be greatly enhanced by this testbed:

A) The Power Laboratory, University of Idaho, in Moscow, Idaho:

This laboratory currently offers power control equipment and control systems analysis functionality essential to carry out power and smart grid cybersecurity research. The equipment in this laboratory will be enhanced and updated by adding: a Real-Time Distributed Simulator (RTDS), 4 substation remote terminal units (RTUs), 4 Substation Real-Time Automation Controllers (RTACs), 2 protective relays and Phasor Measurement Units (PMU), 2 integrated substation communication controllers, 4 time servers, and 4 computers and monitors for digital equipment management and control. In addition, all networking and security appliances needed to connect this equipment to the rest of the testbed through an internal dedicated research and control network. Also, high definition video and audio equipment will be installed to virtually connect the space in this laboratory to the RADICL Moscow and the ICS-RADICL in Idaho Falls.

B) The Reconfigurable Attack-Defend Instructional Computer Lab (RADICL), Moscow, Idaho:

The RADICL computing laboratory is a specialized laboratory where students and researchers can design, implement, and deploy networking and cybersecurity experiments. Through the use of a virtualized infrastructure, the lab offers an isolated environment in which experiments with hundreds

of (virtual) computers and networks can be designed and deployed. The lab also supports attack demonstration and mitigation experiments and tutorials and attack-defend scenarios. For this testbed, this laboratory will be enhanced with a visualization center. This visualization center will enable research on situational awareness and attack detection and visualization techniques and algorithms. In addition, high definition video and audio will be added to connect with the rest of the testbed. This laboratory will be the main computation center for the testbed.

C) The Industrial Control Systems Cybersecurity Laboratory, Coeur d'Alene, Idaho:

As one of the distributed components in this testbed, we propose acquiring and installing 6 workstations with access to their respective Remote Terminal Units (RTUs). This will simulate a small control system or power station. This Industrial Control Systems Cybersecurity Laboratory, which is currently in its design stage, is part of the University of Idaho's efforts to increase its teaching, training, and research capacity in Computer Science and Cybersecurity in Northern Idaho. This with the support from the State of Idaho. The area of reach includes the localities of Coeur d'Alene, Post Falls, Spokane, and Spokane Valley, a wide area with more than 600,000 people and many technology companies. The new equipment will allow researchers and practitioners in Northern Idaho to connect to the testbed, collaborate in research, and actively participate in attack-defend scenarios among other collaborative activities. The equipment will also provide distributed and geographically disperse control equipment, hence increasing the fidelity of the experiments.

D) The Industrial Control Systems RADICL Laboratory (ICS-RADICL) in Idaho Falls, Idaho:

The second geographically distributed component will be located in the ICS-RADICL hosted at the Center for Advanced Energy Studies (CAES) in Idaho Falls, Idaho. The equipment and functionality here will be similar to the equipment and functionality described in point C). The ICS-RADICL laboratory, also currently in design stage, is part of the University of Idaho's efforts to increase its research and graduate education capacity in Idaho Falls, particularly in the focus-area of Cybersecurity of Industrial Controls Systems. The area of reach includes the localities of Idaho Falls and Pocatello, a wide area with more than 100,000 people and home to Idaho National Laboratory and Idaho State University. This addition will allow researchers and practitioners in Southeastern Idaho to connect to the testbed, collaborate in research, and actively participate in attack-defend scenarios among other collaborative activities. Similarly to C), this equipment will provide distributed and geographically disperse control equipment. In addition, a high definition video/audio system is currently being installed in this laboratory but which is not a part of this proposal's budget.

G.2 Initially Proposed Research Projects that will Use the Testbed

We are interested in securing the Energy Management Systems (EMS) used by power operators to monitor and operate the future grid at control centers. As explained, the future smart grid will rely more heavily on automatic decisions and control actions taken on the cyber-domain. Different cybersecurity studies of EMS applications could be enabled by the implementation of the proposed testbed. We are also interested in the development of novel attack detection and situational awareness approaches.

We have developed practical algorithms that will notify the operator at the control center when abnormal measurements are detected. These algorithms are data-driven and power system model-based approaches that could improve the cybersecurity [8-13]. Preliminary simulation studies have shown improved cybersecurity on simple power models. The simulations also revealed the necessity to implement the proposed approaches in a distributed fashion to reduce the computational burden. The testbed is necessary to research the cybersecurity further and produce realistic, innovative and applied research that account for the complexity and the different interactions between the system part and the cyber part of the smart grid in real time conditions. Some of the immediate cybersecurity research topics that we are interested in, and for which the development of the testbed is necessary to extend the obtained preliminary simulation results, are discussed in this section.

Cybersecurity analysis of power state estimation:

Background:

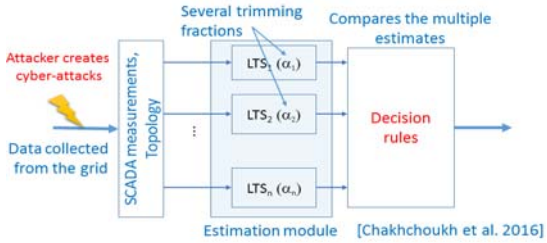

Figure 1. Detecting cyber-attacks by comparing multiple estimators with different robustness characteristics.

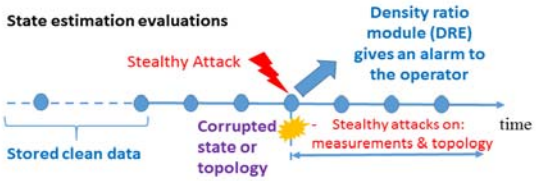

Figure 2. Machine learning technique that detects attacks using a learned model from stored clean data.

The power state estimation (SE) is an important module in the EMS which impacts several other EMS applications [14]. The goal of SE is to determine the voltage magnitudes and phase angles at different buses or substations of the power grid. The SE allows the efficient monitoring, operation and control of the power system. In practice, power companies execute a static power state estimation at regular time intervals, which means that measurements are sensed using Supervisory Control and Data Acquisition (SCADAs) units at Remote Terminal Units (RTUs) and communicated to the central control center. The SCADA measurements consist of a large number of power injections, power flows, voltage and current magnitudes at different locations of the grid sensed every 2 to 5 s. The state of the grid is computed at regular intervals, i.e., every several seconds to a few minutes. Recently, Phasor Measurement Units (PMUs) are being deployed in power systems where they deliver 30 to 120 measurements every second. PMUs measure directly the power states at their installed buses with high accuracy and at a much higher reporting rate than the SCADAs [15]. However, the number of installed PMUs is still limited in practice and it is necessary to combine both SCADAs and PMUs to run a hybrid SE.

Recently, the authors in [16] showed that an intruder could target the SCADA measurements and modify the power state in a stealthy fashion. This means that the state is changed by the malicious measurements while the bad data modules available at the control center do not detect any suspicious data. The operator is misled by this modified state which degrades the normal grid operation. This concern has motivated several researchers in different engineering areas such as computer science, communication networks, signal processing, control and power systems to investigate the state estimation vulnerabilities towards cyber-attacks and propose different ways to overcome or reduce the impacts of adverse intrusions. As discussed in [17], the research could be classified in three categories: 1) vulnerability analysis of SE, 2) consequence analysis on the power grid and 3) countermeasures development.

The security of SCADAs is a major concern since their use is pervasive. SCADA systems require innovative cybersecurity tools that go beyond Information Technology (IT) available solutions [4]. For example, SCADAs installed in power systems are generally cheap, vulnerable, and have long life cycles (a few decades). This means that their defense should be adaptable and with continuous updates. This implies that securing the EMS at control centers is crucial before deploying the future smart grid.

Procedure:

Dr. Chakhchoukh has studied the vulnerabilities of the hybrid SE towards cyber-attacks. In [8], Dr. Chakhchoukh et al. researched a more dangerous case for the operation than the case considered in [16] where both the state and the topology of the grid were targeted by cyber-attacks [8,18]. The topology of the grid reflects the connectivity of the power system and is updated constantly over time in the topology processor. In this context, Dr. Chakhchoukh et al assessed the cybersecurity of power system static state estimation (SE) in the possible presence of phasor measurement units (PMUs). Attack scenarios were outlined considering the number of attacked sensors, a decomposition of the power system to maximize robustness, and whether a Direct Current (DC) or Alternating Current (AC) formulation is used by the operator. Some possible solutions and remedial actions were proposed in the study. Robust state estimation methods were evaluated and compared in the presence of different configurations of attacks through Monte Carlo simulations on the simulated standard IEEE 14- and IEEE 30-bus systems [19].

Dr. Chakhchoukh et al. considered in [9] multiple robust estimators with different robustness properties

to improve the overall cybersecurity of power state estimation. The proposed approach could reduce the investment in expensive secure sensors. Specifically, Dr. Chakhchoukh et al. proposed to run several robust least trimmed squares (LTS) estimators [20] with different breakdown points or rejection percentages in parallel to improve the detection of cyber-attacks targeting both the measurements and the topology of the grid (See Fig. 1). The proposed method was compared with existing practical error detection methods and was shown to be effective in improving the overall cybersecurity of power systems such as the IEEE 14- and IEEE 30-bus systems [19].

To detect the presence of stealthy cyber-attacks, Dr. Chakhchoukh et al. followed in [10] a statistical outlier detection approach using a recently proposed machine learning technique called density ratio estimation (DRE). The proposed DRE has been researched by our collaborators where they have implemented this method for different industrial applications [21]. The DRE offers an improved detection especially since the technique does not require attack models when compared to other machine learning techniques implemented recently in the smart grid literature such as the Support Vector Machine [22]. The simulations were conducted on the larger IEEE 118-bus system where multiple time scans were merged together to enhance the cybersecurity for static state estimation as illustrated in Fig. 2.

At the same time, Dr. Johnson has an ongoing NSF project in partnership with Syracuse University treating the impact of cyber-attacks on phasor measurements and the impact of these attacks on hybrid state estimation schemes that utilize both SCADA data and phasor measurement units. The project will investigate the impact of data intrusion on PMU devices and SCADA systems on power system operation and planning. The outcomes will identify cyber-attacks that can result in cascading blackouts as well as the most critical measurements in power systems that are likely to be targeted by cyber threats. In addition, the findings of the proposed project will establish the foundations for modifications to protection schemes that are able to take action to respond both to cyber-attacks and faults due to accidental faults and abnormal operating conditions.

Scientific Significance:

While the proposed methods were very effective and promising on computer simulated data and theoretically justified, their performance and implementation rely heavily on the power system complexity and collected data used during the estimation or the learning process. The collected data should be as realistic as possible to validate the effectiveness of the proposed methods in practical control centers permitting their real implementation. The proposed cybersecurity testbed will allow researchers to collect large amounts of data from SCADAs and PMUs to assess the performance of the proposed methods in real life conditions. Investigating the sensitivity of the proposed machine learning methods, for example, when attacks are present in the learning process is of great interest. Furthermore, the cyber-attacks considered were theoretically stealthy attacks as proposed by several authors [16,17]. It would be more realistic to collect and separate between two cases: a) cyber-attacks generated by humans such as students and researchers and b) cyber-attacks generated by malicious algorithms and computing devices. For example, cyber-attack data collected from students and researchers in the RADICL cybersecurity laboratory could be used to implement further machine learning techniques that need models of attacks in their learning process. Other approaches such as considering a game theoretical approach to investigate the subject will be enabled by the testbed and the obtained data. Novel solutions against topology attacks such as providing deliberately false information to the intruders in order to mislead potential adversaries and maximize the detection of their attacks will be investigated on the testbed. Optimization algorithms that can find the most sensitive sensors to be secured will be developed. Other conditions such as denial of service type attacks will be studied on the testbed.

Dr. Chakhchoukh et al. also evaluated the execution time of the algorithms on personal computers considering mainly simplistic simulations which did not reflect the complete complexity of the real time behavior and component interactions of large power systems. For example, the communications network was not considered in the model. It was also observed that some sophisticated methods are computationally heavy and need to be executed in parallel or in a distributed fashion. An important research problem is determining how to distribute such algorithms to minimize the execution time while maximizing detection of cyber-attacks. These proposed methods should be extended to run on realistic-sized systems with with PMUs, SCADAs, and realistic representations of the different power system components. The testbed will permit these studies to be conducted.

Tracking the power grid states with Phasor Measurement Units (PMUs):

Background:

Several authors have proposed recently to reconstruct the power states from PMU measurements to increase the SE resolution in order to track the rapid changes expected in the future smart grid [23-25]. This could be used, for example, to monitor voltage sags and collapses which is not always possible with low frequency reporting SCADAs as discussed in [25]. The SE will be refreshed very frequently (i.e., every a few fractions of a second) which will completely change the real-time control of the power grid. For this case, the cybersecurity becomes even more challenging since the procedure will be fully automatic and the algorithms implemented to secure the operation should converge very fast. However, many of the recent works in this area are still at the stage of implementing new methods without considering in detail the question of cybersecurity which is still at its beginning for reconstructing the power states. Reference [25] proposed a method that provides robustness against random errors occurring in PMU sensors but sophisticated cyber-attacks were not studied.

Procedure:

Dr. Chakhchoukh et al. proposed in [12] to exploit the time and space correlation or dependence in the PMU measurements in order to provide rejection of cyber-attacks and improve the SE cybersecurity and accuracy. This improvement is introduced thanks to the availability of large amounts of data sensed from PMUs. Robust signal processing techniques [20] were exploited to fit multichannel or vector autoregressive (VAR) models to buffered signals from adjacent PMUs. The buffering allows to account for the non-stationarities present in real power systems [26-29]. A theoretical analysis was provided to explain the improvement by higher PMU sampling rates and longer periods of SE evaluations. The proposed technique provided a sophisticated defense mechanism against stealthy cyber-attacks and was shown to make the task of cyber-attackers extremely complicated and tedious. The attacker needs to attack all correlated PMUs and over long-periods of time to break the implemented defenses. The proposed method offers an effective protection of the SE against cyber-attacks targeting PMUs, SCADAs and topology processors securing the whole SE. The preliminary simulation results have considered a SE resolution of 2s. This implies that every 2s, a new estimate of the grid state is obtained, which might be considered to be a low resolution in the future smart grid.

Scientific Significance:

We are interested in investigating the subject of increasing the SE resolution while insuring improved cybersecurity to allow for tracking the fast changes in future power systems. This is necessary since the integration of renewable generation, free-electricity markets, demand response will increase the need for more frequent control and monitoring of the grid. For example, our recently proposed approach [12] should be extended to increase the SE resolution which will permit tracking the smart grid states more accurately. The dynamic state estimation, which is also gaining interest and will allow even the anticipation of the control [30], will be researched as well. The implementation of the testbed is crucial in order to evaluate the convergence and feasibility of the proposed methods in real time and realistic conditions, i.e., detailed modeling of large power systems. Analyzing the generated data from the testbed will help researchers finding the most critical and dangerous vulnerabilities. This is important to develop adequate risk-based and practical solutions.

The research topics discussed above are under further investigation as a collaborative work with control, computer science and power faculty from the Tokyo Institute of Technology, the Institute of Statistical Mathematics (Tokyo), the University of Tokyo, Japan and Arizona State University (AZ, USA).

Securing the control in the smart grid against cyber-attacks:

Background:

Control is more critical than ever before in order to reduce the power inter-area oscillations and regulate voltage and frequency in the power grid. This increased need is justified by: a) the introduction of stochastic renewable distributed generation such as PVs and wind, and b) the expanding interconnections and regional power transfers and the rising deregulation of the electricity markets. Control is evolving with the development of Wide Area Measurement Systems (WAMS) technologies thanks to the incentives provided by the U.S. Department of Energy in order to deploy PMU sensors in the power grid [31,32]. Cyber-attacks

targeting the control actions are a high risk to the system because of their potential for catastrophic impacts. For example, the authors in [2] have shown the vulnerability of the Automatic Generation Control (AGC) module in an EMS to potential cyber-attacks. The AGC provides automatic frequency regulation of the power system while insuring that the scheduled power exchanges between adjacent power areas and utilities are met. In [33], the researchers studied the effect of cyber-attacks spoofing the Global Positioning System (GPS) clocks of PMUs. The GPS clocks are used to synchronize PMU measurements collected over widely spread areas to provide highly accurate sensing. The authors proposed algorithmic solutions to secure the damping of inter-area oscillation modes in the WAMs that will be deployed to control the future grid [32]. Voltage control could also be targeted by cyber-attackers where the local control at a regulating transformer such as a tap changing transformer could be misled by the modification of the sensed data. This case was studied at the distribution level in Japan with both increased communication and distributed generation from PVs installed on residential rooftops [34].

Procedure:

We are analyzing and securing different control actions in the WAMS under potential cyber-threats. Several control practical problems will be investigated such as frequency and voltage regulation. For example, securing the identification of models for the power system, damping the oscillation modes and controlling power flows are immediate topics that will be researched. We will also study the impact of cyber-attacks on the protection of the power grid which is critical under disturbances and contingencies.

Scientific Significance:

The implementation of the testbed will help researchers at the University of Idaho perform high quality research in the area of cybersecurity of Distributed Control Systems (DCS) and more specifically Wide Area monitoring and Management Systems (WAMS) when integrating PMUs.

The proposed testbed will support an existing course organized by Dr. Johnson at the University of Idaho, Moscow. The course treats the resilient control of critical infrastructure and involves the smart grid as a practical application since it is considered to be a major critical infrastructure. Researchers from the Idaho National laboratory are also contributing in the lectures providing their research experience in this field. The course investigates how an industrial control system works and how it can fail-including threats from cybersecurity, human error and complex interdependencies. It Introduces concepts from the resilient controls community that attempt to make Industrial Control Systems more resilient to these threats.

Network security analysis and visualization for industrial and power control systems*:*

Background:

Industrial Control Systems (ICS) include the Supervisory Control and Data Acquisition (SCADA) systems [36,37], distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) [4]. ICS are also used in electrical, water and wastewater, oil and natural gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing industries [4,35]. ICS devices have been evolving into powerful digital devices that offer network connectivity and remote control. Today's ICS are connected to corporate computer networks and the Internet. This brings a new set of risks and vulnerabilities for which these systems where not originally designed to mitigate.

Currently, there are many more cybersecurity and network analysis and visualization tools available to the Information Technology (IT) professional which do not have a counterpart in the Operational Technology (OT) and ICS Control realms. This is because, although similar, these domains have their significant differences, both, in the way they operate and at the organizational level.

Procedure:

We will analyze tools currently used for Big Data and Time-Series data logging, analysis, and visualization such as the Elasticsearch, Logstash, and Kibana tool stack (ELK Stack) and DevOps environments. ELK Stack is a tool-set for data logging, analysis, and visualization. This with the purpose of determining which of these tools could be ported and integrated into the ICS and Smart Grid network domains. After selecting a set of network analysis and visualization tools from the Information Technology domain we will begin addressing the challenge of porting them to the ICS Control network domains. This will allow us to discover those major roadblocks involved with such translation and to propose and test

solutions to those roadblocks. The proposed testbed will be an essential component in this research because it will offer a development and testing environment in which the translation roadblocks would be very similar to that of a real distributed cyber-physical control system.

Scientific Significance:

Being able to successfully translate knowledge, lessons learned, and tools from the IT cybersecurity realm into the OT and ICS control realm has the potential for quickly bringing many cybersecurity tools and approaches to help secure our critical infrastructure systems.

Development of resilience metrics to correlate the cognitive, cyber-physical complexities of critical infrastructure:

Background:

Resilient Industrial Control System (ICS) design attempts to synergistically capture both the cyber and the physical aspects of system design and operation, thereby overcoming the limitations of the reliable computing and fault tolerant control perspective. Research and development (R&D) and associated international symposia have developed the technological perspectives and definition of Resilient Control Systems (RCS). It is now timely to establish a means to evaluate technology investment into R&D that will mature technologies into industrial applications, such as the electric grid. In addition, as a ground truth for impacts from manmade and natural events, a method to correlate operational awareness is required. In line with these needs, metrics are necessary to establish the following: 1) *System Integrity*: Establishing Ongoing System Run-Time Performance, and 2) *Business Case for Resilience*: Establishing the Value Proposition Based upon Desired Performance.

Procedure:

The research project started in June 2016, and is conducted by Dr. Brian Johnson in collaboration with researchers at the Idaho National Laboratory (INL), as part of the U.S. Department of Energy (DoE) Grid Modernization Lab Call, will introduce novel Resiliency Metrics for Interconnected Infrastructures such as the future power systems including both the transmission and the distribution systems. For example, at the transmission level, both frequency and voltage fluctuations could be considered in calculating the performance metric. System performance indices are utilized in time-sensitive power system control systems and applications and therefore, need to be computed in real-time. To compute performance indices in real-time, computational and memory constraints need to be satisfied. To satisfy such constraints, it is essential to consider only critical transmission system buses for calculating performance indicators.

Furthermore, the main goal of this project is the creation and refinement of resilience metrics that can be used to evaluate the resilience of the electrical grid based on complex parameters. This has to include estimates of human performance based on a deep understanding of the role that utility operators play within the overall system. Importantly, a clear understanding of resilience metrics will improve the way the critical information is communicated to the operators. If done effectively this will lead to an increase in human performance by increasing resilience awareness and thus an increase in resilience for the overall system. The developed metrics will be evaluated using Computational Intelligence tools such as evolutionary computation [39]. The application and/or revision of previous metrics framework for transmission systems to repurpose for distribution systems will be investigated.

Scientific Significance:

Based on the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards 002-009 [40] it is the responsibility of utilities to identify and protect their critical cyber assets to ensure reliability of the bulk power system. However, there is no systematic methodology to identify critical assets. The goal of this research is to develop resiliency indices for the power system.

The visualization resources and the distributed nature of the testbed will allow us to integrate and analyze human factors that impact cybersecurity in order to propose practical solutions. For example, the interactions between cybersecurity engineers and power operating engineers in the control center are

practical research questions of the future smart grid. Developing best practices to secure the control center must be investigated in a collaborative fashion with experts in computing, control, power, psychology, and sociology. Such combined expertise is available at the Center for Secure and Dependable Systems (CSDS) in the College of Engineering at the University of Idaho.

Cyber-attack resilient HVDC system:

Background:

High Voltage Direct Current (HVDC) systems will play an important role in the future grid to permit large power transfers over long distances. The smart grid is expected to combine both AC and DC systems to provide and efficient, stable, and secure power system. For example, HVDC will be useful in connecting remote renewable generation sources such as offshore wind farms to the grid in a secure way. The HVDC will also encourage the power exchanges over long distances needed in the free electricity markets environment. The control of HVDC systems in this case will impact the behavior of the whole smart grid and should be secure against cyber-attacks.

Procedure:

Dr. Johnson is collaborating with a HVDC equipment supplier in a U.S. DoE funded project that will start in January 2017 in order to develop resilient control for HVDC systems. The objective is to analyze the impact of malicious commands on the operational security of the HVDC system and on the connected AC systems. Methods to detect and defeat malicious commands, within and external to the converter station will be developed. Design and prototyping will permit to propose secure methods to test robustness of actual controllers based on real world conditions and data.

Scientific Significance:

Improving the cybersecurity for HVDC systems will permit to secure the whole power grid. The proposed cybersecurity testbed will help in proposing defense solutions that could be implemented by power companies.

Preparation for cybersecurity competitions and interoperability studies:

The testbed will help prepare researchers, practitioners, and students for national and international competitions such as the Cyber-Physical System (CPS) Based Cyber Defense Competition, the Pacific Rim Collegiate Cyber Defense Competition, and several others. These serve as training exercises and also as scenario-based testing environments where newly developed techniques and algorithms can be tested in a full-fledged simulation. Other universities in the US and across the world are installing testbeds for smart grid and cybersecurity studies [40-42]. The proposed testbed will improve the research, teaching and the attractiveness of U. Idaho as a center of excellence in cybersecurity research and instruction.

Data-set generation and validation:

One of the biggest challenges when performing research for smart grid and industrial control systems cybersecurity is the lack of the availability of validated and adequate data-sets for testing and evaluation. The proposed testbed will allow UI researchers to develop, save, and share significant and validated Data-sets. For example, the competitions described above could be used for developing such data-sets. Other realistic data-sets could be generated and saved for specific experiments. Cyber-attack data is difficult to obtain from power companies and transmission system operators because of the sensitivity of the data. The testbed will solve this issue and will facilitate access to realistic data-sets. In addition, thanks to the testbed, the transfer of cybersecurity technology to power companies will be enabled.

References Cited

[1] E. Hossain, Z. Han, and H. V. Poor, Smart Grid Communications and Networking, Cambridge University Press, 2012.

[2] S. K. Khaitan; J. D. McCalley; Ch. Liu, Cyber Physical Systems Approach to Smart Electric Power Grid, Springer, Heidelberg, 2015

[3] J. Repko and S. Debroux, “Smart cities literature review and analysis,” in IMT 598 Spring 2012: Emerging Trends in Information Technology, May 2012.

[4] T. G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, Wiley, New Jersey, second edition, 2015.

[5] L. Chen-Ching, A. Stefanov, J. Hong, and P. Panciatici, “Intruders in the grid,” IEEE Power Energy Mag., vol. 10, no. 1, pp. 58–66, 2012.

[6] “Terrorism and the Electric Power Delivery System” U.S. National Academy of Engineering Press (NAE), Report 2012.

[7] National Institute of Standards and Technolog (NIST), “Guidelines for smart grid cybersecurity,” NISTIR 7628, Aug. 2010.

[8] Y. Chakhchoukh and H. Ishii, "Coordinated cyber-attacks on the measurement function in hybrid state estimation," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2487-2497, Sept. 2015.

[9] Y. Chakhchoukh and H. Ishii, "Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4395-4405, Nov. 2016.

[10] Y. Chakhchoukh, S. Liu, M. Sugiyama and H. Ishii, “Statistical outlier detection for diagnosis of cyber-attacks in power state estimation,” in *Proc. IEEE Power Energy Society General Meeting*, July 2016.

[11] Y. Chakhchoukh and H. Ishii, "Cyber attacks scenarios on the measurement function of power state estimation," *Proc. American Control Conference (ACC*), Chicago, IL, 2015, pp. 3676-3681.

[12] Y. Chakhchoukh, V. Vittal, G. T. Heydt and H. Ishii, “LTS-based Robust Hybrid SE Integrating Correlation”, *IEEE Transactions on Power Systems*, under review, 2016.

[13] Japan Science and Technology Agency (JST), “Securing Power Control Systems from Cyber Attacks: Development of a Novel High Precision Detection Technique for Stable Control”, Press Release, Feb. 2016. https://www.jst.go.jp/pr/info/info1165/index_e.html.

[14] A. Abur and A. G. Exposito, Power System State Estimation: Theory and Implementation, CRC Press, New York, 2004.

[15] A. G. Phadke and J. S. Thorp, Synchronized Phasor Measurements and Their Applications, Springer, New York, second edition, 2008.

[16] Y. Liu, M. K. Reiter, and P. Ning, “False data injection attacks against state estimation in electric power grids,” in *Proc. 16th ACM Conf. on Computer and Communications Security*, 2009, pp. 21–32.

[17] G. Hug and J. A. Giampapa, “Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks,” *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[18] J. Kim and L. Tong, “On topology attack of a smart grid: Undetectable attacks and countermeasures,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1294–1305, July 2013.

[19] University of Washington, Power System Test Case Archive, [Online]. Available: http://www.ee.washington.edu/research/pstca/.

[20] A. M. Zoubir, V. Koivunen, Y. Chakhchoukh, and M. Muma, “Robust estimation in signal processing: A tutorial-style treatment of fundamental concepts,” *IEEE Signal Procesing. Magazine*, vol. 29, no. 4, pp. 61–80, Jul. 2012.

[21] M. Sugiyama, T. Suzuki, and T. Kanamori, Density ratio estimation in machine learning, Cambridge University Press, 2012.

[22] M. Esmalifalak, N. T. Nguyen, R. Zheng, and Z. Han, “Detecting stealthy false data injection using machine learning in smart grid,” *in Proc. Of the IEEE Global Communications Conference*, Dec 2013.

[23] A. Simões Costa, A. Albuquerque and D. Bez, "An estimation fusion method for including phasor measurements into power system real-time modeling," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1910-1920, May 2013.

[24] M. Glavic and T. Van Cutsem, "Reconstructing and tracking network state from a limited number of synchrophasor measurements," *IEEE Trans. on Power Systems*, vol. 28, no. 2, pp. 1921-1929, May 2013.

[25] M. Göl and A. Abur, "A hybrid state estimator for systems with limited number of PMUs," *IEEE Transactions on Power Systems*, vol. 30, no. 3, pp. 1511-1517, May 2015.

[26] Q. Zhang, V. Vittal, G. Heydt, Y. Chackhchoukh, N. Logic, and S. Sturgill, “The time skew problem in PMU measurements,” *in Proc. IEEE Power Energy Society General Meeting*, July 2012, pp. 1–4.

[27] Q. Zhang, Y. Chakhchoukh, V. Vittal, G. T. Heydt, N. Logic, and S. Sturgill, “The optimal buffer length of for the PMU measurements when integrated into state estimation,” *IEEE Transactions on Power Systems*, vol. 28, no.2, pp.1657-1665, May 2013.

[28] V. Murugesan, Y. Chakhchoukh, V. Vittal, G. T. Heydt, N. Logic and S. Sturgill, "PMU Data Buffering for Power System State Estimators," in *IEEE Power and Energy Technology Systems Journal*, vol. 2, no. 3, pp. 94-102, Sept. 2015.

[29] Y. Chakhchoukh, V. Vittal and G. T. Heydt, “PMU based state estimation by integrating correlation,” *IEEE Transactions on Power Systems*, vol. 29, no. 2, pp. 617--626, March 2014.

[30]O. Kosut, "Malicious data attacks against dynamic state estimation in the presence of random noise," *Proc. Global Conference on Signal and Inf. Processing (GlobalSIP)*, 2013 IEEE, Austin, TX, 2013, pp. 261-264.

[31] U.S. Department of Energy (DOE) National Energy Technology Laboratory (NETL), “A system view of the modern grid,” 2007.

[32] A. Chakrabortty and P. P. Khargonekar, "Introduction to wide-area control of power systems," American Control Conference, Washington DC, 2013, pp. 6758-6770.

[33] M. Liao and A. Chakrabortty, "A Round-Robin ADMM algorithm for identifying data-manipulators in power system estimation," American Control Conference (ACC), Boston, MA, 2016, pp. 3539-3544.

[34] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, “Detection of cyber-attacks against voltage control in distribution power grids with PVs,” *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824-1835, July 2016.

[35] T. Nelson and M. Chaffin. Common cybersecurity vulnerabilities in industrial control systems. Technical report, Department of Homeland Security, Idaho National Laboratory, May 2011.

[36] The National Institute of Standards and Technology. Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework. NIST Standards, pages 1–47, 2013.

[37] Idaho National Laboratory (INL), “National SCADA testbed: Fact sheet,” 2007.

[38] North American Electric Reliability Corporation (NERC), “Critical Infrastructure Protection Standards 002-3 – 009-3”, December 16, 2009. Available at: http://www.nerc.com/page.php?cid=2|20.

[39]M. L. Harrison, and J. A. Foster, “Co-evolving faults to improve the fault tolerance of sorting networks”, Genetic Programming, pp. 57-66, Springer, 2004.

[40] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber–physical system security for the electric power grid”, *Proceedings of the IEEE*, 100(1): 210– 224, 2012.

[41] A. Hahn, A. Ashok, S. Sridhar and M. Govindarasu, “Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid,” *in IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847-855, June 2013.

[42] S. S. Biswas, J. Hun Kim and A. K. Srivastava, “Development of a smart grid testbed and applications in PMU and PDC testing,”*North American Power Symposium (NAPS)*, 2012, Champaign, IL, 2012, pp. 1-6.