INVITED PAPER

Cyber–Physical System Security for the Electric Power Grid

Control in power systems that may be vulnerable to security attacks is discussed in this paper as are control loop vulnerabilities, potential impact of disturbances, and several mitigations.

By Siddharth Sridhar, *Student Member IEEE*, Adam Hahn, *Student Member IEEE*, and Manimaran Govindarasu, *Senior Member IEEE*

ABSTRACT | The development of a trustworthy smart grid requires a deeper understanding of potential impacts resulting from successful cyber attacks. Estimating feasible attack impact requires an evaluation of the grid's dependency on its cyber infrastructure and its ability to tolerate potential failures. A further exploration of the cyber–physical relationships within the smart grid and a specific review of possible attack vectors is necessary to determine the adequacy of cybersecurity efforts. This paper highlights the significance of cyber infrastructure security in conjunction with power application security to prevent, mitigate, and tolerate cyber attacks. A layered approach is introduced to evaluating risk based on the security of both the physical power applications and the supporting cyber infrastructure. A classification is presented to highlight dependencies between the cyber–physical controls required to support the smart grid and the communication and computations that must be protected from cyber attack. The paper then presents current research efforts aimed at enhancing the smart grid's application and infrastructure security. Finally, current challenges are identified to facilitate future research efforts.

KEYWORDS | Cyber–physical systems (CPS); cyber security; electric grid; smart grid; supervisory control and data acquisition (SCADA)

I. INTRODUCTION

An increasing demand for reliable energy and numerous technological advancements have motivated the development of a smart electric grid. The smart grid will expand the current capabilities of the grid's generation, transmission, and distribution systems to provide an infrastructure capable of handling future requirements for distributed generation, renewable energy sources, electric vehicles, and the demand-side management of electricity. The U.S. Department of Energy (DOE) has identified seven properties required for the smart grid to meet future demands [1]. These requirements include attack resistance, self-healing, consumer motivation, power quality, generation and storage accommodation, enabling markets, and asset optimization.

While technologies such as phasor measurement units (PMU), wide area measurement systems, substation automation, and advanced metering infrastructures (AMI) will be deployed to help achieve these objectives, they also present an increased dependency on cyber resources which may be vulnerable to attack [2]. Recent U.S. Government Accountability Office (GAO) investigations into the grid's cyber infrastructure have questioned the adequacy of the current security posture [3]. The North American Electric Reliability Corporation (NERC) has recognized these concerns and introduced compliance requirements to enforce baseline cybersecurity efforts throughout the bulk power system [4]. Additionally, current events have shown attackers using increasing sophisticated attacks against industrial control systems while numerous countries have acknowledged that cyber attacks have targeted their critical infrastructures [5], [6].

A comprehensive approach to understanding security concerns within the grid must utilize cyber–physical system (CPS) interactions to appropriately quantify attack impacts [7] and evaluate effectiveness of countermeasures. This paper highlights CPS security for the power grid as the functional composition of the following: 1) the physical

Manuscript received June 29, 2011; revised August 11, 2011; accepted August 12, 2011. Date of publication October 3, 2011; date of current version December 21, 2011. This work was supported by the National Science Foundation under Grant CNS 0915945.
The authors are with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA (e-mail: sridhar@iastate.edu).

Digital Object Identifier: 10.1109/JPROC.2011.2165269

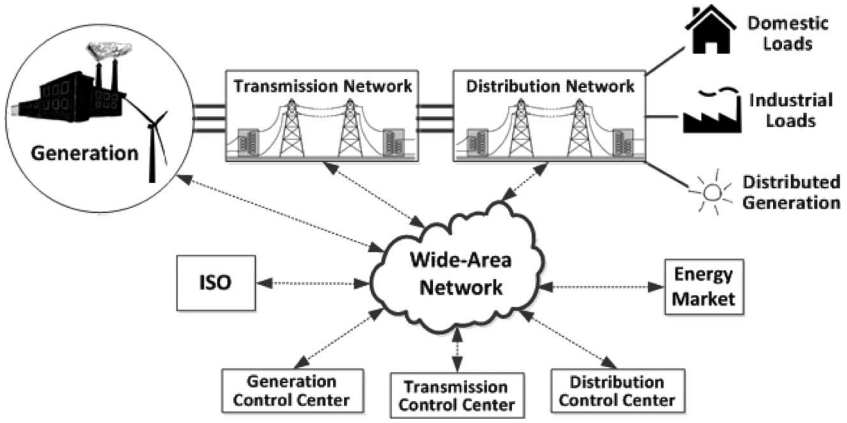

Fig. 1. ***Power grid cyber–physical infrastructure.***

components and control applications; 2) the cyber infrastructures required to support necessary planning, operational, and market functions; 3) the correlation between cyber attacks and the resulting physical system impacts; and 4) the countermeasures to mitigate risks from cyber threats. Fig. 1 shows a CPS view of the power grid. The cyber systems, consisting of electronic field devices, communication networks, substation automation systems, and control centers, are embedded throughout the physical grid for efficient and reliable generation, transmission, and distribution of power. The control center is responsible for real-time monitoring, control, and operational decision making. Independent system operators (ISOs) perform coordination between power utilities, and dispatch commands to their control centers. Utilities that participate in power markets also interact with the ISOs to support market functions based on real-time power generation, transmission, and demand.

This paper addresses smart grid cybersecurity concerns by analyzing the coupling between the power control applications and cyber systems. The following terms are introduced to provide a common language to address these concepts throughout the paper:

- *power application*: the collection of operational control functions necessary to maintain stability within the physical power system;
- *supporting infrastructure*: the cyber infrastructure including software, hardware, and communication networks.

This division of the grid's command and control functions will be utilized to show how cybersecurity concerns can be evaluated and mitigated through future research. Attempts to enhance the current cybersecurity posture should explore the development of *secure power applications* with more robust control algorithms that can operate reliably in the presence of malicious inputs while deploying a *secure supporting infrastructure* that limits an adversary's ability to manipulate critical cyber resources.

The paper is organized as follows. Section II introduces a risk assessment methodology which incorporates both cyber and physical characteristics to identify physical impacts from cyber attacks. Section III presents a classification detailing the *power applications* necessary to facilitate grid control. Each power application contains a review of the information, communication, and algorithms required to support its operation. Additionally, specific cybersecurity concerns are addressed for each application and potential physical impacts are explored. Section IV provides a review of current research efforts focusing on security enhancements for the *supporting infrastructure*. Finally, emerging research challenges are introduced in Section V to highlight areas requiring attention.

II. RISK ASSESSMENT METHODOLOGY

The complexity of the cyber–physical relationship can present unintuitive system dependencies. Performing accurate risk assessments requires the development of models that provide a basis for dependency analysis and quantifying resulting impacts. This association between the salient features within both the cyber and physical infrastructure will assist in the risk review and mitigation processes. This paper presents a coarse assessment methodology to illustrate the dependency between the power applications and supporting infrastructure. An overview of the methodology is presented in Fig. 2.

Risk is traditionally defined as the impact times the likelihood of an event [8]. Likelihood should be addressed through the infrastructure vulnerability analysis step which addresses the supporting infrastructure's ability to limit attacker's access to the critical control functions. Once potential vulnerabilities are discovered, the application impact analysis should be performed to determine effected grid control functions. This information should then be used to evaluate the physical system impact.

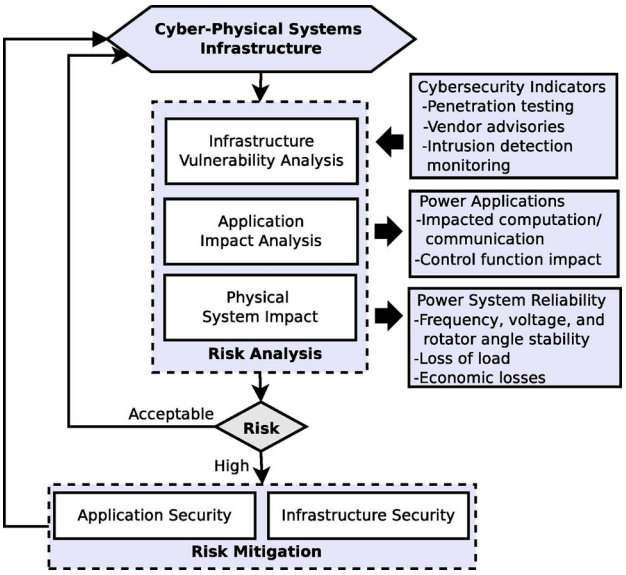

Fig. 2. ***Risk assessment methodology.***

A. Risk Analysis

The initial step in the risk analysis process is the *infrastructure vulnerability analysis*. Numerous difficulties are encountered when determining cyber vulnerabilities within control system environments due to the high availability requirements and dependencies on legacy systems and protocols [9]. A comprehensive vulnerability analysis should begin with the identification of cyber assets including software, hardware, and communications protocols. Then, activities such as penetration testing and vulnerability scanning can be utilized to determine potential security concerns within the environment. Additionally, continued analysis of security advisories from vendors, system logs, and deployed intrusion detection systems should be utilized to determine additional system vulnerabilities. Common control system cyber vulnerabilities have been evaluated by the Department of Homeland Security (DHS) based on numerous technical and nontechnical assessments [10]. Table 1 identifies these vulnerabilities and categorizes whether they were found in industry software products, general misconfigurations, or within the network infrastructure. This list provides greater insight into likely attack vectors and also helps identify areas requiring additional mitigation research.

After cyber vulnerabilities have been identified, the application impact analysis step should be performed to determine possible impacts to the applications supported by the infrastructure. This analysis should leverage the classification introduced in Section III to identify the impacted set of communication and control mechanisms. Once attack impacts on the power applications have been determined, physical impact analysis should be performed to quantify impact on the power system. This analysis can be carried out using power system simulation methods to quantify steady state and transient performances including power flows and variations in grid stability parameters in terms of voltage, frequency, and rotor angle.

B. Risk Mitigation

Mitigation activities should attempt to minimize unacceptable risk levels. This may be performed through the deployment of a more robust supporting infrastructure or power applications as discussed in Sections III and IV. Understanding opportunities to focus on specific or combine approaches may present novel mitigation strategies.

Numerous research efforts have addressed the cyber–physical relationship within the risk assessment process. Interdependency research by Laprie *et al.* focuses on analyzing escalating, cascading, and common-cause failures within the cyber–physical relationship [11]. State machines are developed to evaluate the transitions influenced by the interdomain dependencies. This research then shows how attack-based transitions can lead to failure states. A graph-based cyber–physical model has been proposed by Kundur *et al.* [12]. Here graphs are analyzed to evaluate a control's influence on a physical entity. This model is used to evaluate how power generation can be impacted by the failures or attacks on cyber assets. Additional research into computing likely load loss due a successful cyber attack has been performed by Ten *et al.* [13], [14]. This research uses probabilistic methods based on Petri-nets and attack trees to identify weaknesses in substations and control centers which can then be used to identify load loss as a percentage of the total load within the power system.

Table 1 Common Control System Vulnerabilities/Weaknesses

Software/Product Security Weaknesses	Configuration Weaknesses	Network Security Weaknesses
1. Improper Input Validation	1. Permissions, Privileges, and Access Controls	1. Common Network Design Weaknesses
2. Poor Code Quality	2. Improper Authentication	2. Weak Firewall Rules
3. Permissions, Privileges, and Access Controls	3. Credentials Management	3. Network Component Configuration (Implementation) Vulnerabilities
4. Improper Authentication	4. Security Configuration and Maintenance	4. Audit and Accountability
5. Insufficient Verification of Data Authenticity	5. Planning/Policy/Procedures	
6. Cryptographic Issues	6. Audit and Accountability Configuration	
7. Credentials Management		
8. Configuration and Maintenance		

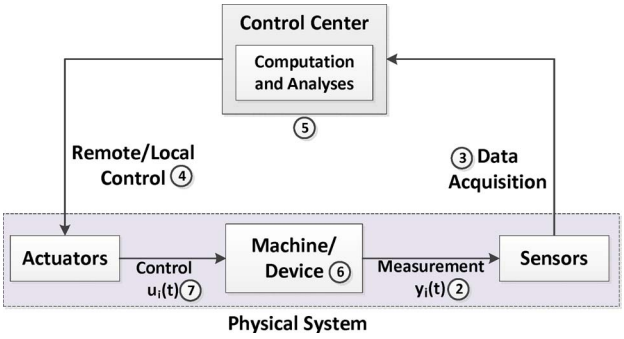

Fig. 3. *A typical power system control loop.*

III. POWER SYSTEM CONTROL APPLICATIONS AND SECURITY

A power system is functionally divided into generation, transmission, and distribution. In this section, we present a classification of control loops in the power system that identifies communication signals and protocols, machines/devices, computations, and control actions associated with select control loops in each functional classification. The section also sheds light on the potential impact of cyber attacks directed at these control loops on system-wide power system stability.

Control centers receive measurements from sensors that interact with field devices (transmission lines, transformers, etc.). The algorithms running in the control center process these measurements to make operational decisions. The decisions are then transmitted to actuators to implement these changes on field devices. Fig. 3 shows a generic control loop that represents this interaction between the control center and the physical system. The measurements from sensors and control messages from the control center are represented by $y_i(t)$ and $u_i(t)$, respectively. In the power system, the measured physical parameters $y_i(t)$ may refer to quantities such as voltage and power. These measurements from substations, transmission lines, and other machines are sent to the control center using dedicated communication protocols. The measurements are then processed by a set of computational algorithms, collectively known as the energy management system (EMS), running at the control center. The decision variables $u_i(t)$ are then transmitted to actuators associated with field devices.

An adversary could exploit vulnerabilities along the communication links and create attack templates designed to either corrupt the content of (e.g., integrity attacks), or introduce a time delay or denial in the communication of [e.g., denial of service (DoS), desynchronization, timing attacks] these control/measurement signals [15]. It is important to study and analyze impacts of such attacks on the power system as they could severely affect its security and reliability. These impacts can be measured in terms of loss of load or violations in system operating frequency and voltage and their secondary impacts. Attack studies will also help develop countermeasures that can prevent attacks or mitigate the impact from attacks. Countermeasures include bad data detection techniques and attack resilient control algorithms.

This section presents a classification of prominent control loops under generation, transmission, and distribution. Traditional supervisory control and data acquisition (SCADA), local, and emerging smart grid controls have been identified. For each control loop known vulnerabilities, attack templates, and potential research directions have also been highlighted.

A. Generation Control and Security

The control loops under generation primarily involve controlling the generator power output and terminal voltage. Generation is controlled by both, local (automatic voltage regulator and governor control) and wide-area (automatic generation control) control schemes as explained in this section. Fig. 4 identifies the various parameters associated with the control loops in the generation system.

1) Automatic Voltage Regulator (AVR): Generator exciter control is used to improve power system stability by controlling the amount of reactive power being absorbed or injected into the system [16]. Digital control equipment for the exciter enables testing of different algorithms for system stability improvement. Hence, this cost-effective

Generation	Communication Messages						
	1 Physical Parameter	2 Measurements & Inputs	3 Data Acquisition	4 Control	5 Computation	6 Machine/ Device	7 Control Action
Automatic Voltage Regulator	Terminal Voltage	Measured and Reference Terminal Voltage	Local measurement from terminal	Local message to excitor control	Calculation of Excitation Current	Generators	Increase/Decrease Excitor Current
Governor Control	Rotor Speed	Measured and Reference Rotor Speed	Local measurement from rotor speed sensor	Local message to prime mover controller	Valve Position	Prime Mover	Open/Close Valve
Automatic Generation Control	Frequency	Frequency & Tie-Line Power Measurement	Wide-Area Communication (IEC 61850)	Point to Point Communication (DNP 3.0)	*Area Control Error* (ACE) Calculation	Generators	Raise/Lower Generation

Fig. 4. *Generation control classification.*

approach is widely preferred and used by generation utilities.

The digital exciter control module is connected to the plant control center via Ethernet and communicates using protocols such as Modbus [17]. This Ethernet link is used to program the controller with voltage setpoint values. The AVR control loop receives generator voltage feedback from the terminal and compares it with the voltage setpoint stored in memory. Based on the difference between the observed measurement and the setpoint, the current through the exciter is modified to maintain voltage at the desired level.

2) Governor Control: Governor control is the primary frequency control mechanism. This mechanism employs a sensor that detects changes in speed that accompany disturbances and accordingly alters settings on the steam valve to change the power output from the generator. The controllers used in modern digital governor control modules make use of Modbus protocol to communicate with computers in the control center via Ethernet [18]. As in the case of AVR, this communication link is used to define operating setpoint for control over the governor.

a) Cyber vulnerabilities and solutions: The AVR and the governor control are local control loops. They do not depend on the SCADA telemetry infrastructure for their operations as both the terminal voltage and rotor speed are sensed locally. Hence, the attack surface for these control loops is limited. Having said that, these applications are still vulnerable to malware that could enter the substation LAN through other entry points such as USB keys. Also, the digital control modules in both control schemes do possess communication links to the plant control center. To target these control loops, an adversary could compromise plant cybersecurity mechanisms and gain an entry point into the local area network. Once this intrusion is achieved, an adversary can disrupt normal operation by corrupting the logic or settings in the digital control boards. Hence, security measures that validate control commands that originate even within the control center have to be implemented.

3) Automatic Generation Control: The automatic generation control (AGC) loop is a secondary frequency control loop that is concerned with fine tuning the system frequency to its nominal value. The function of the AGC loop is to make corrections to interarea tie-line flow and frequency deviation. The AGC ensures that each balancing authority area compensates for its own load change and the power exchange between two control areas is limited to the scheduled value. The algorithm correlates frequency deviation and the net tie-line flow measurements to determine the *area control error*; the correction that is sent to each generating station to adjust operating points once every five seconds. Through this signal, the AGC ensures that each balancing authority area meets its own load changes and the actual power exchanged remains as close as possible to the scheduled exchange.

a) Cyber vulnerabilities and solutions: The automatic generation control relies on tie-line and frequency measurements provided by the SCADA telemetry system. An attack on AGC could have direct impacts on system frequency, stability, and economic operation. DoS type of attacks might not have a significant impact on AGC operation unless supplemented with another attack that requires AGC operation. The following research efforts have identified the impact of data corruption and intrusion on the AGC loop.

Esfahani *et al.* [19] propose a technique using reachability analysis to gauge the impact of an intrusion attack on the AGC loop. In [20], Sridhar and Manimaran develop an attack template that appropriately modifies the frequency and tie-line flow measurements to drive the system frequency to abnormal operating values.

Areas of future research include: 1) evaluating impacts of DoS attacks on the AGC loop in combination with other attacks that trigger AGC operation; and 2) development of domain-specific bad data detection techniques for AGC to identify data integrity attacks.

B. Transmission Control and Security

The transmission system normally operates at voltages in excess of 13 KV and the components controlled include switching and reactive power support devices. It is the responsibility of the operator to ensure that the power flowing through the lines is within safe operating margins and the correct voltage is maintained. The following control loops assist the operator in this functionality. Fig. 5 summarizes the communication protocols and other

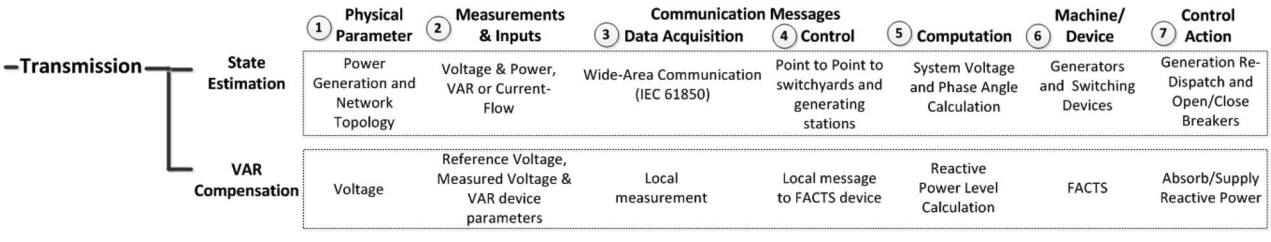

Fig. 5. ***Transmission control classification.***

parameters associated with the control loops in the transmission system.

1) State Estimation: Power system state estimation is a technique by which estimates of system variables such as voltage magnitude and phase angle (state variables) are made based on presumed faulty measurements from field devices. The process provides an estimate of state variables not just when field devices provide imperfect measurements, but also when the control center fails to receive measurements either due to device or communication channel malfunction. This gives the operator details on power flows and voltage magnitudes along different sections of the transmission network and hence assists in making operational decisions. The control center performs computations using thousands of measurements it receives through the wide-area network. A good amount of work has been done in developing techniques to detect bad data in state estimation [21]–[26]. These techniques provide good estimates of state variables despite errors introduced by device and channel imperfections. However, they were not designed to be fault tolerant when malicious data are injected with intent.

a) Cyber vulnerabilities and solutions: Bad data detection in state estimation is well researched. However, these techniques were developed for errors in data that appear due to communication channel or device malfunctioning. When an adversary launches an attack directed at disrupting the smooth functioning of state estimation, these techniques might not be able to detect the presence of malicious data.

Liu *et al.* created a class of attacks, called *false data injection* attacks, that escape detection by existing bad measurement identification algorithms, provided they had knowledge of the system configuration [27]. It was determined that to inject false data into a single state variable in the IEEE 300-bus system, it was sufficient to compromise ten meters. In [28], Kosut *et al.* verify that the impact from false data injection attack discussed in [27] is the same as removing the attacked meters form the network. The authors also propose a graph-theoretic approach to determine the smallest set of meters that have to be compromised to make the power network unobservable.

Bobba *et al.* [29] developed a technique to detect false data injection attacks. The idea was to observe a subset of measurements and perform calculations based on them to detect malicious data. Xie *et al.* show that a successful attack on state estimation could be used in the electricity markets to make financial gains [30]. As settlements between utilities are calculated based on values from state estimation, the authors show that a profit of $8/MWh can be made by tampering with meters that provide line flow information.

2) VAR Compensation: Volt-ampere reactive (VAR) compensation is the process of controlling reactive power injection or absorption in a power system to improve the performance of the transmission system. The primary aim of such devices is to provide voltage support, that is, to minimize voltage fluctuation at a given end of a transmission line. These devices can also increase the power transferable through a given transmission line and also have the potential to help avoid blackout situations. Synchronous condensers and mechanically switchable capacitors and inductors were the conventional VAR compensation devices. However, with recent advancement in thyristor-based controllers, devices such as the ones belonging to the flexible AC transmission systems (FACTS) family, are gaining popularity.

FACTS devices interact with one another to exchange operational information [31]. Though these devices function autonomously, they depend on communication with other FACTS devices for information to determine operating point.

a) Cyber vulnerabilities and solutions: In [32], the authors provide a list of attack vectors that could be used against cooperating FACTS devices (CFDs). Though attacks such as denial of service and data injection are well studied and understood in the traditional IT environment, the authors provide an insight into what these attacks mean in a CFD environment.

1) Denial of cooperative operation: This is a DoS attack. In this type of attack, the communication to some or all the FACTS devices could be jammed by flooding the network with spurious packets. This will result in the loss of critical information exchange and thus affect long-term and dynamic control capabilities.
2) Desynchronization (timing-based attacks): The control algorithms employed by CFDs are time dependent and require strict synchronization. An attack of this kind could disrupt steady operation of CFDs.
3) Data injection attacks: This type of attacks requires an understanding of the communication protocol. The attack could be used to send incorrect operational data such as status and control information. This may result in unnecessary VAR compensation and in unstable operating conditions. Attack templates of this type were implemented on the IEEE 9-bus system and the results are presented in [33].

3) Wide-Area Monitoring Systems: PMU-based wide-area measurement systems are currently being installed in the United States and other parts of the world. The phase angles of voltage phasors measured by PMUs directly help in the computation of real power flows in the network, and could thus assist in decision making at the control center. PMU-based control applications are yet to be used for real-time control. However, Phadke and Thorp [34] identify control applications that could be enhanced by using data

provided by PMUs. It is suggested that HVDC systems, centralized excitation systems, FACTS controllers, and power system stabilizers could benefit from wide-area PMU measurements.

PMUs use global positioning system (GPS) technology to accurately timestamp phasor measurements. Thus, the phase difference between voltages on either end of a transmission line, at a given instant, can be accurately measured by using this technology. Phasor data concentrators combine data from multiple PMUs and provide a time-aligned data set for a particular region to the control center. The North American SynchroPhasor Initiative (NASPInet) [35] effort aims to develop a wide-area communications infrastructure to support this PMU operation. It is recognized that PMU-based control applications will be operational within the next five years. Hence, a secure and dependable WAN backbone becomes critical to power system stability.

C. Distribution Control and Security

The distribution system is responsible for delivering power to the customer. With the emergence of the smart grid, additional control loops that enable direct control of load at the end user level are becoming common. This section identifies key controls that help achieve this. Fig. 6 identifies communication protocols and other parameters for key control loops in the distribution system.

1) Load Shedding: Load shedding schemes are useful in preventing a system collapse during emergency operating conditions. These schemes can be classified into proactive, reactive, and manual. Active and proactive schemes are automatic load shedding schemes that operate with the help of relays. For example, in cases where the system generation is insufficient to match up to the load, automatic load shedding schemes could be employed to maintain system frequency within safe operating limits and protect the equipment connected to the system. When the need arises, load is shed by a utility at the distribution level by the under-frequency relays connected to the distribution feeder.

a) Cyber vulnerabilities and solutions: Modern relays are Internet protocol (IP) ready and support communication protocols such as IEC 61850. An attack on the relay communication infrastructure or a malicious change to the control logic could result in unscheduled tripping of distribution feeders, leaving load segments unserved. The outage that occurred in Tempe, AZ, in 2007, is an example of how an improperly configured load-shedding program can result in large-scale load shedding [36]. The distribution load-shedding program of the Salt River Project was unexpectedly activated resulting in the opening of 141 breakers and a loss of 399 MW. The outage lasted 46 min and affected 98 700 customers. Though the incident occurred due to a poor configuration management by the employees, it goes on to show the impact an adversary can cause if a substation is successfully intruded.

2) AMI and Demand Side Management: Future distributions systems will rely heavily on AMI to increase reliability, incorporate renewable energy, and provide consumers with granular consumption monitoring. AMI primarily relies on the deployment of "smart meters" at consumer's locations to provide real-time meter readings. Smart meters provide utilities with the ability to implement load control switching (LCS) to disable consumer devices when demand spikes. Additionally, demand side management [37] introduces a cyber–physical connection between the metering cyber infrastructure and power provided to consumers. The meter's current configuration is controlled by a meter data management system (MDMS) which lies under utility control. The MDMS connects to an AMI headend device which forwards commands and aggregates data collected from the meters throughout the infrastructure [38]. Networking within the AMI infrastructure will likely rely on many different technologies including RF mesh, WiMax, WiFi, and power line carrier. Application layer protocols such as C12.22 or IEC 61850 will be utilized to transmit both electricity usage and meter control operations between the meters and the MDMS. Fig. 7 provides an overview of the control flows that could impact consumer power availability.

a) Cyber vulnerabilities and solutions: The smart meters at consumer locations also introduce cyber–physical concerns. Control over whether the meter is enabled or disabled and the ability to remotely disable devices through load control switching provide potential threats from attackers. Adding additional security into these functions

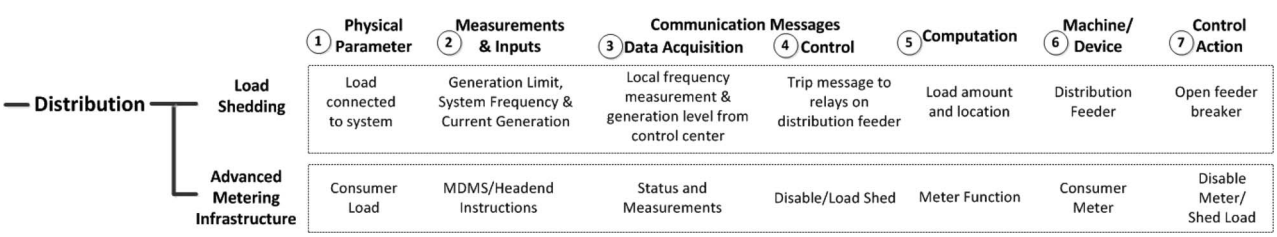

Fig. 6. ***Distribution control classification.***

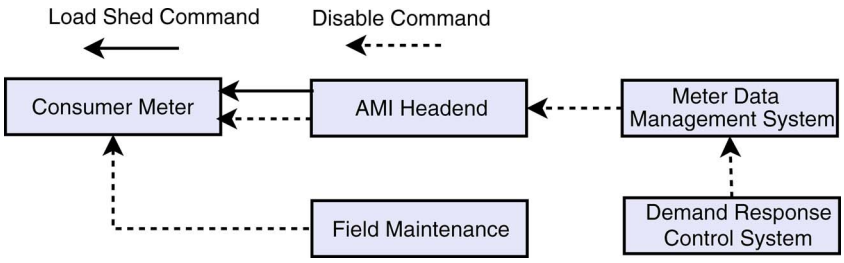

Fig. 7. ***Control functions within AMI.***

presents interesting challenges. A malicious meter disabling command can likely be prevented through the use of time-wait periods [39]. Since meter disabling does not require a real-time response, meters could be programmed to wait some time after receive a command before disabling the device. This prevention would only address remote attacks as the prevention logic could be bypassed if an attacker compromises the meter. Malicious LCS commands could provide a greater challenge due to more strict temporal requirements.

IV. SUPPORTING INFRASTRUCTURE SECURITY

The development of a secure *supporting infrastructure* is necessary to ensure information is accurately stored and transmitted to the appropriate applications. While the supporting infrastructure may share some common properties with traditional IT systems, the variation is significant enough to introduce numerous unique and challenging security concerns [9]. Specific properties include:

- long system lifecycles (> 10 years);
- limited physical environment protection;
- restricted updating/change management capabilities;
- heavy dependency on legacy systems/protocols;
- limited information processing abilities.

A secure information system traditionally enforces the *confidentiality* of its data to protect against unauthorized access while ensuring its *integrity* remains intact. In addition, the system must provide sufficient *availability* of information to *authorized* users. The primary goal of any cyber–physical system is to provide efficient control over some physical process. This naturally prioritizes information integrity and availability to ensure control state closely mirrors the physical system state. Security mechanisms such as cryptography, access control, and authentication are necessary to provide integrity in systems, however, all security mechanism tailored for this environment must also provide sufficient availability. This constraint often limits the utilization of security mechanisms which fail-closed as they may deny access to a critical function.

The development of a trustworthy electric grid requires a thorough reevaluation of the supporting technologies to ensure they appropriately achieve the grid's unique requirements. The remainder of this section will address required security concerns within the supporting infrastructure and provide a review of current research efforts addressing these concerns. While there are a vast number of research areas within this domain, this paper will focus on areas with active security research tailoring to the smart grid's supporting infrastructure.

A. Secure Communication

Power applications require a secure communications infrastructure to cope with the grid's geographic disperse resources. Data transmission often utilizes wireless communication, dialup, and leased lines which provide increased physical exposure and introduces additional risk. The grid is also heavily reliant on its own set of higher level control system protocols, including Modbus, DNP3, IEC 61850, and ICCP. Often these protocols were not developed to be attack resilient and lack sufficient security mechanism. This section will detail how encryption, authentication, and access control can be added to current communications to provide increased security.

1) Encryption: Retrofitting communication protocols to provide additional security is necessary for their continued use within untrusted spaces. Often this level of security can be obtained by deploying encrypted virtual private networks (VPNs) that protect network traffic through encapsulation within a cryptographic protocol [9]. Unfortunately, this solution is not always feasible as the industry is fairly dependent on non-IP networks. In addition, strict availability requirements may not be able to handle the added latency produced by a VPN.

Research into bump-in-the-wire (BITW) encryption hardware attempts to ensure that messages can be appropriately encrypted and authenticated while limiting the latency appended by the solution. Work by Tsang and Smith provides a BITW encryption method that significantly reduces the latency through the reduction of message hold-back during the encryption and authentication [40]. Additional research has focused on retrofitting old

protocols with appropriate security properties. Numerous efforts have addressed the modification of traditional SCADA protocols such as ICCP, DNP3, and Modbus to provide additional security while maintaining integration with current systems [41]–[43]. Deployment and key management activities still provide difficulties within geographically disperse environments.

2) Authentication: Secure remote authentication presents a challenge due to the lengthy deployments and limited change management capabilities. Authentication credentials (e.g., keys and passwords) exposure increases throughout their lifetime and protocols become increasingly prone to attack due to continual security reviews and cryptanalysis advancements. The development of strong, adaptive, and highly available authentication mechanisms is imperative to prevent unauthorized access.

Research by Khurana, *et al.* has defined design principles required for authentication protocols within the grid [44]. By defining authentication principles, future system designers can ensure their systems achieve the efficiency and adaptability required for continued secure use. Additionally, research into more flexible authentication protocols has been proposed by Chakravarthy to provide adaptability to long deployments [45]. The proposed protocol provides re-keying and remoduling algorithms to protect against key compromises and future authentication module vulnerabilities.

3) Access Control: While encryption and authentication can deter external attackers, they do little to prevent against *insider threats* or attackers that have already gained some internal access. Attackers with access to a communication network may be able to leverage various protocol functionality to inject malicious commands into control functions. The likelihood of a successful attack could be significantly reduced by appropriately configuring software and protocol usage to disable unnecessary functionality.

Evaluating industry protocols to identify potentially malicious functions is imperative to ensuring secure system configurations. Work by Mander dissects the DNP3 protocol detailing the function codes and data objects that would be useful for attackers to access data, control, or impact the availability of a remote DNP3 master [46]. This research provides a foundation for understanding the likely physical impact from a compromised communication channel. Additional research in this domain models feasible attacks against a control systems based on the current protocol specification [47]. More sophisticated protocols targeted for smart grid use, such as ANSI C.12.22 and IEC 61850, require additional analysis to ensure secure implementation in new system deployments.

B. Device Security

Embedded systems are used throughout the grid to support monitoring and control functions. The critical role placed on these devices introduces significant cybersecurity concerns due to their placement in physically unprotected environments. Large-scale deployments of embedded devices also incentivizes the use of marginally cheaper hardware leaving little computational capacity to support various security functions such as malware or intrusion monitoring. This also stymies the ability to produce the amount of entropy required to create secure cryptographic keys [48]. The development of secure computation within embedded platforms provides a key challenge throughout CPSs.

1) Remote Attestation: Smart meters provide one particularly concerning utilization of embedded systems due to their expansive deployments and impact to consumers. Research into the development of remotely attestable smart meters has suggested that a small static kernel can be used to cryptographically sign loaded firmware [49]. This resulting signature can then be sent as a response to attestation queries to verify meters have not been corrupted. By also providing support for remote firmware updates the kernel can allow future reconfiguration of the devices while still providing a trusted platform. Unfortunately, these security mechanisms may still remain vulnerable to additional attack vectors [50].

Embedded devices also play important roles in the bulk power system. Intelligent electronic devices (IEDs) utilize embedded devices to control relays throughout the grid. Recent events have shown these devices can be maliciously reprogrammed to usurp intended control functions [5]. The development of improved attestation mechanisms will play a critical role in the cybersecurity enhancement of the grid.

C. Security Management and Awareness

An increased awareness of security risk and appropriately managing security relevant information provides an equally important role in maintaining a trusted infrastructure. This section will address a range of security activities and tools including digital forensics and security incident/event management.

1) Digital Forensics: The ability to perform accurate digital forensics within the electric grid is imperative to identify security failures and preventing future incidents. Strong forensic capabilities are also necessary during event investigation to determine the cause or extent of damage from an attack. While forensic analysis on traditional IT systems is well researched, the large number of embedded systems and legacy devices within the grid provides new challenges.

Research efforts by Chandia *et al.* have proposed the deployment of "forensic agents" throughout the cyber infrastructure to collect data about potential attacks [51]. Information collected by these agents can then be prioritized based on their ability to negatively affect grid operations.

Expanding forensic capabilities within embedded systems including meters and IEDs is necessary to ensure these critical resources maintain integrity. Additionally, operational systems may not be detached for forensics analysis, and research into online analysis methods should be explored for these instances.

2) Security Incident and Event Management: The development of technologies to collect and analyze interesting data sources such as system logs, IDS results and network flow information is necessary to ensure data are properly organized and prioritized. Briesemeister *et al.* researched the integration of various cybersecurity data sources within a control system and demonstrated its ability to detect attacks [52]. This work also coupled visualization tools to provide operators with a real-time understanding of network health. Tailoring this technology to provide efficient analysis of the grid will place an impetus on control system alarms as they provide information on potential physical impacts initiated by cyber attacks.

Incidents and events within the smart grid will vary greatly from their IT counterparts, analysis methods should be correlated with knowledge of the physical system to determine anomalies. Aggregation and analysis algorithms may need tailoring for environments with decreased incident rates due to smaller user bases and segregated networks.

D. Cybersecurity Evaluation

1) Cybersecurity Assessment: The grid's security postures should be continually analyzed to ensure it provides adequate security. The system's complexity, long lifespans, and continuously evolving cyber threats present novel attack vectors. The detection and removal of these security issues should be addressed specific to both the power applications and supporting infrastructure. Current research has primarily focused on the supporting infrastructure as it maintains many similarities with more traditional cyber security testing. Methodologies used to perform vulnerability assessments and penetration testing have raised numerous cybersecurity concerns within the current grid [53], [54].

Smart grid technologies will present increasing interdomain connectivity, thereby creating a more exposed cyber infrastructures and trust dependencies between many different parties. NIST's "Guidelines for Smart Grid Cyber Security" (NISTIR 7628) has proposed more robust set of cybersecurity requirements to ensure the appropriateness of cyber protection mechanism [2]. NIST identifies logical interfaces between systems and parties while assigning a criticality level (e.g., high, medium, low) for the interface's confidentiality, integrity, and availability requirements. The document then presents a list of necessary controls to provide an appropriate baseline security for the resulting interfaces.

2) Research Testbeds and Evaluations: Researching cyber–physical issues requires the ability to analyze the relationship between the cyber and physical components. Real-world data sets containing system architecture, power flows, and communication payloads are currently unavailable. Without these data researchers are unable to produce accurate solutions to modern problems. Increased collaboration between government, industry, and academia is required to produce useful data which can facilitate needed research. While SCADA testbeds provide a foundational tool for the basis of cyber–physical research, ensuring that system parameters closely represent real-world systems remains a challenge.

The development of SCADA testbeds provides critical resources to facilitate research within this domain. The National SCADA Test Bed (NSTB) hosted at Idaho National Laboratory provides a real-world test environment employing real bulk power system components and control software [55]. Resulting NSTB research has resulted in the discovery of multiple cyber vulnerabilities [56]. While this provides an optimal test environment, the cost is impractical for many research efforts. Work done by Sandia National Laboratory has utilized a simulation-based testbed allowing the incorporation of both physical and virtual components. The virtual control system environment (VCSE) allows the integration of various different power system simulators into a simulated network environment and industry standard control system software [57]. Academic efforts at Iowa State University and the University of Illinois at Urbana-Champaign provide similar environments [58], [59].

E. Intrusion Tolerance

While attempts to prevent intrusions are imperative to the development of a robust cyber infrastructure, failures in prevention techniques will likely occur. The ability to detect and tolerate intrusions is necessary to mitigate the negative effects from a successful attack.

1) Intrusion Detection Systems: The successful utilization of intrusion detection in the IT domain suggests it may also provide an important component in smart grid systems. Research by Cheung *et al.* has leveraged salient control system network properties into a basis for IDS technology [60]. Common data values, protocols functions, and communication endpoints were modeled by the IDS such that all violating packets could be flagged as malicious.

While the previous research provides unique detection capabilities, an attacker may still be able to create packets which closely resemble normal communications. For example, a command to trip a breaker cannot be flagged as malicious since it is a commonly used control function. Producing grid-aware intrusion detection will require a built-in understanding of grid functions. Work by Jin *et al.* shows how basic power flow laws leveraging Bayesian

reasoning can help reduce false positives by exhibiting a real-world understanding of the system [61].

The transition to smart grid technologies will likely reduce the number of IDS affable qualities compared to traditional SCADA communications. Performing intrusion detection in such a complex environment will require novel data collection mechanisms as well as the ability to detect and aggregate attack indicators across multiple network domains [62].

2) Tolerant Architectures: Intrusion tolerance mechanisms have recently have gained increased attention as a method to ensure a system's ability to operate effectively during an attack. Research within the Crutial project attempts to explore both proactive and reactive mechanisms to prevent cyber attacks from impacting the system's integrity [63]. This research explores a Byzantine tolerant protection paradigm which assures correct operations as long as no more than f out of $3f + 1$ components are attacked.

Extended research within intrusion tolerance should incorporate the smart grid specific availability requirements and infrastructure designs. Traditional models relaying on Byzantine fault/intrusion tolerance mechanism present significant cost and may not be practical within the smart grid. Future designs can leverage known physical system redundancies and recovery capabilities to assist with traditional intrusion/fault tolerance design models.

V. EMERGING RESEARCH CHALLENGES

As smart grid technologies become more prevalent, future research efforts must target a new set of cybersecurity concerns. This section documents emerging research challenges within this domain.

A. Risk Modeling

The risk modeling methodology and subsequent risk index should capture both, the vulnerability of cyber networks in the smart grid and the potential impacts an adversary could inflict by exploiting these vulnerabilities.

- The cyber *vulnerability assessment* plan in risk modeling should be thorough. It should include all sophisticated cyber-attack scenarios such as electronic intrusions, DoS, data integrity attacks, timing attacks, and coordinated cyber attacks. The tests should be conducted on different vendors solutions and configurations.
- The *impact analysis* should include dynamics introduced by new power system components and associated control, along with existing ones. The analyses must check to see if any power system stability limits are violated for different attack templates. For example, current wind generation turbines offer uneconomical frequency control and do not contribute to system inertia. Hence, attack scenarios should include attacks on the system during high wind penetration.
- Managing *exposure* from increased attacks surfaces due to the inclusion of the AMI and MDMS infrastructures, widespread communication links to distribution control centers, and potentially transmission and generation control centers. Impact studies should include attack vectors that target such devices and evaluate system stability.

B. Risk Mitigation Algorithms

As in the case of risk modeling, risk mitigation must include solutions at both the cyber and power system level. Consider the following attack scenario. One fundamental vision of the smart grid is to allow controllability of domestic devices by utilities to help reduce costs. If an adversary intrudes into the AMI network of a neighborhood to turn on large chunks of load when they are expected to be turned off, the system could experience severe stability problems. Cyber defense mechanisms that are able to detect/prevent such an attack, and power system defense mechanisms that ensure stable operation in the event of an attack, should be developed.

- *Attack resilient control* provides defense in depth to a CPS. In addition to dedicated cybersecurity software and hardware, robust control algorithms enhance security by providing security at the application layer. Measurements and other data obtained through the SCADA and emerging wide-area monitoring systems have to be analyzed to detect the presence of anomalies. For example, an application should first check if the obtained measurement lies within an acceptable range and reject the ones that do not comply. However, a smart attacker could develop attack templates that satisfy these criteria and force the operator into taking wrong control actions. Hence, additional tests that are based on forecasts, historical data and engineering sense should be devised to ascertain the current state of the system.

  An attack might not be successful if the malicious measurements do not conform to the dynamics of the system. In most cases, the physical parameters of the system (e.g., generator constants) are protected by utilities. These parameters play a part in determining the state of the system and system response to an event. Hence, algorithms that incorporate such checks could help in identifying malicious data when an attacker attempts to mislead the operator into executing incorrect commands.
- *Intelligent power system control algorithms* that are able to keep the system within stability limits during contingencies are critical. Additionally, the development of enhanced power management systems capable of addressing high-impact contingency scenarios is necessary.

- *Domain-specific anomaly detection and intrusion tolerance algorithms* that are able to classify measurements and commands as good/bad are key. In addition, built-in intelligence is required so that devices can respond appropriately to anomaly situations.

C. Coordinated Attack Defense

The power system, in most cases, is operated at (N-1) contingency condition and can inherently counter attacks that are targeted at single components. This means, the effect from the loss of a single transmission line can be negated by rerouting power through alternate lines. However, the system was not designed to fend against attacks that target multiple components. Such coordinated attacks, when carefully structured and executed, can push the system outside the protection zone. The increased attack surface introduced by the smart grid provides an opening for an adversary to plan such attacks.

The North American Electric Reliability Corporation (NERC) has instituted the Cyber Attack Task Force (CATF) to gauge system risk from such attacks and develop feasible, and cost-effective mitigation techniques [64]. Future mitigation strategies include the following.

- *Risk modeling and mitigation* of coordinated attacks is key to preventing the occurrence of attacks. Attack detection tools that monitor traffic and simultaneously correlate events at multiple substations could help in early identification of coordinated attack scenarios.
- Future power system *planning and reliability studies* should accommodate coordinated attack scenarios in its scope. Strategic enhancements to the power system infrastructure could help the system operate within stability limits during such scenarios.

D. AMI Security

Geographically distributed architectures with high availability requirements present numerous security and privacy concerns. Specific research challenges with AMI include:

- *remote attestation of AMI components* and tamper detection mechanisms to prevent meter manipulations;
- exploration of *security failures* due to common modal failures (e.g., propagating malware, remotely exploitable vulnerabilities, shared authenticators);
- *model-based anomaly methods* to determine attacks based on known usage patterns and fraud/attack detection algorithms;
- *security versus privacy tradeoffs* including inference capabilities of consumer habits, anonymization mechanisms, anonymity concerns from both data-at-rest and data-in-motion perspectives.

Numerous additional privacy concerns have been raised within the smart grid; NIST has provided a more comprehensive review of these concerns [2].

E. Trust Management

The dynamic nature for the smart grid will require complex notions of trust to evaluated the acceptability of system inputs/outputs.

- *Dynamic trust distribution* with adaptability for evolving threats and likely cybersecurity failures (e.g., exposed authenticator, unpatched systems) and grid emergencies (e.g., cascading failures, natural disasters, personnel issues).
- *Trust management* based on data source (e.g., SCADA field device, adjacent utilities) and verification of trust allocations for low-trust systems (physically unprotected, limited attribution capabilities), along with trust verification mechanisms/algorithms and impact analysis of trust manipulation mechanisms.
- Aggregation of trust with increasing data/verification sources (e.g., more sensors, correlations with previous knowledge of grid status) and accumulation of trust requirements throughout AMI.

F. Attack Attribution

Attack attribution will play an important role in deterrence within the smart grid. High availability requirements limit the ability to disconnect potential victims within the control network, especially when steeping-stone attack methods are used.

- Attribution capabilities within/between controlled networks including AMI, wide area measurement systems, and control networks.
- Leveraging known information flows, data formats, and packet latencies.
- Identifying stepping-stone attacks with utility owned/managed infrastructures based on timing analysis, content inspection, packet marking/logging schemes.
- Methods to reduce *insider threat* impacts while maintaining appropriate adaptability in emergency situations such as improved flexibility of authorization and authentication or defense-in-depth implementations.

G. Data Sets and Validation

Research within the smart grid realm requires realistic data and models to assure accurate results and real-world applicability.

- Data models for SCADA networks, AMI, wide area monitoring networks including communication protocols, common information models (CIM), data sources/sinks.
- Temporal requirements for data (e.g., 4 ms for protective relaying, 1–4 s for SCADA, etc.) and realistic

data sets of control-loop interactions (e.g., AGC, voltage regulation, substation protection schemes).

VI. CONCLUSION

A reliable smart grid requires a layered protection approach consisting of a cyber infrastructure which limits adversary access and resilient power applications that are able to function appropriately during an attack. This work provides an overview of smart grid operation, associated cyber infrastructure and power system controls that directly influence the quality and quantity of power delivered to the end user. The paper identifies the importance of combining both *power application security* and *supporting infrastructure security* into the risk assessment process and provides a methodology for impact evaluation. A smart grid control classification is introduced to clearly identify communication technologies and control messages required to support these control functions. Next, a review of current cyber infrastructure security concerns are presented to both identify possible weaknesses and address current research efforts. Future smart grid research challenges are then highlighted detailing the cyber–physical security relationship within this domain. While this work focuses on the smart grid environment, the general application and infrastructure framework including many of the research concerns will also transition to other critical infrastructure domains. ■

REFERENCES

[1] *A Systems View of the Modern Grid*, National Energy Technology Laboratory (NETL), U.S. Department of Energy (DOE), 2007.

[2] *NISTIR 7628: Guidelines for Smart Grid Cyber Security*, National Institute for Standards and Technology, Aug. 2010.

[3] *GAO-04-354: Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems*, U.S. Government Accountability Office (GAO), Mar. 2004.

[4] *NERC Critical Infrastructure Protection (CIP) Reliability Standards*, North American Electric Reliability Corporation, 2009.

[5] N. Falliere, L. Murchu, and E. Chien, "W32.Stuxnet Dossier, Version 1.3," Symantec, Nov. 2010.

[6] S. Baker, S. Waterman, and G. Ivanov, "Crossfire: Critical infrastructure in the age of cyber war," McAfee, 2009.

[7] *GAO-11-117: Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*, U.S. Government Accountability Office (GAO), Jan. 2011.

[8] G. Stoneburner, A. Goguen, and A. Feringa, "NIST SP 800-30: Risk management guide for information technology systems," National Institute of Standards and Technology, Tech. Rep., Jul. 2002.

[9] K. Stouffer, J. Falco, and K. Scarfone, "NIST SP 800-82: Guide to industrial control systems (ICS) security," National Institute of Standards and Technology, Tech. Rep., Sep. 2008.

[10] *Common Cybersecurity Vulnerabilities in Industrial Control Systems*, Department of Homeland Security (DHS) Control Systems Security Program (CSSP), May 2011.

[11] J.-C. Laprie, K. Kanoun, and M. Kaniche, "Modelling interdependencies between the electricity and information infrastructures," in *Comput. Safety, Reliability, Security*, vol. 4680, F. Saglietti and N. Oster, Eds. Berlin, Germany: Springer-Verlag, 2007, pp. 54–67.

[12] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 244–249.

[13] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst. Man Cybern. A, Syst. Humans*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[14] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[15] Y.-L. Huang, A. A. Cardenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry. (2009). Understanding the physical and economic consequences of attacks on control systems. *Int. J. Critical Infrastructure Protect.* [Online]. *2(3)*, pp. 73–83. Available: http://www.sciencedirect.com/science/article/pii/S1874548209000213

[16] C. J. Mozina, M. Reichard, Z. Bukhala, S. Conrad, T. Crawley, J. Gardell, R. Hamilton, I. Hasenwinkle, D. Herbst, L. Henriksen, G. Johnson, P. Kerrigan, S. Khan, G. Kobet, P. Kumar, S. Patel, B. Nelson, D. Sevcik, M. Thompson, J. Uchiyama, S. Usman, P. Waudby, and M. Yalla, "Coordination of generator protection with generator excitation control and generator capability; working group j-5 of the rotating machinery subcommittee, power system relay committee," in *Proc. IEEE Power Eng. Soc. General Meeting*, Jun. 2007, DOI: 10.1109/PES.2007.386034.

[17] *GE EX2100 Excitation Systems*. [Online]. Available: http://www.ge-mcs.com/en/generator-control-and-protection/ex-excitation-systems/ex2100.html

[18] *ABB 800xA Turbine Governor*. [Online]. Available: http://www.abb.com/product/us/9AAC115756.aspx

[19] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," in *Proc. Amer. Control Conf.*, Jul. 2010, pp. 962–967.

[20] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *Proc. Power Energy Soc. General Meeting*, Jul. 2010, DOI: 10.1109/PES.2010.5590115.

[21] L. Mili, T. Van Cutsem, and M. Ribbens-Pavella, "Bad data identification methods in power system state estimation—A comparative study," *IEEE Power Eng. Rev.*, vol. PER-5, no. 11, pp. 27–28, Nov. 1985.

[22] A. Monticelli and A. Garcia, "Reliable bad data processing for real-time state estimation," *IEEE Trans. Power Apparat. Syst.*, vol. PAS-102, no. 5, pp. 1126–1139, May 1983.

[23] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power Apparat. Syst.*, vol. PAS-94, no. 2, pp. 329–337, Mar. 1975.

[24] A. Garcia, A. Monticelli, and P. Abreu, "Fast decoupled state estimation and bad data processing," *IEEE Trans. Power Apparat. Syst.*, vol. PAS-98, no. 5, pp. 1645–1652, Sep. 1979.

[25] X. Nian-de, W. Shi-ying, and Y. Er-keng, "A new approach for detection and identification of multiple bad data in power system state estimation," *IEEE Trans. Power Apparat. Syst.*, vol. PAS-101, no. 2, pp. 454–462, Feb. 1982.

[26] V. Quintana, A. Simoes-Costa, and M. Mier, "Bad data detection and identification techniques using estimation orthogonal methods," *IEEE Trans. Power Apparat. Syst.*, vol. PAS-101, no. 9, pp. 3356–3364, Sep. 1982.

[27] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*. New York: ACM, 2009, pp. 21–32.

[28] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," in *Proc. 44th Annu. Conf. Inf. Sci. Syst.*, Mar. 2010, DOI: 10.1109/CISS.2010.5464816.

[29] D. Callaway and I. Hiskens, "Detecting false data injection attacks on DC state estimation," in *Proc. 1st Workshop Secure Control Syst.*, Apr. 2010. [Online]. Available: https://www.truststc.org/conferences/10/CPSWeek/papers.htm

[30] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 226–231.

[31] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation and Control*, 2nd ed.

Hoboken, NJ: Wiley-Interscience, Jan. 1996. [Online]. Available: http://www.amazon.com/Power-Generation-Operation-Control-Allen/dp/0471586994

[32] L. R. Phillips, M. Baca, J. Hills, J. Margulies, B. Tejani, B. Richardson, and L. Weiland, *Analysis of Operations and Cyber Security Policies for a System of Cooperating Flexible Alternating Current Transmission System (FACTS) Devices*, Dec. 2005.

[33] S. Sridhar and G. Manimaran, "Data integrity attack and its impacts on voltage control loop in power grid," in *Proc. IEEE Power Energy Soc. General Meeting*, Detroit, MI, Jul. 2011.

[34] A. Phadke and J. S. Thorp, *Synchronized Phasor Measurements and Their Applications*. New York: Springer-Verlag, 2008.

[35] J. Dagle, "The North American synchrophasor initiative (NASPI)," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2010, DOI: 10.1109/PES.2010.5590048.

[36] J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*. New York: Momentum Press, May 2010.

[37] D. Callaway and I. Hiskens, "Achieving controllability of electric loads," *Proc. IEEE*, vol. 99, no. 1, pp. 184–199, Jan. 2011.

[38] *Security Profile for Advanced Metering Infrastructure, v2.0*, The Advanced Security Acceleration Project (ASAP-SG), Jun. 2010.

[39] R. Anderson and S. Fuloria, "Who controls the off switch?" *2010 1st Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, pp. 96–101, Oct. 4–6, 2010, DOI: 10.1109/SMARTGRID.2010.5622026. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5622026&isnumber=5621989

[40] P. Tsang and S. Smith, "YASIR: A low-latency, high-integrity security retrofit for legacy SCADA systems," in *Proc. IFIP TC 11 23rd Int. Inf. Security Conf.*, vol. 278, S. Jajodia, P. Samarati, and S. Cimato, Eds. Boston, MA: Springer-Verlag, 2008, pp. 445–459.

[41] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, "DNPSec: Distributed network protocol version 3 (DNP3) security framework," in *Adv. Comput., Inf., Syst. Sci., Eng.*, K. Elleithy, T. Sobh, A. Mahmood, M. Iskander, and M. Karim, Eds. Amsterdam, The Netherlands: Springer-Verlag, 2006, pp. 227–234.

[42] I. Fovino, A. Carcano, M. Masera, and A. Trombetta, "Design and implementation of a secure Modbus protocol," in *Critical Infrastructure Protection III*, vol. 311, C. Palmer and S. Shenoi, Eds. Boston, MA: Springer-Verlag, 2009, pp. 83–96.

[43] J. T. Michalski, A. Lanzone, J. Trent, and S. Smith, "SAND2007-3345: Secure ICCP Integration Considerations and Recommendations," Sandia National Laboratories, Jun. 2007.

[44] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, "Design principles for power grid cyber-infrastructure authentication protocols," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, Washington, DC, 2010, DOI: 10.1109/HICSS.2010.136.

[45] R. Chakravarthy, C. Hauser, and D. E. Bakken, "Long-lived authentication protocols for process control systems," *Int. J. Critical Infrastructure Protect.*, vol. 3, no. 3–4, pp. 174–181, 2010.

[46] T. Mander, R. Cheung, and F. Nabhani, "Power system DNP3 data object security using data sets," *Comput. Security*, vol. 29, no. 4, pp. 487–500, 2010.

[47] S. East, J. Butts, M. Papa, and S. Shenoi, "A taxonomy of attacks on the DNP3 protocol," in *Critical Infrastructure Protection III*, vol. 311, C. Palmer and S. Shenoi, Eds. Boston, MA: Springer-Verlag, 2009, pp. 67–81.

[48] P. Koopman, "Embedded system security," *Computer*, vol. 37, pp. 95–97, Jul. 2004.

[49] M. LeMay and C. A. Gunter, "Cumulative attestation kernels for embedded systems," in *Proc. 14th Eur. Conf. Res. Comput. Security*. Berlin, Germany: Springer-Verlag, 2009, pp. 655–670.

[50] C. Castelluccia, A. Francillon, D. Perito, and C. Soriente, "On the difficulty of software-based attestation of embedded devices," in *Proc. 16th ACM Conf. Comput. Commun. Security*, 2009, pp. 400–409.

[51] R. Chandia, J. Gonzalez, T. Kilpatrick, M. Papa, and S. Shenoi, "Security strategies for SCADA networks," in *Critical Infrastructure Protection*, vol. 253, E. Goetz and S. Shenoi, Eds. Boston, MA: Springer-Verlag, 2007, pp. 117–131.

[52] L. Briesemeister, S. Cheung, U. Lindqvist, and A. Valdes, "Detection, correlation, visualization of attacks against critical infrastructure systems," in *Proc. 8th Annu. Int. Conf. Privacy Security Trust*, Aug. 2010, pp. 15–22.

[53] R. C. Parks, "SAND2007-7328: Guide to critical infrastructure protection cyber vulnerability assessment," Sandia National Laboratories, Nov. 2007.

[54] M. R. Permann and K. Rohde, "Cyber assessment methods for SCADA security," The Instrumentation, Systems and Automation Society (ISA), Tech. Rep., 2005.

[55] *National SCADA Test Bed: Fact Sheet*, Idaho National Laboratory (INL), 2007.

[56] *NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses*, Idaho National Laboratory (INL), May 2010.

[57] M. J. McDonald, G. N. Conrad, T. C. Service, and R. H. Cassidy, "SAND2008-5954: Cyber effects analysis using VCSE, promoting control system reliability," Sandia National Laboratories, Sep. 2008.

[58] A. Hahn, B. Kregel, M. Govindarasu, J. Fitzpatrick, R. Adnan, S. Sridhar, and M. Higdon, "Development of the POWERCYBER SCADA security testbed," in *Proc. 6th Annu. Workshop Cyber Security Inf. Intell. Res.*, 2010, pp. 21-1–21-4.

[59] D. C. Bergman, D. Jin, D. M. Nicol, and T. Yardley, "The virtual power system testbed and inter-testbed integration," in *Proc. 2nd Workshop Cyber Security Experiment. Test*, Aug. 2009, pp. 1–6.

[60] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, S. K., and A. Valdes, "Using model-based intrusion detection for SCADA networks," in *Proc. SCADA Security Sci. Symp.*, Jan. 2007.

[61] X. Jin, J. Bigham, J. Rodaway, D. Gamez, and C. Phillips, "Anomaly Detection in Electricity Cyber Infrastructures," *Proc. Int. Workshop CNIP 2006*, 2006.

[62] R. Berthier, W. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 350–355.

[63] P. Sousa, A. Bessani, M. Correia, N. Neves, and P. Verissimo, "Highly available intrusion-tolerant services with proactive-reactive recovery," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 4, pp. 452–465, Apr. 2010.

[64] *Scope of Cyber Attack Task Force (CATF)*, North American Electric Reliability Corporation, 2011.

ABOUT THE AUTHORS

Siddharth Sridhar (Student Member, IEEE) received the B.E. degree in electrical and electronics engineering from The College of Engineering, Guindy (Anna University), India, in 2004. He is currently working towards the Ph.D. degree in computer engineering at the Department of Electrical and Computer Engineering, Iowa State University, Ames.

His research interests are in the application of intelligent cybersecurity methods to power system monitoring and control.

Adam Hahn (Student Member, IEEE) received the B.S. degree in computer science from the University of Northern Iowa, Cedar Falls, in 2003 and the M.S. degree in computer engineering from Iowa State University (ISU), Ames, in 2006, where he is currently working towards the Ph.D. degree at the Department of Electrical and Computer Engineering.

He is currently an Information Security Engineer at the MITRE Corporation and has participated in Institute for Information Infrastructure Protection (I3P) projects. His research interests include cyber vulnerability assessment, critical infrastructure cybersecurity, and smart grid technologies.

Manimaran Govindarasu (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the Indian Institute of Technology (IIT), Chennai, India, in 1998.

He is currently a Professor in the Department of Electrical and Computer Engineering, Iowa State University, Ames, and he has been on the faculty there since 1999. His research expertise is in the areas of network security, real-time embedded systems, and cyber-physical security of smart grid. He has recently developed cybersecurity testbed for smart grid at Iowa State University to conduct attack-defense evaluations and develop robust countermeasures. He has coauthored more than 125 peer-reviewed research publications.

Dr. Govindarasu has given tutorials at reputed conferences (including IEEE INCOFOM 2004 and IEEE ComSoc *Tutorials Now*) on the subject of cybersecurity. He has served in technical program committee as chair, vice-chair, and member for many IEEE conferences/workshops, and served as session chair in many conferences. He is a coauthor of the text *Resource Management in Real-Time Systems and Networks* (Cambridge, MA: MIT Press, 2001). He has served as guest coeditor for several journals including leading IEEE magazines. He has contributed to the U.S DoE NASPInet Specification project and is currently serving as the chair of the Cyber Security Task Force at IEEE Power and Energy Systems Society (PES) CAMS subcommittee.