Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid

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

***Abstract*—The development of a smarter electric grid will depend on increased deployments of information and communication technology (ICT) to support novel communication and control functions. Unfortunately, this additional dependency also expands the risk from cyber attacks. Designing systems with adequate cyber security depends heavily on the availability of representative environments, such as testbeds, where current issues and future ideas can be evaluated. This paper provides an overview of a smart grid security testbed, including the set of *control*, *communication*, and *physical system* components required to provide an accurate cyber-physical environment. It then identifies various testbed research applications and also identifies how various components support these applications. The PowerCyber testbed at Iowa State University is then introduced, including the architecture, applications, and novel capabilities, such as virtualization, Real Time Digital Simulators (RTDS), and ISEAGE WAN emulation. Finally, several attack scenarios are evaluated using the testbed to explore cyber-physical impacts. In particular, availability and integrity attacks are demonstrated with both isolated and coordinated approaches, these attacks are then evaluated based on the physical system's voltage and rotor angle stability.**

***Index Terms*—Cyber-physical systems, cyber security, smart grid, testbeds.**

I. Introduction

CYBER security incidents have gained increasing credibility as viable risks to the electric grid. Recent analysis of the grid's current security posture has raised numerous inadequacies [1], [2], while reports have addressed attackers increasingly targeting critical infrastructure [3]. The adoption of smart grid technologies will significantly increase the importance of cyber security due to more substantial ICT dependencies. The U.S. Department of Energy (DOE) has documented attack resiliency as a primary requirement for the next generation grid [4]. The National Institute for Standards and Technology (NIST) has thoroughly enumerated many cybersecurity concerns with the adoption of new technologies such as advanced metering infrastructures (AMI), distributed energy resources (DER), and phasor measurement unit (PMU) based wide area measurement systems (WAMS) [5].

Attempts to research cyber security enhancements are constrained by the availability of realistic cyber-physical environments. Testbeds that integrate both cyber and physical components provide ideal environments to perform and evaluate research efforts. Unfortunately, the testbed development process is not well established due to the complexity of integrating cyber and physical resources while also incorporating simulation mechanisms to model power systems, cyber network dynamics, and security events. Various design strategies will naturally lend themselves to different research areas, therefore, an understanding of development constraints is important to enhance future efforts. This paper provides a review of key testbed research applications and also presents a conceptual testbed architecture.

This paper then documents the implementation of the PowerCyber cyber-physical testbed which integrates industry supervisory control and data acquisition (SCADA) hardware and software along with emulation and simulation techniques to provide an accurate electric grid cyber infrastructure. The testbed employs virtualization technologies to address scalability concerns and reduce development cost. The testbed has also been integrated with the ISEAGE project at Iowa State to provide wide-area network emulation and advanced attack simulation. Power simulations are performed with a real time digital simulator (RTDS) for real time evaluations and DIgSILIENT PowerFactory software for non-real time analysis.

The remainder of the paper is organized as follows. Section II enumerates previous testbed development efforts and identifies salient features of those efforts. Section III introduces applications of a cyber security testbed based on current research demands and testbed capabilities. Section IV provides an introduction of the PowerCyber testbed at Iowa State and presents a thorough review of its capabilities. Finally, Section V demonstrates the utility of the testbed by presenting various research efforts currently being performed in the environment.

II. Related Work

Smart grid testbed have been developed at various universities and national labs to research cyber security concerns. A foundational testbed initiative is the National SCADA TestBed (NSTB) which represents a national lab collaborative project. This environment implements actual physical grid components including generation and transmission, while also incorporating industry standard software products [6]. Resulting research on the testbed has identified numerous cyber vulnerabilities and contributed to the production of SCADA-specific security assessment methodologies [2], [7]. Unfortunately, the substantial

Manuscript received April 11, 2012; accepted August 19, 2012. Date of publication March 07, 2013; date of current version May 18, 2013. This work was supported by the National Science Foundation under Grant 0915945). Paper no. TSG-00205-2012.

The authors are with the Iowa State University, Electrical and Computer Engineering, Ames, IA 50011 USA (e-mail: adamhahn@iastate.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2012.2226919

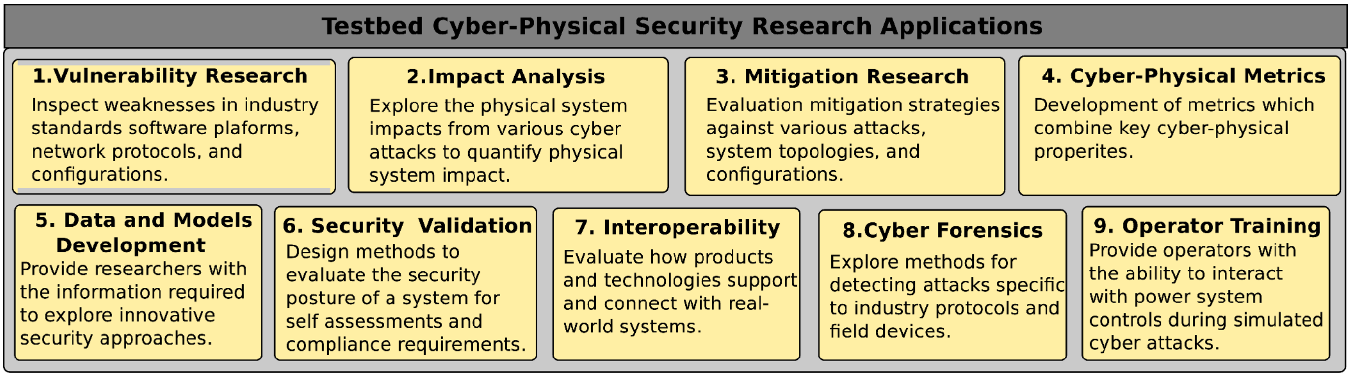
Testbed Cyber-Physical Security Research Applications
1.Vulnerability Research
Inspect weaknesses in industry standards software plaforms, network protocols, and configurations.
2.Impact Analysis
Explore the physical system impacts from various cyber attacks to quantify physical system impact.
3. Mitigation Research
Evaluation mitigation strategies against various attacks, system topologies, and configurations.
4. Cyber-Physical Metrics
Development of metrics which combine key cyber-physical properites.
5. Data and Models Development
Provide researchers with the information required to explore innovative security approaches.
6. Security Validation
Design methods to evaluate the security posture of a system for self assessments and compliance requirements.
7. Interoperability
Evaluate how products and technologies support and connect with real-world systems.
8.Cyber Forensics
Explore methods for detecting attacks specific to industry protocols and field devices.
9. Operator Training
Provide operators with the ability to interact with power system controls during simulated cyber attacks.

Fig. 1. Testbed applications.

cost of deploying purely physical testbed limits the practicality of similar efforts.

Sandia National Laboratory developed the Virtual Control System Environment (VCSE) which integrates simulation, emulation, and physical systems to provide more cost-effective and reconfigurable platform [8], [9]. VCSE utilizes OPNET System-in-the-Loop emulation to allow the integration of physical network devices with the simulated network. This enables communication between both physical and emulated PLCs and the PowerWorld power system simulator. VCSE also utilizes a centralized model/simulation management tool, Umbra, to provide control over the various components. VCSE was designed to provide support for operator training, vulnerability exploration, mitigation development, and evaluation activities.

A similar project at the University of Illinois has produced the Virtual Power System Testbed (VPST) which also combines both simulation and physical elements [10]. The testbed is similar to VCSE as it uses a PowerWorld power system simulator, while network integration is based on the Illinois-developed Real-Time Immersive Network Simulation Environment (RINSE) project. These components are then integrated with physical devices and industry-standard software products to provide a realistic control environment.

The European CRUTIAL project has deployed two different testbeds to explore impacts from various attack scenarios [11], [12]. The first testbed is focused primarily on telecommunications within the electric grid by evaluating the transmission of IEC 60870-5-104 traffic between a set of simulated substations and control centers. Specific experiments have focused on evaluating the communication system's ability to withstand various DoS attacks. Additionally, a microgrid evaluation testbed has been developed through the interconnection of a physical microgrid environment controlled by emulated IED devices. The IEDs then communicate over a LAN to a Matlab/Simulink system which performs the resulting controls. This environment is being used to identify potential vulnerabilities in DER implementations.

The Testbed for Analyzing Security of SCADA Control Systems (TASSCS) has been developed at the University of Arizona to perform anomaly-based intrusion detection research [13]. The testbed utilizes OPNET System-in-the-Loop network emulation similar to Sandia's VCSE and also utilizes PowerWorld software to provide a simulated electric grid. A simulation-based control solution is presented using Modbus RSim software which then communicates with the PowerWorld simulator.

A testbed at the University College Dublin (UCD) is based on industry standard software/hardware with a DIgSILENT power system simulator to provide an environment to both identify attacks and evaluate physical impact [14]. Research on intrusion and anomaly detection capabilities is being performed within this environment.

Finally, the SCADASim testbed has been developed at Royal Melbourne Institute of Technology (RMIT) University to enable the exploration of network performance under cyber attack [15]. The SCADASim testbed focuses on developing an emulated communication infrastructure that can be used to interconnect physical devices utilizing common SCADA protocols. The testbed can then be used to analyze how cyber attacks impact the system's communication requirements.

III. Testbed Research Applications and Design

The review of previous development efforts has demonstrated numerous research applications currently being supported with testbeds. This section provides a more thorough analysis of research efforts which benefit from a cyber-physical testbed. It then introduces high-level testbed design elements and presents a mapping of these application dependencies on testbed control, communication, and physical elements.

A. Research Applications

A comprehensive set of testbed applications are identified in Fig. 1 and elaborated upon in greater detail below.

1) Vulnerability Research: Cyber-physical systems utilize different software, hardware, communications protocols and physical media. Many of the technologies used within this environment are not publicly available which significantly constrains the amount of vulnerability research that can performed by security researchers. Fortunately, testbeds provide areas where vulnerability assessment activities can be performed, including vulnerability scanning, cryptography analysis, and software testing methods such as fuzzing. Other testbed environments, such as INL's NSTB, have been utilized to identify numerous cyber vulnerabilities in various control system components [2], [16]. This research will help ensure that software platforms, configurations, and network architectures have been adequately analyzed for weaknesses.

2) Impact Analysis: Another key testbed application is the evaluation of physical impacts from different types of cyber security attacks and incidents [17]. The complexity and interdependencies within both the cyber and physical systems complicate current impact analysis methods. Testbeds help capture the risk posed by a particular security event through the ability to determine impact on grid stability and power flow. Various attack strategies can be explored including sophisticated coordinated attacks and insider threats. Additionally, various power system topologies, operator responses, and cyber vulnerabilities can be explored to determine their ability to mitigate physical system impacts.

3) Mitigation Evaluation: Testbeds also present a useful environment to explore the effectiveness of various mitigation strategies. Mitigation efforts should attempt to reduce the vulnerability of the cyber infrastructure while increasing the robustness of the power applications [18]. One particular area where testbeds will be useful is in the development of *attack resilient control algorithms* that can be evaluated within a realistic environment to explore their performance and reliability.

4) Cyber-Physical Metrics: The development of cyber-physical metrics is imperative to improving cyber security and increasing grid resiliency. Testbeds produce an environment where controlled evaluations can be performed to support metric development and evaluation. This is specifically relevant within the cyber-physical systems as metrics must combine multiple domains. On the physical side, metrics can be evaluated based on the impact to power flow, stability, and even markets. Cyber security metrics can incorporate vulnerability criticality (such as CVSS [19]), vulnerability patch installation rates, and other methods to explore both system correctness and organizational security objectives [20].

5) Data and Model Development: Currently real world data about the electric grid's cyber resources and vulnerabilities are limited as they are sensitive to the utility's operation. Testbed environments may also help develop models and datasets which can be disseminated to researchers to facilitate more accurate analysis and results. Models and datasets could incorporate power system models, network architectures, protocols, and data.

6) Security Validation: Cyber security compliance requirements (e.g., NERC CIP) are becoming increasingly common as a means to ensure critical resources are appropriately protected. Unfortunately, the process of evaluating security mechanisms is not well established within this environment. The electric grid's high availability demands and the heavy utilization of proprietary systems limit the applicability of common vulnerability scanning techniques [21]. Since the effectiveness of compliance depends heavily on the security validation process, effective methods are required to ensure requirements are appropriately enforced. Testbed environments that implement industry standard software and configurations can help understand both impacts and effectiveness of traditional security assessment techniques while also presenting an environment where new methods can be explored.

7) Interoperability: Testbeds also present a distinct opportunity to explore system interoperability within a realistic environment. This may be beneficial for both vendor products and research efforts from industry, academia, and national laboratories. Interoperability testing may include activities such as 1) communication/protocol connectivity, 2) realistic availability requirements, 3) data collection and aggregation requirements, and 4) operator interface design evaluation.

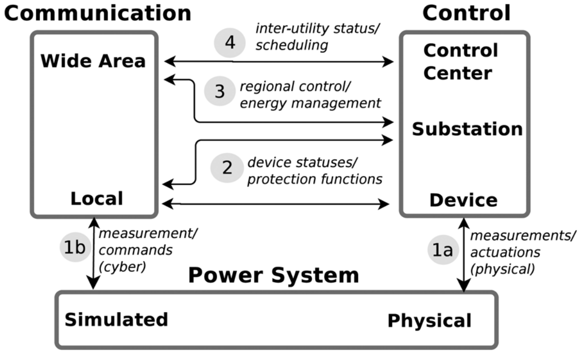
Communication
Control
Wide Area
Local
Control Center
Substation
Device
4
inter-utility status/ scheduling
3
regional control/ energy management
2
device statuses/ protection functions
1b
measurement/ commands (cyber)
1a
measurements/ actuations (physical)
Power System
Simulated
Physical

Fig. 2. Logical testbed architecture.

8) Cyber Forensics: Cyber-based forensics presents another important area of future research [22]. Field devices depend heavily on embedded systems which utilize different operating systems and software platforms. Recent events have also shown that cyber attacks can be used to modify the operational logic of the PLCs [23]. Without some ability to forensically analyze these devices, there is little chance of detecting intrusions. Testbeds play a key role in this analysis as they present an environment where device functionality can be analyzed, specifically, whether they respond correctly to commands and return accurate measurements.

9) Operator Training: Cyber incidents may be responsible for unusual power system failures, especially when combined with physical faults [24]. Testbeds present the opportunity to both analyze these situations and demonstrate how a realistic attack would look to system operators. Therefore, testbeds may provide training applications to help identify differentiated failures from both cyber and physical.

B. Testbed Design Elements

This section presents a high-level overview of testbed components and their support of testbed applications. Testbed components can be categorized into *communication*, *control* and *power systems* elements. Fig. 2 shows a logical testbed architecture and specifically identifies these components. The diagram first displays how measurements and actuations are either sensed from physical devices, *1a*, or simulated and transmitted over network, *1b*. Item 2 displays how information such as device statuses, commands, and protection functions are transmitted through the substation. Item 3 demonstrates the substation communications to other systems in the WAN for regional control and energy management functions. Finally, item 4 shows WAN communication between control centers for system scheduling and status data.

Table I identifies the requirements for the testbed's control, communication, and physical system components in order to support the previously identified research initiatives. The following list identifies the various testbed components in this table.

TABLE I
RESEARCH EFFORTS TO TESTBED CAPABILITY MAPPING

	Control			Communication			Physical System		
Research Objectives	Software	Hardware	Algorithms	Protocols	Architectures	Performance	Scalability	Real Time	HW Interface
Vulnerability Research	●	●	◖	●	●	◖	○	○	○
Impact Analysis	◖	◖	●	◖	◖	◖	●	●	●
Mitigation Evaluation	◖	◖	◖	◖	◖	◖	◖	◖	●
Metric Development	◖	◖	◖	◖	◖	◖	◖	◖	◖
Security Validation	●	●	◖	●	◖	◖	○	○	○
Data Model Development	◖	◖	●	●	●	◖	◖	○	◖
Interoperability	●	●	◖	●	◖	○	○	○	◖
Cyber Forensics	●	●	◖	●	●	○	○	○	◖
Operator Training	◖	◖	●	◖	◖	●	●	●	◖

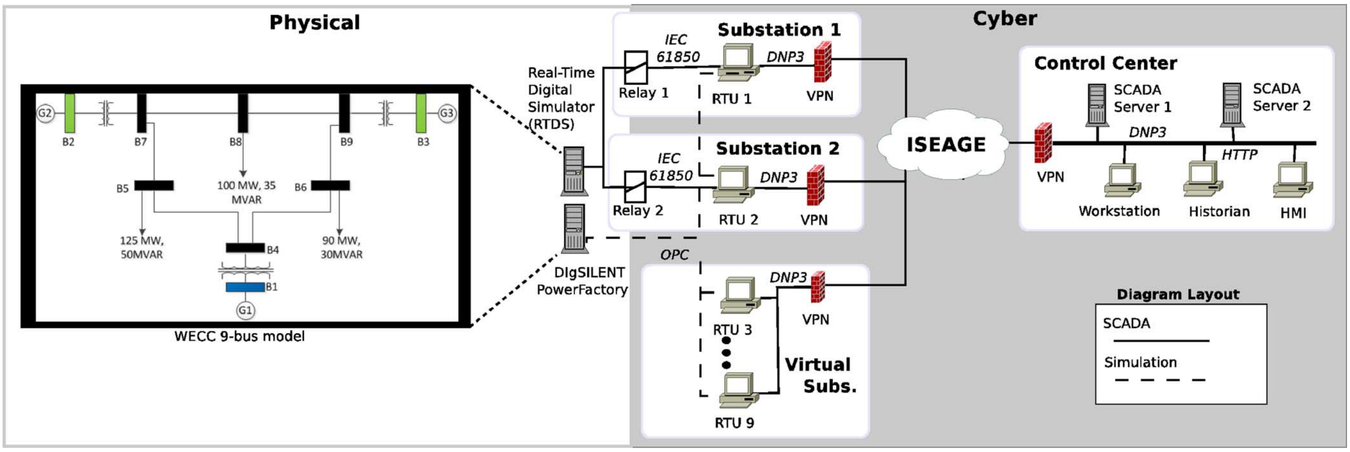

Fig. 3. PowerCyber testbed architecture.

- Software—the various SCADA and energy management system (EMS) applications that monitor and control the physical system.
- Hardware—the IEDs and PLCs that bridge the cyber and physical domains.
- Algorithms—the logic to calculate grid observability and perform automated control functions.
- Protocols—the numerous real-worlds SCADA network protocols.
- Architectures—accuracy of the network layout to current smart grid network topologies.
- Performance—similarities between the networks throughput and latency.
- Scalability—the size of the the power system that can be simulated.
- Real-Time—the simulators ability to compute updated grid state in real-time.
- HW Interface—whether the power system simulator can be interfaced with the actual IEDs.

IV. ISU's PowerCyber Testbed Architecture

This section describes the architecture and capabilities of the PowerCyber testbed at Iowa State University (ISU), specifically highlighting the communication, control, and physical system simulation components. The testbed currently utilizes an array of real, emulated, and simulated components to provide a realistic cyber and physical environment [25]. Fig. 3 demonstrates the testbed's architecture, which will be elaborated upon in the remainder of this section.

A. Control

The control functions within the electric grid consist of a variety of human-in-the-loop and closed loop mechanisms used to manage the grid's reliability and efficiency. The grid's control mechanisms can be divided into those performed by the centralized control centers and those distributed into the substations. The testbed utilizes industry standard software for all control functions to enable realistic cyber vulnerability research.

1) Control Center: The testbed's control center is configured to support general SCADA functions, which includes collecting measurements and device statuses from field devices, forwarding operator commands to various field devices, and managing historic data about system operations. These functions are supported with industry standard SCADA servers, Human Machine Interfaces (HMIs) and Historian servers.

Control operations within the control center focus on human-in-the-loop approaches. The SCADA communications occurs between the SCADA servers and a software-based remote terminal units (RTU) system located within each substation. The SCADA server polls the status of the substation's various devices every second and displays the acquired information to the operator through the HMI. The operator can then choose to modify system's operation by sending commands to the substations. All of the data collected by the control center is then stored within the historian server for future analysis.

2) Substations: In addition to the control center, the testbed also includes substations to interface with the power system simulations. Substations consists of both RTUs and intelligent electronic devices (IEDs). Substations within the testbed are modeled two ways: 1) using a combination of dedicated RTU systems connected to physical IEDs (overcurrent protection relays) and 2) using virtualized substations connected directly to virtual IEDs modeled by the power system simulators. In both scenarios the RTUs are responsible for aggregating data from either physical or virtualized IEDs and transmitting it back to the control center. The IEDs within the environment are over-current protection relays which can be used to perform current and voltage measurements from transmission lines and then communicated with RTUs.

Control functions within the substation include both protection and human-in-the-loop control methods. Various automated protection functions can also be configured between the physical IEDs. The IEDs can be dynamically configured to transmit their status and detected faults to other IEDs to ensure they are automatically cleared before system damage occurs.

B. Communication

The important components of the communication infrastructure include both the physical network architecture and network protocols. Supporting the grid's wide array of monitoring and control functions requires numerous LAN and WAN environments, along with specialized communication protocols.

1) Wide Area Networks: Communication between the control center and substation RTUs is performed with the DNP3 protocol similar to many real-world SCADA systems. DNP3 currently operates over IP to enable routeable networks. Since the WAN will be externally exposed, the communication is protected in transit with IPSec-based VPNs implemented with industry specific network security devices. In addition to the use of DNP3, the ISEAGE project has been integrated into the lab to replicate the scale and exposure properties of a real WAN.

ISEAGE: The Internet-Scale Event and Attack Generation Environment (ISEAGE) testbed was developed independently to provide a scalable Internet environment to perform cyber attack and defense simulations [26]. ISEAGE integration within the testbed provides the following benefits: 1) large cyber infrastructure modeling, 2) network traffic collection, and 3) coordinated attack simulation.

The core function of ISEAGE is a configurable emulation of an IP-based routing topology. ISEAGE will emulate a desired network topology while providing physical interfaces to the various network segments to support integration with physical networks and devices. By utilizing ISEAGE, the PowerCyber lab can be expanded to provide a realistic network path for its WAN communication. Communication between control centers and substations will route across the ISEAGE emulated network. This can then be utilized to perform various attack studies, specifically focusing on availability and integrity requirements of the network. DoS attacks can be simulated to understand network availability requirements and determine communication link resiliency and redundancy requirements.

2) Substations: Within the substations, the IEC 61850 protocol is used to communicate status and commands between both other IEDs and the RTU. IEC 61850 GOOSE messages utilize multicast Ethernet to provide real-time support for protection mechanisms and is used for communications between IEDs. Manufacturing Message Specification (MMS) protocols are used to communicate analog and binary values between the IEDs and RTUs.

C. Physical System

The testbed currently deploys two different tools for performing power system simulation, DIgSILENT PowerFactory and a real-time digital simulator (RTDS) [27], [28]. These simulators are used independently based on the time constraints of the simulation. The power system model for both simulators is based on the Western Electricity Coordinating Council (WECC) 9-bus model as demonstrated in Fig. 3. The system consists of three generating units at buses 1, 2 and 3, and three loads at buses 5, 6, and 8. Nine substations are modeled, such that each substation controls the operations (breaker control) concerned with a bus.

1) Real Time Digital Simulator: The RTDS is a simulation platform that provides the capability to perform real-time power system simulation and allows physical hardware integration and can closely mimic the physical response characteristics of power system equipment when subjected to fault-type scenarios. The RTDS was designed to both interact with physical relays (IEDs) and through various control system protocols, such as IEC 61850 and DNP. This allows integration with both the physical and virtualized relays.

2) DIgSILENT PowerFactory: PowerFactory is a software product that performs non-real-time power system simulation. Additionally, unlike the RTDS, PowerFactory does not provide interconnection of physical devices. However, PowerFactory does provide some advantages to RTDS as it allows the simulation of larger systems with limited real-time constraints. In addition, PowerFactory provides more advanced system analysis capabilities, including algorithms for state estimation and contingency analysis. PowerFactory is interfaced with the testbed components through the OPC protocol communication.

V. Testbed Evaluation and Experimentation

This section reviews current research efforts performed on the testbed. First a high-level overview of current vulnerabilities assessment activities is provided. Next, a more detailed analysis of various cyber-physical attack scenarios is presented to demonstrate both isolated and coordinated attacks that impact physical system stability.

A. Vulnerability Assessment

Numerous vulnerability assessment activities have been performed on the testbed to explore potential security weaknesses in the software and communication protocols. Discovered vulnerabilities are then shared with the product vendor so they can develop and release appropriate mitigations. Our vulnerability identification process has followed well documented security testing methodologies, such as NIST 800-115: "Technical Guide to Information Security Testing and Assessment", which focuses on various scanning and cracking techniques along with a thorough review of implemented technologies and configurations [29]. In addition to the documented methodology, our analysis has also included manual inspection techniques using various open-source tools and software fuzzing tests based on the Mu Security Analyzer [30].

TABLE II
EVALUATED CYBER ATTACKS

ATTACK 1: MALICIOUS BREAKER TRIP	
Method	Command injection
Origin	Internal
Tool	Custom software
Target	IED
Result	Breaker trip
ATTACK 2: SCADA OBSERVABILITY DOS	
Method	DoS - TCP Syn flood
Origin	External
Tool	Mu Security Analyzer [30]
Target	VPN/Firewall
Result	Unobservable Power System
ATTACK 3: REMEDIAL ACTION SCHEME DOS	
Method	DoS - TCP Syn/L2 flood
Origin	Internal
Tool	Mu Security Analyzer [30]
Target	Switch/Relay
Result	Failed Protection Scheme

The resulting analysis has resulted in the discovery of multiple previously undisclosed vulnerabilities within industry software platforms. These efforts have resulted in vendor security advisories and system patches [31].

B. Cyber-Physical Impacts

In addition to the vulnerability assessment efforts, various cyber-physical impact evaluations have been performed to explore how attacks can impact the physical systems. Table II identifies the three attack templates that have been evaluated within the testbed. The remainder of this section will provide further analysis of these situations.

1) Attack 1: Malicious Breaker Trip: This attack scenarios assumes an attacker is able to access an internal network by bypassing the security of either the control center or substation networks. Once this level of access has been obtained, the attacker can initiate their own DNP3 connections to the RTUs due to insufficient authentication requirements. The lack of system authentication is then used to inject a breaker trip command to breaker 1 on bus 1.

The power system is stable when the simulation begins. In 7 seconds the malicious breaker trip command is injected to the network. Once this occurs, generator rotor angles become unsynchronized. Once the breaker is tripped, generator 1 is separated from the rest of this system. The loss of generation creates a large system disturbance which caused the remaining online generators to become unsynchronized. Fig. 4 identifies the rotor angle of generators 2 and 3 during the attack.

2) Attack 2: SCADA Observability DoS: Denial of service (DoS) attacks present another significant concern due to the electric grid's strict availability requirements. In this scenario the attacker floods the VPN's external interface with arbitrary data in order to disrupt the SCADA communications. This attack assumes a external attacker is targeting the external VPN interface with a TCP Syn flood attack. Because the VPN is used to protection the SCADA DNP3 traffic, flooding the VPN will constrain its ability to transmit the SCADA traffic between the control center and substation. The control center is currently configured to poll system status every 1 second with DNP3 packets.

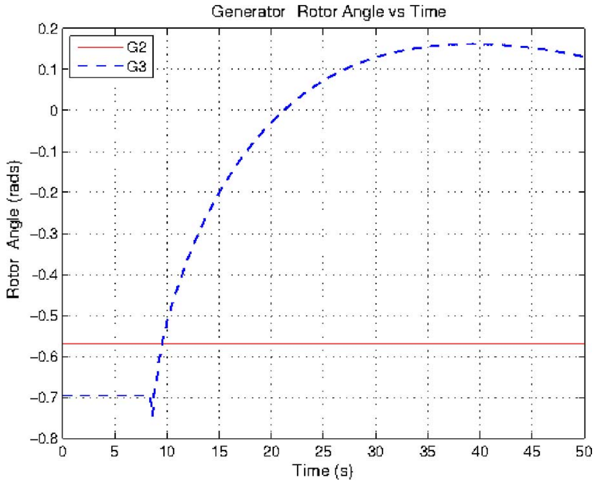

Fig. 4. Generator rotor angles.

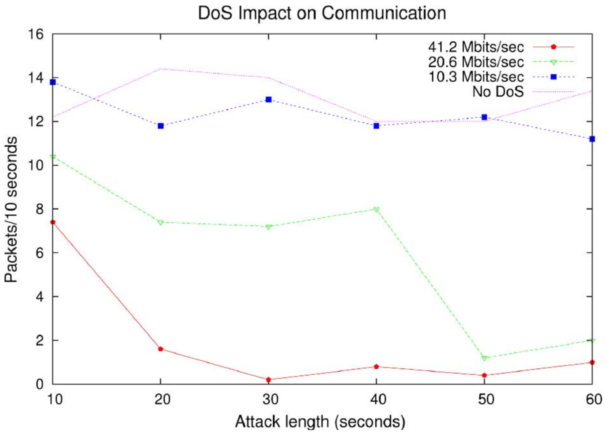

Fig. 5. DoS impact on control system communication.

Cyber Impact: Fig. 5 documents the results of the DoS evaluation by plotting the mean throughput from 5 simulations, the x-axis documents the length of the attack while the y-axis displays the number of probe DNP3 packets received every ten seconds. These results show that as the attack throughput increases, the DNP3 communication decreases. At 10 Mbps the availability starts to decrease and once the DoS attack reaches approximately 20 Mbps the VPN devices are no longer to properly relay the DNP3 traffic between the substation and control center.

Physical System Impact: Once the attack reaches 20 Mbps, the control system begins to obtain a decreasing number of SCADA measurements. These measurements are necessary to compute the state estimations of the physical system and other EMS applications.

3) Attack 3: Remedial Action Scheme DoS: In this particular case study, we show how the testbed can be used to replicate the conditions of a Remedial Action Scheme (RAS) and study the impact of a coordinated cyber attack on the power system. Typically, for every RAS, there is a RAS controller, which determines when the scheme is to be armed and also sends appropriate control commands to the corresponding relays. Because RAS are very critical in maintaining the system stability, they

TABLE III
MAPPING OF POWERCYBER TESTBED COMPONENTS TO RAS

Component in RAS	**Mapping in PowerCyber testbed**
RAS controller	Relay 1
Relay protecting line 7-5	Relay 2
Relay protecting line 7-8	Relay 3 (inside RTDS)
Relay causing generation reduction at bus 2	Relay 4 (inside RTDS)

are often deployed with another redundant backup RAS controller and protection elements, however, for the purpose of this case study, only one controller is modeled.

The WECC 9 bus system, shown in Fig. 3 has been chosen as the power system for our case study. The particular RAS which has been adapted for this case study has been taken from the WECC RAS list [32] and is explained below.

The RAS scheme is designed to trip one of the generation units at bus 2, (modeled by a reduction in the generation), if there is a fault on one of the transmission lines connected to it. In our case there are two transmission lines, namely, 7-8 and 7-5. The RAS scheme would be armed only if generation at bus 2 exceeds a particular value. This generation would have to be reduced to prevent the thermal overloading of one of the transmission lines in case of a fault on the other line and also to maintain the stability of the generation units. Table III shows how the various components of the RAS have been mapped into the PowerCyber testbed environment.

a) Coordinated attack template: The case study involves the execution of a coordinated attack to prevent the RAS from operating, reducing the loading on the transmission line 7-8 and consequently tripping of the line 7-8. Assuming that the RAS is already armed, i.e generation at bus 2 greater than a specified threshold, the actions which are necessary to cause this are:

1) Creating a data integrity attack (similar to Section V-B-1) to trip the Relay 2 which protects line 7-5 to activate the RAS.
2) Creating a Denial of Service attack to prevent the GOOSE trip command to the generation unit at bus 2 to result in a thermal overload on line 7-8 and cause it to trip out.

By looking at Fig. 6, we can explain how the RAS operates by observing the sequence of events and IEC 61850 messages being exchanged between the devices associated with this protection scheme. Generally, the control center operator can manually arm/disarm the RAS through an IEC 61850 message to the RAS controller directly outside the typical flow of events.

1) The Generating station at bus 2 exceeds a threshold, communicates this to the RAS controller (Relay 1) to arm the RAS.
2) Relay 2 associated with the protected line 7-5 sends a message to the RAS controller to indicate a fault.
3) RAS controller performs the necessary validation checks and issues a trip command to the unit at generating station in bus 2 to reduce generation immediately.
4) Because of the successful cyber attack, generation at bus 2 is not reduced and the Relay 3 protecting line 7-8 detects thermal overload.
5) Relay 3 reaches max time for withstanding the thermal overload and trips, isolating the generation station at bus 2.

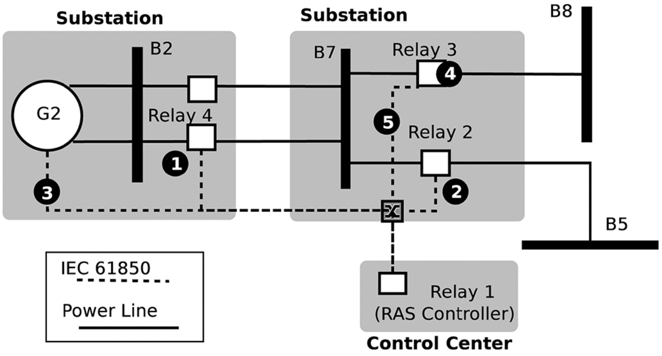

Fig. 6. RAS physical and cyber system.

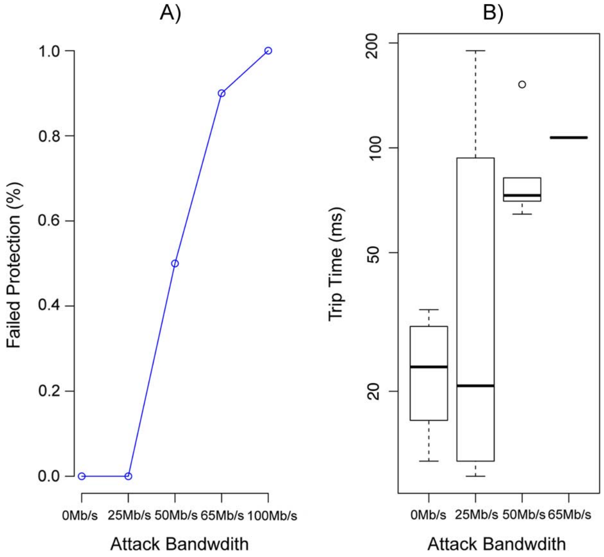

Fig. 7. DoS protection scheme impact (switch flooding).

b) Cyber impact: We evaluate two DoS attacks which could be used to disrupt the RAS communication, first by flooding the switch with broadcast Ethernet frames and also flooding the RAS controller with TCP Syn packets. We evaluate various traffic rates to determine the amount of malicious traffic required to disrupt the RAS, each attack was repeated ten times. The results of this analysis shows that the protection scheme can be disrupted through both methods, though targeting the RAS controller requires significantly less bandwidth.

Fig. 7 demonstrates the impact of the DoS attack by flooding the Ethernet switch. Fig. 7(a) displays that the percentage of times that RAS failed based on various attack rates. Notice as traffic hits 50 Mbps the RAS fails 50% of the time while at greater attack rates the RAS fails consistently. Fig. 7(b) displays averaged time for the RAS communication to travel from the relay to the RAS controller and back (note: these results only include successful RAS methods as the communication never finishes in the failed scenarios). Although RAS only fails after not receiving the communication within 1 second, our results show either the communication occurred within 200 ms or the RAS failed. This occurrence can likely be explained by Ethernet's collision detection exponential back-off and eventual collision timeout.

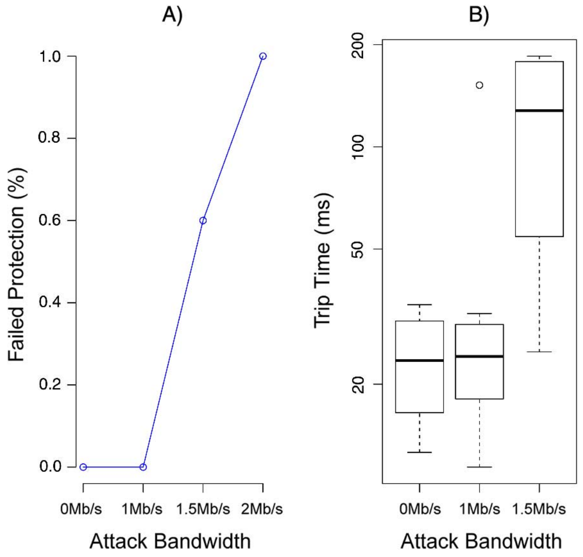

Fig. 8. DoS protection scheme impact (relay Syn flood).

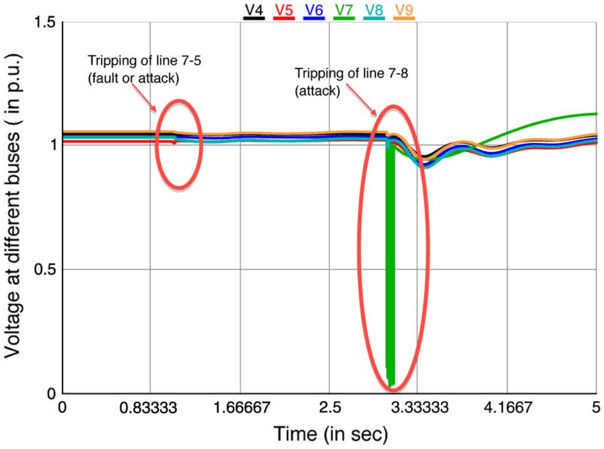

Fig. 9. Impact of attack on system voltages.

The results from the TCP Syn flood attack in Fig. 8 demonstrate that the protection scheme could be disrupted with significantly less bandwidth by targeting the relay. Fig. 8(a) shows that traffic around 1.5 Mbps is sufficient to disrupt the RAS 60% of the time, while as traffic reaches 2 Mbps the RAS continually fails. Fig. 8(b) displays the average delay of the RAS during successful runs.

c) Physical system impact: The impact of the successful coordinated attack on the power system can be seen from Figs. 9 and 10. Fig. 9 shows how the system voltages are impacted by the attack and Fig. 10 shows how the line flows and the generation changed as a result of the attack. Each of these figures have two ovals highlighting the two events which took place as part of the attack. The first event represents the tripping of line 7-5, and could have been either a fault or an attack (in our case), and the second event represents the tripping of line 7-8 due to the attack.

Fig. 9 shows that the first event did not cause much impact on the system voltage and the voltage at all the buses stayed close to 1.0 p.u. Whereas, after the second line tripped, generator two was completely isolated from the grid and this impacted the voltage at several buses significantly. This especially occurs at bus 7, which is linked to bus 2 through a step-up transformer.

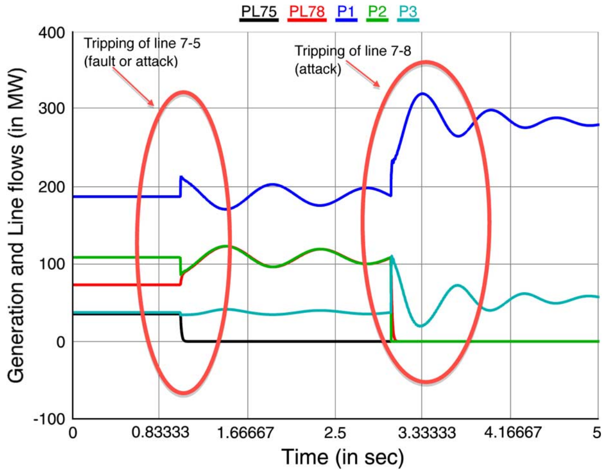

Fig. 10. Impact of attack on generation and line flows.

From Fig. 10, we can see that the tripping of line 7-5 changed the generation in all three generators by a small amount, but it overloaded the line 7-8 significantly and eventually preventing the generation reduction as per the RAS, it led to the tripping of line 7-8. Although the plot shows the tripping of 7-8 due to overload within seconds, the scenario would have resulted in the same impact even after a longer thermal limit threshold, which is typically around a few minutes. It is to be noted here that the tripping of line 7-8 completely isolates generator 2 from the system and therefore it would result in a huge loss of generation which will impact the frequency profoundly. In a real power system such an event could potentially cause some frequency stability related problems. This situation could also lead to tripping of some load if no spare generation is available.

Note: The simulated power system used in this attack was not operating in a N-1 secure state as is required for the North American grid, therefore, the demonstrated attack would unlikely result in similar load and frequency violations on the actual grid.

VI. Conclusion

Research on cyber-physical systems, such as the smart grid, requires the development of testbeds to analyze the complex relationships between the cyber-based control mechanisms and the physical system. This paper introduces various research applications which required cyber-physical testbeds to provide representative environments to explore and validate potential solutions. A high level overview of testbed functionality is documented, including its control, communication, and physical components along with a mapping of components to research requirements. The PowerCyber testbed from Iowa State University is then introduced to provide an example of an operational cyber-physical testbed. The testbed's various components and interconnections are introduced along with methods to increase the scalability and accuracy of the testbed, such as virtualization, ISEAGE, and RTDS. Several attack-impact evaluations were performed on this testbed including isolated attacks which impact the physical system rotor angle stability and the SCADA observability. Additionally, a coordinated attack is demonstrated against a RAS to disrupt the physical system's voltage stability. While these attack templates help demonstrate the testbed capabilities, future research efforts will explore the impacts from more sophisticated coordinated attack templates along with various impact mitigation efforts through both cyber and physical approaches.

Acknowledgment

The authors would like to thank Dr. Venkataramana Ajjarapu and Dr. Doug Jacobson for their help with the RTDS and ISEAGE platforms, respectively.

References

[1] U.S. Government Accountability Office (GAO), "Critical infrastructure protection challenges and efforts to secure control systems," GAO-04-354, Mar. 2004.

[2] "Common cyber security vulnerabilities observed in control system assessments by the INL NSTB program," Idaho National Laboratory (INL), Nov. 2008.

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

[4] "A systems view of the modern grid," U.S. Department of Energy (DOE) National Energy Technology Laboratory (NETL), 2007.

[5] National Institute for Standards and Technology (NIST), "Guidelines for smart grid cyber security," NISTIR 7628, Aug. 2010.

[6] "National SCADA test bed: Fact sheet," Idaho National Laboratory (INL), 2007.

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

[8] M. J. McDonald, G. N. Conrad, T. C. Service, and R. H. Cassidy, "Cyber effects analysis using VCSE," Promoting Control System Reliability, Sandia National Laboratories, SAND2008-5954, Sep. 2008.

[9] M. J. McDonald *et al.*, "Modeling and simulation for cyber-physical system security research," Development and Applications, Sandia National Laboratories, SAND2010-0568, Feb. 2010.

[10] 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 Exp. Test*, Aug. 2009.

[11] G. Dondossola, G. Garrone, J. Szanto, G. Deconinck, T. Loix, and H. Beitollahi, "ICT resilience of power control systems: Experimental results from the CRUTIAL testbeds," in *Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jul. 2009, pp. 554–559.

[12] G. Dondossola, G. Deconinck, F. Garrone, and H. Beitollahi*, Testbeds for Assessing Critical Scenarios in Power Control Systems*. Berlin, Germany: Springer-Verlag, 2009, pp. 223–234.

[13] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Jan. 2011, pp. 1–7.

[14] J. Hong, S.-S. Wu, A. Stefano, A. Fshosha, C.-C. Liu, P. Gladyshev, and M. Govindarasu, "An intrusion and defense testbed in a cyber-power system environment," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, Jul. 2011.

[15] C. Queiroz, A. Mahmood, and Z. Tari, "SCADASim—A framework for building SCADA simulations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 589–597, Dec. 2011.

[16] "NSTB assessments summary report: Common industrial control system cyber security weaknesses," Idaho National Laboratory (INL), May 2010.

[17] J. Cebula and L. Young, "A taxonomy of operational cyber security risks," Carnegie Mellon University Software Engineering Institute (SEI), Dec. 2010.

[18] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[19] K. Scarfone and P. Mell, "An analysis of CVSS version 2 vulnerability scoring," in *Proc. 3rd Int. Symp. Empirical Softw. Eng. Meas.*, 2009.

[20] National Institute for Standards and Technology (NIST), "Directions in security metrics research," NISTIR 7564, Apr. 2009.

[21] D. P. Duggan, "Penetration testing of industrial control systems," Sandia National Laboratories, SAND2005-2846P, Mar. 2005.

[22] M. Fabro and E. Cornelius, "Recommended practice: Creating cyber forensics plans for control systems," Idaho National Laboratory (INL), Aug. 2008.

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

[24] D. Kirschen and F. Bouffard, "Keeping the lights on and the information flowing," *IEEE Power Energy Mag.*, vol. 7, no. 1, pp. 50–60, Jan. 2009.

[25] A. Ashok, A. Hahn, and M. Govindarasu, "A cyber-physical security testbed for smart grid: System architecture and studies," in *Proc. 7th Annu. Workshop Cyber Security Inf. Intell. Res.*, 2011, ser. CSIIRW '11.

[26] D. Jacobson, "ISEAGE: Project overview," Iowa State Univ.. Ames, IA, 2007.

[27] PowerFactory DIgSILENT, 2011.

[28] "Real Time Digital Simulator (RTDS)," RTDS Technologies, 2011.

[29] K. Stouffer, J. Falco, and K. Scarfone, "Technical guide to information security testing and assessment," National Institute of Standards and Technology, Tech. Rep., NIST SP 800-115, Sep. 2008.

[30] Mu-4000 Security Analyzer, Mu Dynamics [Online]. Available: http://www.mudynamics.com/

[31] "Multiple security vulnerabilities in Siemens Scalance S," Siemens ProductCERT, SSA-268149, Apr. 2012 [Online]. Available: http://www.siemens.com/corporate-technology/pool/de/forschungs-felder/siemens_security_advisory_ssa-268149.pdf

[32] "WECC remedial action scheme catalog summary," Western Electricity Coordinating Council, 2008.

Adam Hahn (S'10) received the B.S degree in computer science from the University of Northern Iowa, Cedar Falls, and the M.S. degree in computer engineering from Iowa State University (ISU), Ames. He is currently working toward the Ph.D. degree in the Department of Electrical and Computer Engineering at ISU.

He is currently an Information Security Engineer at the MITRE Corporation, McLean, VA, USA. His research interests include cyber vulnerability assessment, critical infrastructure cybersecurity, and smart grid technologies.

Aditya Ashok (S'10) the B.E. degree in electrical and electronics engineering from the College of Engineering, Guindy, Anna University, Chennai, India. He is currently working toward the Ph.D degree in electrical and computer engineering at Iowa State University, Ames. His research interests are in identifying and studying key application level issues in power system operations that intersect with cyber-physical security in the smart grid.

Siddharth Sridhar (S'10) 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 toward the Ph.D. degree in computer engineering at the Department of Electrical and Computer Engineering at Iowa State University, Ames.

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

Manimaran Govindarasu (SM'10) received the Ph.D. degree in computer science and engineering from the Indian Institute of Technology (IIT), Chennai, in 1998.

He is currently a Professor in the Department of Electrical and Computer Engineering at Iowa State University, Ames, and 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 cyber security 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, and has given tutorials at reputed conferences (including IEEE INCOFOM 2004 and IEEE ComSoc *Tutorials Now*) on the subject of cyber security, 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 co-author of the text *Resource Management in Real-Time Systems and Networks* (MIT Press, 2001). He has served as guest co-editor for several journals including leading IEEE magazines. He had 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.