Position Paper to National CPS Energy Workshop, 2013

Cyber Physical Security Testbed for the Smart Grid: Fidelity, Scalability, Remote Access, and Federation

Manimaran Govindarasu
Dept. of Electrical and Computer Engineering
Iowa State University, Ames, IA
gmani@iastate.edu

Chen-Ching Liu
Dept. of Electrical and Computer Sciences
Washington State University, Pullman, WA
liu@eecs.wsu.edu

1. Background and Motivation

Electric power grid is a complex cyber physical system (CPS) that forms the lifeline of modern society, and its reliable and secure operation is of paramount importance to national security and economic vitality. Recent findings, documented in government reports and in the literature, indicate the growing threat of cyber-based attacks in numbers and sophistication on power grid infrastructures. Various incidents and attempts in the recent past have indicated the extent to which these SCADA systems are vulnerable and the urgent need to protect them against electronic intrusions and cyber-based attack. 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 infrastructures. Therefore, cyber security of the power grid — encompassing attack prevention, detection, mitigation, and resilience — is among the most important R&D priorities today and in the emerging smart grid. In this context, CPS Security Testbeds provide a platform for promoting and sustaining cyber security R&D and education in this critical area of national importance.

2. Need for Cyber Physical Security Testbed

With growing concerns for the cyber security of power grid and other critical infrastructures, it is not possible to do cyber attack-defense experimental studies on real systems. Moreover, it becomes prohibitively expensive to replicate real systems for security and performance evaluations. An alternative is to perform large scale computer based simulations, but that involves making some compromises in the modeling accuracy. Conventional simulators and testbeds either model the physical power system (e.g., real-time simulators) or the cyber system (e.g., SCADA testbeds). Such isolated testbeds/simulators are inadequate to model the coupling between the cyber and physical system components, which is very critical to performing cyber-physical system studies (e.g., wide area monitoring, protection, and control) and to develop effective countermeasures and their validations.

In this respect, Cyber Physical Systems (CPS) Testbeds provide an optimal balance between the low cost and ability to accurately capture real system characteristics. Testbeds also are useful as they provide a methodology to study the complex cyber physical interactions in the power system which cannot be accurately modeled using traditional modeling and simulation tools. Recently, NIST Smart America Challenge calls for CPS testbed creation and collaboration among researchers and industries (http://www.nist.gov/el/smartamerica.cfm).

Unfortunately, attempts to research cyber security enhancements are constrained by the availability of realistic environments which emulate/simulate the acute cyber-physical relationships within the electric grid. Developing and evaluating these cyber systems requires the availability of cyber-physical testbeds which model realistic environments and provide an accurate evaluation of cyber vulnerabilities and the quantification of resulting consequences (impacts) on the operation of the underlying physical system. Include: vulnerability assessment, impact analysis, risk assessment, validating the effectiveness risk mitigation and other real-time defense algorithms against various forms of cyber attacks such as data integrity attacks, timing and replay attacks, denial of service, and intrusion-based attacks. Testbed design decisions must be driven by its intended use due to various implementation trade-offs: high-fidelity (accuracy), scalability, and cost. Testbed design will typically balance the integration of physical, emulation and simulation-based components. While a physical environment with industry standard hardware, software and power system components are deal, the high cost will typically outweigh practicality. The utilization of simulation and emulation techniques can be used to create an environment which maintains critical real-world properties while abstracting certain relationships.

3. Testbed R&D Applications

CPS Security Testbed can be used for a wide range of cyber and physical security experiments that include the following:

- ***Vulnerability analysis:*** analyzing vulnerabilities in the cyber systems – field devices, automation systems, SCADA, communication protocols, servers, Energy Management Systems (EMS) – using state-of-the-art attack tools and techniques.

- ***System impact analysis:*** Studying the consequence of a successful cyber attack on the operation of the physical system, in terms of load loss, cascading outage, equipment damage, or economic loss.

- ***Risk modeling:*** Risk = Threats x Vulnerability x Impacts. Testbeds helps to practically validate the cyber cyber-physical security models and algorithms that are used for quantitative risk assessment.

- ***Attack-Defense evaluations:*** Studying the effectiveness of defense measures against specified attack scenarios. Testbed provides an ideal platform to model not only the interaction between cyber and physical components, but also the interplay between attacks and defense.

- ***Other application include:*** CPS security metrics development. Data and models development – cyber topology, physical models, CPS models; Interoperability testing; Cyber forensics; Operator training.

4. CPS Testbed R&D Questions

There are several R&D challenges need to be pursued to achieve the vision of realistic, scalable, maintainable CPS testbeds that only contribute to developing innovative sustainable CPS technologies, but also contribute to disruptive CPS technologies. The R&D questions include:

1) **Design Tradeoffs:** What are the innovative CPS testbed architectures, design abstractions, and building blocks that balance tradeoffs involving low cost, high accuracy/fidelity, and scalable to large systems?, and how to design them?

2) What are ***interfaces*** and software/hardware modules that allow interactions between heterogeneous cyber components and physical components? and how to develop them?

3) **Fidelity:** How to synchronize time in the cyber domain and physical domain to perform realistic experiments on a large power system?

4) **Scalability:** How to scale the system to study large power systems while maintaining the high-fidelity of the simulations/emulations/implementations? How do create a "***Cyber-In-the-Loop***" Real-Time Power Simulation (CIL-RT-PS) environment?

5) **Remote Access:** What are interfaces, programming abstractions, APIs to provide remote access to CPS testbed? How do build modular software architecture that promotes ***community access model*** where researchers can create, share, and collaborate in testbed developments and experimental evaluations to accelerate innovation in CPS Security.

6) **Federated Testbeds:** What are the architecture principles, abstractions, and interfaces, and APIs that enable loosely-coupled or tightly-coupled integration of heterogeneous testbeds of differing capabilities to create a synergistic integrated platform for promoting research and education in this area of national need?

7) **Data sets, models, and metrics:** What are the realistic CPS data sets, CPS models, and CPS metrics for CPS security evaluations? How to develop them by leveraging testbeds?

8) **Education and Industry outreach:** How to leverage CPS testbed to enhance inter-disciplinary education (e.g., course models, design projects, graduate research) and outreach activities (e.g., industry short course)?
9) **CPS-VO interfacing:** How to leverage CPS-VO to promote R&D in testbed creation, sharing, and experimentations in CPS Security for power grid and in general to all CPS testbeds?