Position Paper to National CPS Energy Workshop, 2013

Cyber Physical Security of Bulk Power System: From Fault-Resilient Grid to Attack Resilient Grid

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

Chen-Ching Liu
Dept. of Electrical Engr. & 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.

Defending against cyber-attacks on SCADA networks is a challenging task, given the wide range of attack mechanisms, the decentralized nature of the control, and deregulation and the lack of coordination among various entities in the electric grid. Securing the power grid infrastructure faces a lot of challenges as there are a huge number of heterogeneous devices, communication protocols, and legacy hardware and software components, the lack of built-in security in grid's communication and computing infrastructures. Until recently, cyber security was not one of the primary requirements in cyber infrastructure design and deployment in power grid environment. Moreover, the attack surface of SCADA network infrastructure to cyber threats has increased enormously due to increased interconnectivity of SCADA and public communication networks, and wide deployment of smart sensors (e.g., PMUs and AMIs) owing to the various Smart Grid initiatives. The cyber resources used to monitor, protect, and control the grid are vulnerable to numerous attacks and the attacks' influence on power system generation, transmission and distribution applications.

2. CPS Security of Bulk Power System

According to North American Electric Reliability Corporation (NERC), Bulk Power System (BPS) defined as follows: ""Bulk Power System" means, depending on the context: (i) Facilities and control systems necessary for operating an interconnected electric energy supply and transmission network (or any portion thereof), and electric energy from generating facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy."

The NERC and DOE Report: The document titled ***High-Impact, Low-Frequency (HILF) Event Risk*** to the North American Bulk Power System jointly commissioned by NERC and the DOE addresses rare events that have the ability to cause catastrophic damages to the North American power grid. Coordinated cyber attacks have been identified as one such threat source that could cause impacts of HILF-scale. The document recognizes that a successful attack on key system nodes has the ability to degrade the system beyond the protection offered by traditional operations and planning criteria. Intelligent cyber security measures and control algorithms that facilitate graceful degradation of the power system to allow system operation with limited resources are key areas that require future attention. Currently, the North American BPS does not have adequate measures to guarantee protection against continuously evolving malicious cyber attacks, which makes the grid highly vulnerable.

BPS is the backbone of the electric power grid infrastructure in North America and is highly automated with a wide variety of sensors, communication protocols, automated control, supervisory control, energy management systems (EMS), etc. In particular, central to BPS operation is ***Wide-Area Monitoring, Protection, and Control (WAMPAC),*** which all rely on measurements from field devices, transmitted via wide-area communication network, and decision making and control are performed at control centers at multiple levels of hierarchy. The various components – field devices, communication networks, and control logics/centers – are susceptible to various forms of cyber attacks, such as man-in-the-middle attacks, data integrity attacks, timing attacks, denial of service attacks, and replay attacks. In this context, attack-resilient infrastructure must be developed to protect the BPS against HILF cyber attacks.

A stealth and coordinated cyber attack on the BPS could have catastrophic consequences on the grid operation (e.g., cascading outage or blackout) and affecting other interdependent critical infrastructures such as the Internet, transportation systems, water distribution systems, etc. Therefore, cyber security of the power grid, in particular the cyber-physical security of BPS — encompassing attack prevention, detection, mitigation, resilience, and deterrence — is among the most important R&D priorities today and in the emerging smart grid. This requires synergistic collaboration in R&D to be undertaken through partnerships among academics, industries, national laboratories, and regulating agencies.

3. FROM Fault-Resilient of Grid today TO Attack-Resilient Grid of the Future

The current North American BPS is designed to be ***fault-resilient***, i.e. the grid has enough operating reserves to handle the failure of any single element in the power system, such as a generator or a transmission line, known as a *(N-1) contingency*. Also in some cases the grid is designed to operate resiliently tolerating certain critical and credible *(N-k) contingencies* which are caused by common failure modes such as lightning strikes. However, the definition of “credible” changes when potential failures from cyber attacks comes into the picture. In the case of coordinated cyber attacks, elements that do not share electrical or physical relationships could be forced to fail simultaneously, resulting in unanticipated consequences. The traditional *(N-1)* approach to determining system reliability becomes inadequate and new analysis tools, techniques which combine infrastructure and application layer information need to be developed to look beyond *(N-1) contingency security*. Therefore, there is a compelling research need to identify new methods, analysis tools, planning and operating procedures to transform the power grid from being fault-resilient to ***attack-resilient*** grid capable of tolerating (N-k) contingencies. One approach is to introduce enough redundancy make the grid attack-resilient, which is a naïve one. The problem with redundancy is that it is not only very expensive, but it cannot possibly be designed to deal with arbitrary number of contingencies ("k" value), which could very well be caused by cyber attacks or through a combination of physical faults (due to extreme events like Hurricanes) and cyber attacks. Therefore, transformative approaches are needed to achieve attack-resiliency beyond using redundancy.

Research questions include:

1) **Develop scientific foundation to transform fault-resilient grid of today to attack-resilient grid of future.** This requires fundamental paradigm shift as how we define system reliability, credible contingencies, and the synergistic application of cyber security tools, real-time computation/communication, and tools from system theory, dynamical systems, and optimization to achieve operational security, reliability, system resiliency of the BPS.

2) Develop a comprehensive **cyber-physical security framework for Bulk Power System** that includes models for HILF cyber events (stealth coordinated attacks, *Advanced Persistent Threats (APTs)*, impact analysis, and robust cyber-physical countermeasures. This includes:
   a) ***Attack modeling and impact analysis*** - systematic identification of stealth coordinated cyber attacks on WAMPAC and the analysis of resulting consequences (impacts) on the operation of the BPS in terms of electric load loss, stability violations, cascading outage, equipment impacts, or economic loss.
   b) ***Risk models and analysis*** against APTs through an integrated modeling that captures both vulnerability of the cyber layer and the resulting impacts on the power grid. Risk = Threat x Vulnerability x Impact. Risk modeling accounting vulnerability and impacts is reasonably well understood, but capturing "threat" in the model is still an art (not a science), and hence scientific models and tools need to be developed accounting all three components to estimate risk credibly.
   c) ***System resiliency algorithms,*** which include: (a) Innovative domain-specific anomaly detection algorithms that correlate temporal and spatial data and works in conjunction with power system mitigation measures; (b) Attack-resilient WAMPAC algorithms that leverage detection, mitigation, resilience both in the cyber and power system domains.

3) CPS Security Testbeds and Evaluations play a fundamental role in advancing cyber security R&D and its deployment to protect and make the grid resilient against cyber attacks. In particular, conducting vulnerability analysis, impact studies, attack-defense evaluations, and in the exploration of future advancements including the development robust countermeasures -- as the functionality of both the cyber and physical infrastructures can be emulated within a controlled environment. Realistic models and data sets, experimentations need to be developed. Also, sharing of testbed development and experimentations need to be promoted.