Cyber-Physical Systems Security for Smart Grid

Future Grid Initiative White Paper

Power Systems Engineering Research Center

Empowering Minds to Engineer
the Future Electric Energy System

Cyber-Physical Systems Security for Smart Grid

Prepared for the Project "The Future Grid to Enable Sustainable Energy Systems" Funded by the U.S. DOE

White Paper Team

Manimaran Govindarasu and Adam Hann
Iowa State University

Peter Sauer
University of Illinois at Urbana-Champaign

PSERC Publication 12-02

February 2012

Information about this white paper

For information about this white paper contact:

Prof. Manimaran Govindarasu,
Iowa State University
Dept. of Electrical and Computer Engineering
3227 Coover Hall
Ames, IA 50011, USA
gmani@iastate.edu; 515-294-9175

Your feedback on the white paper will be welcomed. Send your comments to Manimaran Govindarasu.

Power Systems Engineering Research Center

The Power Systems Engineering Research Center (PSERC) is a multi-university Center conducting research on challenges facing the electric power industry and educating the next generation of power engineers. More information about PSERC can be found at the Center's website: http://www.pserc.org.

For additional information, contact:

Power Systems Engineering Research Center
Arizona State University
527 Engineering Research Center
Tempe, Arizona 85287-5706
Phone: 480-965-1643
Fax: 480-965-0745

Notice Concerning Copyright Material

Acknowledgements

This white paper was developed as one of nine white papers in the project "The Future Grid to Enable Sustainable Energy Systems: An Initiative of the Power Systems Engineering Research Center." This project is funded by the U.S. Department of Energy. More information about the Future Grid Initiative is available at the website of the Power Systems Engineering Research Center (PSERC), www.pserc.com.

We also recognize staff, faculty, and students of the Power Systems Engineering Research Center for their efforts in developing the vision that led to the "Future Grid" project under which this white paper falls. Finally, we express deep appreciation to the reviewers who significantly contributed to the quality of this white paper, as listed below. Their identification here does not constitute endorsement regarding any of the contents of this report.

- Scott Backhaus, Los Alamos National Laboratory, New Mexico
- Jianhu Wang, Argonne National Laboratory, Illinois
- Siddharth Sridhar, Iowa State University
- Aditya Ashok, Iowa State University

Executive Summary

This white paper focuses on identifying a comprehensive set of cyber security challenges and the need for security at multiple levels of the cyber-physical power system, namely, information security, information and communication technologies (ICT) infrastructure security, and application-level security. It identifies cyber security research issues beyond the tradition information technology (IT) security issues. In particular, the white paper identifies research issues such as: (i) cyber attack risk modeling and risk mitigation, (ii) attack-resilient monitoring, protection and control algorithms, (iii) defense against coordinated cyber attacks, (iv) AMI infrastructure security, (v) trust management and attack attributions, and (vi) simulation models, data sets, testbed evaluations. The white paper articulates the need for going beyond (N-1) contingency criteria to deal with coordinated cyber attacks. Also, it highlights the inadequacy of traditional models and algorithms that are robust against random naturally occurring faults to deal with malicious cyber attacks, and hence the need for development of novel models and attack-resilient algorithms which span across generation, transmission, and distribution systems. Finally, the linkage between attack deterrence, prevention, detection, mitigation, and attribution is identified.

Cyber security of the power grid – encompassing attack prevention, detection, mitigation, and resilience – is among the most important R&D needs for the emerging smart grid. One of the overarching goals of the future research is to develop a comprehensive *cyber security risk modeling framework* that integrates the dynamics of the physical system as well as the operational aspects of the cyber-based control network. The models need to quantify the potential consequences of a cyber-attack on the power grid in terms of load loss, stability violations, equipment damage, or economic loss.

Following the risk assessment, the next important research challenge is to develop an integrated set of security algorithms that will protect the grid against various forms of cyber-attacks including denial of service attacks, intrusion-based attacks, malware-based attacks, isolated attacks, and coordinated attacks. The countermeasures must address both outsider and insider attacks, and also operator errors. The algorithms must consider sophisticated attacker model (in addition to brute-force attacks) wherein the attacker(s) has knowledge of both cyber security and power system operation with potential to cause maximum damage. Here are the algorithms that need to be developed and the modeling that needs to be done.

1. ***Cyber risk mitigation algorithms*** through real-time correlation (temporal and spatial) of massive data streams and data logs obtained from substations and control centers are needed. This requires instrumentation of efficient on-line monitoring and analysis in real-time.

2. ***Control theoretic modeling attack resilient monitoring, protection, and control algorithms*** of cyber-physical systems security and analyzing the system stability due to cyber attacks (e.g., denial of service causing delayed or dropped sensing/control signals, replication attacks causing duplicate signals) and

quantifying the degree to which system can withstand its stability properties. Important control functions, such as Automatic Generation Control (AGC), voltage control, and protection functions, require such a modeling and analysis approach and robust countermeasures to be resilient against cyber attacks.

3. ***Robust cyber-physical defense algorithms*** that prevent, detect, and tolerate (resilient against) cyber attacks on the grid. The defense algorithms should include a synergistic combination of cyber defense (e.g., rerouting, network partitioning) and power defense (generation shift, reactive power dispatch, load shedding, and controlled islanding).

4. ***Modeling coordinated cyber attacks*** taking into account the spatial and temporal aspects of the attacks and developing robust defense algorithms to prevent and mitigate such attacks. This requires rethinking of system reliability criteria.

There is a need to develop a *real-time visualization* framework and associated tools that show the outcome of risk analysis (e.g., potential suspicious activities, intrusions, and their degree of severity) to the operators and administrators. The cyber security posture will be improved by conducting security *evaluation studies* through a combination of analytical, simulation, and testbed studies to quantify cyber-based vulnerabilities and associated risks in the grid to evaluate the effectiveness of risk mitigation under realistic and sophisticated attack scenarios.

This version of the white paper will be revised in the coming weeks. Your feedback on the white paper will be welcomed. Send your comments to Manimaran Govindarasu at gmani@iastate.edu.

Table of Contents

1. Introduction and Issue Identification 1
2. Context of the Issue 3
    2.1 Policies and Official Reports 4
    2.2. Cyber Security Requirements 6
    2.3. Cyber Security Roadblocks 7
3. Issue Discussion 8
    3.1 Evaluating Risk from Cyber Attack 9
    3.2 Attacks against Cyber-Physical Systems 10
    3.3 Cyber Infrastructure Security 11
    3.4 Power Application Security 12
    3.5 Human Factors 15
4. Paths to Issue Resolution 16
    4.1 Information & Infrastructure Security 17
    4.2. Application Level Security 17
    4.3. Risk Modeling and Mitigation 23
    4.4. Coordinated Attack-Defense 24
    4.5. Trust Management and Attribution 25
    4.6. Data Sets and Validation 26
5. Conclusions 27
References 28

List of Figures

Figure 1: Cyber Attacks Against Critical Infrastructures 8
Figure 2: Mapping from Cyber Attacks to Control Actions to System Impacts 10
Figure 3: A Taxonomy of Control Loops in the Power Grid 12
Figure 4: Cyber Security for Smart Grid Environment 12
Figure 5: Schematic of Cyber Attacks on Control System 18
Figure 6: Sources of Data for Attack-Resilient Control Algorithms 19
Figure 7: Research Needs for Wide-Area Monitoring and Protection 21
Figure 8: Control System View of Wide Area Monitoring and Protection 22
Figure 9: Risk Modeling and Mitigation Framework 23

List of Tables

Table 1: Key Roadmap or Policy Documents and Cyber Security Issues Addressed 4
Table 2: Smart Grid Cyber Security Requirements 6
Table 3: Cyber Vulnerabilities within Industrial Control Systems 11

1. Introduction and Issue Identification

Smart grid technologies utilize increased monitoring and control of the electric grid to improve reliability and efficiency. Many smart grid initiatives leverage an increased dependency of information and communication technologies (ICT) to integrate more accurate physical parameter measurements and intelligent controller devices. However, the increased ICT dependency also introduces additional risk from cyber attacks. Analysis of the grid's current security posture has raised numerous inadequacies, including poor system configuration, poor network security and insufficient software security [1]. Additionally, recent events, such as Stuxnet, have show that attackers are beginning to focus on critical infrastructures and have the ability to develop target cyber-physical attacks [2].

Attack resiliency is a key attribute of the next generation electric grid; however, the grids size, dependency on legacy systems, and physical exposure present numerous security challenges. This requires a forward thinking approach to cyber security, which integrates both novel cyber security protections together with comprehensive knowledge about grid operations.

Fortunately the grid is currently engineered with redundancies to withstand many physical failures and error detection capabilities, which gracefully handle faulty scenarios. These attributes provide additional attack resiliency that can be used synergistically with cyber protection mechanisms within the supporting infrastructure. This paper suggests the next generation electric grid requires a combination of a secure supporting infrastructure along with secure power applications.

This paper introduces current events and government reports, which identify the scope current cyber security shortcomings. Then it introduces key smart grid applications and identifies cyber security requirements from both an application and infrastructure perspective. Finally, the paper introduces research efforts that must be addressed to ensure the grid is adequately protected from cyber attack. Specific efforts are identified including:

1. Risk Modeling and Mitigation
2. Attack Resilient Control Algorithms
3. Coordinated Attack-Defense
4. Trust Management and Attribution
5. Data Sets and Validation

The power system technology space covers both local devices and networks, such as those found within substations, and very wide area domains across countries and continents, such as major transmission corridors.

There are numerous attack vectors, such as:

1. Attacks on the communication system that degrade system performance, but do not change data. In these attacks, the consequence will be in degraded automatic control. If that automatic control consists of relay signals to breakers, then the

consequence is serious and could result in failure of protection systems. If the automatic control is simply generation control pulses or other optimal operation commands, the consequence is less serious and could result in suboptimal performance, but probably not equipment damage or system failure.

2. Attacks on the communication system that do change data can cause either mis-operation of protection systems or suboptimal performance of generation dispatch or voltage regulation. This would include manipulation of SCADA data with the intent of creating a false state estimate. Such false state estimates could trigger decisions that are detrimental to the physical grid infrastructure or the market economics.

Two challenges to the defense against these attacks are detection and response. The ability to detect and respond to attacks results in a more resilient power system. How do we identify the most damaging attack to either the physical grid or the cyber infrastructure? With the advent of smart grid technologies, two-way communication with demand response elements must be secured.

2. Context of the Issue

The electric power grid, as of today, is a highly automated network. A variety of communication networks are interconnected to the electric grid for the purpose of sensing, protection, monitoring, and control. Most recently, these networks include connections between suppliers, consumers, stakeholders in economic markets, and Independent System Operators. These communication networks are closely associated with the Supervisory Control and Data Acquisition (SCADA) systems for a wide range of system operation functions and real-time control of the power grid [3]. Since the 1970s, the control center framework has gradually evolved from a closed monolithic structure to a more open networked environment. With the recent trend of using standardized protocols, more utilities are moving toward Internet protocol (IP) based system for wide area communication. The North American SychroPhasor Initiative (NASPI) effort offers new opportunities for wide area monitoring and control [4]. However, a tighter cyber integration also results in new vulnerabilities. Vulnerability risks associated with the connection of SCADA systems to the Internet have been known [5]. The security concern over information exchange between various power entities is more challenging as the potential of cyber threats grows [3, 5, 6, 7]. The increasing dependence upon communications over the Internet has added to the significance and magnitude of the problem. Security awareness and personnel training concerning supervisory control systems are crucial [8].

Security threats against utility assets have been recognized for decades [1, 9]. In the aftermath of the terrorist attacks on September 11, 2001, great attention has been paid to the security of critical infrastructures. Insecure computer systems may lead to catastrophic disruptions, disclosure of sensitive information, and frauds. Cyber threats result from exploitation of cyber system vulnerabilities by users with unauthorized access. A potential cyber threat to supervisory control and data acquisition (SCADA) systems, ranging from computer system to power system aspects, is recognized [1]. The increasing power of the Internet facilitates simultaneous attacks from multiple locations. The highest impact of an attack is when an intruder gains access to the supervisory control access of a SCADA system and launches control actions that may cause catastrophic damages. These attacks can be at the very local level of one relay in a substation to modify protection settings, or on a global level where settings can be changed to affect thousands of customers in homes and business. Another primary concern has been the possibility of massive denial of service (DoS) attacks on the SCADA control system and the resulting impacts on the overall performance and stability of the electric power systems.

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. Currently the electric power control system does not have adequate measures to guarantee protection against malicious physical or cyber attacks, which makes them highly vulnerable. Various incidents and attempts [9] 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 critical infrastructures [5, 9].

2.1 Policies and Official Reports

Numerous reports by government agencies and other authoritative organizations have acknowledged current cyber security concerns and potential threats to the electric grid. Table 1 provides an overview recent reports which either 1) address current trends, 2) dictate policy or requirements, 3) report current findings/inadequacies and 4) present future directions for the grid.

The U.S. General Accounting Office (GAO) has addressed numerous reports [5, 6], which critique the security adequacy of the nation's critical infrastructure. These reports highlight cyber threats to electric power grid and other critical infrastructures from terrorist organizations and hostile nations. Additionally, GAO reviews investigations into the grid's cyber infrastructure and identifies key weaknesses [5].

The National Institute of Standards and Technology (NIST) has developed two key reports. NIST 800-82 identifies current cyber security issues within general industrial control systems (ICS) [10]. NISTIR 7628 "Guidelines for Smart Grid Cyber Security" provides a thorough review of cyber security requirements for smart grid environments [8]. The document also suggests necessary security controls for the system and identifies critical research areas.

The Department of Energy (DOE) has also released numerous documents. Their "Roadmap to Achieve Energy Delivery System Cyber Security" document introduces both near-term and long-term milestones required to achieve appropriate grid's cyber security.

In addition to federal efforts, the North American Electric Reliability Corporation (NERC) has recognized these concerns and introduced compliance requirements to enforce baseline cyber security efforts throughout the bulk power system through the Critical Infrastructure Protection (CIP) standards [7]. NERC CIP presents a baseline for implementing and managing cyber security.

Table 1: Key Roadmap or Policy Documents and Cyber Security Issues Addressed

Policies/ Documents	Issues Addressed
Roadmap to Achieve Energy Delivery System Cyber Security (DOE) [3]	Addresses future directions of both cyber and physical grid systems to
NISTIR 7628, "Guidelines for Smart Grid Cyber Security"[8]	Provides a comprehensive overview of cyber security concerns against various smart grid initiatives. Introduces current research efforts and identities necessary security controls for protecting the smart grid.
NIST 800-82, "Guide to Industrial Control Systems (ICS) Security" [10]	Identifies cyber security concerns within industrial control systems (ICS), including:
GAO-11-117: Electricity Grid Modernization: Progress Being Made on Cyber Security Guidelines, but Key Challenges Remain to be Addressed [5]	Prioritizes cyber-physical attributes within cyber security including risks from combined cyber-physical attacks.
The Future of the Electric Grid (MIT) [11]	Provides a thorough review of current grid trends and future . Enumerates cyber security concerns with future smart grid initiatives.
High-Impact, Low-Frequency Event Risk to the North American Bulk Power System (NERC/DOE) [12]	Identifies the grid's inherent vulnerability to coordinated attacks. Specifically from DDOS, rogue devices, unauthorized access attacks, and malware. Additionally, common modal failures and concerns from advanced persistent threats are also addressed.
NERC Critical Infrastructure Protection (CIP) [7]	Cyber security compliance requirements for the bulk power system.
NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses [1]	Reports results from numerous control system cyber vulnerabilities assessments. Identifies commonly found weaknesses in software and networks
DHS Common Cyber Security Vulnerabilities in Industrial Control Systems [13]	Documents results of numerous cyber security assessments against various critical infrastructures.

2.2. Cyber Security Requirements

The smart grid will introduce new applications that rely on cyber infrastructures. An overview of security requirements for key applications is identified in Table 2.

- *Advanced Metering Infrastructures (AMI)* – the systems deployed to provide two-way communication to all customer power meters. This enables more granular control of consumer consumption, real-time pricing, and distributed generation.
- *Distribution Management Systems (DMS)* – set of systems required to control lower voltage, consumer level energy distribution.
- *Energy Management Systems (EMS)* – set of power applications used to control bulk power system generation and transmission.
- *Wide Areas Measurement, Protection and Control (WAMPAC)* – set of applications that collectively provide PMU-based wide-area monitoring (state estimation), protection, and control.
- *Power markets* – Commodity-based energy markets necessary to balance the supply and demand for electricity.

Table 2: Smart Grid Cyber Security Requirements

Smart Grid Applications	Information and Infrastructure Security	Application Security
AMI	I, AT, C	I, N
DMS	I, A, AT	I, A
EMS	I, A, AT	I,
WAMPAC	I, A, AT, C	I, A
Power Markets	I, A, AT, C	I, N

Each application's security requirements are divided into the infrastructure and application layers. The identified security properties include:

- Confidentiality (C) – protection of information from unauthorized disclosure
- Availability (A) – system/information remains operational when needed

- Integrity (I) - protection of system/information from unauthorized modification
- Authentication (AT) – limiting system access to only authorized individuals
- Non-Repudiation (N) – inability to of a user or system to deny their responsibility for a previous action.

.

Integrity is critical to ensure the accuracy of all smart grid systems including billing data, market information, system measurement, and control information. Availability is also critical for most systems, especially for control applications. Confidentiality is necessary to protect user consumption and financial data. Non-Repudiation is important for inter-domain systems where applications, individuals or organization must be held responsible for any fraudulent actions. Finally, authentication is required to ensure that malicious individuals are not able to manipulate critical systems or information.

2.3. Cyber Security Roadblocks

While this concern for lacking cyber security within the electric grid is well documented, the development and deployment a more secure infrastructure is constrained by many factors, which are enumerated below.

a) *Limited physical protections*. The lack of appropriate physical systems means that attacks can more easily access remote networks, such as those used to support a substation.

b) *Long system deployments*. Power equipment has longer life spans than typical IT systems. Therefore, systems must be designed to either be secure from, or adapt to long-term evolutions in security threats.

c) *Restricted use of "fail-closed" security mechanisms*. Many cyber protection methods are designed to restrict access before they leave a secure state, such as locking out an account after multiple failed login attempts. However, this could prevent an operator from accessing a system at a critical time and therefore would not be acceptable in this environment.

d) *Geographically disperse*. System management functions such as patching and maintenance, become more difficult and error prone, which creates tendencies to avoid potential failures by limiting these tasks.

e) *Legacy system dependencies*. The grid is currently dependent on large amounts of legacy systems, which currently implement insufficient security mechanisms.

While improved security mechanisms are required to increase the security of the cyber infrastructures, these constraints will limit the efficacy of this approach. Fortunately, the physical redundancies within the grid, known safe system parameters, and availability of system forecast presents an opportunity to redevelop grid control algorithms to provide additional resiliency to cyber attack.

3. Issue Discussion

The cyber attacks to smart grid, and in general to critical infrastructure systems, could be of many forms. Figure 1 identifies the common form of cyber attacks on these systems.

***Protocol attacks**:* The protocols used in the power system, such as ICCP, IEC 61850, DNP3, could be potentially exploited to launch cyber attacks if they are not secured properly. This calls for secure versions of these protocols that not only provide security guarantees, but also the required latency and reliability guarantees needed by the grid applications.

***Routing attacks**:* This refers to cyber attack on the routing infrastructure of the Internet. Although this attack is not directly related to the operation of the grid, a massive routing attack could have consequences on some of the power system applications, such as real-time markets, that rely on them.

***Intrusions**:* This refers to exploiting vulnerabilities in the software and communication infrastructure of the grid which then provides access to critical system elements. Example intrusion scenario is to gain access to substation HMI bypassing security controls (firewalls, system passwords).

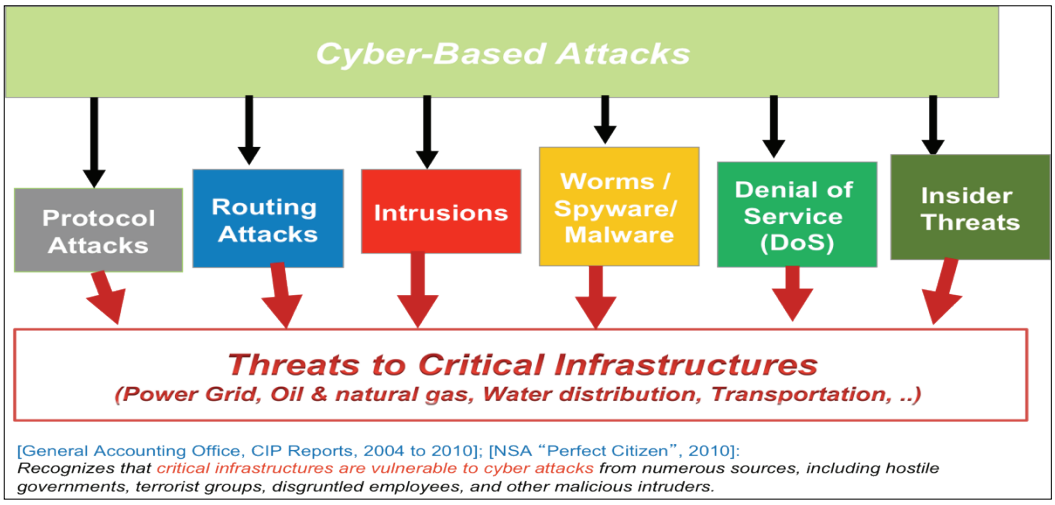

Figure 1: Cyber Attacks Against Critical Infrastructures

***Malware**:* This refers to malicious software that exploits vulnerabilities in system software, programmable logic controllers, or protocols. The malware generally scans the network for potential victim machines, exploits specific vulnerabilities in those machines, replicates the malware payload to the victims, and then self-propagation. In recent years, malware attacks are growing in numbers and sophistication, and this has been a source of major concern for critical infrastructure systems (e.g., Stuxnet) including the power grid.

***Denial of service attacks**:* Any attack that denies normal services to legitimate users is often called denial of service. This could also mean *denial of control* in the power grid context. These attacks are typically created through massive resource exhaustion attacks that flood the communication network or the server with huge volumes of traffic or spurious workloads, thus denying service to legitimate users.

Insider threats: A insider abuses their current system privileges to perform a malicious action. This form of threat is perceived as a source of concern in recent years as identified in many federal documents, including GAO CIP reports [5, 6].

3.1 Evaluating Risk from Cyber Attack

Risk is traditionally defined as the product of available threats, system vulnerabilities, and their resulting impact, as shown by the following equation.

Risk = [Threat] X [Vulnerability] X [Impact]

Therefore, the increase or decrease in current threats, vulnerabilities, or impacts will directly reduce the risk from a cyber attack.

The *threat* can be defined as the presence of potential attacks, their motivation, and available resources. Often threat sources can range to unsophisticated individual hackers, to more advanced organized criminals, and highly motivated nation-states. Threats are often dynamic and are generally motivated by various political and economic agendas.

The *vulnerability* of these systems depends on the grid's cyber *supporting infrastructure*. This typically entails all the computers, software platforms, networks, protocols, and other resources required to support grid control and monitoring functions. The grids supporting infrastructure is currently plagued with vulnerabilities due to its heavy dependency on legacy systems, which were not designed from a security perspective.

The risk of a cyber attacks is also dependent on the *impact* that the attack has on the power systems. This will primarily be determined by how the various cyber vulnerabilities impact that grid's various *power applications* or the set of domain specific control and management functions required to perform necessary to control the physical system. An attacker's ability to impact the power application will be the resulting factor in whether it impacts the physical system.

Developing a secure power system requires that both the applications and supporting infrastructure are designed to be attack resilient. Unfortunately, the grid's cyber-physical properties and tremendous scope place many constraints on the ability to develop a secure cyber infrastructure. It must be assumed that even within significant infrastructure enhancements, an advanced, persistent attacker will still be able to launch successful attacks. Most current grid control mechanisms have been developed to be tolerant to many traditional physical and environmental faults. However, faults initiated by a human attacker will likely be intelligently designed to bypass these currently engineered

redundancies. Therefore, it is *critical to address redesign the grid's fundamental control mechanisms and algorithms to provide a foundational layer of attack resilience* throughout the grid [14].

3.2 Attacks against Cyber-Physical Systems

Attacks against a cyber-physical system greatly differ from those targeting traditional IT systems. While attacker techniques will likely closely resemble traditional attacks, their ability to impact the grid is heavily dependent on the control functions or power applications supported by those systems.

Figure 2 shows how a cyber attack would impact the electric grid. First an attacker would have to degrade the integrity, availability, or confidentiality of some portion of the cyber infrastructure. This degradation would then impact some set of power applications used to support the grid. The attacker's ability to manipulate some power application would then directly lead to some physical system impact.

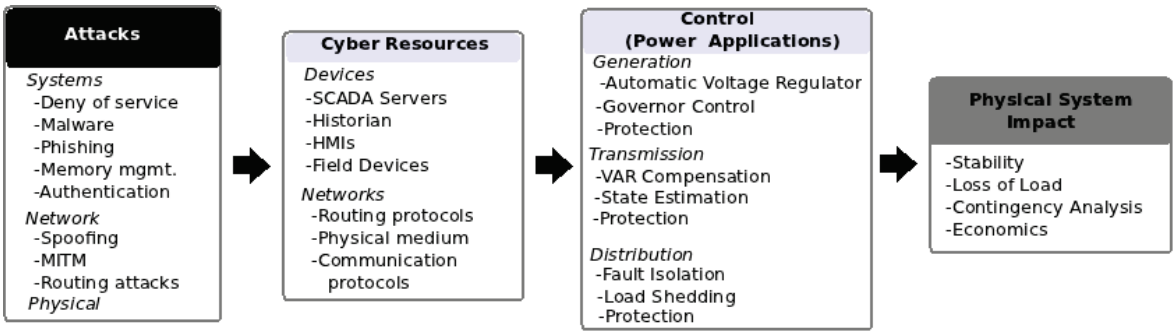

Figure 2: Mapping from Cyber Attacks to Control Actions to System Impacts

3.2.1 Coordinated Attacks

Since the current grid is designed with adequate resiliency to handle numerous scenarios from physical system failures, this resilience may also help limit the impact of any cyber attack targeting a single system. For example NERC has regulations for planning and operation of the power system includes credible and critical, single and multiple event contingencies within its scope. The failure of any single element in the power system, such as a transformer or a transmission line, is a credible contingency (n-1).

However, as identified in the NERC HILF report [12], coordinated attacks present a particularly concerning scenario as multiple, simultaneous system failures can cause the grid to enter an unstable state, potentially resulting in a cascading outage.

While coordinated attacks require greater sophistication, various system properties such as fairly homogenous systems and significant trust between systems will increase the impact of common modal failure. Additionally, unlike physical attacks, cyber attacks assets typically do not incur additional cost when launched against multiple systems

simultaneously. Therefore, coordinated attacks, where performed through entirely cyber or a combination of cyber and physical mechanisms present a significant threat to grid operations.

3.3 Cyber Infrastructure Security

As pointed in earlier sections, the cyber infrastructure used to support the grid's control and monitoring functions is currently insufficient. Table 3 identifies results from recent INL vulnerability assessment efforts within various ISC environments [1].

Table 3: Cyber Vulnerabilities within Industrial Control Systems

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

3.3.1 Software Weaknesses/Vulnerabilities

Many software platforms used within the electric grid were developed to operate on legacy systems, which were not designed to be secure from attack. This software often lacks necessary mechanisms to authenticate all users before allowing system access. These systems also often lack sufficient access control mechanism required to constrain provisioned user privileges and perform auditing of user actions.

3.3.2. Network Weaknesses/Vulnerabilities

In addition to these software concerns, the networks to support these systems also maintain numerous deficiencies. Often the systems and protocols used to communicate SCADA traffic lack adequate encryption and authentication. The means that any unauthorized individual that is able to access the physical network layer will be able to perform man-in-the-middle attack to manipulated valid control functions.

3.4 Power Application Security

The power system is functionally divided into generation, transmission and distribution. Each functional division has systems that control specific machines/devices and work using dedicated communication signals and protocols. By this, each control system has its own vulnerabilities, threat vectors and potential impact on power system operation. Figure 3 presents a classification of these control loops along with further details on their operation.

Power – Cyber Physical Systems Control Taxonomy

Domain	Control	Control Attributes						
		① Physical Parameter	② Measurements & Inputs	③ Communication Data Acquisition	④ Messages Control	⑤ Computation	⑥ Machine/ Device	⑦ Control Action
Generation	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
	Security-Constrained Economic Dispatch	Power Generation	Demand, Network Topology and Line Limits	Wide-Area Communication (IEC 61850)	Point to Point Communication (DNP 3.0)	Generation Set Points	Generators	Generation Re-Dispatch
Transmission	State Estimation	Power Generation and Network Topology	Voltage & Power, VAR or Current-Flow	Wide-Area Communication (IEC 61850)	Point to Point to switchyards and generating stations	System Voltage and Phase Angle Calculation	Generators and Switching Devices	Generation Re-Dispatch and Open/Close Breakers
	VAR Compensation	Voltage	Reference Voltage, Measured Voltage & VAR device parameters	Local measurement	Local message to FACTS device	Reactive Power Level Calculation	FACTS	Absorb/Supply Reactive Power
	HVDC Transmission Control	DC Voltage and Current	Reference Voltage & Measured Voltage	Local measurement of voltage	Local message to converters	Firing Angle	Power Electronic Converters	Increase/ Decrease Firing Angle
Distribution	Demand Side Management	Load Scheduling	Demand, Conventional and Alternate Resources availability	Power demand request	Allotted schedule to factories and homes	Load schedule computation	Loads	Turn On/Off Load
	Load Shedding	Load connected to system	Generation Limit, System Frequency & Current Generation	Local frequency measurement & generation level from control center	Trip message to relays on distribution feeder	Load amount and location	Distribution Feeder	Open feeder breaker
	Advanced Metering Infrastructure	Consumer Load	MDMS/Headend Instructions	NA	Disable/Load Shed	Meter Function	Consumer Meter	Disable Meter/ Shed Load

Figure 3: A Taxonomy of Control Loops in the Power Grid [14]

3.4.1. Generation

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.

Automatic Voltage Regulator

Generator exciter control is used to improve power system stability by controlling the amount of reactive power being absorbed or injected into the system. The digital exciter control module is connected to the plant control center via Ethernet and communicates using protocols such as Modbus and Ethernet Global Data. This Ethernet link is used to program the controller with voltage set-point values. The AVR control loop receives generator voltage feedback from the terminal and compares it with the voltage set-point stored in memory. Based on the difference between the observed measurement and the set point, the current through the exciter is modified to maintain voltage at the desired level.

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. As in the case of AVR, this communication link is used to define operating set-point for control over the governor.

Cyber Vulnerabilities

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 cyber security 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.

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 inter-area 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.

Cyber Vulnerabilities

AGC 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.

3.4.2. Transmission

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.

VAR Compensation

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. Recent advancement in thyristor-based controllers, devices such as the ones belonging to the *Flexible AC Transmission Systems* (FACTS) family, is gaining popularity. FACTS devices that interact with one another to exchange operational information are called Cooperating FACTS devices (CFD). Though these devices function autonomously, they depend on communication with other FACTS devices for information to determine operating point.

Cyber Vulnerabilities

The following are attack vectors that are effective in the CFD environment [14].

- *Denial of Cooperative Operation:* In this type of attack, flooding the network with spurious packets could jam the communication to some or all the FACTS devices. This will result in the loss of critical information exchange and thus affect long-term and dynamic control capabilities.

- *De-synchronization (Timing-based attacks):* The control algorithms employed by CFD are time-dependent and require strict synchronization. An attack of this kind could disrupt steady operation of CFD.

- *Data Injection Attacks:* This type of attack 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 result in unstable operating conditions.

3.4.3. Distribution

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.

Load Shedding
Load shedding schemes are useful in preventing system collapse during emergency operating conditions. In cases where the system generation is insufficient to match up to the load, automatic load shedding schemes could be employed to maintain the system's operating variables within safe operating limits and protect the equipment connected to the system.

Cyber Vulnerabilities
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.

AMI and Demand Side Management
Future distributions systems will rely heavily on an Advanced Metering Infrastructure (AMI) to increase reliability, incorporate renewable energy, and provide consumers with granular consumption monitoring through *Demand Side Management*. 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 and reschedule them to hours when wind energy is available.

Cyber Vulnerabilities
The smart meters at consumer locations introduce cyber-physical concerns. Control over whether the meter is enabled or disabled and the ability to remotely disable devices through load control switching (LCS) provide potential threats from attackers. Adding additional security into these functions presents interesting challenges. Additionally, meter tampering will likely continue to be a significant problem as consumer's attempt to reduce their energy costs.

3.5 Human Factors

In addition to security concerns with the cyber infrastructure and power applications, human factors must also be incorporated into the development of a more resilient electric grid. While many grid control functions are closed-loop systems, many large-scale control functions are performed as human-in-the-loop control. Therefore, understanding and enhancing how operators monitor system state, make critical decisions, and perform resulting controls will also critical to the security of the electric grid.

An intelligent attacker with intrinsic knowledge about grid operations and common operator decision processes may be able to devise an attack which exploits these mitigation actions to compound the severity of the cyber attack.

4. Paths to Issue Resolution

Research initiatives are required to develop protected cyber infrastructures, secure critical information, and produce resilient power system applications. Figure 4 provides an overview of future research requirements and methods that could be used to address these issues [14].

Smart Grid Cyber Security = Information Security + Cyber Infrastructure Security + Power System Application Security

Traditional information security and infrastructure security solutions need to be tailored to the smart grid environment dealing with legacy nature of the infrastructure and the real-time nature of the communication involved. In addition, the security must be built into the applications themselves. Conventionally, the power applications (e.g., EMS, markets) are designed to deal with random faults that occur in the power system or information/communication systems. These are not clearly inadequate to deal with malicious faults (cyber attacks) with possibility of coordinated attack events. Therefore, the security of the future grid must have security built in all three levels to provide defense-in-depth to deal with known and emerging cyber attacks.

	Information Security	Infrastructure Security	Application Security
NEEDS	▫ Information Protection ▪ Confidentiality ▪ Integrity ▪ Availability ▪ Authentication ▪ Non-repudiation	▫ Infrastructure protection ▪ Routers ▪ DNS servers ▪ Links ▪ Internet protocols ▫ Service availability	▫ Generation control apps. ▫ Transmission control apps. ▫ Distribution control apps. ▫ Real-Time Energy Markets
MEANS	▫ Encryption/Decryption ▫ Digital signature ▫ Message Auth.Codes ▫ Public Key Infrastructure	▫ Firewalls ▫ Intrusion detection ▫ Secure Protocols ▫ Authentication Protocols ▫ Attack Attribution ▫ Secure Servers	▫ Attack-Resilient Control Algos ▫ Model-based Algorithms - Anomaly detection - Intrusion Tolerance - Bad data elimination ▫ Risk modeling and mitigation

Figure 4: Cyber Security for Smart Grid Environment

Emerging Research Challenges

Developing a secure smart grid environment will require substantial research efforts which addressing various different areas and approaches. The following section will document critical research areas.

4.1 Information & Infrastructure Security

4.1.1. Communication

Methods are required to protection communication from malicious modifications, denial or service, or spoofing attacks. This requires specially tailored encryption, authentication and access control mechanism.

4.1.2. Device Security

The grid's heavy dependency on embedded systems with for field devices and meters create numerous security concerns, specifically because they are often resource constrained and lack security mechanisms. Additionally, since these devices often lack physical protections, greater device attestation is required to detect malicious modifications.

4.1.3. Cyber Security Evaluation

There are increasing security assessment requirements for the electric grid, specifically to achieve compliance requirements for regulatory agencies. This creates a need for methods to accurately assess the infrastructure without negatively affecting system operations. Additionally, research testbed are required to perform evaluation of assessment techniques without negatively impacting the operational systems.

4.1.4. Intrusion Tolerance

Unfortunately, some cyber attacks may bypass protection mechanism. This requires specially tailored intrusion detection systems (IDS) which can detect attacks against the system and protocols used within these environments. Additionally, the development of intrusion tolerant cyber architectures can reduce the severity of a successful attack.

4.1.5. Security Management and Awareness

The environments utilization of different communications and platforms requires the development of new digital forensics capabilities as attacks will likely different from traditional IT environments. Additionally, methods to manage and correlate both emerging and normal system events are required to address increasing utilization of cyber assets.

4.2. Application Level Security

The redevelopment of current grid control algorithms is imperative to ensure they can tolerate both traditional system faults as well as cyber attack aimed at intentionally manipulating their operation. Algorithm redevelopment should target all system control, monitoring, and protection requirements.

4.2.1. Attack-Resilience Control

A resilient industrial control system is one that is designed and operated in a way where-the following requirements can be met [16, 17]:

- The occurrence of undesirable incidents can be minimized
- Most of the undesired incidents can be mitigated
- The impact from undesired events can be minimized
- The system returns to normal operating point in a short time

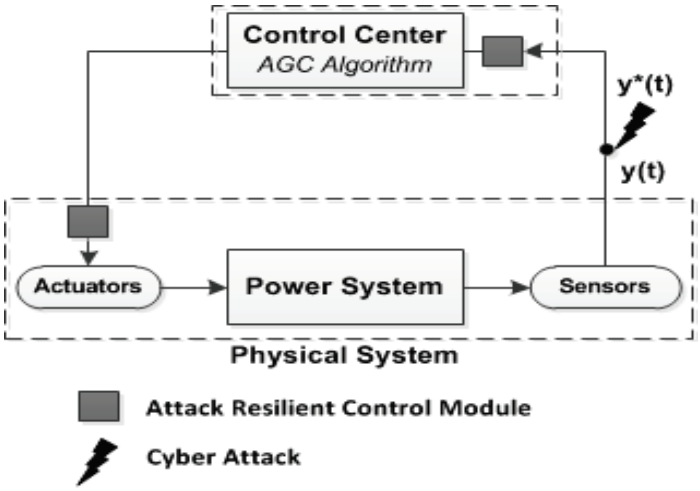

Figure 5: Schematic of Cyber Attacks on Control System

In automated control systems (Figure 5), the control center typically accepts measurements as input ($y(t)$) from field devices and processes them to obtain the output control signal ($u(t)$). The control center relies on these measurements to assess the true state of the system. As long as the measurement is within an acceptable range $[y_{\min}(t), y_{\max}(t)]$, the control center processes the output even if the input is not reflective of the true system state. This was acceptable as errors introduced in the field measurement signals were traditionally due to transducer errors and channel noise, which are not significant. However, a smart attacker could manipulate measurements such that the manipulated measurements still lie within the acceptable range, but differ significantly from the true values [14, 18]. Any operational decision made based on these measurements could cause instabilities to the underlying power system as it could trigger control actions that are not required for true system state. The control module does not possess intelligence or situational awareness to check if the reported system state is consistent with the true state. The need is for attack resilient control systems that are a combination of smart *attack detection* and *mitigation*. The following are potential approaches to attack resilient control design.

Intelligent/resilient control algorithms*:* Developing control algorithms that aid in graceful system degradation and quick restoration will aid in minimizing the duration and

magnitude of the impact. At the power system level, redundancy will definitely help in reducing the criticality of certain elements. Greater correlation of known physical system state will provide the ability to develop more attack resilient algorithms.

Domain-specific anomaly detection and intrusion tolerance: The development of anomaly-based intrusion detections and intrusion tolerant architectures can also leverage improved cyber event correlations. This is an approach to extract and analyze the data from power instruments and cyber-related logs to distinguish if a threat is credible. Event correlations can be categorized as (i) temporal, (ii) spatial, or (iii) spatio-temporal. These combinations introduce a different perspective of threat that may capture local or global abnormality.

The grey box in Figure 5 represents a control application-dependent attack resilient control module that should be programmed with intelligence to detect attacks directed at the control loop it is associated with. In other words, we propose that it is important for each control application in power systems to have grey box that is provided with the correct information (intelligence) in order to detect attacks that are successful in that domain.

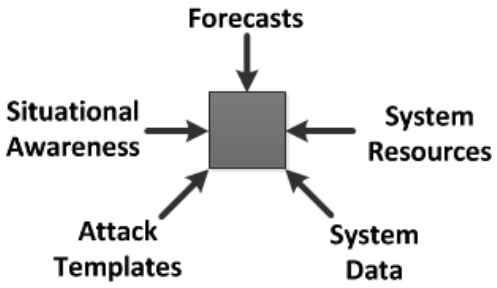

Figure 6: Sources of Data for Attack-Resilient Control Algorithms

Figure 6 identifies potential information that could be used to program attack resilient control modules for control applications in power systems. The figure shows five broad classes (not exhaustive) of power system information that could be used in building the grey box. The text below presents some ideas on how some of this information could be used to detect attacks.

Forecasts*:* Power system forecasts could be of significant assistance in attack detection. Load forecasts of various time scales (day-ahead, short-term) could be used to detect attacks that reflect unprecedented load increases or drops. An example scenario is in which the attacker changes the value of P*ref* (reference power) in a wind turbine to force a reduction in the active power output. In this scenario, an attack resilient control module provided with wind forecast information could have possibly detected the attack.

Situational Awareness*:* Information such as stability limits, current system topology, time of the day, geographic location, weather details, market operation, nature of loads

(e.g. industries, domestic) could potentially help identify cyber attack situations. For example, phasor measurements from phasor measurement units in two different geographic locations could help confirm if the measurements reported by the power flow meters are accurate. Situational awareness could also help the control module process the correct mitigation strategy. A version of this already applied in load shedding strategies where special load zones such as hospitals are given priority in scenarios where load shedding has to be performed.

System Resources*:* Examples of power system resources are - generation reserves, VAR reserves, available transmission capacity, standby computers, backup communication paths, etc. The available resources should be taken into account when the control module processes mitigation strategies in the event of an attack at the physical layer. For example, if the cyber logs of a transmission substation reveal a potential attack scenario, the power that is carried by those transmission lines could be re-distributed to other lines to prevent severe consequences if the attacker is successful.

Attack Templates*:* The control module should be aware of attack templates (vectors) that are effective against each control loop. Similarly, the control module should also know signatures of attacks for a specific implementation in the ICS. This could assist in early attack detection and defense at the cyber layer.

System Data: System parameter data, such as machine data, is not publicly available and utilities like to protect this information. Such data play a critical role in system response to disturbances. Infeasible values of for system parameters should be identified as anomalies and possible signs of a cyber attack.

4.2.3. Attack-Resilient Wide Area Monitoring

The information obtained from the traditional SCADA field devices and several synchrophasors deployed over a wide-area are crucial in providing the operators a tool to monitor and provide situational awareness about the operating conditions of the grid. A cyber attack on the monitoring algorithms can deceive the operators or provide false information about the current operating conditions for several of the EMS applications like SCOPF, SCED, Contingency Analysis, and other emerging wide-area disturbance monitoring applications. Developing attack resiliency in these applications is essential to maintain adequate and accurate situational awareness of the grid operating conditions.

In particular, State Estimation (SE) is one of the most important monitoring algorithms in power system operations as it provides a reasonably accurate estimate of system voltages and phase angles. Research on how different aspects of SE are impacted by cyber attack is a promising area. Some of the past research efforts in this area were to develop possible attack vectors for specific types of attacks like data integrity or false data injection [19], characterizing unobservable cyber attacks [20] using PMU's to mitigate data injection attacks by strategic placement [21], and studying how market prices can be manipulated through data injection attacks [22]. Though there are some unanswered questions in these areas, there are some new research directions which also merit their due attention. Studying how topology errors could play a part in creating cyber attacks,

modeling how the attacker would respond to an operator's actions in an intelligent attack scenario where there are more than one attack stages as in a game theoretic framework, analyzing how PMU's are being integrated into conventional SE. Also, identifying possible vulnerabilities and attack vectors in this hybrid SE algorithm, developing some relevant attack impact metrics for such attacks, and more importantly developing new algorithms that can tolerate these different types of attacks. The following figure summarizes the current and future research directions in the area of attack resilient monitoring and protection algorithms.

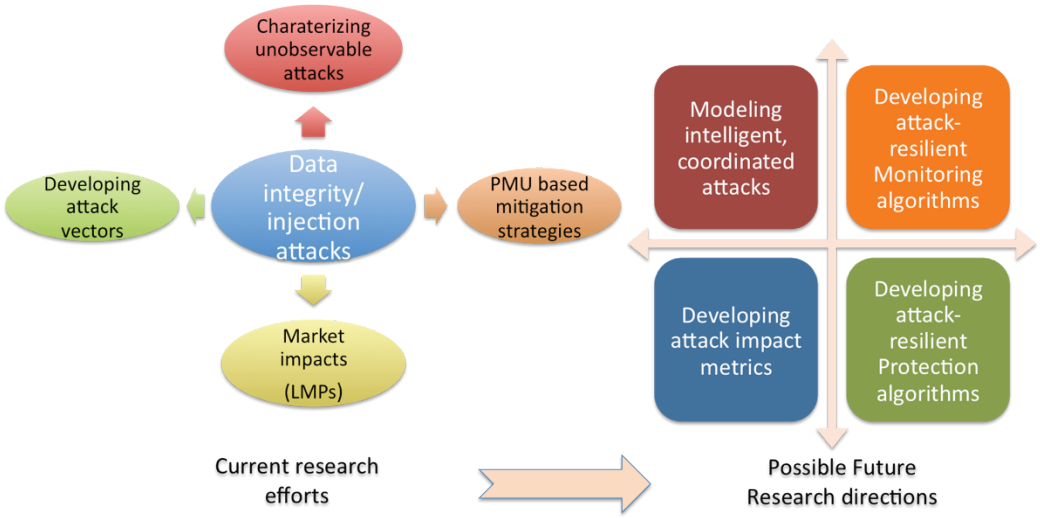

Figure 7: Research Needs for Wide-Area Monitoring and Protection

4.2.3. Attack-Resilience Protection

Wide-Area Protection (WAP) involves the use of system wide information collected over a wide geographic area to perform fast decision-making and switching actions in order to counteract the propagation of large disturbances [23]. The advent of Phasor Measurement Units (PMU) has transformed protection from a local concept into a system level wide-area concept to handle disturbances. The inherent wide area nature of these schemes presents several vulnerabilities in terms of possible cyber intrusions to hinder or alter the normal functioning of these schemes. Even though wide-area protection schemes like Special Protection Schemes (SPS) are designed to cause minimal or no impact to the power system under failures, they are not designed to handle failures due to malicious events like cyber attacks. Also, as more and more SPS are added in the power system, it introduces unexpected dependencies in the operation of the various schemes and this increases the risk of increased impacts like system wide collapse, due to a cyber attack. It therefore becomes critical to reexamine the design of the Wide- Area Protection schemes with a specific focus on cyber-physical system security. This is also supported well by the WECC RAS Guide [24], which recommends that specific cyber security protection methods must be determined by each utility and applications to protect RAS equipment be made similar to other critical cyber assets in the power system. Figure 7 highlights potential research directions in attack-resilient wide area monitoring and protection.

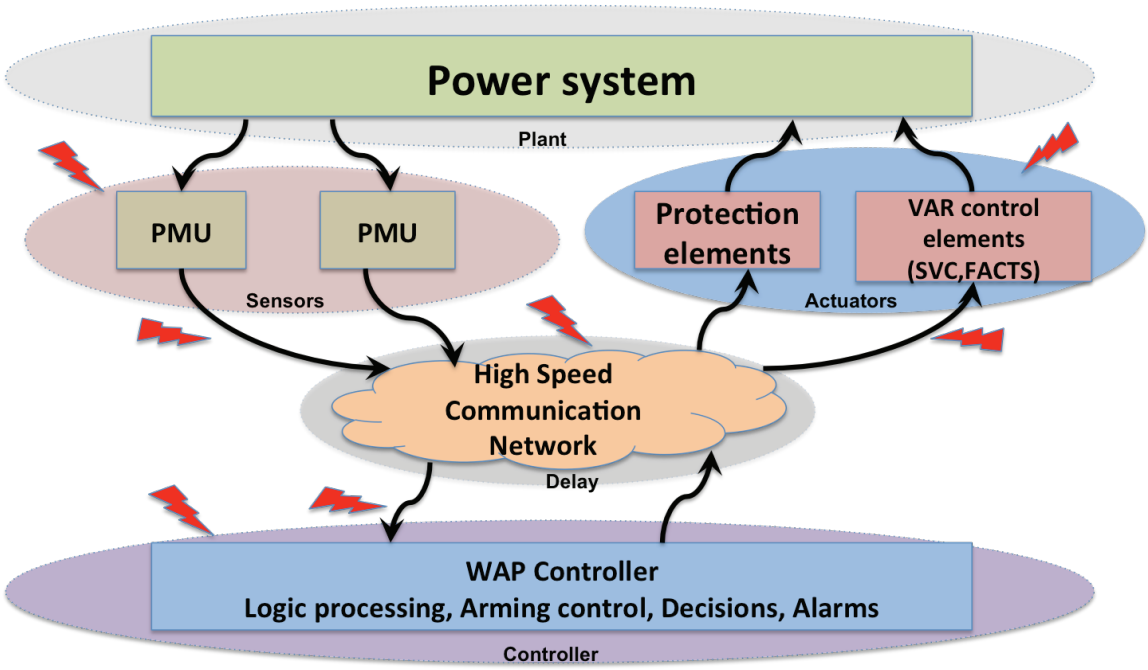

Figure 8: Control System View of Wide Area Monitoring and Protection

A control systems view of the power system and the wide-area protection scheme is illustrated in Figure 8. The power system is the plant under control, where the parameters like currents and voltages at different places are measured using sensors (PMUs) and sent through the high-speed communication network to the Wide-Area Protection controller for appropriate decision making. The controller decides based on the system conditions and sends corresponding commands to the actuators which are the protection elements and VAR control elements like SVC and FACTS devices for voltage control related applications.

There are different places where a cyber attack can take place in this control system model. The cyber attack could affect the delays experienced in the forward or the feedback path or it could directly affect the data corresponding to sensors, the actuators or the controller. The lightning bolts indicate the attack points on this control system model.

Some of the research challenges and research tasks in developing attack resilient wide-area protection schemes are:

1. Systematically identifying the various vulnerabilities that exist in current and emerging Wide Area Protection Systems.
2. Identifying and classify the different cyber-attack templates on some of the SPS architectures. Based on a very generic classification we can identify two main types of cyber attacks that can impact wide-area protection schemes. They are timing based and data integrity based attacks.

3. Analyzing the various impacts on the power system that can occur due to individual and coordinated cyber-attacks through cyber-physical test-bed based simulations and developing relevant attack impact metrics.
4. Developing suitable mitigation strategies using the cyber and physical systems to create attack-resilient WAP schemes and validating them using cyber-physical test-bed based simulations. The mitigation can come in terms of increasing the security measures like intrusion detection systems, access controls, etc., or in terms of intelligent SPS design schemes which are resilient to cyber attacks.

4.3. Risk Modeling and Mitigation

The overarching goal of cyber risk modeling framework for smart grid security should integrate the dynamics of the physical system as well as the operation of the cyber-based control network. The integration of cyber-physical attack/defense modeling with physical system simulation capabilities makes it possible to quantify the potential damage a cyber attack can cause on the physical system in terms of capacity/load loss, stability violations, equipment damage, or economic loss [15]. The integrated model also provides a foundation to design and evaluate effective countermeasures, such as mitigation and resilience algorithms against large-scale cyber-based attacks.

The purpose of the proposed methodology (shown in Figure 9) is to model intrusions and evaluate the consequences of a cyber-attack on the power grid. Understanding risks from attacks requires analysis of interdependencies of cyber-physical systems.

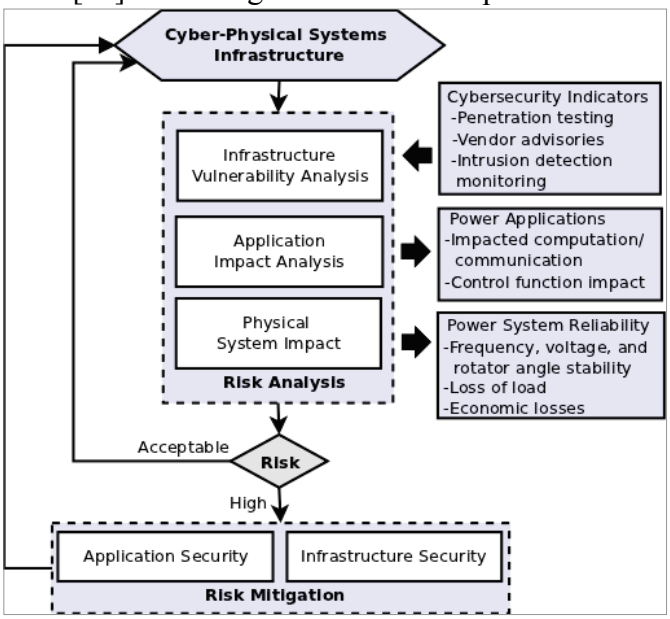

Fig. 9: Risk Modeling and Mitigation Framework [14]

1. ***Cyber vulnerability assessment****:* Traditional vulnerability assessment techniques such as penetration testing and vulnerability scanning are not appropriate for this environment as they frequently cause failures in legacy systems. Methods to perform safer and more reliable assessments are necessary to ensure that critical cyber assets are protected from attack.

2. ***Impact analysis****:* The criticality of cyber vulnerabilities should be evaluated based on their ability to impact either the physical power system or supporting functions such as billing or market data. The evaluation of the physical system should include analysis of the power applications and their ability to impact 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 grids stability parameters in terms of voltage, frequency, and rotor angle.

3. ***Mitigation****:* Risk mitigation efforts can address both infrastructure and application perspectives. Infrastructure enhancements will primarily consist of both novel and tailored traditional cyber security protections such as cryptography, access control, and authentication mechanisms that can provide both adequate security, high-availability, and can be easily integrated with legacy systems.

4.4. Coordinated Attack-Defense

An intelligent coordinated attack would involve a series of attacks launched almost at the same time or within a short span of carefully regulated time intervals in such a way that the primary attack is launched on a critical system component and the followup (secondary) attacks are launched on the components that inherently respond to mitigate the failure of that primary component. In other words, if a coordinated attack plan includes actions to nullify the effect of existing mitigation strategies at every step along the way, the physical impact caused could be severe. NERC's High Impact Low Frequency (HILF) report [12] identifies digital relays, remote terminal units (RTU), circuit breakers, static VAR compensators, capacitor bank controllers, demand response systems, meters, plant control systems, plant emission monitoring systems, and Energy Management Systems (EMS) as potentially vulnerable elements in the system.

An intelligent attacker can create an attack template that includes attacking more than one of the above devices, to create critical contingencies that were not considered to be credible during the planning stage. Coordinated cyber attacks also change the scope of "credible multiple contingencies". System planning and operational studies should include new sets of failed system states. Joint failures of elements that are geographically dispersed and have no direct relationship will now have to be accounted.

The NERC and DOE Report 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 inflict 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.

Intelligent coordinated attacks Template: To create maximum impact, an attacker would create smart attack templates that involve strategic targeting of elements to cripple the power system. In our view, an intelligent coordinated attack would involve a series of attacks launched almost at the same time or within a short span of carefully regulated time intervals in such a way that the primary attack is launched on a critical system component and the follow-up (secondary) attacks are launched on the components that

inherently respond to mitigate the failure of that primary component. In other words, if a coordinated attack plan includes actions to nullify the effect of existing mitigation strategies at every step along the way, the physical impact caused could be severe.

Cyber contingency requirements: The dynamic environment of the smart grid requires a reassessment of traditional credible cyber contingencies. In the case of cyber attacks, elements that do not share electrical or physical relationships can be forced to fail simultaneously, resulting in unanticipated consequences. The traditional approach to determining system reliability with (N-1) contingencies and a restricted set of multiple contingencies is not sufficient. It becomes critical to understand the impacts of and analyze the performance of existing system defense contingency defense mechanisms during (N-n) contingencies, where $n > 1$.

Research needs: (1) An efficient computational algorithm that systematically enumerates all coordinated attack templates (HILF events) for a given power system by analyzing the topological properties and criticality of the system components. (2) Systematic impact evaluation for the created attack templates quantifying impacts in terms of load loss and stability violations. (3) Develop deeper insights into the timing dimension of the attacks, which will aid in developing effective attack-resilient algorithms.

4.5. Trust Management and Attribution

The cyber infrastructure in the power system domain can be viewed as interconnected "islands of automation". This interconnection brings about inherent trusts concerns as vulnerabilities in other domains may abuse trust relationships [25]. In addition, if an organization has system affected by a security event, that information may not be communicated to all concerned domains, therefore, the decreased trust is not appropriately communicated to all the other systems.

1. ***Trust Management Lifecycle***: The dynamic environment of the smart grid requires a trust model, which allows continual reevaluation. Since the smart grid will likely exhibit emergent behaviors, trust management must remain flexible to address continual modifications in usage and misuse patterns. The trust management policies should allow specific tailoring of these changes.
2. ***Formal Trust Representation***: Investigate quantified notions of trust, specifically representing impact to control and privacy data. Develop algorithms to evaluate a trust revisions impact on grid reliability.
3. ***Insider Threat Management****:* While most cyber protections attempt to limit external attacks, recent events have increased concerns from malicious insiders. Utility employees are typically highly trusted to efficiently manage and operate the grid, however, nefarious actions by these individuals could produce disastrous results.
4. ***Attribution****:* The ability to attribute actions back to a system or user is imperative to identify malicious actors. By developing strong attribution mechanisms, the

individuals responsible for a cyber attack can be identified and penalized. Additionally, attribution provides a method to deter future malicious activities.

4.6. Data Sets and Validation

Performing research within this domain is often constrained by the lack of accurate data about current system deployments. This requires that research make often inaccurate assumptions, and limits the applicability of the results. The development of accurate datasets is necessary to ensure academic efforts can be transitioned to current environments.

1. ***Cyber/Physical Network Data Sets****:* The development of open and accurate models of the networks and traffic are necessary to ensure that research efforts accurately represent realistic system implementations. The development of accurate network models should include realistic network topologies, communication protocols, temporal data requirements, supported power applications, and physical power system.
2. ***Cyber Attack Data Sets****:* Along with accurate network models, accurate information about possible cyber attacks is necessary to ensure that researchers are able to understand current threats and attacker techniques. Accurate attack data has main applications including the development of intrusion detection systems and intrusion tolerant architectures.
3. ***Realistic Testbeds****:* Having accurate data sets is critical to designing more attack resilient systems, realistic testbed are also required to explore cyber-physical interdependencies and their resulting security impacts. Additionally, testbeds provide a platform where research and vendor products can be evaluated with simulated power system requirements.

5. Conclusions

The development of an attack resilient electric grid is necessary to address increasing concerns to the security of the nation's critical infrastructure. As cyber attacks become more prevalent, attackers are expanding their focus to address industrial control system environments, such as the electric grid. Additionally, the deployment of smart grid technologies expand the grid becomes increasingly dependent on ICT for control and monitoring functions which introduces greater exposure to cyber attack.

The development of an attack resilient electric requires substantial research efforts, which explore methods to create a secure supporting infrastructure along with robust power applications. The developing of a secure cyber infrastructure will limit an attacker's ability to gain unauthorized access to critical grid resources. Infrastructure security enhancements require the expansion and tailoring of current cyber protection mechanisms such as authentication, encryption, access control, and intrusion detection systems. Unfortunately infrastructure level protection mechanisms may not prevent all cyber attacks. The development of more robust control applications will ensure the grid can still operate reliably during an attack by leveraging information about expected system states and operating conditions.

This paper introduced future research initiatives that should be addressed to ensure the grid maintains adequate attack resilience. The developments of strong *risk modeling* techniques are required to help quantify risks from both a cyber and physical perspective. Improved *risk mitigation* efforts are also required focusing on both the infrastructure and application perspectives. Particularly, *attack resilient control, monitoring, and protection algorithms* should be developed to utilize increased system knowledge to reduce the impact from a successful attack. Risk information must also be provided to operators and administrators through the development of *real-time visualization* mechanism, which can be integrated with current grid monitoring functions to assist in the development of appropriate attack responses.

References

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

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

[3] DoE Roadmap to Achieve Energy Delivery Systems cyber security. Energy Sector Control Systems Working Group September 2011.

[4] NASPInet, North American SynchroPhasor Initiative network. www.naspi.org

[5] GAO-11-117, Electricity Grid Modernization: Progress Being Made on cyber security Guidelines, but Key Challenges Remain to be Addressed . Government Accountability Office (GAO). January 2011.

[6] GAO-08-526: Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks, May 2008.

[7] NERC CIP standards, www.nerc.com

[8] NISTIR 7628: Guidelines for Smart Grid Cyber Security, National Institute for Standards and Technology, August 2010.

[9] "In the Crossfire: Critical Infrastructure in the Age of Cyber War", McAfee report, 2010.

[10] NIST 800-82 document.

[11] The Future of the Electric Grid. Massachusetts Institute of Technology (MIT). 2011. http://web.mit.edu/mitei/research/studies/the-electric-grid-2011.shtml

[12] High-Impact, Low-Frequency Event Risk (HILF) to the North American Bulk Power System, Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy, Nov. 2009.

[13] DHS, Control Systems Security Program.

[14] S. Sridhar, A. Hahn, M. Govindarasu, "Cyber Physical System Security for Electric Power Grid," Proceedings of the IEEE, Jan. 2012.

[15] C.-W. Ten, C.-C. Liu, and M. Govindarasu, "Vulnerability assessment of cyber security for SCADA systems," IEEE Trans. on Power Systems, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.

[16] Y. Huang, A. A. Cardenas, S. Sastry, "Understanding the Physical and Economic Consequences of Attacks on Control Systems", Elsevier, International Journal of Critical Infrastructure Protection, 2009.

[17] Ross Anderson, Shailendra Fuloria, Who controls the off switch? University of Cambridge, 2010.

[18] S. Sridhar and M. Govindarasu, "Data integrity attacks and their impacts on SCADA control system," in Proc. IEEE PES General Meeting, Jul. 2010.

[19] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in Proceedings of the 16th ACM Conference on Computer and communications security, 2009, pp. 21–32. [

[20] Giani, A.; Bitar, E.; Garcia, M.; McQueen, M.; Khargonekar, P.; Poolla, K; "Smart grid data integrity attacks: characterizations and countermeasures$^{\pi}$," IEEE International Conference on Smart Grid Communications (SmartGridComm), pp.232-237, 17-20 Oct. 2011

[21] T. Kim and H. Poor, "Strategic protection against data injection attacks on power grids," Smart Grid, IEEE Transactions on, vol. 2, no. 2, pp. 326 –333, June 2011.

[22] L.Xie, Y.Mo, and B.Sinopoli,"False data injection attacks in electricity markets," IEEE Intl. Conf. on Smart Grid Communications (SmartGridComm), Oct. 2010, pp. 226 –231.

[23] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. Begovic, and A. Phadke, "Wide-area monitoring, protection, and control of future electric power networks," Proceedings of the IEEE, vol. 99, pp. 80 –93, Jan. 2011.
[24] Western Electricity Coordinating Council, "WECC Remedial Action Scheme Guide."
[25] A. Hahn and M. Govindarasu, "Cyber Attack Exposure Evaluation for the Smart Grid," IEEE Trans. on Smart Grid, vol. 2, no. 4, pp. 835-843, Dec. 2011.
[26] Security Profile for Advanced Metering Infrastructure, v2.0, The Advanced Security Acceleration Project (ASAP-SG), June 2010.
[27] Smart grid communications & security, IEEE Power & Energy, Jan. 2012, Editors: M. Govindarasu and P. Sauer.