PSERC

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 Hahn
Iowa State University

Peter Sauer
University of Illinois at Urbana-Champaign

PSERC Publication 12-02

May 2012

For more information about this white paper, contact

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

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.org.

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
- Jianhu Wang, Argonne National Laboratory
- Siddharth Sridhar, Iowa State University
- Aditya Ashok, Iowa State University
- Chen-Ching Liu, Washington 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) security issues at information and communication infrastructure levels, (ii) cyber attack risk modeling and risk mitigation, (iii) application level security including attack-resilient monitoring, protection and control algorithms, (iv) defense against coordinated cyber attacks, (v) trust management and attack attributions, (vi) real-time situation awareness, and (vii) datasets and validations. 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 the development of innovative 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. These models should quantify the potential consequences of a cyber-attack on the power grid in terms of load loss, stability violations, equipment damage, and 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) possesses knowledge in 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.

5. ***Real-time situational awareness*** framework with an associated grid-wide security architecture for seamless sharing of information such as security alerts and remedies, and analytical tools to do online risk analysis (e.g., monitoring suspicious activities, intrusions, and their degree of severity) and provide visualization and control capabilities to the operators and administrators.

The cyber security posture needs to 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. Finally, the security models, metrics, architectures, algorithms, and protocols must take into the legacy nature of the grid infrastructure and the evolving nature of the threat.

Table of Contents

Table of Contents (continued)

List of Figures

List of Tables

1. Introduction and Issue Identification

Many smart grid initiatives will utilize recent innovations in information and communication technologies (ICT) to improve system monitoring, control, data analysis, and resource optimization. However, this increased dependency on ICT will also expand the grid's 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 shown 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. Information & Infrastructure Security Solutions
2. Application Level Security
3. Risk Modeling and Mitigation
4. Attack Resilient Control Algorithms
5. Coordinated Attack-Defense
6. Real-Time Situational Awareness
7. Trust Management and Attribution
8. 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. However, 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]. The North American SychroPhasor Initiative (NASPI) effort offers new opportunities for wide area monitoring and control [4]. NASPInet relies on Phasor Measurement Units (PMUs) as the key sensing technology, uses high-speed real-time communication infrastructure for data transport, and utilizes advanced computational algorithms and data analytics.

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 primary control center of a SCADA system and launches control actions that may cause catastrophic damages. These attacks can be at the very local level (e.g., substation) to modify protection settings, or on a global level to the extent of controlling the grid operation (e.g., control center). 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 identified current cyber security concerns and potential threats to the electric grid. Table 1 provides an overview of recent reports which either 1) address current trends, 2) dictate policy or requirements, 3) report current cyber weaknesses/inadequacies and/or 4) present future directions for the grid.

The U.S. General Accounting Office (GAO) has presented numerous reports [e.g., 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) developed two reports identifying key concerns and solutions in this domain. 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 released numerous documents focusing on vision and future directions for smart grid. Their "Roadmap to Achieve Energy Delivery System Cyber Security" document provides a comprehensive review of 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 compliance is mandated by the Federal Energy Regulatory Commission (FERC).

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]	Framework for innovation, goals, and milestones for all stakeholders involved with improving the security of the grid.
NISTIR 7628, "Guidelines for Smart Grid Cyber Security"[8]	Provides a comprehensive overview of cyber security concerns against various smart grid initiatives, including current research efforts, and 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 SCADA, distributed control systems (DCS), and programmable logic controllers (PLC).
GAO-11-117: Electricity Grid Modernization: Progress Being Made on Cyber Security Guidelines, but Key Challenges Remain to be Addressed [5]	Assessments of NIST security guidelines, FERC standards development, and key outstanding challenges including metrics, information sharing, insufficient security engineering, and regulatory issues.
The Future of the Electric Grid (MIT) [11]	Identifies key grid communications, security lifecycles, vulnerability sources, security regulatory issues, and information privacy concerns.
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 critical cyber assets supporting 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.

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

Common Cyber Security Vulnerabilities in Industrial Control Systems (DHS) [13]	Comprehensive report of ICS-CERT advisories and assessments of cyber vulnerabilities within a wide range of industrial control systems
A Policy Framework For the 21st Century Grid: Enabling Our Secure Energy Future [28]	An official Whitehouse strategy to address fundamental concerns to the security of the nation's electric grid, specifically requirements for security standards and the development of a security-aware culture.
Cross-Sector Roadmap for Cybersecurity of Control Systems [29]	A DHS funded roadmap of cyber security critical infrastructure/key resources (CIKR), including stakeholders, current challenges, and milestones.
NERC Cyber Attack Task Force (CAFT) Draft Report [48]	Results of an industry technical committee analyzing the possible attacks and responses, specifically focusing on coordinated cyber attacks against the bulk power system.

2.2 Cyber Security Requirements

The smart grid will introduce a number of new power system applications which will depend heavily on cyber architectures for communication and control functions. This section provides a brief overview of these applications and the security requirements necessary for their effective operations.

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) – ensuring the 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 interdomain 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. An overview of security requirements for key applications is identified in Table 2.

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, A
WAMPAC	I, A, AT, C	I, A
Power Markets	I, A, AT, C	I, N

2.2.1 Advanced Metering Infrastructure (AMI)

Consumer sites will be enhanced with the addition of "smart meters" which provide two-way communication between the customer and utilities. Smart meters provide users with more granular control over their consumption, enables real-time pricing, and supports the integration of distributed renewable energy sources. A MI will require a large communication network which will likely combine various media, including wireless, power line carrier (PLC), and traditional broadband. The large quantities of data transmitted by these meters must be stored and processed in some backend server owned either by a utility or some third party.

AMI presents its own unique security requirements [30]. Confidentiality is of greater concerns than other grid domains due to the large quantities of end user billing and privacy data. Integrity is necessary for both the meter's operation and control, along with the communication of both pricing and status information. A uthentication and non-repudiation of both utility and consumer activities are critical.

2.2.2 Distribution Management Systems (DMS)

Management and automation systems are becoming increasingly important to meet the demands of the energy distribution infrastructure. DMS typically incorporates a number of unique power applications including forecasting, state estimation, fault management, Volt/VAR control, and automatic feeder restoration. Additionally, DMS functions and AMI functions may share information on loads, consumption, and forecasts. Information provided to the DMS originates from a combination of related EMS/DMS systems, along with sensors and actuators deployed within the local distribution infrastructure.

DMS systems inherit their own set of security concerns due to their geographically disperse communication requirements [31]. Since DMS primarily performs control applications, it demands both high integrity and availability of all supporting control and communication resources. In addition to integrity and availability demands, all critical system functions and messages must be authenticated to ensure malicious individuals cannot send fraudulent data or commands.

2.2.3 Energy Management Systems (EMS)

Unlike DMS system, EMS focuses on the bulk power system generation and transmission domain. E MS systems have historically utilized real-time communications for control and monitoring, with applications such as Automatic Generation Control (AGC), State Estimation, and Flexible AC Transmission Systems (FACTS). Smart grid initiatives look to expand current EMS solutions through improved algorithms for operational applications.

EMS systems and networks maintain obvious requirements for strong integrity and availability. These attributes are especially important due to the criticality of the applications controlling the bulk power system. Additionally, strong authentication should be supported for all grid-related communications, especially remote field devices, such as IEDs and PLCs.

2.2.4 Wide Area Measurement, Protection, and Control (WAMPAC)

Phasor measurement units (PMUs) are the primary enabler of WAMPAC technologies. The ability to perform real-time grid state measurements will enable the development of increasingly effective protection schemes and control functions. However, WAMPAC systems will be extremely dependent on high speed networks, additionally, phasor data concentrators (PDC) and gateways that can both authenticate and authorize the sharing of PMU readings with various utilities and independent system operators.

The cyber security concerns and requirements for WAMPAC are well documented [32]. Authentication plays a critical role in WAMPAC environments. Proposed architectures such as NASPInet have identified the need for sophisticated access control mechanisms to limit the transmission of PMU measurements on onl y authorized parties [4]. Availability and integrity are again critical for the high speed communications. Finally, PMU measurements depend on GPS technology for timestamp data. This dependency inherits additional security concerns from potential jamming or spoofing attacks.

2.2.5 Power Markets

The future grid will be increasingly dependent on commodity-based energy markets to balance the supply and demand for energy. Markets can focus on day-ahead pricing based on estimated load and generation data. Additionally, consumers may be able to access a retail electric market where they'll have options to purchase from various retailers depending on current prices.

Power markets have obvious requirements for the confidentiality, integrity, and availability of the energy bid data. Non-repudiation also becomes a co ncern as various parties place bids for energy and therefore, must be held accountable for their actions. Finally, the large number of involved parties requires strong authentication of user activities.

2.3 Cyber Security Roadblocks

The design of a more secure smart grid environment is constrained by various physical, geographical, and, historical factors. This section will identify the key roadblocks that currently impede the development of a resilient grid. A number of these critical characteristics are enumerated below.

a) *Limited physical protections*. The lack of strong physical protections for all cyber resources means that attackers may be able to physically tamper the cyber-enabled devices or networks, especially those found within remote substations.

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) *Real-time system operation*. The grid's cyber-physical properties require that the information system communicate and process data in near real-time. This produces constraints with any security mechanisms that add latency, such as message encryption.

d) *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.

e) *Geographically disperse resources*. 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.

f) *Legacy system dependencies*. The grid is currently dependent on large amounts of legacy systems. Legacy systems were generally not developed to be attack resilient and do not implement necessary security controls such as authentication, and encryption.

g) *Privately owned infrastructures*. The U.S. electric grid is primarily owned and operated by private utilities. This presents challenges in the development of effective policy and standards for cyber security due to lack of an authoritative enforcement agency or organization.

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

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 attackers, their motivation, and available resources. 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 grid's 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 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. Therefore, an attacker's ability to impact the power application will be the primary factor in whether it impacts the physical system.

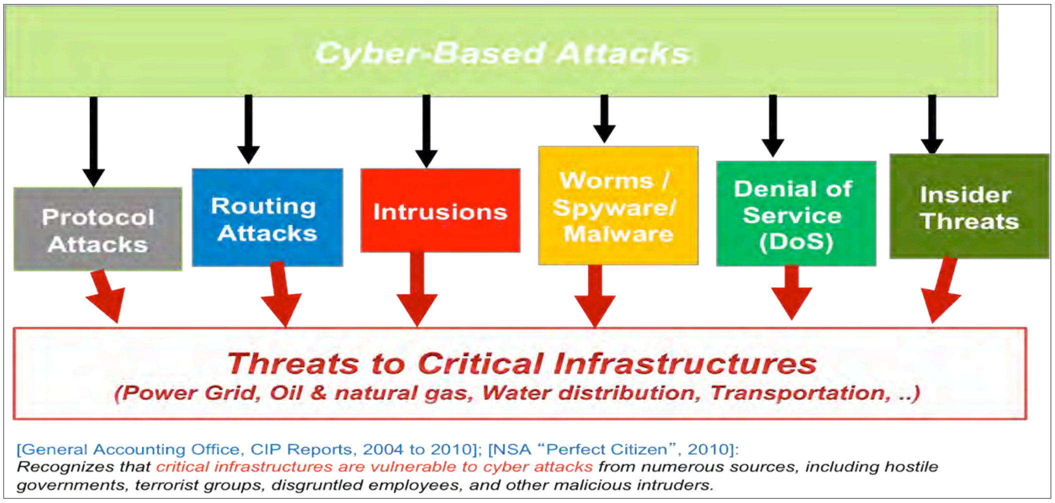
Developing a secure power system requires that both the applications and supporting infrastructure are designed to be attack resilient. Unfortunately, the grid's cyber-physical properties and tremendous scope place many constraints on t he ability to develop a secure cyber infrastructure. It must be assumed that even with significant infrastructure enhancements, an advanced and persistent attacker will still be able to successfully compromise some set of cyber assets. 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 decision 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 t he control functions or power applications supported by those systems. This section will provide a brief categorization of cyber attacks which could be used to compromise the security of the grid.

3.2.1 Cyber Attack Categorization

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



[General Accounting Office, CIP Reports, 2004 to 2010]; [NSA "Perfect Citizen", 2010]:
Recognizes that critical infrastructures are vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders.

Figure 1: Cyber Attacks against Critical Infrastructures

***Protocol attacks**:* The network protocols used in the power system, such as ICCP, IEC 61850, and DNP3; could be potentially exploited to launch cyber attacks if they are not secured properly. Since these protocols are used to control remote devices and substations, once an attacker is able to gain network access they could manipulate the communications to inject malicious system state and controls. Therefore, the grid requires secure versions of these protocols that not only provide security guarantees, but also meet 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 and other wide area networks. By manipulating the routing of packets, attackers could perform man-in-the-middle (MITM) attacks, spoofing, or delaying the delivery of the authentic traffic. A massive routing attack could have consequences on real-time operations of the grid and on real-time markets that rely on wide area communication.

***Intrusions**:* This refers to exploiting vulnerabilities in the software and communication infrastructure of the grid which then provides access to critical system elements. Network intrusions are specifically concerning due to recent reports identifying numerous weaknesses in software and networks used in the utility industry [13]. Example intrusion scenario is to gain access to substation HMI bypassing security controls (firewalls, system passwords).

***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 (DOS) attacks*:* A DOS is any attack that denies normal services to legitimate users. This could also mean denial of control or observability in the power grid's 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: The electric grid also faces risk from insider threats, such as those identified by the NERC HILF report [12]. A malicious insider with access to a control system network could easily abuse their trusted status to install malware or directly inject malicious commands into the network. Malicious insiders are especially dangerous because they also possess detailed knowledge about the system topologies and operations, and therefore could easily design an attack scenario that causes the system to operate outside safe operating points.

3.2.2 Attack Impacts to the Grid

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.

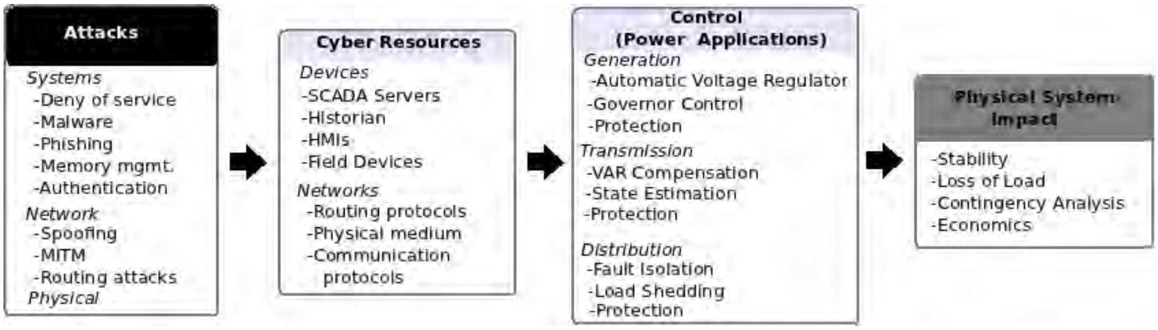


Figure 2: Mapping from Cyber Attacks to Control Actions to System Impacts

3.2.3 Coordinated Attacks

Since the current grid is designed with adequate resiliency to deal with 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 Weaknesses

As pointed in earlier sections, the cyber infrastructure used to support the grid's control and monitoring functions currently lacks appropriate security features. This section will introduce numerous areas with technical inadequacies, including cyber-enabled devices, communication networks, control software, and other automation functions.

3.3.1 Communication Security

Communication security becomes a k ey concern as the electric grid becomes more dependent on w ide-area communication. Secure communication is primarily enforced through a combination of message encryption and authentication. Often legacy systems and protocols were not developed to incorporate necessary authentication and encryption mechanisms to protect them from attacks. Tradition IT communication security mechanisms can be leveraged to secure these systems, however, these systems often increase communication latency to unacceptable levels, specifically for near real-time applications such as PMU-based real-time control or remedial action schemes (RAS).

Additionally, cryptanalysis techniques are continually improving, especially as computation continues to scale with Moore's law. T his creates concerns that the cryptographic mechanism currently deployed will not remain secure for a device's expected operating timeframe, which could be greater than 10 years. These issues provide significant difficulties in the development of secure communications approaches.

3.3.2 Software and Network Security

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.

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. These previously addressed concerns have been documented by numerous reports, including the results of recent INL vulnerability assessment efforts within various ISC environments as documented in Table 3 [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

In addition to traditional software platforms, the grid is threatened by its heavy dependencies on embedded devices to support the large number of field devices such as IEDs, PLCs, PMUs, and smart meters. However, large deployments of embedded devices introduce significant security concerns. First, embedded devices are often resource constrained, which presents limitations to performing various security functions, such as malware detection or various encryption protocols. Additionally, remote attestation of a devices operation is a difficult task. Therefore, utilities have no ability to inspect a device to ensure it has not been compromised and is not operating maliciously. Many of the devices deployed with the grid maintain limited physical protections, often hosted within substations guarded with simple locks, which leaves them vulnerable to physical manipulation.

3.3.3 Cyber Security Evaluation

There are increasing requirements for utilities to assess and validated their current cyber security posture, specifically to achieve compliance requirements for regulatory agencies (i.e., NERC CIP). However, current evaluation techniques are focused on IT systems and are insufficient for SCADA environments. Many assessment approaches depend on network and vulnerability scanning tools which may cause failures in legacy software platforms with poorly developed applications and network stacks. Additionally, the unique set of software applications and network protocols contain domain specific vulnerabilities which may not be addressed by many tools. Therefore, novel evaluation approaches are required to accurately identify critical vulnerabilities without negatively impacting system operation. The development of improved testing strategies and assessment methodologies must be tailored towards the grids' critical cyber assets, common vulnerabilities, and system availability requirements.

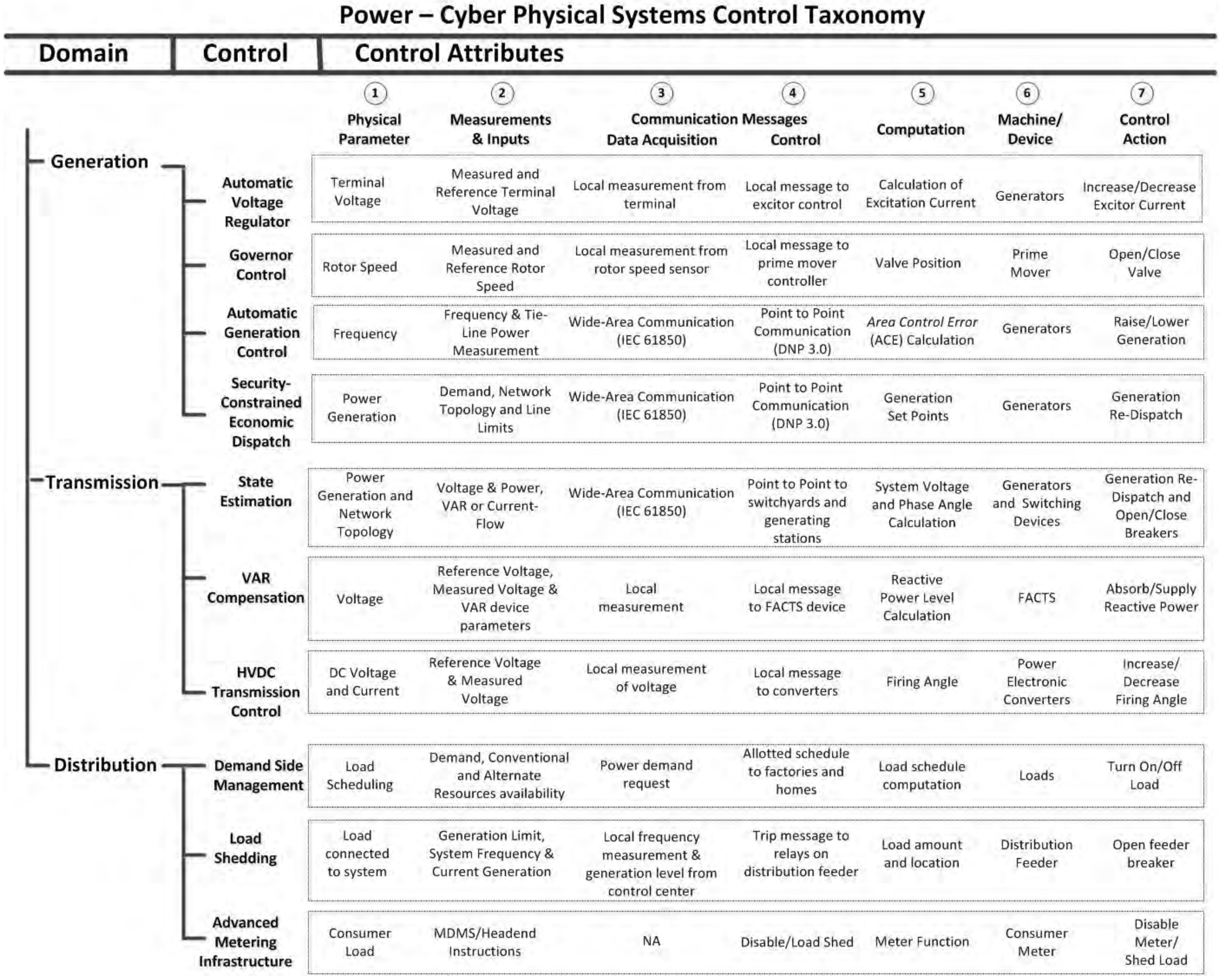
3.3.4 Intrusion Detection and Tolerance

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. However, attacks against control systems will likely differ greatly from their IT counterparts. Therefore, domain-specific intrusion detection techniques should be developed to efficiently detect attacks within the smart grid.

To complement improved detection capabilities, control system architectures should be redesigned to provide improved attack tolerance. Current control architectures focus only on the development of a secure network perimeter, which leaves the network vulnerable after a single successful attack. Intrusion tolerant cyber architectures should be designed to operate reliably even during successful cyber attacks. Tolerant cyber architectures should incorporate increased diversity and redundancy of cyber elements to limit feasible attack impacts.

3.4 Power Application Security Concerns

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	① Physical Parameter	② Measurements & Inputs	③ Communication Messages Data Acquisition	④ 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 is 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. These concerns have been supported by NERC. In particular, [48] states that in order to cause a large scale blackout attackers must negatively impact operator situational awareness along with the instigating instabilities on the bulk power system [48].

3.6 Supply Chain Security

As networks and systems rely more and more on commercial off-the-shelf components to provide customer choice and operator flexibility, the need to ensure the integrity and resilience of communication and control equipment has increased. Supply chain security has emerged as an important concern which can create the need for extensive testing and validation of performance [33]. A recent workshop on “Securing the Smart Grid: Best Practices in Supply Chain Security, Integrity and Resilience” has identified several key concepts that can contribute to cyber vulnerabilities.

http://www.usresilienceproject.org/workshop/participants/index.html

The workshop indicated that “The solutions needed to prevent or detect corrupt, compromised or counterfeit components are rooted in more traditional approaches to supply chain risk management.” This workshop included case studies which provided best practices and examples of “end-to-end” operational excellence. It provided macro trends from the “World Economic Forum” which included globalization (outsourcing, offshoring), specialization (geographical concentration of production), complexity (product/network complexity), lean processes (single sourcing, buffer stock reduction), information availability (track and trace), and government legislation (cargo screening). An IBM source was quoted as indicating supply chains of the future will be” Instrumented”,” Interconnected”, and “Intelligent”. The challenges of secure supply chain design and implementation include cyber issues with all sub-components as well as integrated performance.

3.7 Cyber Security Standards and Policy

The cyber security issues within the grid cannot be addressed through purely technical approaches. The adoption of cyber security specific standards and policies is necessary to ensure both utilities and regulatory agencies actively address these issues.

3.7.1 Standards

Currently, efforts like NERC CIP have focused on enforcing that utilities operating the bulk power system provide adequate security of their critical cyber assets. While this is a critical step towards developing secure grid, additional standards are necessary to ensure that the grid maintains appropriate attack tolerance in the face of evolving cyber threats.

Future standards are also required to ensure adequate security of smart grid initiatives, specifically supporting AMI. While attacks against distribution and AMI systems may not damage the bulk power systems, they still cause serious damage through local power disruption. It is unclear whether utilities will have to demonstrate that these systems implement some minimum security baseline. Additionally, the granular meter readings gathered by smart meters create customer privacy concerns. These concerns could possibly be alleviated by standardized data collection and usage methods.

Another shortcoming of current security standards is their focus on s ystem implementation rather than development. Vulnerability researchers have recently begun to focus their efforts on control system software and have discovered large numbers of critical vulnerabilities. While utilities bear the burden of ensuring their systems security, there is little they can do to improve inherently insecure software platforms and field devices.

Security standards in the software engineering and product acquisitions process could help ensure that utilities procure systems with adequate security capabilities. Software quality standards, such as Common Criteria have been leveraged in other industries to provide a framework to evaluate the security of software [34]. An adoption of similar requirements for the electric grid would ensure that vendors provide utilities with appropriately secure systems.

3.7.2 Public-Private Partnerships

A key component on the nation's cyber security policy is the development of public-private partnerships, specifically for critical infrastructures such as the power grid. Since the grid is primarily owned and operated by private industry, the federal government maintains little control over its daily operation. The relationships between the privately owned utilities and federal government must be enhanced to assure they appropriately share critical data, especially information about current cyber threats. This requirement has been addressed by recent government reports [35].

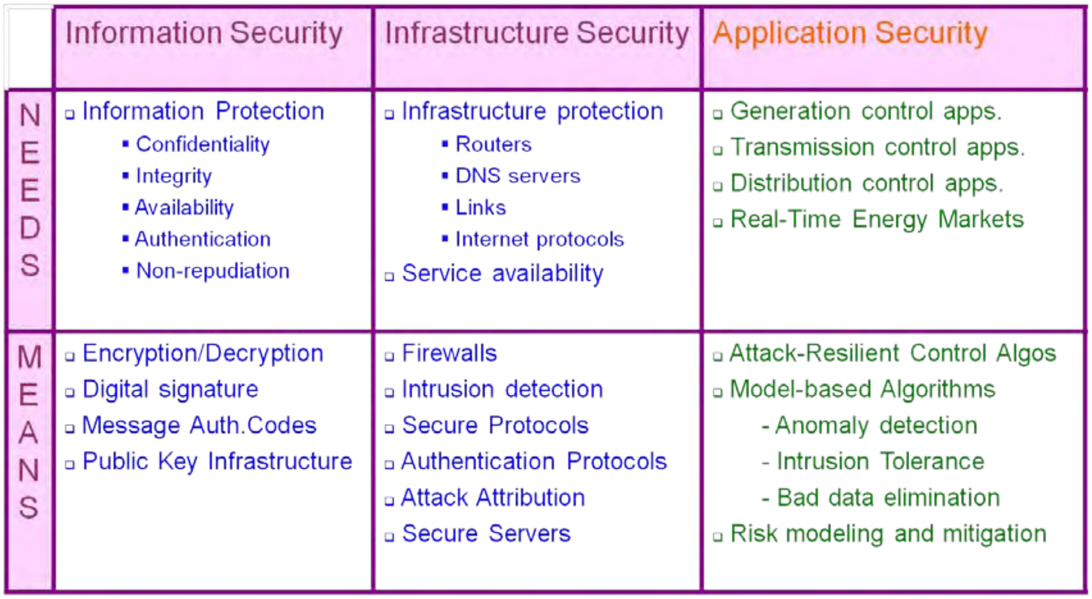
While the federal government maintains a wealth of information on advanced threats and attacker techniques, this information is often classified and withheld from public release. However, without this information utilities cannot verify that their security efforts adequately address currently faced threats. Therefore, new approaches to threat information sharing are required to ensure that both security approaches are adequately scoped.

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 these critical research areas.

4.1 Information & Infrastructure Security Solutions

This section identifies both information and infrastructure security together as they are both provided by the supporting ICT infrastructure. In particular, issues such as communication security, security evaluation, intrusion detection, and event management are discussed.

4.1.1 Communication Security

New encryption protocol and authentications schemes must be developed to address the high availability and low latency requirements of the smart grid. Recent research efforts have explored new cryptographic schemes. One method that has been explored is to refactor current network protocols to include both authentication and encryption. Numerous papers have been published recommending secure modifications to these protocols [36-38].

Often older proprietary systems and protocols cannot be easily redeveloped and deployed. However, the development of bump-in-the-wire (BITW) encryption techniques can be used to retrofit encryption techniques to legacy systems. The work reported in [39] has shown that BITW solutions tailored to minimize additional latency.

The smart grid will also require tailoring of authentication mechanisms to deal with high availability and long lifespans. In [40], design principles for authentication protocols used in electric grid are identified. In [41], authentication methods to support long deployments through re-keying and remodeling algorithms are reported.

4.1.2 Cyber Security Evaluation

Increased concerns for cyber security will result in requirements to perform official audits of utility cyber assets to verify that they adequately implement protection mechanisms. Novel evaluation approaches must be developed to appropriately meet these demands. National laboratories, such as Sandia and INL, have substantial background in the testing and assessment of control system environments. These facilities have released numerous official reports documenting methodologies for performing penetration tests and vulnerability assessments within such environments [42-43]. In addition, they have released various documents addressing the results of their findings, including categorization and frequencies of vulnerabilities [1].

4.1.3 Intrusion Detection

Intrusion detection techniques within the electric grid have gained significant attention from security researchers in recent years. By tailoring detection techniques to focus on unique properties and predictable operations of control systems, researchers have designed effective intrusion detection approaches. [44] has focused on identifying malicious events within control system environments by focusing on known, static network communication patterns. Additionally, [45] has demonstrated how specification-based intrusion detection methods can be leveraged within AMI deployments to detect malicious communication patterns.

4.1.4 Security Event Management

One of the critical research areas within control system environments is cyber forensics. Cyber-physical attacks will likely focus on sensors and actuators, as demonstrated as by the Stuxnet incident. [46] has suggested the deployment of agents which can collect and forensically analyze data.

As networks begin to collect increasing amounts of intrusion and forensic data, increasing intelligent systems will be required to assist administrators interpret and understand the scope of incidents. [47] has developed methods to collect various sources of security data and analyze it to facilitate improved attack detection.

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 functions.

4.2.1 Attack-Resilient 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.

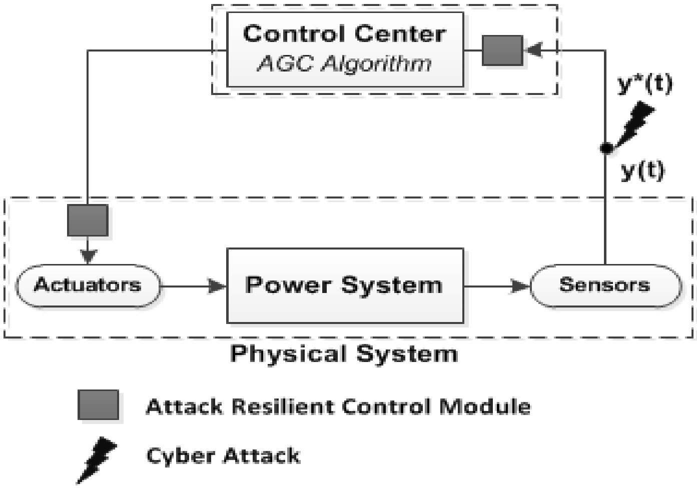


Figure 5: Schematic of Cyber Attacks on Control System

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 approach focuses on extracting and analyzing 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.

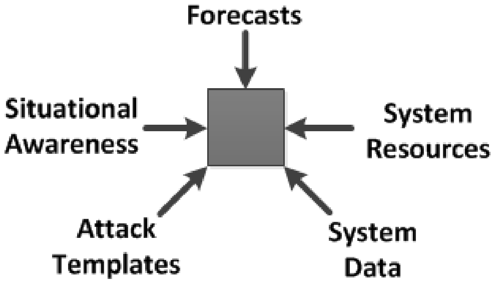


Figure 6: Sources of Data for Attack-Resilient Control Algorithms

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.

4.2.2 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 t he 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.

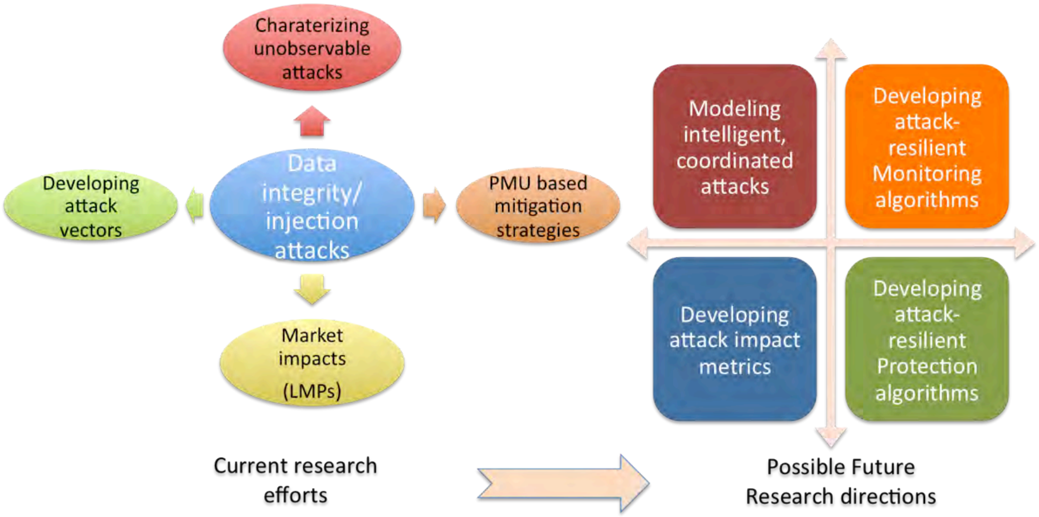

Charatering unobservable attacks
Developing attack vectors
Data integrity/ injection attacks
PMU based mitigation strategies
Market impacts (LMPs)
Modeling intelligent, coordinated attacks
Developing attack-resilient Monitoring algorithms
Developing attack impact metrics
Developing attack-resilient Protection algorithms
Current research efforts
Possible Future Research directions

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 hi ghlights potential research directions in attack-resilient wide area monitoring and protection.

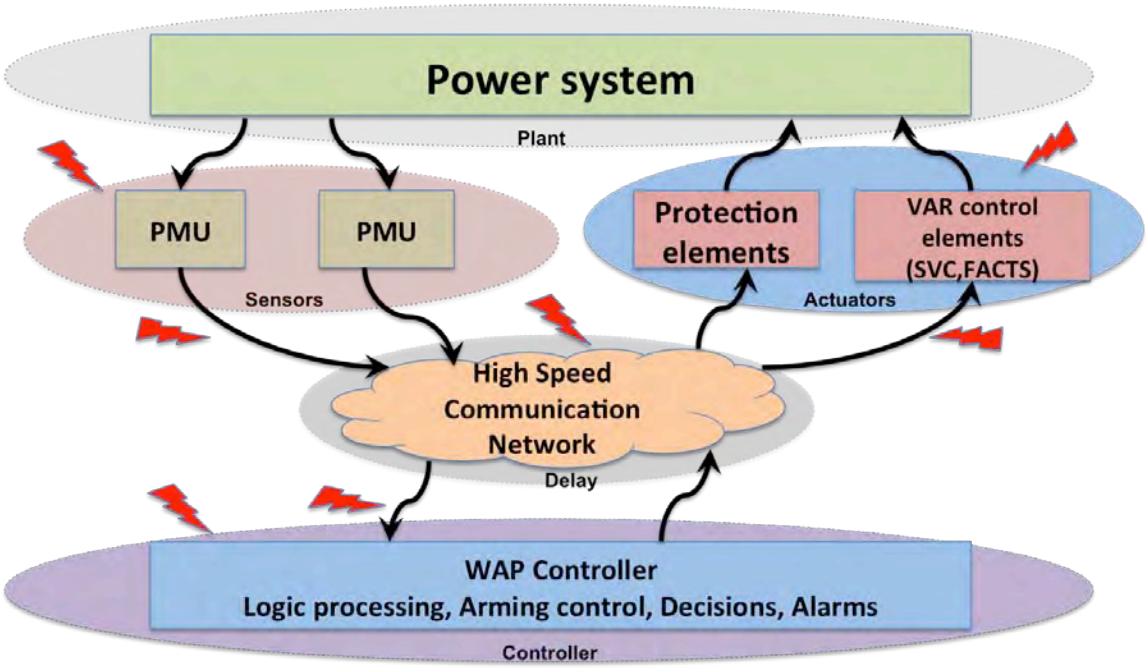

Power system
Plant
PMU
PMU
Sensors
Protection elements
VAR control elements (SVC,FACTS)
Actuators
High Speed Communication Network
Delay
WAP Controller
Logic processing, Arming control, Decisions, Alarms
Controller

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 t he 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 c yber 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 classifying the different cyber-attack templates on some of the SPS architectures. Based on a v ery 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 t he 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 with 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. The key steps in the risk modeling and mitigation process are identified below.

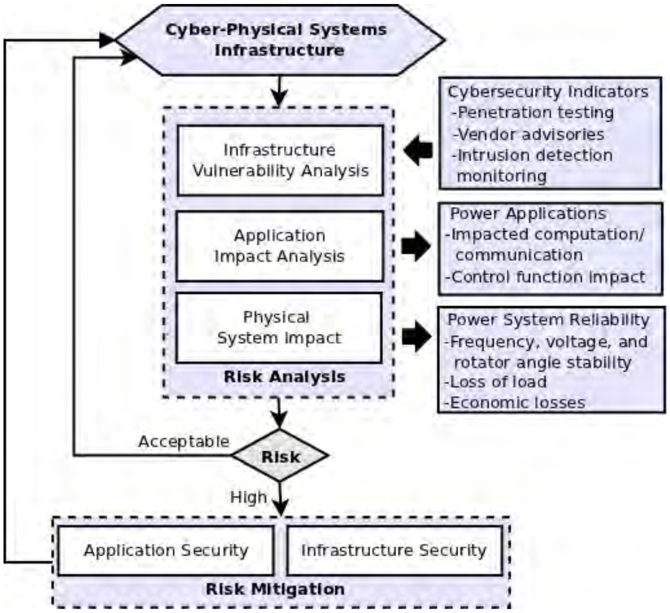


Figure 9: Risk Modeling and Mitigation Framework [14]

1. ***Cyber vulnerability assessment**:* Many 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, such as those identified in section 4.1, 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. Section 4.2 introduced mitigations approaches through the engineering of more attack resilient system control and monitoring functions.

4.4 Coordinated Attack-Defense

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 [12]. 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.

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 HILF report 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", as cyber attacks can be easily coordinated to target multiple systems. 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.

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.

4.5 Real-Time Situational Awareness

One of the key building blocks of secure grid infrastructure is its ability to collect data about security alerts, perform data analytics at different levels of the grid hierarchy, and disseminate remedial actions to mitigate potential attack scenarios. The design and deployment of such a real-time situation awareness infrastructure requires the following.

Data Schema for Cyber-Physical Power System: Development of standardized data model for cyber layer of the power grid to complement the existing CIM-based physical models, and defining the relationship between the cyber and physical layer models. The cyber layer needs to incorporate communication topology, protocols, security technologies, and software platforms (e.g., operating system and EMS) with their configurations.

Data Sharing Architecture: Development of hierarchical information architecture for data sharing to facilitate seamless exchange of data between utilities, regional, and national organizations. This includes identification of the relevant hierarchical as well as peer-to-peer information flows: (i) upstream information flow (e.g., utilities to regional/national level), such as data schemes, real-time cyber and physical events at different granularities, and their abilities to detect and mitigate the events; (ii) downstream information flow such as notification of threat alerts, incident data including related observables, and possible mitigations. Defining and managing trust relationship among the entities needs to be a key attribute of the architectures.

Data Analytics: Development of visual analytics framework with scalable algorithms to complement the existing EMS capability to incorporate threat analysis, vulnerability analysis, and system impact analysis (in terms of adequacy, stability, and market impacts), system planning studies, and mitigation algorithms. The algorithms need to rely on real-time cyber-physical events coupled with known system schemas and historical system operation data. Modeling emergent behavior, using machine-learning tools and game-theoretic approaches, will be core of the analytical engine to discover unknown cyber events from known threat, vulnerability data, and real-time alerts.

4.6 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. This section identifies critical research initiatives in the management of trust relationships between the various entities involved of the smart grid.

1. ***Dynamic Trust Management Lifecycle***: The dynamic environment of the smart grid requires a trust model that 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***: The numerous information flows and interdomain communications within the smart grid will warrant variable levels of trust between the entities. Research should investigate quantified notions of trust to specifically represent the authenticity and validity of data sources.

3. ***Insider Threat Management**:* While most cyber protections focus on limiting 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 any of 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.

4.7 Data Sets and Validation

Performing research within this domain is often constrained by the lack of accurate data about current system deployments. Without accurate data, researchers may make inaccurate assumptions which then leads to incorrect results. Therefore, the development of accurate datasets is necessary to ensure research efforts can be transitioned to operational 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 many applications including the development of intrusion detection systems and intrusion tolerant architectures.

3. ***Realistic Testbeds**:* Cyber-physical testbeds provide realistic environments for evaluating the performance properties of the cyber system, performance and stability properties of the physical system, and more importantly the interaction between the cyber and physical systems. They allow researchers to explore the likelihood of cyber attacks, their impacts, and the effectiveness of defense measures within an accurate and safe environment. They can also be used to evaluate the efficacy of attack-resilient control algorithms and robust cyber infrastructures.

5 Conclusions

The development of an attack resilient smart 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 situational awareness infrastructure*, which can be integrated with current grid monitoring functions to assist in dissemination of cyber alerts and remedies, and the development of appropriate attack responses. Table 4 summarizes the document by identifying the key issues, current state of knowledge or practice, and paths to resolve those issues.

Table 4: Summary of key issues and paths to resolution

	Key Issues	Current State	Path to Resolve Issues
1	Risk Modeling	Qualitative & quantitative models exist. Lack of realistic metrics, data sets, and validation studies	Realistic cyber-physical models, metrics, data sets, and validation studies. Metrics need to consider efficiency, reliability, stability, and market performance
2	Risk Mitigation (Information & Infrastructure Security concerns)	NERC CIP compliance, secure protocols, secure perimeter, and secure devices. Lack of grid-wide deployment of strong security features	Need to go beyond the current effort. In particular, Real-time risk modeling and mitigation, Cyber-physical system models and computation tools, and application level security
3	Cyber Situational Awareness	Current information sharing of cyber alerts and potential remedies are ad-hoc. No enforceable policy, architecture, and protocol exist for real-time information sharing across the grid	Define data formats and schemas, develop data sharing architectures and protocols; develop real-time visualization methods and tools; define and enforce policy for data sharing
4	Advanced Persistent Threats & Application-layer Security	Fault-Resilient Design of current grid, e.g., (N-1) contingency criteria	Attack-Resilient Design for the Future Grids; Attack-resilient monitoring, protection, and control algorithms
5	Defense against Coordinated Attacks	NERC HILF Task Force	Risk modeling coordinated attacks; System planning for (N-k) contingency criteria
6	Data sets and validations	Power system data sets exist. However, there is lack of realistic data sets on the cyber topologies and cyber-physical couplings of the power grid; lack of cyber attack traces	Realistic metrics, realistic data sets (topologies, traces); realistic CPS testbeds and attack-defense studies; evolving metrics, data sets, and studies
7	Trust management	Load and other system data sharing exist at various levels. However, there is no notion of dynamic trust and formalized trust management cycle exist	Trust representation, dynamic trust, and enforceable trust management lifecycle

References

1. National SCADA TestBed (NSTB) Assessments Summary Report: *Common Industrial Control System Cyber Security Weaknesses*, Idaho National Laboratory (INL), May 2010.
2. Falliere, N.; 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. Available at: 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. U.S. Government Accountability Office. GAO-08-526: Information Security: *TVA Needs to Address Weaknesses in Control Systems and Networks*, May 2008.
7. North American Electric Reliability Corporation (NERC), *Critical Infrastructure Protection(CIP) Standards*, Available at: 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. National Institute of Standards and Technology (NIST) SP 800-82. *Guide to Industrial Control System (ICS) System Security*. June 2011.
11. *The Future of the Electric Grid.* Massachusetts Institute of Technology (MIT). 2011. Available at: 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, November. 2009.
13. DHS, Control Systems Security Program.
14. Sridhar, S.; A. Hahn, M. Govindarasu. *Cyber Physical System Security for Electric Power Grid*, Proceedings of the IEEE, January 2012.
15. Ten, C.-W.; C.-C. Liu, and M. Govindarasu. *Vulnerability Assessment of Cyber Security for SCADA Systems*, IEEE Trans. on Power Systems, vol. 23, no. 4, pgs. 1836-1846, November. 2008.
16. Huang, Y.; 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. Anderson, Ross; Shailendra Fuloria. *Who Controls the Off Switch?* University of Cambridge, 2010.

18. Sridhar, S; M. Govindarasu. *Data Integrity Attacks and Their Impacts on SCADA Control System*, in Proc. IEEE PES General Meeting, July 2010.

19. Liu,Y; P. Ning, 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, pgs. 21-32, 2009.

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), pgs. .232-237, October 2011.

21. Kim, T; H. Poor. *Strategic Protection Against Data Injection Attacks on Power Grids*, Smart Grid, IEEE Transactions on, vol. 2, no. 2, pgs. 326 –333, June 2011.

22. Xie,L; Y.Mo, B.Sinopoli,*False Data Injection Attacks in Electricity Markets*, IEEE Intl. Conference on Smart Grid Communications (SmartGridComm), pgs. 226 – 231, October 2010.

23. Terzija, V.; 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, pgs. 80 –93, January 2011.

24. Western Electricity Coordinating Council, *WECC Remedial Action Scheme Guide*.

25. Hahn, A.; M. Govindarasu, *Cyber Attack Exposure Evaluation for the Smart Grid*, IEEE Transmission on Smart Grid, vol. 2, no. 4, pgs. 835-843, December 2011.

26. Security Profile for Advanced Metering Infrastructure, v2.0, The Advanced Security Acceleration Project (ASAP-SG), June 2010.

27. Govindarasu, M.; P. Sauer. *Smart Grid Communications & Security*, IEEE Power & Energy, Jan. 2012.

28. *A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future*. The Whitehouse. June 2011.

29. *Cross-Sector Roadmap for Cybersecurity of Control Systems*. Industrial Control Systems Joint Working Group (ICSJWG) Roadmap Working Group. September 30, 2011.

30. *Security Profile for Advanced Metering Infrastructure Version* 2.0. The Advanced Security Acceleration Project (ASAP-SG). June 22, 2010.

31. *Security Profile for Distribution Management*. Version 1.0. The Advanced Security Acceleration Project (ASAP-SG). February 20, 2012.

32. *Security Profile for Wide-Area Monitoring, Protection, and Control*. Version 0.8. The Advanced Security Acceleration Project (ASAP-SG). May 16, 2011.

33. U.S. Department of Energy and George Mason University, *Smart Grid Supply Chain Security , Integrity and Resilience Workshop*, March 16, 2012.

34. "Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model." July 2009. Version 3.1, Revision 3. http://www.commoncriteriaportal.org.

35. U.S. Government Accountability Office. GAO 10-628 Critical Infrastructure Protection: *Key Private and Public Cyber Expectations Need to Be Consistentl Addressed*. July, 2010.

36. Majdalawieh,M; F. Parisi-Presicce, D. Wijesekera, *DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework*, in Advances in Computer, Information, and Systems Sciences, and Engineering., K. Elleithy, T. Sobh, A. Mahmood, M. Iskander, and M. Karim, Eds. Amsterdam, The Netherlands: Springer-Verlag, pgs. 227–234, 2006.

37. Fovino, I; A. Carcano, M. Masera, A. Trombetta. *Design and Implementation of a Secure Modbus Protocol*, in Critical Infrastructure Protection III, vol. 311,C. Palmer and S. Shenoi, Eds. Boston, MA: Springer-Verlag, pgs. 83–96, 2009.

38. Michalski, J.T.; A. Lanzone, J. Trent, S. Smith. *SAND2007-3345: Secure ICCP Integration Considerations and Recommendations*, Sandia National Laboratories, June 2007.

39. Tsang, P.; S. Smith, *YASIR: A low-latency, high-integrity security retrofit for legacy SCADA systems*, in Proceedings of the IFIP TC-11 23rd International Information Security Conference, vol. 278, S. Jajodia, P. Samarati, and S. Cimato, Eds. Boston, MA: Springer-Verlag, pgs. 445–459, 2008.

40. Khurana, H.; R. Bobba, T. Yardley, P. Agarwal, E. Heine. *Design Principles for Power Grid Cyber Infrastructure Authentication Protocols*, in Proc. 43rd Hawaii Int. Conf. Syst. Sci., Washington, DC, 2010, DOI: 10.1109/HICSS.2010.136.

41. Chakravarthy, R.; C. Hauser, D. E. Bakken. *Long-lived Authentication Protocols for Process Control Systems*, International Journal of Critical Infrastructure Protection, vol. 3, no. 3–4, pgs. 174–181, 2010.

42. Parks, R.C. *SAND2007-7328: Guide to Critical Infrastructure Protection Cyber Vulnerability Assessment*, Sandia National Laboratories, November 2007.

43. Permann, M.R.; K. Rohde. *Cyber Assessment Methods for SCADA Security*, The Instrumentation, Systems and Automation Society (ISA), Technology Report, 2005.

44. Cheung, S.; B. Dutertre, M. Fong, U. Lindqvist, S. K., A. Valdes, *Using Model-Based Intrusion Detection for SCADA Networks*, in Proceedings of the SCADA Security Science Symposium, January 2007.

45. Berthier, R.; W. Sanders. *Specification-Based Intrusion Detection for Advanced Metering Infrastructures*, pgs. 184-193, PRDC 2011.

46. Chandia, R.; J. Gonzalez, T. Kilpatrick, M. Papa, S. Shenoi, *Security Strategies for SCADA Networks*, in Critical Infrastructure Protection, vol. 253, E. Goetz and S. Shenoi, Eds. Boston, MA: Springer-Verlag, pgs. 117–131, 2007.

47. Briesemeister, L.; S. Cheung, U. Lindqvist, A. Valdes, *Detection, Correlation, Visualization of Attacks Against Critical Infrastructure Systems,* in Proceedings of the 8th Annual International Conference on Privacy Security, and Trust, pgs. 15–22, August 2010.

48. North American Electric Reliability Corporation (NERC). Cyber Attack Task Force (CAFT) Draft Report, March 2012.