Cyber security of the smart grid: Attack exposure analysis, detection algorithms, and testbed evaluation

Adam Hahn
Iowa State University

Follow this and additional works at: http://lib.dr.iastate.edu/etd
Part of the Computer Engineering Commons, and the Library and Information Science Commons

Recommended Citation
Hahn, Adam, "Cyber security of the smart grid: Attack exposure analysis, detection algorithms, and testbed evaluation" (2013).
Graduate Theses and Dissertations. 13098.
http://lib.dr.iastate.edu/etd/13098

This Dissertation is brought to you for free and open access by the Graduate College at Iowa State University Digital Repository. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.
Cyber security of the smart grid: Attack exposure analysis, detection algorithms, and testbed evaluation

by

Adam Lee Hahn

A dissertation submitted to the graduate faculty
in partial fulfillment of the requirements for the degree of
DOCTOR OF PHILOSOPHY

Major: Computer Engineering

Program of Study Committee:
Manimaran Govindarasu, Major Professor
Venkataramana Ajjarapu
Thomas Daniels
Doug Jacobson
Johnny Wong

Iowa State University
Ames, Iowa
2013
Copyright © Adam Lee Hahn, 2013. All rights reserved.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST OF TABLES</td>
<td>vi</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>vii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>ix</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>x</td>
</tr>
<tr>
<td>CHAPTER 1. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 The smart grid</td>
<td>2</td>
</tr>
<tr>
<td>1.2 Growing threats within cyberspace</td>
<td>4</td>
</tr>
<tr>
<td>1.3 Vulnerabilities within the smart grid</td>
<td>6</td>
</tr>
<tr>
<td>1.4 Research needs</td>
<td>10</td>
</tr>
<tr>
<td>1.5 Thesis contributions</td>
<td>11</td>
</tr>
<tr>
<td>CHAPTER 2. SMART GRID BACKGROUND AND LITERATURE SURVEY</td>
<td>13</td>
</tr>
<tr>
<td>2.1 Traditional electric grid overview</td>
<td>13</td>
</tr>
<tr>
<td>2.1.1 Generation</td>
<td>15</td>
</tr>
<tr>
<td>2.1.2 Transmission</td>
<td>15</td>
</tr>
<tr>
<td>2.1.3 Distribution</td>
<td>16</td>
</tr>
<tr>
<td>2.1.4 Markets and system operators</td>
<td>16</td>
</tr>
<tr>
<td>2.1.5 SCADA architectures</td>
<td>16</td>
</tr>
<tr>
<td>2.2 Smart grid technologies and communications</td>
<td>20</td>
</tr>
<tr>
<td>2.2.1 AMI</td>
<td>22</td>
</tr>
</tbody>
</table>
2.2.2 Substation automation systems ................................. 25
2.2.3 WAMS ................................................................. 31
2.2.4 CIM ................................................................. 32
2.3 Cyber threats to the smart grid ........................................ 33
  2.3.1 Communications .................................................. 34
  2.3.2 Systems and devices .............................................. 36

CHAPTER 3. CYBER ATTACK EXPOSURE EVALUATION FRAMEWORK ........................................ 38
3.1 Introduction .............................................................. 38
3.2 Related work .............................................................. 39
  3.2.1 Attack surface analysis ............................................ 39
  3.2.2 Attack trees ....................................................... 40
  3.2.3 Privilege/attack graphs .......................................... 40
3.3 Exposure evaluation framework ........................................ 41
  3.3.1 Identifying cyber risk .............................................. 42
  3.3.2 Exposure graph development ..................................... 47
  3.3.3 Exposure evaluation .............................................. 48
3.4 Exposure metric applications ........................................ 49
  3.4.1 Vulnerability analysis ............................................. 50
  3.4.2 Cyber security investment optimization ........................ 51
  3.4.3 Cyber contingency analysis ..................................... 51
3.5 Metrics evaluation ...................................................... 53
  3.5.1 Simulated environment ............................................ 53
  3.5.2 Simulation Results ............................................... 55

CHAPTER 4. MODEL-BASED HIERARCHICAL INTRUSION DETECTION FOR THE SMART GRID (MHINDS) ........................................ 59
4.1 Introduction .............................................................. 59
4.2 Related work ................................................................. 60
  4.2.1 Misuse-based IDS .................................................. 61
  4.2.2 Anomaly-based IDS .............................................. 62
  4.2.3 Specification-based IDS ....................................... 62
  4.2.4 Model-based IDS ................................................ 63
4.3 Threats to substation automation functions ..................... 63
  4.3.1 Protection schemes ............................................. 64
  4.3.2 Threat model .................................................... 66
4.4 MHINDS detection methodology .................................... 66
  4.4.1 Substation level detection .................................... 67
  4.4.2 System level detection ........................................ 74
  4.4.3 Security analysis and evaluation ............................ 77

CHAPTER 5. CPS SECURITY TESTBED FOR THE SMART GRID 84
  5.1 Introduction .......................................................... 84
  5.2 Related work ........................................................ 85
  5.3 Testbed research applications and design ....................... 87
    5.3.1 Research applications ....................................... 88
    5.3.2 Testbed design elements .................................... 92
  5.4 ISU’s PowerCyber testbed architecture .......................... 95
    5.4.1 Control .......................................................... 95
    5.4.2 Communication ................................................ 96
    5.4.3 Physical system .............................................. 98
  5.5 Testbed evaluation and experimentation ........................ 99
    5.5.1 Vulnerability assessment .................................... 99
    5.5.2 Cyber-physical impacts ...................................... 99

CHAPTER 6. CONCLUSION AND FUTURE WORK ......................... 110
  6.1 Future work .......................................................... 112
APPENDIX

PUBLISHED WORK ........................................ 114

BIBLIOGRAPHY ............................................. 116
## LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1.1</td>
<td>Roadmaps and security guidelines for cyber security concerns</td>
<td>9</td>
</tr>
<tr>
<td>Table 2.1</td>
<td>Smart grid communications (I: Integrity, A: Availability, C: Confidentiality)</td>
<td>21</td>
</tr>
<tr>
<td>Table 2.2</td>
<td>Sample of IEC 61850 LN names and definitions</td>
<td>26</td>
</tr>
<tr>
<td>Table 3.1</td>
<td>Example security mechanisms and privileges</td>
<td>45</td>
</tr>
<tr>
<td>Table 3.2</td>
<td>Example security mechanism for an AMI architecture</td>
<td>52</td>
</tr>
<tr>
<td>Table 3.3</td>
<td>Example set of information objects</td>
<td>54</td>
</tr>
<tr>
<td>Table 4.1</td>
<td>MHINDS Petri net places</td>
<td>69</td>
</tr>
<tr>
<td>Table 4.2</td>
<td>Detectability of IED malicious control operations</td>
<td>73</td>
</tr>
<tr>
<td>Table 4.3</td>
<td>Line and bus protection systems and relays</td>
<td>76</td>
</tr>
<tr>
<td>Table 5.1</td>
<td>Research efforts to testbed capability mapping</td>
<td>89</td>
</tr>
<tr>
<td>Table 5.2</td>
<td>Evaluated cyber attacks</td>
<td>100</td>
</tr>
<tr>
<td>Table 5.3</td>
<td>Mapping of PowerCyber testbed components to RAS</td>
<td>104</td>
</tr>
</tbody>
</table>
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.1</td>
<td>Power system domains[34]</td>
<td>6</td>
</tr>
<tr>
<td>Figure 2.1</td>
<td>Schematic of the smart grid cyber infrastructure</td>
<td>14</td>
</tr>
<tr>
<td>Figure 2.2</td>
<td>Commodity vs. SCADA-specific ICT</td>
<td>19</td>
</tr>
<tr>
<td>Figure 2.3</td>
<td>61850 control operation</td>
<td>28</td>
</tr>
<tr>
<td>Figure 2.4</td>
<td>61850 protection operation</td>
<td>29</td>
</tr>
<tr>
<td>Figure 2.5</td>
<td>61850 breaker failure operation</td>
<td>30</td>
</tr>
<tr>
<td>Figure 2.6</td>
<td>Attacks to the smart grid</td>
<td>34</td>
</tr>
<tr>
<td>Figure 3.1</td>
<td>Attack exposure evaluation framework</td>
<td>42</td>
</tr>
<tr>
<td>Figure 3.2</td>
<td>a) Testbed network architecture, b) Testbed data flow diagram</td>
<td>43</td>
</tr>
<tr>
<td>Figure 3.3</td>
<td>a) Testbed DFD with security mechanisms, b) Resulting exposure graph</td>
<td>46</td>
</tr>
<tr>
<td>Figure 3.4</td>
<td>Exposure metric applications</td>
<td>50</td>
</tr>
<tr>
<td>Figure 3.5</td>
<td>Simulation AMI use cases</td>
<td>53</td>
</tr>
<tr>
<td>Figure 3.6</td>
<td>Exposure metrics for normal/vulnerable scenarios</td>
<td>55</td>
</tr>
<tr>
<td>Figure 3.7</td>
<td>Exposure after security enhancements</td>
<td>57</td>
</tr>
<tr>
<td>Figure 4.1</td>
<td>Traditional IT and smart grid IDS approaches</td>
<td>60</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>Threats against grid security and reliability</td>
<td>66</td>
</tr>
<tr>
<td>Figure 4.3</td>
<td>MHINDS architecture and logical functionality</td>
<td>67</td>
</tr>
<tr>
<td>Figure 4.4</td>
<td>Substation Petri net model</td>
<td>69</td>
</tr>
<tr>
<td>Figure 4.5</td>
<td>14-bus example power system [61]</td>
<td>75</td>
</tr>
</tbody>
</table>
Figure 4.6 Power system protection configuration [61] .......................... 75
Figure 4.7 Probability of failures in protection scheme operations ........ 79
Figure 4.8 Max. relay pickups to ensure < 5% false positives ............... 80
Figure 4.9 Attacks required to spoof protection operation .................... 81
Figure 4.10 Relay detectable vs undetectable attacks .......................... 82
Figure 4.11 Substation detectable vs undetectable attacks .................... 83

Figure 5.1 Testbed applications ...................................................... 85
Figure 5.2 Logical testbed architecture ......................................... 92
Figure 5.3 PowerCyber testbed architecture ................................. 94
Figure 5.4 Generator rotor angles ............................................... 101
Figure 5.5 DoS impact on control system communication ............... 102
Figure 5.6 RAS physical and cyber system ................................. 103
Figure 5.7 DoS protection scheme impact (switch flooding) ............ 105
Figure 5.8 DoS protection scheme impact (relay Syn flood) ............. 106
Figure 5.9 Impact of attack on system voltages ............................ 109
Figure 5.10 Impact of attack on generation and line flows ................ 109
ACKNOWLEDGEMENTS

I’d first like to express my thanks to Manimaran Govindarasu for accepting me as a student, providing support for my time as a graduate student, and investing countless hours into my professional development. His motivating personality was fundamental to my success in the Ph.D. program and pushed me far beyond my own expectations.

I’d like to thank Doug Jacobson and Thomas Daniels. They taught my first courses in Information Assurance, were members of my Masters thesis committee years ago, and continued to provide support and encouragement throughout my Ph.D. program. In addition, I’d like to express my appreciation to Venkataramana Ajjarapu and Johnny Wong for their valued contributions to my research as members of my committee.

I’d also like to thank my fellow graduate students, especially Siddharth Sridhar, Aditya Ashok, and Benazir Fateh. Both Siddharth’s and Aditya’s expertise in power systems has been invaluable to my research. They significantly contributed to my understanding of basic power system operations and future smart grid initiatives. Additionally, I’d like to acknowledge Siddharth’s and Aditya’s assistance in the development of the PowerCyber testbed, specifically their help in developing power system simulations, evaluating attack impacts to the physical grid, and helping debug endless technical issues. I’d also like to thank Benazir for her many engaging conversations about research, coursework, and running.

Last, but not least, I’d like to thank all of my family and friends whose continual support was paramount to this work. Specifically, Mom and Dad for their tolerance of my continual frustrations. I’d also like to thank the rest of my amazing family, especially Emily, Sam, John, Amy, Max, and Issac for their perpetual encouragement.
ABSTRACT

While smart grid technologies are deployed to help achieve improved grid resiliency and efficiency, they also present an increased dependency on cyber resources which may be vulnerable to attack. This dissertation introduces three components that provide new methods to enhancing the cyber security of the smart grid.

First, a quantitative exposure analysis model is presented to assess risks inherited from the communication and computation of critical information. An attack exposure metric is then presented to provide a quantitative means to analyze the model. The metric’s utility is then demonstrated by analyzing smart grid environments to contrast the effectiveness of various protection mechanisms and to evaluate the impact of new cyber vulnerabilities.

Second, a model-based intrusion detection system is introduced to identify attacks against electric grid substations. The system expands previous research to incorporate temporal and spatial analysis of substation control events in order to differentiate attacks from normal communications. This method also incorporates a hierarchical detection approach to improve correlation of physical system events and identify sophisticated coordinated attacks.

Finally, the PowerCyber testbed is introduced as an accurate cyber-physical environment to help facilitate future smart grid cyber security research needs. The testbed implements a layered approach of control, communication, and power system layers while incorporating both industry standard components along with simulation and emulation techniques. The testbed’s efficacy is then evaluated by performing various cyber attacks and exploring their impact on physical grid simulations.
CHAPTER 1. INTRODUCTION

Dependencies on Information and Communication Technology (ICT) have propagated throughout our modern society. While these technologies present resounding benefits across commercial, government, academic, and personal ventures their usage is continually hindered by our inability to engineer systems with adequate levels of security. Malicious actors have continually abused security weaknesses by stealing confidential data, compromising data integrity, and degrading system availability.

Critical infrastructure domains, such as transportation, chemical, medical, and energy have also greatly benefited from ICT as a means to monitor and control various physical domains. However, a successful attack against critical infrastructure may result in a catastrophic impact to the economy, natural resources, and even human safety. These systems often were not engineered to provide the robust levels of security needed to protect against an increasingly hostile cyberspace. In addition, there is a current trend to expand the connectivity of many critical infrastructure systems to provide improved control and monitoring capabilities.

While all critical infrastructure domains inherit some risk from cyber attack, the electric power grid is likely the most critical and vulnerable of these domains. The electric grid is a core foundation of our modern society and is imperative for the operation of all other critical infrastructure sectors. The grid is also more exposed to cyber attack than many domains due to its large number of involved parties, primarily private ownership, and heavily interconnected communications which leave it exposed to attack. In addition, the grid is particularly vulnerable to large cascading failures due to physical phenomena.
However, a cyber attack could potentially initiate equivalent failures.

While the electric grid has long been dependent on ICT to manage the various components of the generation, transmission, and distribution systems, current smart grid initiatives are focusing on expanding the use of ICT to modernize the current grid. However, this expanded use of ICT will lead to a greater attack surface which presents a currently undetermined level of risk.

1.1 The smart grid

The U.S. Department of Energy (DOE) has identified seven properties required for a next generation power grid including attack resistance, self-healing, consumer motivation, power quality, generation and storage accommodation, enabling markets, and asset optimization [104]. Smart grid technologies are being used to enhance all areas of the electric grid, including the generation, transmission, distribution, and markets. Many of these advances are enabled by continually improving communication and information processing capabilities. The remainder of this section identifies smart grid initiative impacts which cause significant influences on the use of ICT within the grid.

Advanced Metering Infrastructure (AMI): AMI enhances electricity distribution by deploying smart meters at consumer locations with a goal to reduce cost, increase electricity reliability, and support distributed generation. These meters provide the customer with granular control over their consumption and also facilitate increased integration of Distributed Energy Resources (DER). Utilities benefit from being able to remotely detect outages, perform remote meter readings and offer prepaid options to customers. AMI also enables Demand Side Management (DSM) which exercises direct/indirect control over consumer power consumption.

Wide Area Measurements Systems (WAMS): Increased grid monitoring techniques are required to accurately analyze the flow of electricity through the bulk power
systems. WAMS are predicated upon Phasor Measurement Units (PMU), which provide high sampling rates and accurate GPS-based timing to enable highly accurate and synchronized phasor readings. While the deployment of PMUs provides increasingly accurate readings, the full potential will not be realized unless these readings can be shared among utilities and regulators. Additionally, power system applications must be reviewed and redeveloped to determine the extent these granular readings may provide to both grid efficiency and reliability. The development of advanced control applications will depend on WAMS that will effectively distribute the information in a secure and reliable manner.

**Substation automation systems:** To improve the performance and reliability of device communication within substations, new communications paradigms are being deployed. Older substations often utilized point-to-point communications and serial (RS-232) physical layers. Newer substations deploy faster Ethernet networks which allow multicast transmission of device status to provide real-time awareness of all substation events. Improved field devices, such as Intelligent Electronic Devices (IEDs), can be deployed to perform more sophisticated operations, such as grid protection schemes.

**Common Information Models (CIM):** The smart grid will also increase the use of CIMs to provide a common format for expressing and communicating the information required to support the grid [42]. As the interconnectivity of smart grid systems increase, CIMs will ensure the interoperability of these communications. Current CIM standards such as IEC 61968, which primarily focus on distribution systems, and IEC 61970 for transmission systems, are represented as an ontology that formalizes the information and relationships necessary to support the grid [73]. CIMs have been primarily developed to facilitate increased system integration through consistent data representation and exchange formats.
1.2 Growing threats within cyberspace

Early computing technologies such as multi-user systems and networking created a need for secure computer platforms. Since this time, both threats and cyber dependencies have continued to evolve. The 1980’s presented the Morris worm, which was the first example of self-propagating malicious software. This occurrence became prevalent in the 1990’s and early 2000’s with malware such as Slammer and Conficker which infected large numbers of systems and inflicted a substantial economic burden to the victims [90][77].

While many of the early computer worms did not intentionally damage the infected systems, more recently attacks have been used as a means to gain political and economical advantage. In 2007 and 2008, sophisticated Denial of Service (DoS) attacks were launched against the countries of Georgia and Estonia as a means to influence political agendas [100].

While the large scale DoS attacks required highly skilled attackers, recent events suggest the presence of increasingly sophisticated attackers. Attacker campaigns identified by high sophistication, determination, and financial support have been coined Advanced Persistent Threat (APT) [43]. Intrusions such as Operation Aurora and Operation Shady RAT represent to specific examples of APT type capabilities. Operation Aurora targeted many large technology companies, such as Google, and exfiltrated large amounts of intellectual property [70]. Operation Shady RAT demonstrated similar capabilities and targeted over 70 companies and governments over a five year period [3].

As our nation’s dependency on cyber infrastructure grows, these systems become an increasingly attractive target for well funded nation-state attackers. Many nations are focusing on the development of cyber-based military capabilities [49]. For example, a 2009 report by the U.S.-China Economic and Security Review Commission claimed that China’s People’s Liberation Army (PLA) sponsors cyber attacks targeting U.S. systems, specifically focusing on espionage of military secrets [108]. Similar claims have been
asserted by a recent report by Mandiant which identifies the PLA as the party responsible for the infiltration of over 150 U.S. companies for the purpose of stealing valuable intellectual property and other corporate secrets. The report specifically identifies Chinese locations, military branches, and even the individuals responsible for many of these attacks [65].

While the efforts of the PLA cyber capabilities are heavily documented, many other sophisticated attacks have been identified within the past few years which suggest nation-state involvement. Malware samples such as Stuxnet, Duqu, Flame, Gauss, and Shamoon all include many advanced features which suggest nation-state involvement [26][11]. While the objectives of Duqu, Flame, and Gauss focus on traditional espionage objectives, Stuxnet presented a foundational shift in malware with its ability to usurp the operation of an Industrial Control System (ICS).

Recent surveys have suggested that most critical infrastructure asset owners have been targeted by some form of cyber attack [6]. However, Stuxnet remains the first example of a sophisticated attack targeting the physical domain. Stuxnet’s key salient feature is its ability to propagate malware into a control system and reconfigure the Programmable Logic Controllers (PLC) to perform potentially harmful actions [36]. While it is speculated that Stuxnet targeted Iranian nuclear refinement facilities in order to damage Uranium centrifuges, a similar attack approach could likely be used to target other critical infrastructures in many domains, including the electric power grid, which depends heavily on similar PLCs.

The U.S. government has recently identified the gravity of the these concerns. Efforts such as Homeland Security Presidential Directive 7 (HSPD-7) have prioritized the protection of critical infrastructures, including the electric power grid [112]. Additionally, the 2013 White House Executive Order, titled “Improving Critical Infrastructure Cybersecurity” emphasizes the need for improved cyber security of critical infrastructure, specifically identifying requirements for a “framework to reduce cyber risk to critical
infrastructure” and “information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk” [113].

### 1.3 Vulnerabilities within the smart grid

The combination of an increasingly interconnected smart grid and growing sophistication of cyber threats presents concerns for the grid’s current security posture. As demonstrated in Figure 1.1, threats could target the generation, transmission, distribution, and market domains. In addition, each domain not only has a set of core operational assets to defend, but must also be concerned with the exposure of their critical business and corporate environments.

Unfortunately, as cyber security concerns have grown, researchers have begun to identify many critical vulnerabilities within the communication protocols and software platforms used to support the electric grid. Analysis performed by the Department of Homeland Security (DHS) and Idaho National Laboratory (INL) have determined that serious vulnerabilities are pervasive throughout ICS software platforms and network con-
figurations [45, 46]. Additionally, the U.S. Government Accountability Office (GAO) has reported that these system lack relevant patches, maintain poor system configurations, provide insufficient communication protection, and face a dearth of appropriate intrusion detection capabilities [106][105].

Based on these findings, more secure systems must be developed to provide sufficient resiliency to cyber attack. Although a wealth of research has been performed addressing traditional cyber security paradigms, many solutions do not adequately address the additional constraints required to support the electric grid. The following list identifies known constraints which result in deficient smart grid cyber security.

- Long system lifespans. Unlike more traditional IT systems, many systems within the smart grid will be deployed for 10-20 years. This means more secure systems cannot be deployed as cyber threats evolve.

- Heavy dependency on proprietary systems. Most proprietary systems do not have well understood operations, which leaves the owners unable to make intelligent decisions concerning their risk and what security mechanisms are appropriate to protect them.

- Geographically disperse resources. Systems are strongly dependent on wide area networks, which are more vulnerable to external attacks.

- Limited physical protections. Many systems are physically exposed, such as substations. This leaves them more vulnerable to physical tampering.

- Real-time requirements. Many security mechanisms, such as cryptography, cause unacceptable overhead on the communication. Therefore, systems with real-time requirements often cannot adopt many security controls.

- Restricted use of “fail-closed” security mechanisms. Systems need to be accessible by operators in critical situations and, therefore, cannot restrict access to operators
if they are unable to authenticate.

The previously identified concerns have been recognized by both the U.S. government and electric industry. Table 1.1 identifies roadmaps and security guidelines addressing smart grid cyber security. There have been multiple initiatives by both parties to attempt to improve the security. For example, the National Institute for Standards and Technology (NIST) published the “Guide to Industrial Control Systems (ICS) Security” specifically identifying threats, vulnerabilities, and security controls required to provide a robust cyber infrastructure [54]. Acknowledging future demands for both cyber security and privacy for smart grid initiatives, NIST has released the NISTIR 7628, “Guidelines for Smart Grid Cyber Security” document to provide future guidance as cyber assets proliferate throughout the electric grid [80]. This document identifies likely cyber architectures, enumerates required research initiatives, and documents critical security controls.

In the private sector, the North American Electric Reliability Corporation (NERC) has also acknowledged the threat to the electric grid. In 2009 they released the “High-Impact, Low-Frequency Event Risk to the North American Bulk Power System” report which enumerated major threats to the grid, specifically those from coordinated attacks which blend cyber and physical methods [52]. Additionally, NERC created a Cyber Attack Task Force (CAFT) to explore cyber vulnerabilities in the grid and identify feasible detection, deterrence, and response capabilities [84]. NERC also developed and enforces a set of Critical Infrastructure Protection (CIP) standards which require the identification and protection of all cyber assets supporting the bulk power system [82].
### Table 1.1 Roadmaps and security guidelines for cyber security concerns

<table>
<thead>
<tr>
<th>Policies/Documents</th>
<th>Issues Addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>NISTIR 7628: Guidelines for Smart Grid Cyber Security [80]</td>
<td>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.</td>
</tr>
<tr>
<td>NIST 800-82: Guide to Industrial Control Systems (ICS) Security [54]</td>
<td>Identifies cyber security concerns within industrial control systems (ICS), including SCADA, distributed control systems (DCS), and programmable logic controllers (PLC).</td>
</tr>
<tr>
<td>GAO-11-117: Electricity Grid Modernization: Progress Being Made on Cyber Security Guidelines, but Key Challenges Remain to be Addressed [107]</td>
<td>Assessments of NIST security guidelines, FERC standards development, and key outstanding challenges including metrics, information sharing, insufficient security engineering, and regulatory issues.</td>
</tr>
<tr>
<td>The Future of the Electric Grid (MIT) [68]</td>
<td>Identifies key grid communications, security lifecycles, vulnerability sources, security regulatory issues, and information privacy concerns.</td>
</tr>
<tr>
<td>High-Impact, Low-Frequency Event Risk to the North American Bulk Power System (NERC/DOE) [52]</td>
<td>Identifies the grids inherent vulnerability to coordinated attacks, common modal failures, and APTs. Specifically from DoS, rogue devices, unauthorized access attacks, and malware.</td>
</tr>
<tr>
<td>NERC Critical Infrastructure Protection (CIP) [82]</td>
<td>Cyber security compliance requirements for critical cyber assets supporting the bulk power system.</td>
</tr>
<tr>
<td>Common Cyber Security Vulnerabilities in Industrial Control Systems (DHS) [45]</td>
<td>Comprehensive results of various ICS-CERT reports and assessments of cyber vulnerabilities within various control system domains.</td>
</tr>
<tr>
<td>A Policy Framework For the 21st Century Grid: Enabling Our Secure Energy Future [99]</td>
<td>An official White House strategy to address fundamental concerns to the security of the nations electric grid, specifically requirements for security standards and developing a security culture.</td>
</tr>
<tr>
<td>NERC Cyber Attack Task Force (CAFT) Draft Report [84]</td>
<td>Industry technical committee analysis of possible attacks and responses, specifically focusing on coordinated cyber attacks against the bulk grid.</td>
</tr>
</tbody>
</table>
1.4 Research needs

The development of a secure smart grid requires a vast amount of research in many domains. While many security technologies are available for traditional ICT systems, they frequently aren’t usable for smart grid applications due to excessive overhead or concerns that they may prevent an operator from accessing certain critical functions. Therefore, novel approaches must be explored for these technologies. Additionally, cyber security must be addressed from a cyber-physical perspective, thereby analyzing how the grid’s physical systems attributes influence the need for security and tailors the approaches to security. This research focuses on the latter point, specifically identifying the following three core research needs.

1. Models and metrics for the smart grid cyber security which incorporate:
   - the ability to quantify risk to a system,
   - incorporates current smart grid information models, and
   - provides flexibility for both known and unknown vulnerabilities.

2. Tailored intrusion detection approaches which:
   - integrated with smart grid communication protocols,
   - incorporates awareness of both cyber and physical anomalies, and
   - enables the analysis of sophisticated, coordinated attacks.

3. Smart grid research testbeds that:
   - accurately integrate both cyber and physical system properties,
   - provides environments to explore cyber vulnerabilities and physical system impacts, and
   - supports evaluation of various novel security mechanisms.
1.5 Thesis contributions

This dissertation is structured as follows:

- Chapter 2 provides an overview of smart grid technologies and a background of related work for this dissertation. The smart grid overview identifies how the grid currently uses ICT to perform monitoring and control functions. It then introduces new smart grid technologies and provides an overview of cyber attacks and how they may impact the grid.

- Chapter 3 introduces work done on the development of security models and metrics specifically tailored for the smart grid. It first presents a graph-based model representing the security mechanisms which protect the grid’s critical data from attacks. Then it computes an exposure metric which represents the level of protection for each data item. It then demonstrates the metric’s applicability to various security decisions such as analyzing the impact of a vulnerability and evaluating the efficacy of different security mechanisms.

- Chapter 4 identifies novel approaches to intrusion detection for the smart grids. It demonstrates how attacks to the smart grid differ from traditional attacks by also incorporating smart grid commands. It then demonstrates how a Petri net model can be used to identify whether a device causes a malicious communication by modeling the set of preconditions necessary for an event. It then demonstrates how events can be correlated hierarchically to more accurately analyze events.

- Chapter 5 presents the contributions in the development of a smart grid cyber-physical security testbed. It introduces various research applications which depend on testbeds and analyzes various trade-offs in testbed designs. It then provides an overview of the development of the PowerCyber testbed. Finally, it demonstrates
the testbed’s utility with the execution of various integrity and availability attacks which are then analyzed in terms of their impact on grid stability.
CHAPTER 2. SMART GRID BACKGROUND AND LITERATURE SURVEY

The smart grid will combine both traditional electric grid control functions with cutting edge technologies. Fig. 2.1 provides a high-level overview of the smart grid including the various domains and systems found within it. This chapter provides an introduction to the smart grid, known cyber vulnerabilities, and related research to this work. It will first introduce the foundational domains of the electric power grid and provide an overview of the SCADA architectures currently used to perform monitoring and control. It then introduces various smart grid initiatives including AMI, WAMS, CIM, and substations automation enhancements. The chapter then identifies the various protocols used to support the various communications requirements and identifies various cyber attacks that could be used by a malicious individual to damage the smart grid. Finally, it presents a literature survey of works related to this dissertation.

2.1 Traditional electric grid overview

The electric grid can divided into four core domains, generation, transmission, distribution, and third parties, such as markets and system regulators. These domains have all been dependent on various ICT systems to support communication with other systems within the domain and externally. This section will explain each domain in greater detail, along with the traditional Supervisory Control And Data Acquisition (SCADA) architecture used to support the communication and computation requirements
Figure 2.1  Schematic of the smart grid cyber infrastructure
2.1.1 Generation

The generation domains focuses on the production of electricity. Electricity generation is primarily done with a spinning turbine; therefore, most of the control algorithms focus on managing the frequency, voltage, and power output of the generator. Multiple control systems are required to support these algorithms. Local control systems include Governor Control, which is used to control the generator’s frequency, and Automatic Voltage Regulator (AVR), which is used to control the generator’s reactive power. In addition to these local control systems, generation must also communicate with third-party balancing authorities to ensure each remains appropriately synchronized. The wide-area Automatic Generation Control (AGC) is used to perform this function by monitoring and adjusting a generator’s frequency as loads change. In addition, generation systems also must implement various protection algorithms to prevent against any physical faults which may occur. This system is explained in more detail in Section 2.2.2.

2.1.2 Transmission

The transmission domain focuses on the transportation of high-voltage electricity from large generators to the distribution domain. Control over the operation of the transmission systems primarily occurs within substations where power lines interconnect. Substations primarily support needs to convert power between different voltages on neighboring lines and also provide a place to deploy various control mechanisms. Transmission lines must be continually monitored to ensure that the load on the lines does not surpass their physical limitations. This is performed with state estimation control algorithms, which is a wide-area monitoring system that collects telemetry from power lines and transmits them back to the control center where they are used to calculate the flow on the transmission system. Additionally, protection systems are very important in transmission because the lines are physically exposed and are frequently impacted by faults which perturb power flow. Protection schemes are implemented in
both wide and local forms.

2.1.3 Distribution

The distribution domain focuses on transporting electricity from the transmission lines to the consumer through lower voltage lines. Distribution systems have traditionally had less automation than the transmission and generation domains. Traditionally, load shedding has been a primary control function within distribution, which uses breakers to trip relays on distribution feeders. Similar to the generation and transmission domains, the protection systems are heavily used within distribution systems to protect equipment from faults.

2.1.4 Markets and system operators

There are many other functions which are critical to the grid’s daily operations. Specifically, the oversight and management of the various utilities. Independent System Operators (ISO) are authoritative parties that coordinate the generation and transmission amongst multiple utilities to ensure that load remains balanced. ISO also provide markets that are used to balance the supply and demand of electricity between energy producers and consumers. While the systems used to support these functions do not perform control functions, they are critical for the grid’s daily operation.

2.1.5 SCADA architectures

The power grid has historically been dependent on SCADA technologies to perform monitoring, alarms, and control functions throughout the generation, transmission, and distribution domains. SCADA systems utilize a hierarchical paradigm where a centralized control center manages many geographically distributed field devices [54].
2.1.5.1 Control centers

Control centers provide a central location for analysis and control over some section of the grid, whether it be generation, transmission, or distribution. The control center is typically staffed with operators that make human-in-the-loop control decisions over many grid control functions. Control centers typically include the systems identified below.

**SCADA servers** - SCADA servers manage the telemetry and control operations between the control center and the field devices within the various substations. SCADA servers are a critical component as they have the ability to send commands to the remote field devices and are the central means for operators to evaluate the state of the network. To obtain telemetry data, the SCADA server continually polls the field devices for state updates. This collected information can then be shared with other SCADA systems such as the EMS and Historian. Additionally, the SCADA server can also process any alarm data correlating to any anomalous physical events.

**Energy Management Systems (EMS)** - An EMS utilizes SCADA data to perform higher level analysis of a system state to analyze potential problems and mitigations. Specifically, EMS are often used to execute generation control, state estimation, fault location algorithms and contingency analysis.

**Human Machine Interfaces (HMI)** - HMIs provide an interface between the operator and the SCADA and EMS systems. The HMI is typically a graphical user interface (GUI) based interface that presents operators with the ability to analyze and control the states of various system components.

**Historian** - A historian is a system which contains a database of events which occurred on the physical system. The system is primarily used to analyze events off-line and generally is not used for real-time functions like the other previously identified systems.

Control centers are dependent on both local and wide area communications. Local Area Networks (LAN) support communications between all the control center devices.
In addition, Wide Area Networks (WAN) are used to support communication between the SCADA server and the various substations. These WAN connections are primarily used to transmit the telemetry data and commands. Various forms of physical media are used for this communication, however, these often consist of leased lines and wireless microwave links. In addition, control centers often support some communication to non-operational business systems in order to provide awareness about system operations to other corporate entities.

2.1.5.2 Substations

Substations are where the SCADA technologies actually acquire the telemetry and send commands to the various field devices to control the physical grid. Therefore, these field devices provide the primary bridge between the grid’s cyber and physical domains. Field devices typically include PLCs, Remote Terminal Units (RTU), and IEDs.

**PLC** - PLCs are legacy devices which typically execute some form of programmable *ladder logic* to control some physical systems. Often these devices have very limited communication and processing capabilities. These are often implemented as relays in control systems.

**RTU** - RTUs are also legacy devices which were developed to support communication needs between field devices such PLCs and some other controller. Therefore, these devices should have some ability to communicate over a network to support various control requirements.

**IED** - While substations historically used PLCs and RTUs to obtain telemetry and control actuators, recent trends are towards IEDs which have more capable computation and communication capabilities. IEDs are currently heavily deployed to perform many different functions such as controlling protection schemes and relaying telemetry from power lines along with send device statuses.
Substation Automation (SA) Systems - Modern substations also implement some SA system which provides a central system to manage the various IEDs, PLCs, and RTUs found within the substation. In addition to providing a central control point, these systems may also provide a human operator with a local interface to the substations.

2.1.5.3 Software platforms and communication protocols

While SCADA systems require many tailored communication protocols and software platforms, they also incorporate many shared elements with traditional ICT systems as demonstrated in Fig. 2.2. SCADA communication protocols are tailored toward transmitting commands and telemetry data which requires strong availability and integrity. Common protocols used within the traditional power grid include Modbus, Distributed Network Protocol (DNP), Object Linking and Embedding (OLE) for Process Control (OPC), and Inter-Control Center Communications Protocol (ICCP).

In addition to the tailored SCADA protocols, many standard ICT protocols are also used to provide auxiliary services. Lower level protocols such as Ethernet and Internet Protocol (IP) are common to provide the ability to route packets between networks. Additionally, many higher level protocols are required to support both operations and administrative functions. For example, Network Time Protocol (NTP) is used to ensure
that all systems have synchronized clocks which is imperative when transmitting telemetry data. Additionally, many administrative and management protocols are needed, such as Telnet, File Transfer Protocol (FTP), Simple Network Management Protocol (SNMP), and Transport Layer Security (TLS).

In addition to the tailored software used for the power grid, these systems all currently depend on many standard platforms and communications found in ICT. Many SCADA specific software products exist which incorporate the various protocols which were previously identified. However, these products are often dependent on many commodity operating systems and services to support the SCADA applications. Commodity operating systems such as Microsoft Windows and many Unix derivatives are commonly used along with many different embedded operating systems. In addition, these software platforms are also heavily dependent on commodity applications, such as web servers, database servers, and file servers to support the SCADA functions. Therefore, electric grid environments must understand risk from vulnerabilities which impact both commodity and domain specific systems.

2.2 Smart grid technologies and communications

Each of the previously identified electric grid domains has its own set of communication requirements to support its various control systems. Smart grid initiatives extend this dependency by integrating additional communication and control capabilities throughout each domain. Table 2.1 presents an overview of the communications necessary to support each smart grid domain, including the various applications enabled by the protocols. Additionally, it identifies the communication protocols used to support this communication and their needs for integrity (I), availability (A), and confidentiality (C).

While key smart grid initiatives were identified in Section 1.1, this section will provide
Table 2.1  Smart grid communications (I: Integrity, A: Availability, C: Confidentiality)

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>NETWORKS</th>
<th>APPLICATION</th>
<th>SECURITY</th>
<th>PROTOCOLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMI</td>
<td>Home Areas</td>
<td>1. Consumption monitoring</td>
<td>I - Med</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network</td>
<td>2. Pricing information</td>
<td>A - Med</td>
<td>ZigBee</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C - High</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Field Area</td>
<td>1. Usage data</td>
<td>I - High</td>
<td>ANSI C12.22,</td>
</tr>
<tr>
<td></td>
<td>Network</td>
<td>2. Update energy pricing</td>
<td>A - Med</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Meter maintenance/mgmt.</td>
<td>C - High</td>
<td>ZigBee</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Distribution</td>
<td>1. Distribution Automation</td>
<td>I - High</td>
<td>IEC 61850,</td>
</tr>
<tr>
<td></td>
<td>SCADA</td>
<td>2. Fault detection/mgmt.</td>
<td>A - High</td>
<td>DNP3,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Distributed energy resources</td>
<td>C - Low</td>
<td>Modbus</td>
</tr>
<tr>
<td></td>
<td>Distribution</td>
<td>1. Protective relaying</td>
<td>I - High</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Substation</td>
<td></td>
<td>A - High</td>
<td>IEC 61850</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C - Low</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transmission</td>
<td>1. Telemetry and control data</td>
<td>I - High</td>
<td>IEC 61850,</td>
</tr>
<tr>
<td></td>
<td>SCADA</td>
<td>2. EMS functions</td>
<td>A - High</td>
<td>DNP3,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C - Low</td>
<td>Modbus</td>
</tr>
<tr>
<td></td>
<td>Transmission</td>
<td>1. Protective relaying</td>
<td>I - High</td>
<td>IEC 61850</td>
</tr>
<tr>
<td></td>
<td>Substation</td>
<td>2. Special protection schemes</td>
<td>A - High</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C - Low</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WAMS</td>
<td>1. Publish PMU readings</td>
<td>I - High</td>
<td>IEC 68150-90-5,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Process external PMU data</td>
<td>A - High</td>
<td>C37-118</td>
</tr>
<tr>
<td></td>
<td>Inter-</td>
<td>1. Generation scheduling</td>
<td>I - High</td>
<td>ICCP</td>
</tr>
<tr>
<td></td>
<td>control</td>
<td>2. Transmit grid status</td>
<td>A - Med</td>
<td></td>
</tr>
<tr>
<td></td>
<td>center</td>
<td></td>
<td>C - Low</td>
<td></td>
</tr>
</tbody>
</table>
an overview of the these technologies, their communications requirements, and potential security concerns.

2.2.1 AMI

AMI attempts to reduce cost and increase electricity reliability through the deployment of smart meters at consumer locations. These meters provide the customer with granular control over their consumption and facilitate increased integration of distributed generation. Utilities benefit from being able to remotely detect outages, perform remote meter readings, and offer prepaid options to customers. Because AMI requires that smart meters be deployed at all consumer locations, deployments can range into hundreds of thousands of devices for a large city. Each meter requires network connectivity back to the utility in order to transmit usage, status, and control information. Therefore, AMI deployments require large cyber infrastructures and many new technologies to meet these demands.

While utilities will deploy smart meters to consumer locations, the meters also provide consumers the option to deploy Home Area Networks (HAN) in order to integrate all their devices and appliances. This will then provide the devices and appliances with the ability to obtain real-time pricing which can then be used to schedule operations around energy costs. However, HAN deployments will require communication interfaces between the consumer and meter.

In addition to the HAN-meter interface, meters must also be able to communicate with the utility to transmit control, pricing, and consumption data. This communication is supported with a Field Area Network (FAN) that connects the smart meters back to an AMI headend device. The FAN will support the communication requirements of a large number of meters and must be a geographically disperse environment throughout both urban and rural environments. Numerous wired and wireless communication protocols have been proposed to support FAN requirements.
AMI will also require additional communication and control technologies to manage the large number of smart meters under their control, specifically the billing and meter management functions. This includes methods to support communication between the AMI headend, billing systems, and Meter Data Management Systems (MDMS). This communication will likely occur within the segmented utilities network and will more closely resemble traditional ICT systems.

2.2.1.1 Protocols

Multiple new network protocols have been developed to support the HAN and FAN communication demands. This section introduces two leading protocols, ZigBee Smart Energy Profile (SEP) and ANSI C12.22, along with their security attributes.

**ZigBee SEP** This provides a full protocol stack standard for HAN and FAN communications, including link, network, transport, and application layers [118]. This standard natively supports AMI functions such as dynamic pricing, billing, and DER. ZigBee SEP provides support for two different physical/data link layers including wireless 802.15.4 and power line carrier-based HomePlug. The network layer implements IPv6-based routing protocols instead of mesh network approaches commonly found within other ZigBee networks. The SEP application protocol is based on Hypertext Transfer Protocol (HTTP) utilizing Representational State Transfer (REST) web services to define domain specific event messages.

The standard also identifies numerous layers of security mechanisms to support AMI communications. It proposes AES-based symmetric encryption algorithms, SHA family hash functions, and various public key mechanisms (e.g., elliptic curve, RSA, Diffie-Hellman). Additionally, the protocol provides support for secure transport layers with TLS, secure network layers with IPSec, and a secure link-layer base on AES-CCM.
ANSI C12.22  Another competing standard for AMI infrastructures is ANSI C12.22, which extend upon previous meter reading standards, ANSI C12.18. ANSI C12.18 presents a standard for two-way meter communication, but focuses on optical ports, C12.22 extends this standard to enable networked communication [4]. The standard identifies various devices, including end devices (or meters), and communication relays and gateways required to support routing. Security within C12.22 is supported with symmetric key ciphers which utilize the EAX’ protocol to support both encryption and authentication of meter data [76].

2.2.1.2 Security concerns

Specific cyber security concerns within AMI stem from the large-scale device deployments, dependency on embedded systems, and constrained network bandwidth which limit security monitoring. Because the meter allows interactions from multiple parties, specifically consumers and utilities, it will likely need to support remote access which could be abused by an attacker. Additionally, because these meters are deployed throughout urban and rural environments, the devices and communications are both physically exposed leaving them more vulnerable to both physical tampering and cyber attack.

Traditional meters have long been a target for tampering by consumers in an attempt to steal energy. This trend will likely continue with the transition to smart meters. While tampering with traditional meters only allows energy theft, these techniques could prove more damaging within AMI. Since a meter must be able to authenticate itself to the headend devices, it must maintain some shared key or password within the meter. This will be a likely attack target as it will allow the user to fabricate valid meter commands and responses to utility requests.

The large scale of AMI deployment depends on a substantial number of authentication keys. Therefore, key compromises must be considered probable occurrences and should be engineered into system designs. Additionally, automated methods to update meter
software and communication protocols are imperative to ensure security failures can be quickly mitigated.

Unlike many other grid resources, data confidentiality becomes increasingly important as granular meter readings have been shown to strongly infer consumer’s at-home activities. Privacy issues currently hinder consumer acceptance due to concerns that data will be provided to marketers, law enforcement, or other third parties. [33].

2.2.2 Substation automation systems

Substation communication previously relied heavily on dedicated wiring between PLCs, RTUs, and physical devices such as transformers and circuit breakers. The IEC 61850 standard has been developed to support a networked approach in order to reduce costs and improve reliability [1]. This section provides a brief description of the IEC 61850 protocol which is being used to incorporate increased ICT within substations. IEC 61850 is unlike many protocols in that it also defines the following network elements:

- data models for devices,
- Substation Configuration Languages (SCL),
- the substation network architecture, and
- multiple communication protocols.

2.2.2.1 IEC 61850 data models

The IEC 61850 protocol implements a standard data model that provides a common naming format for all devices, data objects, and attributes used to support the necessary substation automation communication functions. This common naming structure ensures interoperability of many different devices and presents easily understood naming conventions for human interpretation.
Table 2.2 Sample of IEC 61850 LN names and definitions

<table>
<thead>
<tr>
<th>LN</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>XCBR</td>
<td>Switch with circuit breaker</td>
</tr>
<tr>
<td>TCTR</td>
<td>Instrument transformer/transducer for current</td>
</tr>
<tr>
<td>CSWI</td>
<td>Switch/breaker control</td>
</tr>
<tr>
<td>PDIS</td>
<td>Distance protection</td>
</tr>
<tr>
<td>PTRC</td>
<td>Protection trip conditioning</td>
</tr>
<tr>
<td>IHMI</td>
<td>Human machine interface</td>
</tr>
<tr>
<td>RREC</td>
<td>Recloser</td>
</tr>
<tr>
<td>RBRF</td>
<td>Related function breaker failure</td>
</tr>
</tbody>
</table>

Physical devices are functionally divided into logical nodes (LN) based on the different functions of the device. Each LN has a standard naming convention (i.e., XCBR) and includes a set of data objects necessary to support the operation of that specific logical node. Additionally, each data object possesses a set of data attributes necessary to represent the operation of that data object. Data attributes can contain information such as the object’s data type, valid ranges, and time stamps. Table 2.2 identifies common logical nodes used in this paper and defines their name.

2.2.2.2 Communication protocols

IEC 61850 presents three different communication protocols for various communication needs. These are Generic Object Oriented Substation Event (GOOSE), Sample Values (SV), and Manufacturing Message Specification (MMS) [75].

GOOSE is tailored for fast intra-substation communication with a focus on transmitting information about substation events. GOOSE is based on a publish/subscribe network architecture where each LN can choose the set of messages it subscribes to. Communication is performed directly using broadcast and multicast Ethernet messages between devices. Additionally, systems statuses are continually transmitted; therefore, devices can identify when other device’s statuses change [2]. SV are used primarily to transmit measurements from sensor to devices such as relays and IEDs. SV communi-
cation requires low latency and is generally only transmitted across the local network; therefore, SV packets are also transmitted directly in Ethernet packets. Finally, MMS is used for client-server communication as opposed to the multicast Ethernet used in GOOSE and SV. This supports needs to communication substation data with devices on different networks, such as control centers or other substations.

Numerous substation automation functions are required to perform the required control, monitoring, and protection functions. Within IEC 61850 each function is supported through various LNs communicating together. The remainder of this section will demonstrate how various substation automation functions are performed with the IEC 61850 GOOSE protocol.

**Control operations** The remote operation of a circuit breaker is a basic substation automation requirement. The breaker command, as demonstrated in Fig. 2.3, originates from an operator located at a HMI, represented by the IHMI LN [75]. The operator sends the command to the control IED, which is responsible for managing a circuit breaker’s control state with the CSWI LN. The control IED then updates its status, CSWI.Pos.ctlVal, to tell the circuit breaker to operate by updating the status of XCBR.Pos.ctlVal. After this has occurred, the breaker should update open and its current status, XCBR.Pos.stVal, should change to represent its new state.

**Protection scheme operation:** Fig. 2.4 demonstrates how a protection scheme operation can be enabled by IEC 61850 based on work demonstrated in [2]. As demonstrated in Fig. 2.41a and 1b, a protection IED continually receives the current and voltage level from transformers. If the fault identification LN (e.g., PDIS) identifies a fault on the line, it will update its fault status signaling the operation of the protection trip controller, PTRC (2). When the protection trip control LN receives the fault identification (3), it updates its status and sends a message to the circuit breaker. Once the circuit breaker receives this command, it will trip to clear the fault and then update its status,
XCBR.Pos.stVal (4).

Because most faults are transient, once the breaker trips and the fault clears, the breaker can be reclosed and the line can be re-energized. To enable the breaker reclosing, a reclosure LN (RREC) will be enabled when it receives the PTRC trip status (3). This initiates a timer in RRC which waits for the fault to clear. Once the timer expires, the reclosure IED updates its status to identify the breaker of the reclosing (5). Upon receiving this update, the circuit breaker will reclose and then update its status (6).

Breaker failure protection: Protection schemes must also incorporate methods to deal with failures of circuit breakers. Various circuit breaker failures can occur, such as a breaker not opening appropriately, or a breaker opening successfully, but not clearing the fault. Circuit breaker failure functions attempt to mitigate both situations by sending a breaker trip command to backup breakers which can then be tripped in order to clear a fault. A breaker failure operation is initiated as soon as a fault is discovered by a protection relay. Once this occurs, a timer is started to provide sufficient time so that the primary protection relays to clear the fault. If the fault has not been cleared in this time period, a command will be sent to operate backup circuit breakers.

IEC 61850 implements breaker failure protection through the RBRF LN as demon-
Figure 2.4  61850 protection operation
Figure 2.5 61850 breaker failure operation

strated in [21] and [115]. Fig. 2.5 demonstrates the sequence of a breaker failure operation. It begins similar to a normal protection function, except the added RBRF device is enabled by the PTRC status (3). Once the RBRF timer expires, it verifies that the breaker’s status has been updated to reflect the trip. If the fault has not been cleared, a retrip packet will be first sent to the primary circuit breaker (4). If this does not clear the fault, an external trip request is sent to the backup breakers with the RBRF.OpEx packets (5). Once this data has been sent, the backup breakers should operate to clear the fault.

### 2.2.2.3 Security concerns

Substations automation systems are critical to the reliability of the electric power grid, especially in the transmission and generation domains. Substation communications must also provide high performance. Many substation applications, such as protective relaying, which requires tripping breakers to protect physical equipment from spikes in
current, must be executed within milliseconds. Additionally, because substations are
geographically dispersed and often maintain limited physical network protections, they
are often very exposed to attackers.

An attack against a substation could have a major impact to the power grid. Research
in [15] proposed methods to compute how cyber attacks against a substation could result
in a loss of load. In addition, real-world situations have demonstrated that attacks to
relays could cause instabilities to generators and the grid’s voltage [117].

2.2.3 WAMS

Increasing strain on bulk transmission, dynamic generation due to renewable energies,
and increased sensing capability has instigated the development of WAMS to provide
increased awareness of grid status. PMU’s provide high sampling rates and accurate
GPS-based timing to provide highly accurate and synchronization of phasor readings.
While the deployment of PMUs provide increasingly accurate readings, the full potential
will not be realized unless these readings can be shard among utilities and regulators.
Additionally, power system applications must be reviewed and redeveloped to determine
the extent these granular readings may provide to both grid efficiency and reliability. The
development of advanced control applications will depend on WAMS that will effectively
distribute the information in a secure and reliable manner. Recently, the NASPInet
initiative has focused on developing an architecture sufficient for a North American
based WAMS deployment [20]. NASPInet has identified publisher/subscriber access
control mechanisms to support the dynamic sharing of PMU data.

Unfortunately, the development of a WAMS presents numerous cyber security con-
cerns [13]. The infrastructure must provide both high availability and integrity of the
PMU data, while also providing some confidentiality of certain utility data. The develop-
ment of such an architecture presents numerous constraints on the cyber infrastructure.
The support for confidentiality and integrity will be primarily based on cryptographic
primitives specifically, asymmetric, public key cryptography. It must also provide support for publisher/subscriber access control mechanisms and multi-cast communications.

2.2.3.1 Protocols

IEC 61850-90-5 WAMS deployments will depend on the availability of effective standards to storing and communicating PMU measurements. While the IEC 61850 standard primarily focuses on the substation automation identified in Section 2.2.2, IEC 61850-90-5 is an emerging standard that will support the need to transmit PMU measurements across a network [67]. The standard expands upon the IEEE C37.118 standard which focuses on data storage formats to also provide support of both serial and IP-based multicast transmission. IEC 61850-90-5 maps PMU data formats into current IEC 61850 protocols to support communications with Phasor Data Concentrators (PDC) and other PMU devices.

2.2.3.2 Security concerns

The deployment of a WAMS presents numerous cyber security concerns [12]. The infrastructure must provide both high availability and integrity of the PMU data, while also providing some confidentiality of certain utility data. The infrastructure must simultaneously send PMU readings to many different parties to ensure everyone has a real-time system view. Therefore, the infrastructure must utilize multicast traffic to conserve network bandwidth. The design of adequate access control and authentication is also challenging. Malicious individuals must not be able to spoof or modify PMU messages as this would result in inaccurate utility estimations of the grid’s state.

2.2.4 CIM

The smart grid presents an increased need for CIMs to provide a common format for expressing and communicating the information required to support the grid [73]. The
development of standard data models provide consistent data representation to help facilitate improved interoperability, configuration, and management. Current CIM standards such as IEC 61968 and IEC 61970 present ontologies that formalize the information and its relationships. IEC 61790 presents a standard of the data objects necessary to support the transmission system. Data classes for this model include loads, measurements, topologies, wires, generators, SCADA, and protection. Similar to IEC 61970, IEC 61968 provides an equivalent standard for the distribution systems. Core data classes for this model include assets, consumers, work flows, and documentation.

The models provide a standard for data objects which may be stored and transmitted in multiple different formats. Therefore, the use of CIMs also requires mappings to many other data formats used in the smart grid. For example, Section 2.2.2.1 introduces the data model used for the IEC 61850 protocol. Objects in this model can be mapped to those in IEC 61790 to provide an overarching view of data used in various domains and systems [42].

While CIMs have primarily been developed as a mechanisms to support grid interoperability, they also present a key element to understanding the security requirements of the system by providing a mapping of data to the networks and systems that must protect it. This research leverages these properties as a key component in understanding impacts from cyber security failures.

2.3 Cyber threats to the smart grid

Attacks against the smart grid will likely differ from many traditional attacks against cyber environments. First, an attacker must be able to compromise the grid’s cyber elements. However, in order for the attack to cause negative system impact, the attacker must also know how to control the cyber elements in order to manipulate the physical system. Fig. 2.6 demonstrates this relationship.
An attacker could potentially use a number of approaches to compromise the grid’s cyber resources. These resources will be the same set of devices and communications previously identified. By compromising some set of cyber resources, an attacker can then gain some degree of control over the various power applications. Depending on that set of compromised power applications, an attacker may then be able to cause physical system impact. Physical impacts could include grid instabilities, loss of load, and influencing market prices. Work in [94] more thoroughly explores the set of power applications used to support the various smart grid domains along with weaknesses in the supporting cyber infrastructure.

This section will introduce potential attacks which could impact the communications of smart grid, along with those that could compromise the sets of systems and devices.

2.3.1 Communications

As demonstrated in Table 2.1, the smart grid depends on many different communication flows which have varying importance and security requirements. If an attacker is able to manipulate these communications, they could control the computations performed by various connected systems which would then impact the physical grid. Potential attack against communications include the following items:
**Spoofing** - A spoofed message is one that an attacker injects into the network to make it appear as if it originates from a trusted system. While this is possible in both wired and wireless systems, the latter remain more vulnerable as the attacker can more easily access the physical medium. Spoofing is generally prevented by employing some form of cryptographic authentication which requires that the attacker sign or encrypt the spoofed message with a shared or private key in order to verify its integrity. However, the smart grid communications present numerous concerns, specifically because many protocols were designed with inadequate authentication [47]. Additionally, the high availability requirements and large number of devices present challenges when applying more secure approaches [38].

**Denial of Service (DOS)** - Networks are vulnerable to DoS attacks if an attacker is able to inject large number of packets into the network which cause congestion and limits the network’s availability to the intended functions. While both wired and wireless networks are vulnerable, wireless networks remain extremely vulnerable to DoS because the physical medium cannot be more easily accessed by an attacker. Additionally, DoS can also occur if a malicious packet causes the server to crash when attempting to process the packet.

**Man-in-the-Middle (MitM)** - The network is also vulnerable to many different MitM attacks if the physical medium is not protected or the attacker can manipulate some network address (e.g., Address Resolution Protocol (ARP)) or routing mechanisms (e.g., Border Gateway Protocol (BGP)). If an attacker performs a MitM attack they would be able to manipulate the authentic communications in transit. Because the smart grid incorporates many new protocols for systems such as AMI, there are documented concerns about possible routing layer vulnerabilities which may enable DoS attacks [80].
Misconfigurations - Network misconfigurations also present serious vulnerabilities to communication networks. Configurations in devices such as firewalls focus on segmenting trusted and untrusted portions of a network. Therefore, a misconfiguration of these devices may result in an untrusted user gaining access to critical system components. Incorrect and insufficient network segregations have been identified as a core concern throughout the smart grid [80].

2.3.2 Systems and devices

In addition to the communication networks, the systems and devices used to control the grid are also vulnerable to attack. This section previously enumerated the common types of devices found within the smart grid. The remainder of this section will identify attacks against these systems.

Software vulnerabilities - Software vulnerabilities, such as buffer overflows, integer overflows, and structured query language (SQL) injection, can provide an attacker with the ability bypass authentication to usurp control of a system. Numerous recent studies have suggested software vulnerabilities significantly plague smart grid systems [47][24]. Additionally, control systems, such as the smart grid, are especially difficult to patch due to a need for high up-time. This constraint will likely leave systems extremely vulnerable to software vulnerabilities.

Authentication issues - Many devices within the smart grid do not use strong methods to authenticate users. While devices are configured with default or weak passwords, additionally, many system features often completely lack authentication support [114]. Authentication issues could provide unauthorized users with the ability to manipulate system settings and operations.
Malware  - Malware is any malicious software which an attacker is able to execute on a target system in order to usurp its control. While malware is frequently used for data exfiltration in traditional ICT environments, malware which manipulates or denies control of a physical system will likely be more damaging against the smart grid. While researchers have proposed that malware could impact SCADA systems by injecting malicious control communications [37], Stuxnet introduced the first real-world instance of malware specifically infecting and performing nefarious actions within field devices [36].

Portable medial  - Most smart grid devices are not directly connected to the untrusted Internet. While this significantly increases the difficulty for an attacker to access the system, it does not provide complete security. A sophisticated attacker may be able to transfer malware into the system using some form of portable media. Stuxnet demonstrated that malware could infect air-gapped control systems by spreading through portable media [36].

Supply chain  - A supply chain attack could include any attacker technique that compromises a system’s integrity before it is deployed. While attacking the supply chain requires high sophistication, recent reports suggest many foreign network devices may contain back-doors that provide access to unauthorized users [109]. Supply chain attacks are similar to portable media in that they do not require an attacker to have physical system access. Supply chain issues also incorporate the need for trusted system updates and patches which have been used in sophisticated cyber attacks [27].
CHAPTER 3. CYBER ATTACK EXPOSURE
EVALUATION FRAMEWORK

3.1 Introduction

The coupling of the power infrastructure with complex computer networks substantially expand current cyber attack surface area and will require significant advances in cyber security capabilities. Strong security metrics are necessary to ensure security-based decisions accurately reflect a realistic understanding of cyber risk. NIST specifically addresses this requirement and recommends research in “tools and techniques that provide quantitative notions of risks, that is, threats, vulnerabilities, and attack consequences for current and emerging power grid systems” [80].

Attack trees and graphs have previously been used to model network security, unfortunately these models will not scale to large networks. While they provide detailed information on potential attack methods, their development is based on an understanding of potential attacker goals. Current trends show attackers increasingly rely on exploiting zero-day vulnerabilities [101], which reduces the accuracy of models depending on the evaluation of known vulnerabilities.

Developing security models for a large, networked environments such as the smart grid should focus on the critical information necessary to support the grid and the resulting security mechanisms deployed to protect it. The electric grid can typically be categorized into domains including generation, transmission, distribution, and market operations. While a significant amount of intra-domain communication occurs, inter-domain com-
munication is imperative for grid stability as shown in Fig. 1.1. Since inter-domain trust is a key characteristic for grid communication, a strong security model must accurately represent the trust levels and any associated risks.

Smart grid technology has developed increasing sophisticated common information models (CIMs) which standardize the information necessary to support system operation and assist with increasing requirements for communication between domains. Fortunately, CIMs also provide increasing awareness of information dependencies which should be leveraged to improve cyber security. This research provides a novel network security model tailored to provide a quantitative exposure metric based on these information objects by identifying and analyzing their dependency on security mechanisms as they traverse a network. This research also demonstrates how the exposure metric can be utilized to perform various cyber security related activities such as vulnerability impact analysis and security investment analysis.

3.2 Related work

Multiple research efforts have focused on the development of security models in order to analyze and calculate metrics to represent a system’s resiliency to attack. Three specific examples are attack trees, privilege/attack graphs, and attack surface metrics. Each of these will be introduced below.

3.2.1 Attack surface analysis

Research on attack surface evaluation has been introduced by Manadhata and Wing [64][63]. This work defines a service’s attack surface as the set of entry points, exit points and data channels in a system and utilizes this information to produce quantitative measurements of security. The relationship between excessive attack surface area and decreased security is then shown through the comparison of similar software platforms.
While this work is a useful component in software engineering, the metric requires a formal review of software functionality and does not address the complexity of large-scale, distributed systems.

### 3.2.2 Attack trees

An attack tree is a model which enumerates all potential vectors an attacker could use to gain access to some target resource. Each branch in the tree represents a set of intermediate steps the attacker must take prior to gaining access to the target. Previous attack tree work by Ten has shown applicability to modeling SCADA cyber security [96, 98]. Attack tree models such as Morda demonstrate how system risk can be calculated based on an understanding of attack objectives, strategy and potential mission impact [35]. Unfortunately the development of accurate trees is a difficult process when attacker capabilities and objectives are not well known.

### 3.2.3 Privilege/attack graphs

Previous work on security modeling was performed by Dacier, et al. through the implementation of privilege graphs which evaluate various privilege states in a computer system to determine whether known security states are violated [19]. This work was then expanded upon to show that the transitioning between nodes in a privilege graph can be used to model attacks against a system as an attacker escalates their privilege level [17]. In addition, this research addresses the relationships between security and various path characteristics, specifically length and quantity [18].

Attack graphs take a different approach to modeling security concerns by producing a privilege graph and analyzing the attack paths provided by all known vulnerabilities [59]. Detailed analysis of feasible attack capabilities can then be determined to establish whether critical resources are appropriately secured. Work by Wang, et al. has utilized attack graphs for security metrics based on both path length and quantity [58]. Research
performed by Idika and Bhargava has extended the path-based analysis by comparing potential metrics [48]. While the attack graph approach provides comprehensive view of a system’s security, the difficulty of the vulnerability discovery and mitigation process reduces model accuracy and applicability to a large architecture with unknown vulnerabilities.

### 3.3 Exposure evaluation framework

The development of a secure infrastructure is contingent on the ability to accurately assess the effectiveness of the current security mechanisms. The proposed framework achieves this goal by evaluating all paths an attacker must take in order to access critical resources. This work models the flow from security mechanisms to their protected privileges and the information accessible by that privilege. With this model the various sets of security mechanisms required to protect information as it traverses through a network can be reviewed.

The risk management process requires a comprehensive and continuous set of operations to ensure adequate system security. NIST provides a suggested framework which identifies all required activities and details the efforts necessary to perform risk management within industrial control systems [54]. The proposed exposure evaluation integrates with NIST’s management framework to provide a more accurate assessment of risk. The interactions between the risk management and exposure analysis framework are displayed in figure 3.1.

The proposed model and metric leverage data from the security control selection process to determine the set of implemented security mechanisms. These security mechanisms along with the system’s information model are necessary for the exposure graph development, which is detailed in section 3.3.2. Once this graph has been developed it can be utilized to compute the proposed exposure metric which is discussed in section 3.3.3.
The resulting exposure metric has applicability throughout the risk management process. Proposed applications include:

- Security Control Selection - security mechanisms comparisons and investment evaluation
- Control Assessment - prioritization of security mechanisms and impact analysis
- Control Monitoring - security event impact analysis

### 3.3.1 Identifying cyber risk

Determining the set of security mechanisms required to support the cyber architecture is a challenging research area. There are currently numerous risk management and processes which require the implementation of baseline security mechanisms within an environment [54, 82].
Figure 3.2  a) Testbed network architecture, b) Testbed data flow diagram
Traditional computer security models attempt to evaluate the current state of a computer and analyze whether the state corresponds to a known security status. A set of security mechanisms or controls are utilized to restrict system use to only those secure states. This paper presents a similar model based on a set of privileges, $P$, which identify the set of available states in the systems. Each privilege represents user/system access to some set of attributes within a CIM representation of the information within the system. These attributes, or information objects, are represented by the set $IO$. The model also assumes privileges are enforced with a set of security mechanisms, $SM$, such as access control, authentication, and encryption.

To determine an appropriate set of security mechanisms this paper utilizes the Threat Modeling process introduced by Microsoft [95]. The process first requires the identification of users, processes, data flows, entry/exit points, and data stores within the architecture. Next, each of the data flows are reviewed for possible (S)poofing, (T)ampering, (R)epudiation, (I)nformation disclosure, (D)enial of service, and (E)scalation of privileges. The threat modeling process begins with the development of a data flow diagram (DFD) which is then utilized to identify trusted boundaries and identify potential untrusted input.

The PowerCyber SCADA testbed at ISU, detailed in Fig. 3.2a), is utilized to produced the example DFD between the control center and one substation in Fig. 3.2b) [40]. In this example there are two trusted zone, the first is the control center where operators interact with a human-machine interface (HMI) to control the SCADA server. This provides the ability to remotely monitor and control the substation. The substation contains a remote terminal unit (RTU) that aggregates data from an intelligent electric device (IED), which performs various sensing and actuation functions. Additionally, all data flows between trust zones are considered untrusted as they are potentially vulnerable to external attack.

The information transmitted within the system is fairly limited. Since only one IED
Table 3.1  Example security mechanisms and privileges

<table>
<thead>
<tr>
<th>SYSTEMS</th>
<th>SECURITY MECH./PRIVILEGES</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN 1</td>
<td>Enc1</td>
<td>VPN encryption algorithm</td>
</tr>
<tr>
<td></td>
<td>Ath1</td>
<td>Management authentication</td>
</tr>
<tr>
<td></td>
<td>P1</td>
<td>VPN network access privilege</td>
</tr>
<tr>
<td></td>
<td>P2</td>
<td>VPN management privilege</td>
</tr>
<tr>
<td>VPN 2</td>
<td>Enc1</td>
<td>VPN encryption algorithm</td>
</tr>
<tr>
<td></td>
<td>Ath2</td>
<td>Management authentication</td>
</tr>
<tr>
<td></td>
<td>P1</td>
<td>VPN network privilege</td>
</tr>
<tr>
<td></td>
<td>P2</td>
<td>VPN management privilege</td>
</tr>
<tr>
<td>SCADA</td>
<td>Ath3</td>
<td>Administrator authentication</td>
</tr>
<tr>
<td>Server</td>
<td>AC1</td>
<td>OS access control</td>
</tr>
<tr>
<td></td>
<td>P4</td>
<td>Server access privilege</td>
</tr>
<tr>
<td>HMI</td>
<td>Ath4</td>
<td>Operator authentication</td>
</tr>
<tr>
<td></td>
<td>P5</td>
<td>HMI access privilege</td>
</tr>
</tbody>
</table>

is utilized on each substation, only the following information is necessary to control the IEDs from the control center:

1. Operate Breaker (Control Center → RTU → IED)
2. Status Reading (Control Center ← RTU ← IED)
3. Voltage Reading (Control Center ← RTU ← IED).

In order to protect this environment from cyber attacks, security mechanisms must be provided to specifically target the untrusted areas. Fig. 3.3a) extends the original DFD to model the necessary set of security mechanisms required to protect the system from malicious attack. Table 3.3.1 explains these security mechanisms in greater detail. This information will be utilized in the proposed model development along with the definition of information necessary to support the system.
Figure 3.3  a) Testbed DFD with security mechanisms, b) Resulting exposure graph
3.3.2 Exposure graph development

This section introduces the exposure graph which formalizes the relationship between the security mechanisms, privileges and information objects within a system. The relationship between these objects will then be evaluated to determine the exposure of the information objects through the analysis of feasible attack paths. This exposure graph, defined as the directed graph $G = (SM, P, IO, A, E)$ contains the following vertex and edge definitions:

- $SM$ - vertex (security mechanisms)
- $P$ - vertex (system privileges)
- $IO$ - vertex (information objects)
- $A$ - vertex (untrusted users)
- $E$ - edges (directed)

Developing the exposure analysis graph should begin by identifying the untrusted data flows within a network. This is modeled through a node, $A$, that represents potential attackers access. This node should connect to all possible systems accessible by the attacker. Since the system’s security policy should ensure untrusted users cannot access any system resources without first bypassing some security mechanisms, all edges from $A$ should connect to the set of accessible mechanisms $SM$ and apply an edge weight of 1 to represent the attack effort required to bypass this mechanism. Each node in $SM$ should then be connected to the set of privilege nodes, $P$, representing the set of privileges obtained if this security mechanism fails, these nodes should have a weight of 0. Edges can also exist between the privileges, as a privilege $p_i$ could dominated another privilege $p_j$ if it contains a superset of privileges. In this case a directed edge would be $(p_j, p_i)$ added with a weight of 0. Finally information object, $IO$, nodes must be created
for each object in the CIM for that architecture. A directed edge should then be placed between each node in \( IO \) and the set of nodes in \( P \) that either consume or produce that information. Fig. 3.3b) provides an example of the resulting exposure graph developed based on the DFD in Fig. 3.3a).

### IOExposureAnalysis

Input: \( G = (\{SM, P, IO, A\}, E) \)

Output: \( exp \)

for all \( io \in IO \) do

\[ exp_{io} = EvalPath(io, \{\}, 0) \]

end for

### EvalPath()

Input: \( node, VisitedSM, length \)

if \( node \in A \) then

\[ return \frac{1}{max(len,0.1)} \]

else if \( node \in P \) then

for all \( i \in incident(node) \) do

\[ evalPath(i, VisitedSM, length) \]

end for

else if \( node \in SM \) then

if \( node \notin VisitedSM \) then

\[ VisitedSM = VisitedSM \cup node \]

for all \( i \in incident(node) \) do

\[ evalPath(i, VisitedSM, length + 1) \]

end for

end if

end if

end if

Algorithm 1 Exposure analysis algorithm

### 3.3.3 Exposure evaluation

After the exposure graph has been developed, analysis can be performed to evaluate the exposure of the information objects. The exposure metric \( exp \) determines the attack surface of an information object as it traverses through various systems and networks. The exposure metric is computed through the analysis of all security mechanisms utilized to protect the set of privileges that either produce or consume the information object.
Metric computation incorporates the number of attack paths through the security mechanisms protecting this asset while also factoring the path length as a method to evaluate the effort required to exploit a path.

Algorithm 1 documents the exposure metric calculation for the information objects within the graph $G$. Starting from each $IO$ node, the algorithm identifies all privilege nodes with incoming edges into $IO$. Each incident edge is reviewed for neighboring nodes until the paths are traced back to $A$. Since edges incident to an element of $SM$ are assigned with a weight of 1, paths length will be determined by number of $SM$ elements within that path. Once a potential attack path has been traced back, the inverse of that path’s length is the added to the exposure value for that information object. After all relevant attack paths have been traced, the resulting $exp_{io}$ value can be determined.

The documented algorithm outputs an exposure computation for each information object. In this example, all three objects are communicated along the same path and will result in the same $exp$ value. For this example the computed exposure for all 3 information objects is 4. This score is determined as there are only four potential paths, each with a length of one, required to access the $IO$ set. These paths are $\{A, Ath1, P2, P1, IO\}$, $\{A, Enc1, P1, IO\}$, $\{A, Ath2, P3, P1, IO\}$, and $\{A, Enc2, P3, P1, IO\}$. The remaining paths are not relevant since once privilege $P1$ has been obtained the attacker can gain access to the $IO$ set without requiring any additional effort. Section 3.5 provides a more detailed evaluation with increased $exp$ variations.

### 3.4 Exposure metric applications

This section presents applications of the exposure metric to assist in the development and management of a robust cyber infrastructure. Fig. 3.4 identifies three proposed metric applications including: vulnerability and impact analysis, cyber security investment optimization, and contingency analysis within cyber resources.
3.4.1 Vulnerability analysis

Computer systems are continuously affected with new vulnerabilities which present security challenges and unknown system impact. As documented within the NIST Risk Framework, continuous monitoring for possible security weaknesses is an important aspect of a strong risk management process. The first step in the monitoring process should be the collection of new information on possible threats or attack trends. Information sources should include security alerts from US-CERT and product vendors, individual vulnerability assessment results, intrusion detection alerts and system events occurring within the environment.

Exposure analysis should be re-computed during the continual monitoring process and whenever significant changes have been found within system security mechanisms. The re-computation should address all information sets that depend on the security mechanisms in concern. For example, a failure of security mechanism $sm_i$ will propagate to some privilege set $P'$ and also some information object set $IO'$. Determining the exact exposure can be done by setting $w(e(\{x\}, sm_i)) = 0$ where $x$ represents all incident nodes, since the mechanisms can no longer be trusted to protect the system. The resulting exposure analysis should then be re-computed to determine the new, increased exposure due to the shortening of the path lengths.
Once the re-computation of all exposure values have been performed, the resulting architecture can be reviewed for its adequacy. The vulnerability's impact on critical information may leave it in an unacceptably exposed state. In this situation additional security mechanisms would be necessary. An example of this analysis is shown in Section 3.5.2.1.

### 3.4.2 Cyber security investment optimization

Determining the effectiveness of cyber security enhancements presents a difficult strategy in large, distributed environments. Numerous possible investment strategies could be utilized to reduce the probability of a successful cyber attack. Two possible enhancement, $E_1$ and $E_2$, may have very different impacts on an infrastructure’s security as they protect different subsets of privileges on different systems. The exposure metric provides a novel mechanism to compare the resulting additional security provided by the additional enhancements.

Enhancements can be evaluated by redeveloping the $SM$ set to represent the infrastructure assuming the enhancement has been deployed. Once the new graph has been developed, the exposure can be re-computed and then utilized to compare various enhancements to determine their ability to protect critical information objects. Section 3.5.2.2 provides a detailed example of performing security enhancement evaluations.

### 3.4.3 Cyber contingency analysis

Traditional compliance within power system requires n-1 and n-2 contingency throughout the physical components [81]. However, there is limited current understanding of whether cyber architectures remain survivable during security failures. Cyber contingency analysis should be targeted towards the information required to support the physical system. By analyzing $IO$ sets and the $SM$ sets that enforce the current security policy, direct correlations can be made between failures of cyber security mechanism and
Table 3.2 Example security mechanism for an AMI architecture

<table>
<thead>
<tr>
<th>Domain</th>
<th>Device/Protocol</th>
<th>Security Requirement</th>
<th>Implementation Type</th>
<th>Protected Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>HAN GW</td>
<td>Authentication</td>
<td>x.509 Cert (Meter)</td>
<td>Individual HAN gateway</td>
</tr>
<tr>
<td></td>
<td>Zigbee</td>
<td>Encryption</td>
<td>Link/Network Key Exchange</td>
<td>All HAN gateways &amp; meters</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Link/Network Algorithm</td>
<td>All HAN gateways &amp; meters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authentication</td>
<td>Network Key</td>
<td>Individual HAN gateway &amp; meter</td>
</tr>
<tr>
<td>NAN</td>
<td>Meter</td>
<td>Physical Authentication</td>
<td>Meter-NAN private key</td>
<td>Individual meter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key Establishment Access Control</td>
<td>DAC (customer/mgmt function)</td>
<td>Individual meter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>All meters</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>All meters</td>
</tr>
<tr>
<td></td>
<td>Zigbee</td>
<td>Encryption</td>
<td>Link/Network Key Exchange</td>
<td>All NAN meters</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Link/Network Algorithm</td>
<td>All NAN meters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authentication</td>
<td>Network Key</td>
<td>All NAN meters</td>
</tr>
<tr>
<td>FAN</td>
<td>Headend</td>
<td>Authentication</td>
<td>x509 Cert (Meter)</td>
<td>Individual meter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key Signer</td>
<td>Key Signer</td>
<td>All FAN Stations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DAC (inter-customer)</td>
<td>DAC (inter-customer)</td>
<td>All FAN Stations</td>
</tr>
<tr>
<td></td>
<td>WiMax [7]</td>
<td>Authentication</td>
<td>x509 (meter), EAP</td>
<td>All FAN Stations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key Establishment Encryption</td>
<td>KEK, TEK</td>
<td>All FAN Stations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DES/AES (Payload)</td>
<td>All FAN Stations</td>
</tr>
<tr>
<td>Enterprise LAN</td>
<td>MDMS</td>
<td>Authentication</td>
<td>x509 Cert (Headend)</td>
<td>All FAN Stations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Control</td>
<td>DAC (inter-customer)</td>
<td>All FAN Stations</td>
</tr>
</tbody>
</table>
physical system occurrences. Additionally, this could instigate the development of cyber contingency analysis policies which mirror those found within physical systems.

### 3.5 Metrics evaluation

To evaluate the metric’s applicability within a smart grid environment, this section presents an example AMI architecture and then computes the resulting exposure calculations based on various cyber security relevant events. These results are then interpreted to demonstrate the metric’s applicability to this environment.

#### 3.5.1 Simulated environment

The simulated environment will model an AMI architecture that includes a HAN domain containing user meter gateways, a NAN domain containing smart meters, and FAN domain containing an AMI headend and Meter Data Management System (MDMS). Both the HAN and NAN networks will be assumed to be using a wireless network such as Zigbee while the FAN is assumed to utilize a wireless WiMax network.
Table 3.3 Example set of information objects

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Data Objects</th>
<th>IEC 61968-9 [51]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Meter Reading</strong></td>
<td>1. Read Request</td>
<td>MeterReadSchedule</td>
</tr>
<tr>
<td></td>
<td>2. Usage (Response)</td>
<td>MeterReadings</td>
</tr>
<tr>
<td></td>
<td>3. Usage (Protected)</td>
<td></td>
</tr>
<tr>
<td><strong>Meter Disconnection</strong></td>
<td>4. Off Message</td>
<td>EndDeviceControl</td>
</tr>
<tr>
<td></td>
<td>5. Confirm: Meter</td>
<td>EndDeviceEvent</td>
</tr>
<tr>
<td><strong>Meter Firmware Upgrade</strong></td>
<td>6. Firmware update</td>
<td>EndDeviceFirmware</td>
</tr>
<tr>
<td></td>
<td>7. Execute firmware</td>
<td>EndDeviceFirmware</td>
</tr>
<tr>
<td></td>
<td>8. Status check</td>
<td>EndDeviceEvent</td>
</tr>
</tbody>
</table>

The information model for the simulation is based upon a subset of the AMI Use Cases published by Southern California Edison’s (SCE) [93]. Fig. 3.5 reviews the use-cases which provided a basis for system requirements for this simulation and demonstrate the flow of information between systems.

Based on these use cases, Table 3.3 provides a description of the information objects referenced in Fig. 3.5 and also cites likely attributes from an IEC 61968-9 based CIM. Future analysis within this section will reference the exposure of these information objects.

A set of security mechanisms is also presented to provide a realistic set of protections. Table 3.2 documents all of the assumed security mechanisms utilized to protect the various systems and networks within this environment. The Protected Privileges column is utilized to determine the set of systems privileges that are protected by the resulting security mechanisms.
3.5.2 Simulation Results

Based on the previously proposed environment we perform the resulting exposure computation and then provide demonstrations of the impact on the systems security.

![Exposure metrics for normal/vulnerable scenarios](image)

**Figure 3.6** Exposure metrics for normal/vulnerable scenarios

3.5.2.1 Vulnerability assessment

Fig. 3.6 provides the result from the exposure calculation on the simulation environment. The Normal State calculations provide the evaluation of a system that is operating in its intended state and is not impacted from any outstanding security concerns. Note that IO1-IO2 and IO4-IO8 maintain similar exposure values due to their similar paths throughout the network while IO3 has a limited exposure based on an assumption that certain granular meter readings with privacy concerns are protected by only being stored on the meter. Next the exposure for the same architecture is evaluated with the following two vulnerability scenarios.

- A. Compromised meter management authenticator
• B. Vulnerable meter customer/management access control

Fig. 3.6 also provides the resulting exposure calculations after vulnerability A is discovered. In this simulation it is assumed that vulnerability A has compromised the certificate utilized to perform meter management function which provides the attacker with the ability to modify configuration data and obtain access to some usage data. Note that the resulting exposure of all information objects except IO3 have significantly increased, IO3 exposure still remains relatively low since the meter’s access control mechanism enforces separation between granular customer reading and management functions.

Next, assume that a vulnerability B is discovered which allows the bypassing of the meter’s customer/management access control mechanism. This vulnerability significantly increases the exposure of IO3, but does not notably increase that of IO1 and IO2 as they are already accessible from both the customer and management privileges. Also, note that meter firmware upgrade information, IO6-IO8, and meter management information, IO4-IO5, have been significantly increased. Since this information was originally protected from customer access, but now may be potentially exposed due from the resulting vulnerability.

3.5.2.2 Security investment

In addition to the vulnerability and impact assessment application, evaluation results have also been utilized to demonstrate the exposure metrics utility within the security investment process. The current exposure value of various resources is first evaluated on the system’s normal state, then the exposure resulting from the insertion of additional security mechanism is performed and the resulting exposure is computed to evaluate the improvement.

Fig. 3.7 provides the results of the enhancements. The x-axis contains the various security enhancement results. The first set labeled 'Orig' assumes no enhancement has occurred. The next two sets of results assume that enhancement E1 and E2 have been
implemented individually while the final set assumes that both $E1$ and $E2$ have been implemented together. The proposed enhancements for this evaluation include:

- **E1** - Application layer authentication/encryption
- **E2** - Tamper resistant meter hardware

The first enhancement, $E1$, assumes that the additional encryption and authentication is being performed on the meter application level (i.e. IEC 61850) which, for example could be implemented by the IEC 62351 security protection standard. This would increase the amount of effort required for an attacker to access this information when it is in transit between the system. The second enhancement, $E2$, assumes a tamper resistant hardware is utilized within the environment which limits the smart meters accessibility to physical attacks.

The results show that the additional encryption and authentication provide a greater impact to the general system’s exposure and will likely constitute a more useful investment. This is primarily due to the fact that it protects information throughout its life.
span as opposed to $E2$ which focuses primarily on the protection of data-at-rest within the meter. However, the combination of both $E1$ and $E2$ further reduce the exposure for the resources, although there still remains a number of potential attack vectors.
CHAPTER 4. MODEL-BASED HIERARCHICAL INTRUSION DETECTION FOR THE SMART GRID (MHINDS)

4.1 Introduction

These concerns present a strong need for tailored security mechanisms, such as IDSs, to be developed to ensure these systems can operate in a secure state. NIST 7628, “Guidelines for Smart Grid Cyber Security”, identifies the need for future IDS technology with a “deep contextual understanding of device operation and state to be able to detect when anomalous commands might create an unforeseen and undesirable impact” [80].

Attacks against the electric power grid will likely combine elements of traditional cyber attacks, along novel techniques tailored towards smart grid elements. While a major attack has not yet targeted the smart grid, the recent Stuxnet malware presents an example of sophisticated cyber-physical attack [36]. Stuxnet provided an example where a cyber attack propagated from traditional ICT systems into the control domain, resulting in a malicious reconfiguration of field devices. Once this occurred, the field devices were used to manipulate the physical domain by sending fraudulent control packets to manipulate the operation of the attached centrifuges. While many current current IDS techniques focus on detecting traditional ICT attacks, methods to detect malicious control system communications are currently needed.

In a smart grid context, IDS approaches are needed which understand the models of system communications and the smart grid applications which they support. Fig. 4.1
Figure 4.1 Traditional IT and smart grid IDS approaches

demonstrates how traditional IDS approaches must be expanded to incorporate the cyber-physical properties of the smart grid. While multiple research projects have focused on incorporating smart grid protocols into current IDS approaches, future work is needed to demonstrate how these efforts can incorporate increased physical system awareness.

This research presents a novel intrusion detection approach which specifically targets the salient network characteristics of the smart grid. The proposed approach expands upon current IDS efforts targeting the electric grid by exploring the networks data flows required to support different power system applications. It then identifies how attacks against the network will establish both temporal and spacial anomalies within the data flows. This research then presents a Petri-net based model and associated algorithms to detect attacks within individual substations and correlate them across the entire power system.

### 4.2 Related work

IDS are a well explored research area within the computer security field. Numerous approaches have been studied to characterize potential malicious activity within both
computers and networks. IDS technologies are primarily categorized based on how they
gather information and analyze this information.

Information gathering techniques include both host-based and network-based approaches [10]. Host-based intrusion detection methods focus on detecting malicious operations within the software running on a system. This generally requires the installation of an
IDS agent on the host to analyze the various system calls and network activity in order to identify malicious behavior. Network-based approaches focus on detecting malicious activity based on the analysis of the network events.

IDS approaches can be further categorized by the method they use to distinguish benign and malicious activity. These approaches can be categorized as anomaly-based, misuse-based, and specification-based methods [10]. Each of these methods will be explained below, along with smart grid related research efforts.

4.2.1 Misuse-based IDS

Misuse-based IDS focuses on the development of signatures to match known nefarious network events. This method is frequently used by many commercial IDS tools, such as Snort, which performs pattern matching of all network traffic against a database of known attack signatures [92]. Misuse-based IDS can generally perform highly accurate attack detection, but their efficacy is predicated on the assumption that the database contains signatures for all possible attacks against the system. If this assumption fails, an attack will remain undetected. Specific misuse-based IDS research has been explored for various industrial control systems. DigitalBond creates misuse-based IDS Snort patterns to help mitigate against known control system vulnerabilities [28]. However, many unknown vulnerabilities are likely to exist within smart grid control systems without published signatures [46].
4.2.2 Anomaly-based IDS

Anomaly-based IDS is based on the development of models representing normal system behaviors and then using these models to flag anomalous system behaviors as potentially malicious. Therefore, this approach does not fall under the same limitations of signature-based IDS as it does not need to be previously aware of all possible vulnerabilities in order to detect them. However, because not all anomalous behavior is actually malicious, this often leads to high false positive rates from benign anomalies [39].

Numerous efforts have explored anomaly detection approaches within the smart grid. Work performed by Rrushi has specifically targeted the operation of electric grid substation stations [87]. This work presented a probabilistic approach for detecting malicious IEC 61850 communication patterns based on stochastic models. While this work introduces the probabilistic correlation of substation operations, it does not demonstrate how this analysis could be fully incorporated into an IDS. Additionally, accurate probabilities for this approach cannot be easily calculated. Ten, et al. explored methods to correlate anomalous system functions with the impact the attack would have on the loss of load (LOL) in a power system [97]. Anomalies in this work focused on authentication failures, file system changes, and IED reconfiguration. While this work presents novel approaches for correlating cyber and physical events, it does not explore the specific operations of the smart grid communications and protocols.

4.2.3 Specification-based IDS

Specification-based detection methods require the development of formal specification of normal system operations. The system state is then continually verified by the IDS to ensure it does enter a malicious state. While specification-based can achieve low false positive rates similar to misuse-based detection, developing the specification remains a challenging task [103].

Specification-based IDS techniques have been explored for AMI by Berthier and
Sanders [9][8]. This work develops specifications based on the ANSI C12.22 communication protocol for AMI and verifies both network and application layer properties. While specification-based methods can accurately model the state of the network communications, they have not been used to capture the physical system properties of various smart grid applications.

4.2.4 Model-based IDS

Cheung, et al. originally explored the development of a model-based SCADA detection technique focusing on deriving detection methods based on the known characteristics of the physical system and the intended operations of the supporting communication network [16]. This work specifically analyzed communications following known static communication patterns, hosts, and data values for an industrial control system.

MHINDS extends this approach by focusing on the development of a model-based IDS for substation communications. It augments previous work by incorporating spatial and temporal characteristics of substation application communication requirements and physical system properties. Additionally, it demonstrates the feasible bounds for detecting malicious activity in a substation based on known preconditions and through the ability to correlate events across substations.

MHINDS utilizes a Petri net model to detect intrusions by modeling system states and identifying malicious transitions. Petri net models has been previously used as a means to perform pattern matching of malicious computer states [57].

4.3 Threats to substation automation functions

Substations present a serious threat from cyber attack because their systems have weaker physical security than control center systems. Also, substations frequently depend on unsecured wireless communication protocols. Attacks against substations could
be catastrophic as the incorrect operation of circuit breakers could significantly impact grid stability. For example, 75% of major grid disturbances can be attributed to the misoperation of protection systems [110]. Therefore, this research will explore how intrusion against substations could lead to power failures based on known physical system faults.

Substation automation functions include both human-in-the-loop and closed-loop operations. Human-in-the-loop operations often include operators opening and closing breakers for maintenance purposes and manipulating tap positions on transformers. Closed-loop functions, such as protection schemes, are used to de-energize lines in the case of a fault to protect systems from damage. These systems rely on near real-time operation and, therefore, do not depend on human involvement. Substation automation applications are typically distributed across the substation’s various HMIs, RTUs, and field devices. This work will specifically look at applications used to control the operation of the circuit breakers and switches which are a core means for controlling power flow in the grid.

4.3.1 Protection schemes

Protection schemes are a more complex substation function and are the core mechanisms of protecting power system components from various faults. Protection schemes protect grid components, such as transformers and generators, from faults by initiating the opening of circuit breakers and de-energizing the lines, thereby letting the fault clear out of the system. Once the fault clears, the scheme can re-close breakers and allow the grid to return to normal operating conditions. Protection schemes employ various algorithms to infer faults in a power system based on inputs from current and voltage transformers [102][55].

Protection zones: Protection schemes are designed around the components they intend to protect. Major components such as transmission lines and buses will have
schemes specifically configured to provide protection for faults on that component. The schemes will then overlap due to the interconnectivity of components. Since a protection schemes failure to operate may result in substantial damage, schemes are allocated into zones which provide backup protection in case one device in a scheme fails to operate correctly.

Protection reliability properties: The reliability of a protection scheme is defined by the combination of its dependability and security [83], where security is referenced in the power domain, as opposed to cybersecurity. These terms can be defined as follows:

- **Dependability** of the protection system can be defined as “the ability to detect and respond to a fault in a correct and timely manner [102].” The electric grid’s dependability is based on both 1) the protection schemes ability to detect the fault, along with 2) the ability to differentiate the faults within or external to a breaker’s protection zone.

- **Grid Security** of a protection system is defined as “the quality of not operating for faults outside the zone of protection or not operating under heavy load conditions” [102].

Substations are typically engineered towards dependability [25]. Protection scheme zones provide added dependability as they ensure that faults are appropriately cleared in the event of a failed relay. Additionally, these systems also incorporate breaker failure functions to ensure nearby breakers can be tripped in the event of a failed breaker.

Substations have much lower margins for grid security. The misoperation of a protection function, such as a “undesired tripping” presents a major concern for power system reliability [116]. Multiple undesired tripping will result in multiple lines being removed from the power system, which has been demonstrated the protection scheme “hidden failure” problem. This presents a clear violation of the grid’s N-1 contingency analysis [25].
4.3.2 Threat model

A cyber attack could result in the previously identified security and dependability violations if it is capable of injecting or denying the required protection scheme communications. Fig. 4.2 demonstrates how cyber attacks which violate a system’s integrity and availability requirements could result in security and reliability failures. In order to initiate a failure to operate or an undesired tripping event, this research assumes an attacker would able to compromise a substation devices, specifically a relay or HMI, to send malicious commands. Therefore, MHINDS focuses on the identification of malicious operations of the substation’s various systems by attempting to distinguish both benign and malicious communications that could impact these reliability properties.

4.4 MHINDS detection methodology

The MHINDS intrusion detection methodology consists of three major components. First, a model of a substation communication architecture is developed using a Petri net representation of the various devices and communications. Next, the Petri net model is used to monitor and detect malicious packets transmitted in the network at the substation level. Finally, the results from the substation level analysis is used as an input for system
level analysis which correlates multiple substation inputs to detect coordinated attacks and validate physical system events.

Fig. 4.3a) demonstrates the hierarchical approach of MHINDS. Agents are deployed in substations to perform local detection algorithms and collect potential alerts. This data is then transmitted back to the control center across the same communication channel as the other SCADA information. Within the control center, system level analysis is then performed on all collected data. Fig. 4.3b) presents a flow chart which documents the flow of model development which includes network traffic, substation topologies, and system wide topologies. Additionally, it demonstrates the flow of local alerts from the station level analysis to the system level analysis components.

4.4.1 Substation level detection

The MHINDS detection algorithm is based on a Petri net model representing the substation communications. Much of the information to develop this model is located in the substation’s SCD file, including the various physical devices, logical devices, and communications in a substation. This model will then be used to evaluate the network to ensure it does not enter a malicious state. Once this model has been created, incoming packets will be continually analyzed against the Petri net model to detect incorrect
A Petri net model consists of a tuple, $N = (P, T, F, M_0)$, where $P = \{p_1, p_2, \ldots, p_m\}$ represents the set of places, $T = \{t_1, t_2, \ldots, t_n\}$ represents the set of transitions, $F \subset (P \times T) \cup (T \times P)$ is a mapping of the flow of markings between places, and $M_0$ is an initial marking. Additionally, $\sigma$ represents the sequence of transitions that have previously fired. This model also incorporates both cyber and physical system states and transitions. These are divided into the following sets, $P_p \cup P_h \cup P_d = P$ and $T_p \cup T_n = T$, which are further defined below.

- $P_p$ - physical system states (e.g., breaker closed/tripped)
- $P_d$ - cyber host states (e.g., device’s perception of a breaker’s status)
- $P_h$ - current states of human operators (e.g., human initiation of a breaker command)
- $T_p$ - physical system transitions (e.g., breaker closing/tripping)
- $T_n$ - cyber network events (e.g., IEC 61850 message between systems)

For this work, an example substation will be demonstrated based on the control and protection functions identified in Section 2.2.2. Table 4.1 identifies the elements that will be used in this Petri net. Notice that the elements of $T_d$ and $P_d$ contain the same elements names. This is because the GOOSE communications publish their status to the network as a means to communicated their state changes. A transition is defined as firing when this status changes.

$D$ represents the set of all devices in the substation where an individual device, $d_i$, includes a set of places (LNs) and the transitions representing the published GOOSE data for that LN. The set of published GOOSE data for each $d_i$ will be the set $d'_i$ accordingly. Based on the Petri net demonstrated in Fig. 4.4, these sets will be allocated as shown in Table 4.1.
Table 4.1 MHINDS Petri net places

<table>
<thead>
<tr>
<th>Domain</th>
<th>Device</th>
<th>Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_p$</td>
<td>-</td>
<td>CB_On CB_Off Fault E_CB_Off</td>
</tr>
<tr>
<td>$T_p$</td>
<td>-</td>
<td>CB_Off_t CB_On_t Fault_t</td>
</tr>
<tr>
<td>$P_h$</td>
<td>(d_1)</td>
<td>IHMI</td>
</tr>
<tr>
<td>$T_h$</td>
<td>(d_1)</td>
<td>IHMI_t</td>
</tr>
<tr>
<td></td>
<td>(d_2)</td>
<td>CSIW_t</td>
</tr>
<tr>
<td></td>
<td>(d_3)</td>
<td>PDIS_t PTRC_t RREC_t RBRF_t</td>
</tr>
<tr>
<td>$P_d$</td>
<td>(d_2)</td>
<td>CSIW</td>
</tr>
<tr>
<td></td>
<td>(d_3)</td>
<td>PDIS PTRC RREC RBRF</td>
</tr>
<tr>
<td></td>
<td>(d_4)</td>
<td>XCBR_S_On XCBR_S_Off XCBR_C_On XCBR_C_Off</td>
</tr>
</tbody>
</table>

Figure 4.4 Substation Petri net model
4.4.1.1 Identifying malicious devices

MHINDS detects malicious substation operations by verifying that all transitions can be correlated by some set of enabling transitions which occur in either cyber, physical, or human domains. A device, $d_i$, should only be able to initiate a transition if the set of transitions which have enabled places of that device also fired. Therefore, MHINDS classifies malicious and benign transitions as follows.

$$
t = \begin{cases} 
M + A[t] \geq 0 & t \text{ is benign} \\
M + A[t] < 0 & t \text{ is malicious}
\end{cases}
$$

The set of enabling transitions can be verified by inspecting the transitions and places in the Petri net’s incidence matrix, $A$. $A_{(m,n)}$ is a matrix, such that $A_{(i,j)} = -x$ if $x$ is the number of markings which transition $t_j$ removes from place $p_i$, while $A_{(i,j)} = x$ if transition $t_j$ adds $x$ markings to $p_i$, finally $A_{(i,j)} = 0$ if transition $t_j$ does not impact the markings of $p_i$. Below is an example of matrix $A$ as defined for the example Petri net in Fig. 4.4.

$$
A = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & -1 & 1 & 0 \\
0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 1 & -1 & 0 & 0
\end{bmatrix}
$$
When a transition fires, MHINDS will attempt to validate whether the places which enable that transition have sufficient markings. This set of enabling places, referenced as \( E(d^t_i) \), is defined below.

\[
E(d^t_i) = \{ p | A_{p,t} < 0 \land t \in d^t_i \}
\]

Because MHINDS focuses only on network layer detection, it cannot validate the markings of \( E(d^t_i) \). Instead, it must identify malicious behavior by analyzing the presence of the transitions that enable these places based on previously identified transition. The set of transitions that can verify markings in the set \( E(d^t_i) \) is defined as the set, \( V(d^t_i) \).

\[
V(d^t_i) = \{ t | A_{p,t} > 0 \land p \in E(d^t_i) \}
\]

Based on this analysis, the various transitions in Fig. 4.4 will be explored for each device to determine the set of transitions that must be explored in order to validate a suspected transition.

### 4.4.1.2 Detection classes

This work proposes the following detection classes for transitions based on the information required to validate their firing. These classes will then be used to explain how the various transitions in Fig. 4.4 can be identified.

- **Network Verified** - The transition can be validated based solely on the presence of previous network transitions, \( \{ \forall t | t \in V(d^T_i) \land t \in T_n \} \).

- **Physically Verified** - The transition cannot be validated based solely on previous network transitions and requires additional analysis of physical system events, \( \{ \exists t | t \in V(d^T_i) \land t \in T_p \} \).
• Human Verified - The transition cannot be validated based solely on previous network transitions and requires additional analysis of operator actions, \( \{\exists t | t \in V(d^T_i) \land t \in T_h\} \).

Based on these sets, Table 4.2 categorized all the devices located in the example Petri net, including the transitions, impact, \( E(d^t_i) \), \( V(d^t_i) \), and the detection class for each transition.

4.4.1.3 Substation level detection algorithm

MHINDS implements a detection algorithm based on the previously identified approach for validating the firing of a transition. By exploring the transitions which cause invalid markings it can identify what network packets should and should not be sent in various states.

To perform this detection, MHINDS must store the current marking of the Petri net \( M_c \). Then all networked packets are correlated against known GOOSE messages and, if they are identified as such, they should be converted to the appropriate transition, \( t \). The transition is then explored to whether \( M_c \) contains the appropriate places are marked to ensure \( t \) can fire.

The proposed algorithm is identified below, assuming \( M_c \) is the current marking, \( \beta \) represents an incoming GOOSE packet’s LN and object. \( \beta \) is first checked to see if it resides in the set of valid GOOSE packets and flags an invalid formate alert otherwise. Then it is checked to see if the transition is equivalent to a the current marking or represents an updated state. If its the latter, \( \beta \) is considered a new transition. This transition is then checked to see whether it resides in the Physically Verified or Human Verified classes which trigger the system level analysis algorithm.
<table>
<thead>
<tr>
<th>System</th>
<th>Transition</th>
<th>Impact</th>
<th>Enabled Places</th>
<th>Verified Transitions</th>
<th>Detection Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>IHMI</td>
<td>IHMI</td>
<td>Breaker Trip (Local)</td>
<td>IHMI ($P_h$)</td>
<td>null ($T_h$)</td>
<td>Human Verified</td>
</tr>
<tr>
<td>Control IED</td>
<td>CSWI</td>
<td>Breaker Trip (Local)</td>
<td>CSWI ($P_d$)</td>
<td>IHML_t ($T_n$)</td>
<td>Network Verified</td>
</tr>
<tr>
<td>Protection IED</td>
<td>PDIS</td>
<td>Protection Enabled</td>
<td>PDIS ($P_d$)</td>
<td>Fault ($T_p$)</td>
<td>Physically Verified</td>
</tr>
<tr>
<td></td>
<td>PTRC</td>
<td>Breaker Trip (Local)</td>
<td>PTRC ($P_d$)</td>
<td>PDIS_t ($T_n$)</td>
<td>Network Verified</td>
</tr>
<tr>
<td></td>
<td>RREC</td>
<td>Breaker Close (Local)</td>
<td>RREC ($P_d$)</td>
<td>PTRC_t ($T_n$)</td>
<td>NetworkVerified</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>XCBR_S_Off</td>
<td>XCBR_S_Off_t ($T_n$)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RBRF</td>
<td>Breaker Trip (External)</td>
<td>RBRF ($P_d$)</td>
<td>PTRC_t ($T_d$)</td>
<td>Network Verified</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>XCBR_S_On</td>
<td>XCBR_S_On_t ($T_n$)</td>
<td></td>
</tr>
</tbody>
</table>
Input: \( M_c, \beta, SCD \)

\[
\text{if } \beta \in SCD \text{ then} \\
\quad \text{if } \beta_v \neq M_c(\beta) \text{ then} \\
\quad \quad t \leftarrow \beta \\
\quad \quad \text{if } t \in \text{Physically Verified} \cup \text{Human Verified} \text{ then} \\
\quad \quad \quad \text{SystemLevel()} \\
\quad \quad \text{else} \\
\quad \quad \quad \text{for all } i \in M \text{ do} \\
\quad \quad \quad \quad \text{if } M_i + A_{i,t} < 0 \text{ then} \\
\quad \quad \quad \quad \quad \text{Alarm(Unreachable } t) \\
\quad \quad \quad \quad \text{end if} \\
\quad \quad \quad \text{end for} \\
\quad \quad \text{end if} \\
\quad \text{end if} \\
\text{end if} \\
\text{else} \\
\quad \text{Alert(Invalid Format/Source } t) \\
\text{end if}
\]

Algorithm 2 Station level detection

### 4.4.2 System level detection

As explained in Section 4.4.1.1 the operation of protection systems cannot be deterministically detected due to the difficulty in verifying a fault. However, as identified in Section 4.3, protection schemes rely on multiple layers of redundancy in order to ensure dependability. Protection schemes will generally have independent main, primary backup, and secondary backup protection relays deployed to ensure a fault can be adequately cleared. These relays are also typically allocated across multiple substations in case a failure at one substation prevents a relay from firing. This section will demonstrate how this level of redundancy can be leveraged to differentiate between benign and malicious protection operations.

Fault location algorithms are a well studied research area for power systems which explore various methods of correlating relay and breaker operation data in order to identify a fault while accounting for some degree of error in the protection scheme’s operations.
This work proposes a similar approach to demonstrate how attacks causing protection scheme operations could be detected.

Work in [61] introduces a 14-bus power system along with the logic for a set of protection schemes for both lines and buses. A line protection scheme will include main (MLRXXYY) and backup relays (BLRXXYY) on both ends of the line to provide primary backup, where XX and YY reference the buses at each end of the line. Additionally, secondary backup relays (SLRXXYY) will be included on substations adjacent to the main relays to provide secondary backup. A bus protection scheme is intended to protect a fault if it occurs on a bus. It will contain bus relay (BRXX) that trips all lines connected.
Table 4.3  Line and bus protection systems and relays

<table>
<thead>
<tr>
<th>FAULT</th>
<th>COMPONENT</th>
<th>RELAYS</th>
<th>SUBSTATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line1314</td>
<td>CB1314</td>
<td>MLR1314</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BLR1314</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SLR1213</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SLR0613</td>
<td>06</td>
</tr>
<tr>
<td></td>
<td>CB1413</td>
<td>MLR1413</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BLR1413</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SLR0914</td>
<td>09</td>
</tr>
<tr>
<td>Bus13 All</td>
<td>BR13</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>CB1312</td>
<td>BLR1213</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>CB1306</td>
<td>BLR0613</td>
<td>06</td>
<td></td>
</tr>
<tr>
<td>CB1314</td>
<td>BLR1413</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>Bus14 All</td>
<td>BR14</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>CB1413</td>
<td>BLR1314</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>CB1409</td>
<td>BLR0914</td>
<td>06</td>
<td></td>
</tr>
</tbody>
</table>

to a bus as the primary protection. As backup protection, it will use the BLRXXYY relays in those substations adjacent to the bus. Table 4.3 identifies the main, primary backup, and secondary backup protection schemes for line (Line1314) and for two buses (Bus13 and Bus14).

4.4.2.1 System level detection algorithm

This section introduces a system level detection algorithm to help identify whether breaker operations performed in substations can be validated by correlating events from other stations. The algorithm receives data from the substation level analysis algorithm and then determines whether the identified fault closely matches an expected protection scheme.

Assuming a protection scheme operates correctly, a fault should cause the entire set of relays in the device to detect the fault. Additionally, it should cause a number of relays to trip to ensure it is properly cleared. Therefore, if a fault is identified by a relay in a substation, it should also be identified by neighboring relays in neighboring
substations. This analysis will be based on a set of protection schemes, $PS$. Each $ps_i$ in $PS$ represents the set of relays used to protection bus or line $i$.

The algorithm’s inputs include $\sigma$ and $PS$. For this application $\sigma$ is assumed to only includes relay pickup and operation transitions from all substations and human initiated transitions. Additionally, $\theta$ is a threshold value that will be explained in Section 4.4.3.1. The algorithm verifies that for each breaker operation command (e.g., PTRC) there is a protection scheme whose associated relays have identified the faults. It does that by comparing the expected fault pickup elements in each protection scheme to those found in the set of protection related firings from the substation layer analysis. It then identifies the best fit based on the maximum number of relay pickups found in both sets. Finally, $k_{PTRC_i}$ is compared to see if it meets some detection threshold and then otherwise raises an alert.

```
Input: $\sigma$, $PS$, $\theta$
for all $PTRC_i \in \sigma$ do
    $k_{PTRC_i} = 0$
    for all $ps_j \in PS \cap PTRC_i \in ps_j$ do
        $k_{PTRC_i} = \max(k_{PTRC_i}, |ps_j \cap \sigma|)$
    end for
    if $k_{PTRC_i} < \theta_i$ then
        Alert $PTRC_i$
    end if
end for
for all $IHMI_i \in \sigma$ do
    Validate_Human()
end for
```

Algorithm 3  System level detection

4.4.3 Security analysis and evaluation

This section will explore the capabilities of the proposed system level detection algorithm. The objective of the evaluation is to explore the feasible bounds of the detection
approach against varying attack sophistication. Additionally, it will explore trade-offs in attack impacts, false positives, and false negatives.

4.4.3.1 False positives

The efficacy of the proposed approach requires that the number of false positives remain under some acceptable threshold. The algorithm only raises alerts when the number of observed relay pickups are below a threshold, $\theta$. Therefore, this section will infer the various sources of false positives, specifically from undesired relay tripping and failed relays, and then relate them to this threshold.

**Undesired tripping** A false positive will arise if the relay fails and initiates an “undesired tripping” event. Because the relay misoperates, there will not be any associated relays identifying the fault in the protection scheme. Therefore, this event will result in an alert and will strongly resemble a situation where a single relays is compromised and then initiated a trip. Fortunately, these events are very rare due to the reliability of relays. Research has documented that only 36 inadvertent trips occurred between 1984 and 1999 [71], therefore, this error type will not produce large number of false positives.

**Failed relay or communication** In addition to undesired trip events, false positives could occur due to errors in the pickup or operation of relays during an actual fault. This could either occur due to a failed relay or communication channel. In either case, all elements in $\psi_i$ will not be obtained by the system level analysis algorithm which will then return an error. This class of false positives presents a direct trade-off with the level of effort required for an attacker to perform an undetectable coordinated attack.

To compute the likelihood of a failed relay causing a false positive, every relays will be assumed to operate successfully with probability, $p$. Because there are multiple relays in each protection scheme, a failure in any one relay could cause the protection scheme to report back an incomplete set of values for each $\psi_i$. If all relays have the same
probability of success, then the probability of the protection scheme operating correctly
determined by $p^{|ps_i|}$. These values are demonstrated in Fig. 4.7, assuming the relays
operate successfully 90% (black) and 99% (gray) of the time.

To ensure the MHINDS does not consistently result in false positives, the number of
relay pickups that can reliably be expected to be identified should be reduced to account
for possible faults. By assuming that only a percentage of the relays can be expected to
operate for each protection scheme, a maximum bound can be identified to determine
number of relays that can be required to achieve some desired false positive rates. The
binomial distribution is used to compute a threshold value $k$, such that the probability of
a false positive stays under 5% based on some probability of relay success is $p$. Therefore,
some value $k$ is needed such that $Pr(X \leq 5\%) = \sum_{k=1}^{k} \binom{n}{k} p^k q^{n-k}$, where $n = |ps_i|$ is
the number of relays in the protection scheme and $q = p - 1$.

Fig. 4.8 demonstrates the number of relay threshold, $\theta_i$, that must successfully re-
port from each $ps_i$ in order to ensure a false positive rate below the desire threshold.
Figure 4.8  Max. relay pickups to ensure < 5% false positives

Notice that if the relays are 99% reliable, they more relays can be required by the analysis algorithm which increases the level of effort required for an attacker to perform an unobservable coordinated attack. Therefore, there is a direct correlation between relay reliability and the level of effort for an attacker to avoid detection.

4.4.3.2 False negatives

The system level analysis has detection limitations based on the number of devices an attacker is able to control. If the attacker intends to attack a protection scheme while remaining undetected, they must be able to successfully spoof the operations of all devices in some protection scheme, $ps_i$, in order to ensure that the events correspond the expected fault pickup and operation events. The occurrence where a protection scheme is a subset of the number compromised devices, $\theta_i \subseteq attacked(d_i)$, is defined as an undetectable coordinated attack as it will require the coordination of all devices within the targeted protection scheme.
Protection schemes for various system components will include a varying number of relays. Therefore, launching an undetectable coordinated attack against each scheme will require a varying effort for the attack based on the value of $\theta_i$. Fig. 4.9 demonstrates the level of effort for each attack based on the number of relays and substations an attacker must compromise in order to initiate an undetectable coordinated attack against that grid component from the system in Fig. 4.5.

### 4.4.3.3 Attack impact analysis

While Fig. 4.9 demonstrated the level of effort needed to launch an undetectable coordinated attack against one protection scheme, an advanced attacker may try to co-
ordinate attacks against multiple protection schemes in order to remove multiple system components simultaneously. The electric grid is currently operated on an N-1 contingency analysis which mandates that grid operators ensure grid reliability remains intact if any one component is removed. Therefore, a sophisticated attacker may focus on removing multiple system components in order to cause increased system damage.

Fig. 4.10 and Fig. 4.11 demonstrate the minimal level of effort in terms of number of relays and number of substations that an attacker must compromise in order to cause some number of de-energizing power lines assuming that main relays trip the breakers, assuming $\theta_i = |ps_i|$. These figures demonstrate that attacker level of effort scales accordingly to the number of power lines they intend to remove. While an attack that causes lines to be de-energized may result in neighboring lines being removed from the power system due to overload, this analysis assumes that attacks occur instantaneously and does not account for cascading failures.
Figure 4.11  Substation detectable vs undetectable attacks
CHAPTER 5. CPS SECURITY TESTBED FOR THE SMART GRID

5.1 Introduction

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

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

The remainder of the paper is organized as follows. Section 5.2 enumerates previous testbed development efforts and identifies salient features of those efforts. Section 5.3 introduces applications of a cyber security testbed based on current research demands and testbed capabilities. Section 5.4 provides an introduction of the PowerCyber testbed at Iowa State and presents a thorough review of its capabilities. Finally, Section 5.5 demonstrates the utility of the testbed by presenting various research efforts currently being performed in the environment.

<table>
<thead>
<tr>
<th>Testbed Cyber-Physical Security Research Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Vulnerability Research</td>
</tr>
<tr>
<td>2. Impact Analysis</td>
</tr>
<tr>
<td>3. Mitigation Research</td>
</tr>
<tr>
<td>4. Cyber-Physical Metrics</td>
</tr>
<tr>
<td>5. Data and Models Development</td>
</tr>
<tr>
<td>6. Security Validation</td>
</tr>
<tr>
<td>7. Interoperability</td>
</tr>
<tr>
<td>8. Cyber Forensics</td>
</tr>
<tr>
<td>9. Operator Training</td>
</tr>
</tbody>
</table>

Figure 5.1 Testbed applications

5.2 Related work

Smart grid testbed have been developed at various universities and national labs to research cyber security concerns. A foundational testbed initiative is the National SCADA Test Bed (NSTB) which represents a national lab collaborative project. This environment implements actual physical grid components including generation and transmission, while also incorporating industry standard software products [44]. Resulting research on the testbed has identified numerous cyber vulnerabilities and contributed to the production of SCADA-specific security assessment methodologies [45][69]. Unfortunately, the
substantial cost of deploying purely physical testbed limits the practicality of similar efforts.

Sandia National Laboratory developed the Virtual Control System Environment (VCSE) which integrates simulation, emulation, and physical systems to provide more cost-effective and reconfigurable platform [74, 72]. VCSE utilizes OPNET System-in-the-Loop emulation to allow the integration of physical network devices with the simulated network. This enables communication between both physical and emulated PLCs and the PowerWorld power system simulator. VCSE also utilizes a centralized model/simulation management tool, Umbra, to provide control over the various components. VCSE was designed to provide support for operator training, vulnerability exploration, mitigation development, and evaluation activities.

A similar project at the University of Illinois has produced the Virtual Power System Testbed (VPST) which also combines both simulation and physical elements [22]. The testbed is similar to VCSE as it uses a PowerWorld power system simulator, while network integration is based on the Illinois-developed Real-Time Immersive Network Simulation Environment (RINSE) project. These components are then integrated with physical devices and industry-standard software products to provide a realistic control environment.

The European CRUTIAL project has deployed two different testbeds to explore impacts from various attack scenarios [31, 30]. The first testbed is focused primarily on telecommunications within the electric grid by evaluating the transmission of IEC 60870-5-104 traffic between a set of simulated substations and control centers. Specific experiments have focused on evaluating the communication system’s ability to withstand various denial of service (DoS) attacks. Additionally, a microgrid evaluation testbed has been developed through the interconnection of a physical microgrid environment controlled by emulated IED devices. The intelligent electronic devices (IED) then communicate over a local area network (LAN) to a Matlab/Simulink system which performs the resulting con-
trols. This environment is being used to identify potential vulnerabilities in distributed energy resources (DER) implementations.

The Testbed for Analyzing Security of SCADA Control Systems (TASSCS) has been developed at the University of Arizona to perform anomaly-based intrusion detection research [62]. The testbed utilizes OPNET System-in-the-Loop network emulation similar to Sandia’s VCSE and also utilizes PowerWorld software to provide a simulated electric grid. A simulation-based control solution is presented using Modbus RSim software which then communicates with the PowerWorld simulator.

A testbed at the University College Dublin (UCD) is based on industry standard software/hardware with a DIgSILENT power system simulator to provide an environment to both identify attacks and evaluate physical impact [41]. Research on intrusion and anomaly detection capabilities is being performed within this environment.

Finally, the SCADASim testbed has been developed at Royal Melbourne Institute of Technology (RMIT) University to enable the exploration of network performance under cyber attack [85]. The SCADASim testbed focuses on developing an emulated communication infrastructure that can be used to interconnect physical devices utilizing common SCADA protocols. The testbed can then be used to analyze how cyber attacks impact the system’s communication requirements.

5.3 Testbed research applications and design

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

A comprehensive set of testbed applications are identified in Fig. 5.1 and elaborated upon in greater detail below.

5.3.1.1 Vulnerability research

Cyber-physical systems utilize different software, hardware, communications protocols and physical media. Many of the technologies used within this environment are not publicly available which significantly constrains the amount of vulnerability research that can performed by security researchers. Fortunately, testbeds provide areas where vulnerability assessment activities can be performed, including vulnerability scanning, cryptography analysis, and software testing methods such as fuzzing. Other testbed environments, such as the National SCADA Test Bed, have been utilized to identify numerous cyber vulnerabilities in various control system components [46, 45]. This research will help ensure that software platforms, configurations, and network architectures have been adequately analyzed for weaknesses.

5.3.1.2 Impact analysis

Another key testbed application is the evaluation of physical impacts from different types of cyber security attacks and incidents [14]. The complexity and interdependencies within both the cyber and physical systems complicate current impact analysis methods. Testbeds help capture the risk posed by a particular security event through the ability to determine impact on grid stability and power flow. Various attack strategies can be explored including sophisticated coordinated attacks and insider threats. Additionally, various power system topologies, operator responses, and cyber vulnerabilities can be explored to determine their ability to mitigate physical system impacts.
Table 5.1 Research efforts to testbed capability mapping

<table>
<thead>
<tr>
<th>Research Objectives</th>
<th>Control</th>
<th>Communication</th>
<th>Physical System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SW</td>
<td>HW</td>
<td>Algs.</td>
</tr>
<tr>
<td>Vulnerability Research</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Impact Analysis</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Mitigation Evaluation</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Metric Development</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Security Validation</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Data Model Dev.</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Interoperability</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Cyber Forensics</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Operator Training</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
5.3.1.3 Mitigation evaluation

Testbeds also present a useful environment to explore the effectiveness of various mitigation strategies. Mitigation efforts should attempt to reduce the vulnerability of the cyber infrastructure while increasing the robustness of the power applications [94]. One particular area where testbeds will be useful is in the development of attack resilient control algorithms that can be evaluated within a realistic environment to explore their performance and reliability.

5.3.1.4 Cyber-physical metrics

The development of cyber-physical metrics is imperative to improving cyber security and increasing grid resiliency. Testbeds produce an environment where controlled evaluations can be performed to support metric development and evaluation. This is specifically relevant within the cyber-physical systems as metrics must combine multiple domains. On the physical side, metrics can be evaluated based on the impact to power flow, stability, and even markets. Cyber security metrics can incorporate vulnerability criticality (such as CVSS [89]), vulnerability patch installation rates, and other methods to explore both system correctness and organizational security objectives [79].

5.3.1.5 Data and model development

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

Cyber security compliance requirements (e.g., NERC CIP [82]) are becoming increasingly common as a means to ensure critical resources are appropriately protected. Unfortunately, the process of evaluating security mechanisms is not well established within this environment. The electric grid’s high availability demands and the heavy utilization of proprietary systems limit the applicability of common vulnerability scanning techniques [23]. Since the effectiveness of compliance depends heavily on the security validation process, effective methods are required to ensure requirements are appropriately enforced. Testbed environments that implement industry standard software and configurations can help understand both impacts and effectiveness of traditional security assessment techniques while also presenting an environment where new methods can be explored.

5.3.1.7 Interoperability

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

5.3.1.8 Cyber forensics

Cyber-based forensics presents another important area of future research [66]. Field devices depend heavily on embedded systems which utilize different operating systems and software platforms. Recent events have also shown that cyber attacks can be used to modify the operational logic of programmable logic controllers (PLC) [36]. Without some ability to forensically analyze these devices, there is little chance of detecting intrusions. Testbeds play a key role in this analysis as they present an environment where device
functionality can be analyzed, specifically, whether they respond correctly to commands and return accurate measurements.

5.3.1.9 Operator training

Cyber incidents may be responsible for unusual power system failures, especially when combined with physical faults [56]. Testbeds present the opportunity to both analyze these situations and demonstrate how a realistic attack would look to system operators. Therefore, testbeds may provide training applications to help identify differentiated failures from both cyber and physical.

5.3.2 Testbed design elements

This section presents a high-level overview of testbed components and their support of testbed applications. Testbed components can be categorized into communication, control and power systems elements. Fig. 5.2 shows a logical testbed architecture and specifically identifies these components. The diagram first displays how measurements and actuations are either sensed from physical devices, 1a, or simulated and transmitted
over network, \textit{1b}. Item 2 displays how information such as device statuses, commands, and protection functions are transmitted through the substation. Item 3 demonstrates the substation communications to other systems in the wide area network (WAN) for regional control and energy management functions. Finally, item 4 shows WAN communication between control centers for system scheduling and status data.

Table 5.1 identifies the requirements for the testbed’s control, communication, and physical system components in order to support the previously identified research initiatives. The following list identifies the various testbed components in this table.

- **Software** - the various SCADA and energy management system (EMS) applications that monitor and control the physical system.

- **Hardware** - the IEDs and PLCs that bridge the cyber and physical domains.

- **Algorithms** - the logic to calculate grid observability and perform automated control functions.

- **Protocols** - the numerous real-worlds SCADA network protocols.

- **Architectures** - accuracy of the network layout to current smart grid network topologies.

- **Performance** - similarities between the networks throughput and latency.

- **Scalability** - the size of the the power system that can be simulated.

- **Real-Time** - the simulators ability to compute updated grid state in real-time.

- **HW Interface** - whether the power system simulator can be interfaced with the actual IEDs.
Figure 5.3 PowerCyber testbed architecture
5.4 ISU’s PowerCyber testbed architecture

This section describes the architecture and capabilities of the PowerCyber testbed at Iowa State University (ISU), specifically highlighting the communication, control, and physical system simulation components. The testbed currently utilizes an array of real, emulated, and simulated components to provide a realistic cyber and physical environment [5]. Fig. 5.3 demonstrates the testbed’s architecture, which will be elaborated upon in the remainder of this section.

5.4.1 Control

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

5.4.1.1 Control center

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

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

5.4.1.2 Substations

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

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

5.4.2 Communication

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

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

ISEAGE: The ISEAGE testbed was developed independently to provide a scalable Internet environment to perform cyber attack and defense simulations [32]. ISEAGE integration within the testbed provides the following benefits: 1) large cyber infrastructure modeling, 2) network traffic collection, and 3) coordinated attack simulation.

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

5.4.2.2 Substations

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

5.4.3 Physical system

The testbed currently deploys two different tools for performing power system simulation, DIgSILENT PowerFactory and a RTDS [29, 88]. These simulators are used independently based on the time constraints of the simulation. The power system model for both simulators is based on the Western Electricity Coordinating Council (WECC) 9-bus model as demonstrated in Fig. 5.3. The system consists of three generating units at buses 1, 2 and 3, and three loads at buses 5, 6 and 8. Nine substations are modeled, such that each substation controls the operations (breaker control) concerned with a bus.

5.4.3.1 Real Time Digital Simulator

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

5.4.3.2 DIgSILENT PowerFactory

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

5.5 Testbed evaluation and experimentation

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

5.5.1 Vulnerability assessment

Numerous vulnerability assessment activities have been performed on the testbed to explore potential security weaknesses in the software and communication protocols. Discovered vulnerabilities are then shared with the product vendor so they can develop and release appropriate mitigations. Our vulnerability identification process has followed well documented security testing methodologies, such as NIST 800-115: “Technical Guide to Information Security Testing and Assessment”, which focuses on various scanning and cracking techniques along with a thorough review of implemented technologies and configurations [53]. In addition to the documented methodology, our analysis has also included manual inspection techniques using various open-source tools and software fuzzing tests based on the Mu Security Analyzer [78].

The resulting analysis has resulted in the discovery of multiple previously undisclosed vulnerabilities within industry software platforms. These efforts have resulted in vendor security advisories and system patches [91].

5.5.2 Cyber-physical impacts

In addition to the vulnerability assessment efforts, various cyber-physical impact evaluations have been performed to explore how attacks can impact the physical sys-
Table 5.2 Evaluated cyber attacks

<table>
<thead>
<tr>
<th>Attack 1: Malicious Breaker Trip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
</tr>
<tr>
<td>Origin</td>
</tr>
<tr>
<td>Tool</td>
</tr>
<tr>
<td>Target</td>
</tr>
<tr>
<td>Result</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attack 2: SCADA Observability DoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
</tr>
<tr>
<td>Origin</td>
</tr>
<tr>
<td>Tool</td>
</tr>
<tr>
<td>Target</td>
</tr>
<tr>
<td>Result</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attack 3: Remedial Action Scheme DoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
</tr>
<tr>
<td>Origin</td>
</tr>
<tr>
<td>Tool</td>
</tr>
<tr>
<td>Target</td>
</tr>
<tr>
<td>Result</td>
</tr>
</tbody>
</table>

tems. Table 5.2 identifies the three attack templates that have been evaluated within the testbed. The remainder of this section will provide further analysis of these situations.

5.5.2.1 Attack 1: Malicious breaker trip

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

The power system is stable when the simulation begins. In 7 seconds the malicious breaker trip command is injected to the network. Once this occurs, generator rotor angles become unsynchronized. Once the breaker is tripped, generator 1 is separated from the
rest of this system. The loss of generation creates a large system disturbance which caused the remaining online generators to become unsynchronized. Fig. 5.4 identifies the rotor angle of generators 2 and 3 during the attack.

5.5.2.2 Attack 2: SCADA observability DoS

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

**Cyber impact:** Fig. 5.5 documents the results of the DoS evaluation by plotting the mean throughput from 5 simulations, the x-axis documents the length of the attack while the y-axis displays the number of probe DNP3 packets received every ten seconds. These results show that as the attack throughput increases, the DNP3 communication decreases. At 10 megabits per second (Mbps) the availability starts to decrease and once the DoS attack reaches approximately 20 Mbps the VPN devices are no longer to properly relay the DNP3 traffic between the substation and control center.

**Physical system impact:** Once the attack reaches 20 Mbps, the control system begins to obtain a decreasing number of SCADA measurements. These measurements are necessary to compute the state estimations of the physical system and other EMS applications.
5.5.2.3 Attack 3: Remedial Action Scheme DoS

In this particular case study, we show how the testbed can be used to replicate the conditions of a Remedial Action Scheme (RAS) and study the impact of a coordinated cyber attack on the power system. Typically, for every RAS, there is a RAS controller, which determines when the scheme is to be armed and also sends appropriate control commands to the corresponding relays. Because RAS are very critical in maintaining the system stability, they are often deployed with another redundant backup RAS controller and protection elements, however, for the purpose of this case study, only one controller is modeled.

Fig. 5.3, labeled “PowerCyber testbed architecture”, displays the WECC 9 bus system that was chosen as the power system for our case study. The particular RAS which has been adapted for this case study has been taken from the WECC RAS list[111] and is explained below.

The RAS scheme is designed to trip one of the generation units at bus 2, (modeled by a reduction in the generation), if there is a fault on one of the transmission lines connected to it. In our case there are two transmission lines, namely, 7 – 8 and 7 – 5. The RAS scheme would be armed only if generation at bus 2 exceeds a particular value.
This generation would have to be reduced to prevent the thermal overloading of one of the transmission lines in case of a fault on the other line and also to maintain the stability of the generation units. Table 5.3 shows how the various components of the RAS have been mapped into the PowerCyber testbed environment.

### Table 5.3  Mapping of PowerCyber testbed components to RAS

<table>
<thead>
<tr>
<th>Component in RAS</th>
<th>Mapping in PowerCyber testbed</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAS controller</td>
<td>Relay 1</td>
</tr>
<tr>
<td>Relay protecting line 7-5</td>
<td>Relay 2</td>
</tr>
<tr>
<td>Relay protecting line 7-8</td>
<td>Relay 3 (inside RTDS)</td>
</tr>
<tr>
<td>Relay causing generation reduction at bus 2</td>
<td>Relay 4 (inside RTDS)</td>
</tr>
</tbody>
</table>

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

1. Creating a data integrity attack (similar to section V-B-1) to trip the Relay 2 which protects line 7–5 to activate the RAS.

2. Creating a Denial of Service attack to prevent the GOOSE trip command to the generation unit at bus 2 to result in a thermal overload on line 7–8 and cause it to trip out.

By looking at Fig. 5.6, we can explain how the RAS operates by observing the sequence of events and IEC 61850 messages being exchanged between the devices associated with this protection scheme. Generally, the control center operator can manually arm/disarm the RAS through an IEC 61850 message to the RAS controller directly outside the typical flow of events.
1. The Generating station at bus 2 exceeds a threshold, communicates this to the RAS controller (Relay 1) to arm the RAS.

2. Relay 2 associated with the protected line $7 - 5$ sends a message to the RAS controller to indicate a fault.

3. RAS controller performs the necessary validation checks and issues a trip command to the unit at generating station in bus 2 to reduce generation immediately.

4. Because of the successful cyber attack, generation at bus 2 is not reduced and the Relay 3 protecting line $7 - 8$ detects thermal overload.

5. Relay 3 reaches max time for withstanding the thermal overload and trips, isolating the generation station at bus 2.
Figure 5.8  DoS protection scheme impact (relay Syn flood)
ii) Cyber impact: We evaluate two DoS attacks which could be used to disrupt the RAS communication, first by flooding the switch with broadcast Ethernet frames and also flooding the RAS controller with TCP Syn packets. We evaluate various traffic rates to determine the amount of malicious traffic required to disrupt the RAS, each attack was repeated ten times. The results of this analysis shows that the protection scheme can be disrupted through both methods, though targeting the RAS controller requires significantly less bandwidth.

Fig. 5.7 demonstrates the impact of the DoS attack by flooding the Ethernet switch. Fig. 5.7A displays that the percentage of times that RAS failed based on various attack rates. Notice as traffic hits 50 Mbps the RAS fails 50% of the time while at greater attack rates the RAS fails consistently. Fig. 5.7B displays averaged time for the RAS communication to travel from the relay to the RAS controller and back (note: these results only include successful RAS methods as the communication never finishes in the failed scenarios). Although RAS only fails after not receiving the communication within 1 second, our results show either the communication occurred within 200ms or the RAS failed. This occurrence can likely be explained by Ethernet’s collision detection exponential back-off and eventual collision timeout.

The results from the TCP Syn flood attack in Fig. 5.8 demonstrate that the protection scheme could be disrupted with significantly less bandwidth by targeting the relay. Fig. 5.8A shows that traffic around 1.5 Mbps is sufficient to disrupt the RAS 60% of the time, while as traffic reaches 2 Mbps the RAS continually fails. Fig. 5.8B displays the average delay of the RAS during successful runs.

 iii) Physical system impact: The impact of the successful coordinated attack on the power system can be seen from Fig. 5.9 and Fig. 5.10. Fig. 5.9 shows how the system voltages are impacted by the attack and Fig. 5.10 shows how the line flows and the generation changed as a result of the attack. Each of these figures have two ovals highlighting the two events which took place as part of the attack. The first event
represents the tripping of line 7 − 5, and could have been either a fault or an attack (in our case), and the second event represents the tripping of line 7 − 8 due to the attack.

Fig. 5.9 shows that the first event did not cause much impact on the system voltage and the voltage at all the buses stayed close to 1.0 p.u. Whereas, after the second line tripped, generator two was completely isolated from the grid and this impacted the voltage at several buses significantly. This especially occurs at bus 7, which is linked to bus 2 through a step-up transformer.

From Fig. 5.10, we can see that the tripping of line 7 − 5 changed the generation in all three generators by a small amount, but it overloaded the line 7 − 8 significantly and eventually preventing the generation reduction as per the RAS, it led to the tripping of line 7 − 8. Although the plot shows the tripping of 7 − 8 due to overload within seconds, the scenario would have resulted in the same impact even after a longer thermal limit threshold, which is typically around a few minutes. It is to be noted here that the tripping of line 7 − 8 completely isolates generator 2 from the system and therefore it would result in a huge loss of generation which will impact the frequency profoundly. In a real power system such an event could potentially cause some frequency stability related problems. This situation could also lead to tripping of some load if no spare generation is available.

Note: The simulated power system used in this attack was not operating in a N-1 secure state as is required for the North American grid, therefore, the demonstrated attack would unlikely result in similar load and frequency violations on the actual grid.
Figure 5.9  Impact of attack on system voltages

Figure 5.10  Impact of attack on generation and line flows
CHAPTER 6. CONCLUSION AND FUTURE WORK

Critical infrastructures have gained increased concern as targets from future cyber attacks. The electric power grid is extremely dependent on cyber infrastructures to perform automated monitoring and control functions. Smart grid initiatives, such as AMI, WAMS, and substation automation will significantly expand this dependency. The exposure of these ICT assets and their increasing adoption in smart grid initiatives introduces numerous concerns questioning the adequacy of the grids current security posture. AMI presents both utilities and consumers with improved control over their electricity consumption. However, this large infrastructure presents numerous vulnerabilities which could be exploited by attackers to cut off power, falsify billing data, or access sensitive consumer privacy data. WAMS will incorporate PMUs to improve the accuracy of state estimation of the bulk power system. Although if critical PMU data is manipulated by an attacker, utilities may compute incorrect estimations which may result in improper control actions. Additionally, increased substation automation attempts to improve the reliability of critical control and protection applications. However, if an attacker is able to gain access to substation systems, they could trip breakers to cause significant damage to the grid.

Recent government reports have identified numerous cyber security shortcomings within the grid including missing patches, poor system configurations, insufficient communication protection, and inadequate intrusion detection capabilities. While grid security mechanisms are weak, cyber attacks are being identified with greater frequency and sophistication. Recently advanced APT tactics, such as Stuxnet, demonstrate the
feasibility of cyber-physical malware that can usurp a control system in order to manipulated a physical system. More secure systems must be developed to provide sufficient resiliency to cyber attack. Although a wealth of research has been performed addressing traditional cyber security paradigms, many solutions do not adequately address the additional constraints required to support the electric grid.

This dissertation identifies three key contributions that will enhance the security of the smart grid. First, it presents novel models and metrics for evaluating the security posture of the smart grid. It presents a graph-based model integrating known information about system privileges and critical information in the architecture based on the contents of the CIM. Then an exposure metric is computed for each CIM object to represent its vulnerability to attack. Various applications of this model are then explored on an example AMI architecture, including comparisons of the efficacy of different security enhancements and methods to calculate the impact that a new vulnerability in the system.

Next, a model-based intrusion detection system is designed to identify attacks against electric substations. This work extends previous smart grid IDS research in that it incorporated a Petri net model to support both temporal and spatial analysis of substation events. Additionally, it uses a hierarchical approach by collecting and processing events within the substation, and then passing them to the system level where they can be analyzed to correlate physical events and identify coordinated attacks. The approach is then demonstrated based on the IEC 61850 protocol and recently published research papers demonstrating smart grid substation applications. The results show that attacks can be reliably detected unless the attacker is able to perform a sophisticated coordinated attach which compromises all relays within a protection scheme.

Finally, this work introduces the cyber-physical PowerCyber testbed. The testbed is an accurate representation of both cyber and physical elements of the smart grid so that research can be explored within a controlled environment. The testbed’s design strategies
are presented including trade-offs on cost, scalability, and accuracy. The testbed’s hybrid architecture is then introduced including its integration of physical and emulated control, communication, and power system components. Finally, the dissertation demonstrates the testbed’s utility to research applications with the execution of various vulnerability assessment activities, as well as integrity and availability attacks and their resulting impact on grid stability.

6.1 Future work

While this research presents multiple contributions to the area smart grid cyber security, continued research is needed in all three domains. Research on models and metrics is imperative to ensure risk can be accurately evaluated, which is critical to the selection of appropriate security mechanisms. As demonstrated by this research, CIMs present a novel way to look at the information which must be stored and communicated in order to support smart grid operations. Future risk analysis and modeling approaches should focus on identifying how vulnerable elements of the CIM are to attack, but should further incorporate physical system impact analysis to evaluate the true risk to the power grid. Essentially, these approaches should more strongly emphasize the cyber-physical relationship of the smart grid.

Continued research is needed in intrusion detection approaches for the smart grid. MHINDS demonstrates how deterministic control network properties can be combined with spatial and temporal analysis of both cyber and physical events to accurately identify malicious control communications. This research should be expanded in multiple ways.

First, future research should incorporate greater awareness about the operation of substation protections schemes into the model. This should be incorporated into the detection algorithms to reduce false positives and negatives. This research focus should
closely parallel related efforts in fault location algorithms. In addition, future research
should explore similar spatial and temporal approaches on other power system applica-
tions, potentially including applications in control centers and AMI. Future work should
focus on the continued development of the research so that the contributions can be
realized first within the PowerCyber testbed and then in real-world smart grid systems.

Finally, continued research is needed to explore pragmatic methods to extend the
testbed’s accuracy and usability. The testbed’s accuracy can be improved by increasing
the size of the simulations, including both the cyber and physical systems. Larger power
systems are helpful to explore the dynamic properties of power systems. In addition,
larger power systems must be accompanied by larger control system and communication
networks. The accuracy of the testbed can also be improved by integrating more control
algorithms used within the electric grid, specifically protection schemes, state estima-
tion, AGC, and contingency analysis. The ability to explore an attacks impact to these
algorithms is critical to accurately evaluating the effectiveness of novel mitigation strate-
gies. Finally, the testbed requires greater research into the development of a platform
which can be remotely accessible. This environment should be accessible to researchers
both within and external to ISU to facilitate both educational research efforts. Users
must be able to easily configure the various power system topologies, control algorithms,
control architectures, and security mechanisms to understand cyber attacks impact and
to explore methods to enhance the security of the smart grid.
APPENDIX
PUBLISHED WORK

Journals


Conferences


**Book Chapters**


**Technical Reports**

BIBLIOGRAPHY


