

# Public Interest Energy Research (PIER) Program INTERIM PROJECT REPORT

## SMART GRID CYBER SECURITY POTENTIAL THREATS, VULNERABILITIES AND RISKS

Prepared for: California Energy Commission  
Prepared by: California State University Sacramento



MAY 2012  
CEC-500-2012-047

**Prepared by:**

Primary Author:

Isaac Ghansah, Ph.D.

Center for Information Assurance and Security  
College of Engineering and Computer Science  
California State University Sacramento (CSUS)  
6000 J Street  
Sacramento, CA 95819-6021



Contract Number: 500-08-027

**Prepared for:**

**California Energy Commission**

David Chambers

**Project Manager**

Mike Gravely

**Office Manager**

**Energy Systems Research Office**

Laurie ten Hope

**Deputy Director**

**RESEARCH AND DEVELOPMENT DIVISION**

Robert P. Oglesby

**Executive Director**

**DISCLAIMER**

This report was prepared as the result of work sponsored by the California Energy Commission. It does not necessarily represent the views of the Energy Commission, its employees or the State of California. The Energy Commission, the State of California, its employees, contractors and subcontractors make no warrant, express or implied, and assume no legal liability for the information in this report; nor does any party represent that the uses of this information will not infringe upon privately owned rights. This report has not been approved or disapproved by the California Energy Commission nor has the California Energy Commission passed upon the accuracy or adequacy of the information in this report.

## Preface

The California Energy Commission's Public Interest Energy Research (PIER) Program supports public interest energy research and development that will help improve the quality of life in California by bringing environmentally safe, affordable, and reliable energy services and products to the marketplace.

The PIER Program conducts public interest research, development, and demonstration (RD&D) projects to benefit California.

The PIER Program strives to conduct the most promising public interest energy research by partnering with RD&D entities, including individuals, businesses, utilities, and public or private research institutions.

PIER funding efforts are focused on the following RD&D program areas:

- Buildings End-Use Energy Efficiency
- Energy Innovations Small Grants
- Energy-Related Environmental Research
- Energy Systems Integration
- Environmentally Preferred Advanced Generation
- Industrial/Agricultural/Water End-Use Energy Efficiency
- Renewable Energy Technologies
- Transportation

*Smart Grid Cyber Security Potential Threats, Vulnerabilities And Risks* is the interim report for the Smart Grid Information Assurance and Security Technology Assessment project (Contract Number 500-08-027) conducted by Center for Information Assurance and Security (CIAS) at California State University Sacramento (CSUS). The information from this project contributes to PIER's Energy Systems Integration Program.

For more information about the PIER Program, please visit the Energy Commission's website at [www.energy.ca.gov/research/](http://www.energy.ca.gov/research/) or contact the Energy Commission at 916-654-4878.

Please cite this report as follows:

Ghansah, Isaac, 2009. *Smart Grid Cyber Security Potential Threats, Vulnerabilities And Risks*  
California Energy Commission, PIER Energy-Related Environmental Research Program.  
CEC-500-2012-047.



# TABLE OF CONTENTS

Preface .....	i
Abstract .....	vii
EXECUTIVE SUMMARY .....	1
1.0 INTRODUCTION.....	3
1.1. What is Smart Grid?.....	3
1.2. Report Organization .....	7
2.0 REPORTED VULNERABILITIES OF SMART GRID .....	8
3.0 INFORMATION ASSURANCE AND SECURITY CONCEPTS AND POLICIES .....	12
3.1. Confidentiality.....	12
3.2. Integrity .....	12
3.3. Availability.....	12
3.4. Accountability.....	12
3.5. Security Concepts and Smart Grid .....	12
4.0 ADVANCED METERING INFRASTRUCTURE (AMI) SECURITY ISSUES.....	15
4.1. Introduction .....	15
4.2. AMI Security Threats .....	16
5.0 DEMAND RESPONSE SECURITY ISSUES.....	21
5.1. Introduction .....	21
5.2. Demand Response and Security Concerns.....	22
5.2.1. Confidentiality.....	23
5.2.2. Authentication.....	23
5.2.3. Data Integrity.....	24
5.2.4. Availability.....	24
5.2.5. Accountability .....	24
5.3. Open Automated Demand Response.....	24
5.3.1. Open Automated Demand Response Communications Infrastructure.....	24
5.3.2. Demand Response Automation Server (DRAS).....	26
5.3.3. OpenADR and Security Concerns .....	27
5.4. Demand Response at Residential Sites and Security Issues.....	32
5.4.1. Possible Attacks in PCT .....	32
6.0 CUSTOMER DOMAIN – HOME AREA NETWORK, GATEWAY, AND NEIGHBORHOOD AREA NETWORK SECURITY ISSUES.....	34

6.1.	Introduction .....	34
6.2.	Home Area Network (HAN).....	35
6.2.1.	ZigBee .....	35
6.2.2.	Z-Wave .....	36
6.3.	Gateway Component.....	36
6.4.	Wireless Neighborhood Area Network (WNAN).....	36
6.5.	Potential Security Issues/Risks .....	37
6.5.1.	ZigBee .....	37
6.5.2.	Z-Wave .....	38
6.5.3.	Gateway.....	38
6.5.4.	WNAN.....	39
	IEEE 802.11 .....	39
	IEEE 802.15.4 .....	40
	IEEE 802.16 .....	41
6.6.	Comprehensive Security issues with HAN/ Gateway/ NAN.....	42
7.0	SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEM SECURITY ISSUES.....	43
7.1.	Introduction .....	43
7.1.1.	SCADA Architecture in detail.....	45
7.1.2.	Security Issues In SCADA .....	45
	Public Information Availability.....	45
	Platform Configuration Vulnerabilities .....	46
	Platform Software Vulnerabilities.....	46
	Network Configuration Vulnerabilities.....	47
	Network Perimeter Vulnerabilities.....	47
	Network Communication (DNP 3) Vulnerabilities.....	48
8.0	PLUG IN ELECTRIC VEHICLES (PEV) SECURITY ISSUES.....	51
8.1.	Introduction .....	51
8.2.	Privacy of Movement.....	52
8.3.	Secure Payment .....	52
8.4.	Smart Metering.....	53
8.5.	Critical Infrastructure & Physical Security .....	53
8.6.	Communication .....	54
9.0	GENERIC SECURITY ISSUES OF THE SMART GRID .....	55

9.1.	Introduction .....	55
9.2.	Authenticating and Authorizing Users (People) to Substation IEDs .....	55
9.3.	Authenticating and Authorizing Maintenance Personnel to Smart Meters .....	56
9.4.	Authenticating and Authorizing Users (People) to Outdoor Field Equipment (e.g. Pole-Top Device) .....	56
9.5.	Authenticating and Authorizing Consumers to Meters .....	56
9.6.	Authenticating Meters to/from AMI Head Ends (Mutual Authentication .....	57
9.7.	Authenticating HAN Devices to/from HAN Gateways .....	57
9.8.	Securing Serial SCADA Communications .....	57
9.9.	Protection of Routing Protocols in AMI Layer 2/3 Networks .....	57
9.10.	Key Management for Meters .....	58
9.11.	Insecure Firmware Updates .....	58
9.12.	Side Channel Attacks on Smart Grid Field Equipment .....	58
9.13.	Key Management and Public Key Infrastructure (PKI) .....	58
9.14.	Patch Management .....	59
	GLOSSARY .....	60
	REFERENCES .....	64
	APPENDIX A .....	67

## List of Figures

Figure 1.	Smart grid network. ....	4
Figure 2.	Smart grid working. ....	5
Figure 3.	AMI components. ....	16
Figure 4.	Demand response use case shows the interfaces between each component (from NIST) .....	23
Figure 5.	Generic open automated demand response interface architecture .....	25
Figure 6.	DRAS Interfaces .....	26
Figure 7.	Path of attack in PCT .....	33
Figure 8.	HAN/Gateway .....	34
Figure 9.	SCADA general layout. ....	43
Figure 10.	SCADA architecture .....	45

## List of Tables

Table 1. Security threats on AMI with respect to security goals .....	19
Table 2. Possible attacks utility/ISO operator interfaces.....	28
Table 3. Possible attacks and impacts of DRAS client interfaces.....	29
Table 4. Possible attacks and impacts of participant interfaces.....	31
Table 5. HAN security issues .....	42
Table 6. SCADA security issues.....	50

## Abstract

This report is about potential Smart Grid Information Assurance and Security Issues. Issues specifically addressed are threats, vulnerabilities and risks. Mitigation and countermeasures to address those vulnerabilities will be covered in subsequent reports.

This report is the first in a series of research tasks specified in the statement of work for the California Energy Commission as follows (in brief):

- 1) Identify the potential issues affecting the confidentiality, integrity, and availability of information flow in the Smart Grid system. Group the issues with respect to confidentiality, integrity, and availability.
- 2) Investigate which of information security best practice(s) apply to smart grid and to what extent can they be applied. These best practices are intended to mitigate actions that violate confidentiality, integrity, and availability of the information flow.
- 3) Explore possible cyber security R&D issues that should be addressed in Smart Grid. Some of these could involve wireless sensors, wireless communication systems, monitoring, and, incident response systems.
- 4) Identify and recommend which potential R&D efforts should and should not be confidential.
- 5) Identify technical and non-technical solutions to ensure the privacy of end user information.

The researchers used information from various Smart Grid working groups that are dealing with Cyber security issues. These groups included Utility Security, Open Smart Grid, National Institute of Standards and Technology, Intelligrid. Information was also obtained from web sources, journals, and magazines.

The results show that Smart Grid has a number of potentially significant cyber security issues that must be addressed. They include confidentiality of user information, integrity of demand response systems, integrity and availability of SCADA (grid) systems, and integrity and availability of Plug-In Electric Vehicles.

Because the smart grid will have extensive Information Systems component, best practices used on those systems can be used to mitigate those vulnerabilities. On the other hand because of the unique characteristics of Smart Grid, especially as a critical infrastructure further research will be needed to address security issues in those unique cases. The researchers plan to report on them in future documents.

**Keywords:** Public Interest Energy Research, PIER, smart grid, electric grid, cyber security, critical infrastructure, information assurance.



# EXECUTIVE SUMMARY

## Introduction

At the request of California Energy Commission Public Interest Energy Research (PIER), the Center for Information Assurance and Security (CIAS) at Sacramento State University provides this report on Cyber Security vulnerabilities, threats, and risks of the Smart Grid.

The main goal of the agreement was to determine information assurance, security, and privacy issues associated with Smart Grid infrastructure and recommend research and development (R&D) priorities in those areas. The project will also identify best practices in information security that can be applied to the Smart Grid system.

This report is the first in a series of research documents covering Cyber Security issues of the Smart Grid namely:

- Potential threats, vulnerabilities and risks
- Best practices to mitigate those risks
- Research issues to be addressed in smart grid cyber security
- Privacy issues in smart grid infrastructure

The research specifically focused on Cyber Security issues of the following Smart Grid components: Advanced Meter Infrastructure, Demand Response Systems, Home Area Network (HAN), Neighborhood Area Networks, which connects the home to the utility systems, Supervisory Control and Data Acquisition (SCADA) system, which is used for the controlling generation, transmission and distribution systems, and Plug-in Electric Vehicles.

To achieve these objectives the researchers:

- Participated in both conference calls and face to face meetings with experts on the Smart Grid
- Performed literature search on the web
- Interviewed some utility experts on the electricity generation, transmission, and distribution processes
- Attended workshops on demand response research and smart grid interoperability

## Outcome:

As is indicated in the report, the results show that Smart Grid has a number of potentially significant cyber security issues that must be addressed. They include confidentiality of user information, integrity of demand response systems, integrity and availability of SCADA (grid) systems, and integrity and availability of Plug-in Electric Vehicles. Additionally Cyber Security issues of communication systems are addressed. Because the smart grid will have an extensive Information Systems component, best practices used on those systems can be used to mitigate those vulnerabilities. On the other hand, because of the unique characteristics of Smart Grid,

one of which is a critical infrastructure, further research will be needed to address security issues in those unique cases. The researchers plan to report on them in future documents.

**Benefits for California:**

- Increase customer trust of the Smart Grid.
- Increase regulator understanding of the security issues in Smart Grid that need to be addressed by Manufacturers and Utilities.
- Increase understanding of the privacy issues in Smart Grid and how they can be addressed.
- Because the project will identify security and privacy issues in the Smart Grid infrastructure and propose solutions and research areas to be examined, its results will ultimately enable acceptance of wide deployment of the Smart Grid resulting in increase energy efficiency and low energy costs.

## 1.0 INTRODUCTION

This document contains the Comprehensive Smart Grid Security Issues researched by Smart Grid Research Group which is part of the Center for Information Assurance and Security (CIAS) at California State University Sacramento (CSUS). This report is about potential Smart Grid Information Assurance and Security issues. Issues specifically addressed in this report are threats, vulnerabilities and risks. Mitigation and countermeasures to address those vulnerabilities will be covered in subsequent reports.

This report is the first of a series of research tasks specified in a statement of work for the California Energy commission as follows:

- 1) Identify the potential issues affecting the confidentiality, integrity, and availability of information flow in the Smart Grid system. For instance, hacker/terrorist use of malicious software to perform denial of service attacks on critical infrastructure such as the Smart Grid will be examined. Group the issues with respect to confidentiality, integrity, and availability.
- 2) Investigate which information security best practice(s) apply to smart grid and to what extent can they be applied. Best practices such as use of firewalls for perimeter defense, intrusion detection, incident response handling, defense in depth, etc are well known in the information security arena. These best practices are intended to mitigate actions that violate confidentiality, integrity, and availability of the information flow.
- 3) Explore possible cyber security R&D issues that should be addressed in Smart Grid. Some of these could involve wireless sensors, wireless communication systems, monitoring, and incident response systems.
- 4) Identify and recommend which potential R&D efforts should and should not be confidential.
- 5) Identify technical and non-technical solutions to ensure the privacy of end user information. Because Smart Grid systems will contain end user information, privacy is critical.

This report is about the first task listed above. Subsequent reports will discuss other tasks.

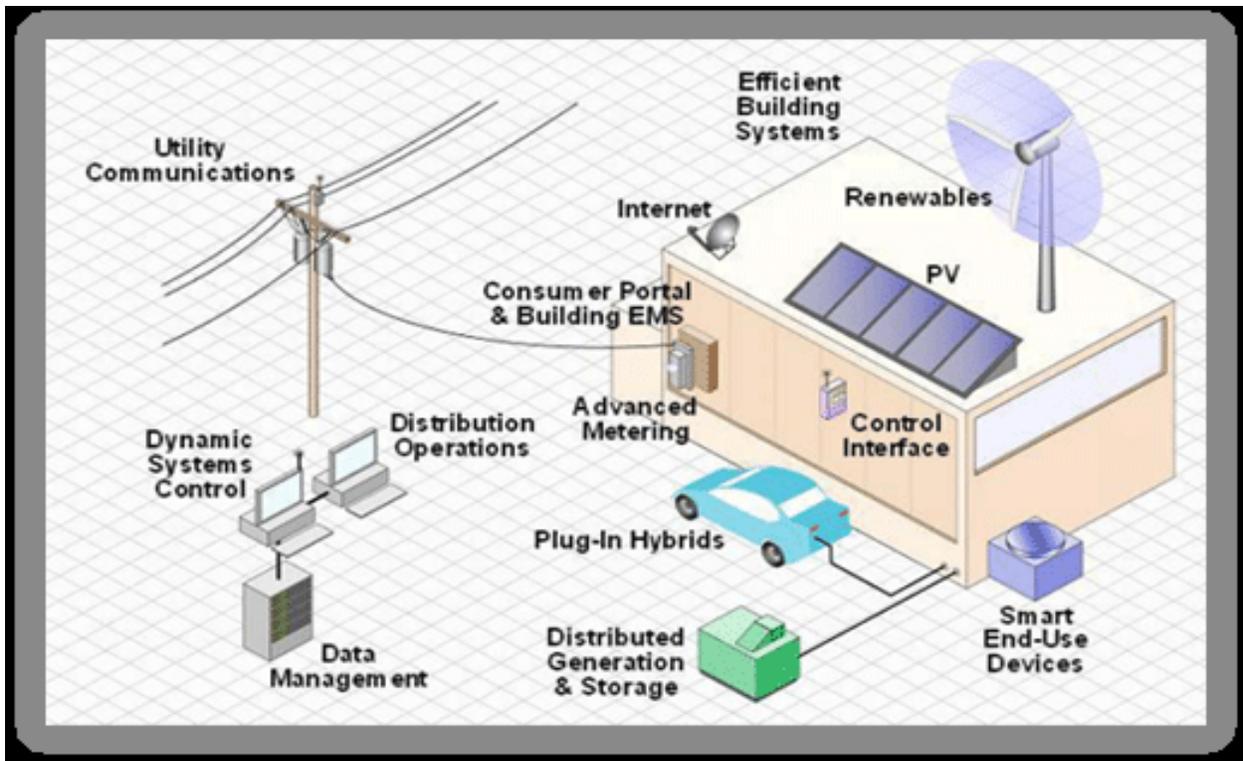
### 1.1. What is Smart Grid?

A smart grid (See Figure 1 and Figure 2) delivers electricity from suppliers to consumers using digital technology to save energy, reduce cost and increase reliability and transparency. It is a modernized [electricity network](#) which is being utilized as a way of addressing [energy independence](#), [global warming](#) and emergency [resilience](#) issues.<sup>1</sup>

The primary components of Smart Grid are shown in Figure 1. Figure 2 explains how the Smart Grid works.

---

1. Wikipedia [http://en.wikipedia.org/wiki/Smart\\_grid](http://en.wikipedia.org/wiki/Smart_grid).



**Figure 1. Smart grid network.**

Source: Federal Stimulus and Cleantech Infrastructure; Lee Bruno, Innovation Pipeline<sup>2</sup>

Smart Grid has the following characteristics<sup>3</sup>

- Self-healing from power disturbance events
- Enabling active participation by consumers in demand response
- Operating resiliently against physical and cyber attack
- Providing power quality for 21st century needs
- Accommodating all generation and storage options
- Enabling new products, services, and markets
- Optimizing assets and operating efficiently

---

2. <http://www.larta.org/lartavox/articles/5-2009/Federal-Stimulus-and-Cleantech-Infrastructure.htm>

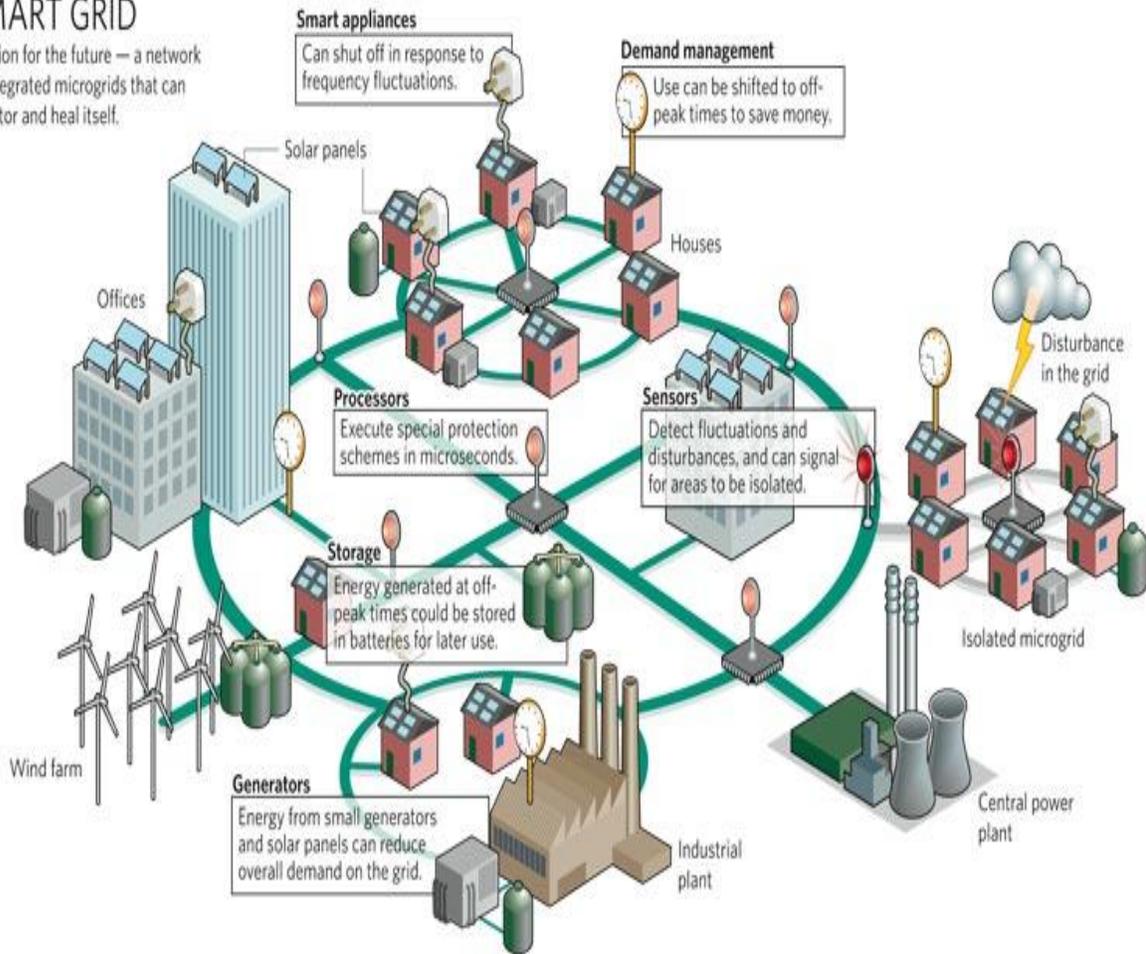
3. National Energy Technology Laboratory (2007-07-27 (pdf). A Vision for the Modern Grid. United States Department of Energy. Page 5

[http://www.netl.doe.gov/moderngrid/docs/A%20Vision%20for%20the%20Modern%20Grid\\_Final\\_v1\\_0.pdf](http://www.netl.doe.gov/moderngrid/docs/A%20Vision%20for%20the%20Modern%20Grid_Final_v1_0.pdf). Retrieved 2008-11-27

Figure 2. Smart grid working.

## SMART GRID

A vision for the future — a network of integrated microgrids that can monitor and heal itself.



Source: The Smart Grid Frontier<sup>4</sup>

4. The Smart Grid Frontier: Wide Open; David Heyerman; May 3, 2009

Available [Online]: [tinycomb.com/2009/05/03/what-is-the-smart-grid/](http://tinycomb.com/2009/05/03/what-is-the-smart-grid/)

Technically, the Smart Grid is unique in many respects. First by its nature the Smart Grid is a complex system. Second, Smart Grid is one of 18 critical infrastructures identified by DHS. These systems are so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.<sup>5</sup> Third, smart grid is a large system because it is used to control electricity which is present in almost every home. Fourth smart grid is a 'special' critical infrastructure because many of the 18 critical infrastructures depend on it. For instance, electricity is needed by banks, emergency services such as hospitals, telecommunications, computers, etc. Indeed, the Cyber Security Strategy for the 44<sup>th</sup> President of the United States cites energy, financial, Information Technology (IT), and telecommunications as the four critical infrastructures with the most critical cyber assets.

The unique characteristics of smart grid stated above are the reasons why cyber security of the smart grid is imperative. The smart grid has many anticipated benefits.<sup>6</sup>

- Improves power reliability and quality
- Optimizes facility utilization and averts construction of back-up (peak load) power plants
- Enhances capacity and efficiency of existing electric power networks
- Improves resilience to disruption
- Enables predictive maintenance and "self-healing" responses to system disturbances
- Facilitates expanded deployment of renewable energy sources
- Accommodates distributed power sources
- Automates maintenance and operation
- Reduces greenhouse gas emissions by enabling electric vehicles and new power sources
- Reduces oil consumption by reducing the need for inefficient generation during peak usage periods
- Improves cyber security
- Enables transition to plug-in electric vehicles and new energy storage options
- Increases consumer choice

Because of its many benefits the federal government and many other state governments including California, are funding research and demonstration efforts for the smart grid. Both US departments of commerce and energy are pushing for interoperability standards for smart grid. NIST, as a branch of the commerce department is leading the effort to create those standards. Additionally, organizations as diverse as Electric Utilities, US DOE, NIST, Google, Microsoft, GE, IEEE, NERC, FERC, IEC, and ANSI have published documents about Smart Grid.

---

5. DHS Website [http://www.dhs.gov/files/programs/gc\\_1189168948944.shtm](http://www.dhs.gov/files/programs/gc_1189168948944.shtm) Retrieved 2009-10-14

6. NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft).

Major reason for this cyber security research is because of the complexity of the smart grid, the importance of the smart grid as a super-critical infrastructure, and the fact that many reports of potential attacks on the grid have been disseminated in the media. This research should help put some these media reports in perspective. However, the primary purpose of this current report is to discuss threats and vulnerabilities, and general security problems. Subsequent reports will address controls to mitigate those risks and countermeasures, using best practices; and where best practices are not adequate the researchers will suggest research topics that need to be addressed in the future to help solve those problems.

## 1.2. Report Organization

This document is organized as follows:

- Examples of reported vulnerabilities of the smart grid are first introduced in Chapter 2.
- Information assurance and security concepts and terminology that are used throughout the document are discussed in Chapter 3.
- Security issues of important smart grid components, namely Advance Metering Infrastructure, Demand Response, Customer Domain Systems (i.e. Home Area Networks, Gateways, and Neighborhood Area Networks), Grid (Supervisory Control and Data Acquisition and Distributed Network Protocol), and Plug in Electric Vehicles are discussed in Chapters 4 through 8.
- Important security issues that are critical in smart grid but that do not fit cleanly in the above smart grid components are included in Chapter 9. Most of the issues listed in Chapter 9 will eventually become research topics that will be discussed in more detail in subsequent documents.

Most of the information in that chapter is currently being discussed in the NIST Bottom-up Security Group which is subgroup within the NIST Smart Grid Cyber Security Coordination Task Group (CSCTG) followed by a list of References.

Finally, Appendix A is a list of Use Cases for the various components of the Smart Grid and corresponding Cyber security requirements. It is part of NISTIR 7628.<sup>7</sup> The Appendix can be viewed as an excellent summary of most of the cyber security issues discussed in this report.

---

7. NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft).

## 2.0 REPORTED VULNERABILITIES OF SMART GRID

This section cites a number of smart grid vulnerabilities reported in the media and elsewhere. The intent is to bolster the reason for this research.

Most of the nation's electricity system was built when primary energy was relatively inexpensive. Grid reliability was mainly assured by having excess capacity in the system, with unidirectional electricity flow to consumers from centrally dispatched, coal-fired power plants. Recognizing these challenges, the energy community is starting to combine advancements in information technology with electricity infrastructure, allowing the electric system to become "smart." This system uses interconnected elements that optimize the communications and control across the different segments of energy generation, distribution, and consumption. But the unfortunate reality is that because of the critical nature of the technology and the services that it provides, the grid becomes a prime target for acts of terrorism and cyber attacks.<sup>8</sup>

The Smart Grid has several network layers and every network layer and technology used represents a potential avenue of attack. The legacy grid already uses many different communication paths and protocols to connect utility operation centers with system operators such as Independent Service Operators (ISOs) and Regional Transmission Operators (RTOs). A wide variety of data transfer protocols are used. Most existing protocols have some form of vulnerability or another. Advanced meter infrastructure and its network of smart meters provide a foundation for smart grid. Research firm Parks Associates estimates that 8.3 million smart meters have been installed in US homes, about 6% penetration. These meters must be accessible for ongoing maintenance and operations. Once a meter is compromised it can be used to attack other parts of the network. Smart thermostats, in-home displays, appliances, charging stations and various plug-loads are connected together by an Energy Management System (EMS) application running on the Home Area Network (HAN). Even though these are less likely to be used in large-scale assaults they represent vulnerability for tampering with meter data and the related customer billing. Transmission and distribution substations contain many power control devices such as circuit breakers, transformers, capacitors, and monitoring devices. The smart grid increases the level of automation in substations and with this increase, the number of electronic control elements increases the potential vulnerabilities. Smart Grid uses new sensors which will enhance the situational awareness of the grid and enable operators to react to power anomalies more quickly but sensor network itself opens up an additional line of attack. The operations center is often ignored in discussions of smart grid security, but it is one of the most important elements of the network. Vulnerabilities can exist in the utility enterprise firewall, its enterprise applications, and/or its operator authentication and training systems. This makes the operation center vulnerable to a top-down attack from an intruder or to an insider-attack from a disgruntled employee.<sup>9</sup>

---

8. [http://www.cisco.com/web/strategy/docs/energy/aag\\_c45\\_539956.pdf](http://www.cisco.com/web/strategy/docs/energy/aag_c45_539956.pdf)

9. [http://carbon-pros.com/blog1/2009/08/smart\\_grid\\_security\\_vulnerabil.html](http://carbon-pros.com/blog1/2009/08/smart_grid_security_vulnerabil.html)

Every day we get reports from different sources regarding the potential attacks to Smart Grid. The Department of Homeland Security (DHS) has reported that cyber spies, likely from China and Russia, have managed to inject malicious software into the electric grid, water, sewage, and other infrastructure control software. This software could enable malicious users to take control of key facilities or networks via the Internet, causing power outages and tremendous damage to all sectors of the economy.<sup>10</sup> As the grid becomes more central to our energy infrastructure, it will become more important to ensure its security. Smart Grid systems create a link between physical systems and software systems, both of which can fail.<sup>11</sup> IOActive, a professional security services firm, determined that an attacker with \$500 of equipment and materials and a background in electronics and software engineering could "take command and control of the AMI allowing for the en masse manipulation of service to homes and businesses. The Reports from CNN questioned the smartness of Smart Grid to forge ahead with the high technology, digitally based electricity distribution and transmission system. It also reported that the tests have shown that a hacker can break into the system, and cybersecurity experts said a massive blackout could result.<sup>12</sup> The American Society for Industrial Security (ASIS) International Chief Security Officer (CSO) Roundtable reported that the electric grid is highly dependent on computer-based control systems. These systems are increasingly connected to open networks such as the internet, exposing them to cyber risks. Any failure of our electric grid, whether intentional or unintentional, would have a significant and potentially devastating impact on our nation. The Wall Street Journal recently reported that cyber spies from China, Russia, and other countries may have penetrated the US electrical grid and implanted software programs that could be used to disrupt the system.<sup>13</sup>

The communications of Association for Computing Machinery (ACM) reported that vulnerabilities in the smart grid also can be caused by inadequate patch, configuration, and change management processes, insufficient access controls, and the failure to create risk assessment, audit, management, and incident response plans. There are also a number of privacy concerns associated with the real-time, two-way communication between consumers and suppliers that the smart grid will allow. One important issue that needs to be dealt with is

---

10. [http://www.smartgridnews.com/artman/publish/News\\_Blogs\\_News/Foreign\\_Cyber-Spies\\_Inject\\_Spyware\\_into\\_U\\_S\\_Grid\\_with\\_Potential\\_for\\_Serious\\_Damage-562.html](http://www.smartgridnews.com/artman/publish/News_Blogs_News/Foreign_Cyber-Spies_Inject_Spyware_into_U_S_Grid_with_Potential_for_Serious_Damage-562.html)

11. [http://www.smartgridnews.com/artman/publish/Technologies\\_Security\\_News/Smart-Security-for-a-Smart-Grid-New-Threats-on-the-Horizon-1226.html](http://www.smartgridnews.com/artman/publish/Technologies_Security_News/Smart-Security-for-a-Smart-Grid-New-Threats-on-the-Horizon-1226.html)

12. <http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/index.html>

13. [http://www.ensec.org/index.php?option=com\\_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345](http://www.ensec.org/index.php?option=com_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345)

the data that will be collected automatically from smart meters and how that information will be distributed and used throughout the grid.<sup>14</sup>

The Smart Grid attacks were also tested in laboratories. IOActive have created a worm that could quickly spread among Smart Grid devices, small computers connected to the power grid that give customers and power companies better control over the electricity they use.<sup>15</sup> Yao Liu, Peng Ning from North Carolina State University and Michael K. Reiter from University of North Carolina, Chapel Hill have reported a new class of attacks, called *false data injection attacks*, against state estimation in electric power grids and they show that an attacker can take advantage of the configuration of a power system to launch such attacks to successfully bypass the existing techniques for bad measurement detection and demonstrated the success of these attacks through simulation using the IEEE 9-bus, 14-bus, 30-bus, 118-bus, and 300-bus systems.<sup>16</sup>

The Smart Grid and related fields have been attacked in the real world. CIA's report from the Associated Press has reported that hackers literally turned out the lights in multiple cities after breaking into electrical utilities and demanding extortion payments before disrupting the power. Reports from Washington Post also claim that the CIA Analysts said cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities. The attacker's information was not known but the intrusion came from the Internet.<sup>17</sup> The National Journal Magazine reported that Computer hackers in China, including those working on behalf of the Chinese government and military, have penetrated deeply into the information systems of U.S. companies and government agencies, stolen proprietary information from American executives in advance of their business meetings in China, and, in a few cases, gained access to electric power plants in the United States, possibly triggering two recent and widespread blackouts in Florida and the Northeast. The hacker triggered a cascade effect, shutting down large portions of the Florida power grid which created the Florida Black Out<sup>18</sup>. The interconnected nature of the bulk electric system requires all entities whose operations can affect the operation of the bulk electric system to be as secure from cyber incidents as practicable to ensure bulk electric system reliability. The North American Electric Reliability Corporation (NERC) reported that on January 25, 2003, the SQL Slammer Worm was released by an unknown source. The worm

---

14. <http://cacm.acm.org/news/43974-smart-grid-vulnerabilities-could-cause-widespread-disruptions/fulltext>

15. <http://hardware.slashdot.org/article.pl?sid=09/03/22/082236>

16. <ftp://ftp.csc.ncsu.edu/pub/tech/2009/TR-2009-5.pdf>

17. <http://www.cyberpunkreview.com/news-as-cyberpunk/the-cias-latest-claim-hackers-have-attacked-foreign-utilities/>

18. [http://www.nationaljournal.com/njmagazine/cs\\_20080531\\_6948.php](http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php)

significantly disrupted many Internet services for several hours. It also adversely affected the bulk electric system controls.<sup>19</sup>

Smart Grid will simultaneously expand the infrastructure for transporting electricity and present a more physically challenging infrastructure to protect. Smart Grid's use of internet technologies should have full protection prior to its deployment as it is a matter of national security.<sup>20</sup>

---

19. <http://www.nerc.com/docs/standards/Chuck-Noble-RBB-Letter.pdf>

20. [http://www.smartgridnews.com/artman/publish/News\\_Blogs\\_News/Foreign\\_Cyber-Spies\\_Inject\\_Spyware\\_into\\_U\\_S\\_Grid\\_with\\_Potential\\_for\\_Serious\\_Damage-562.html](http://www.smartgridnews.com/artman/publish/News_Blogs_News/Foreign_Cyber-Spies_Inject_Spyware_into_U_S_Grid_with_Potential_for_Serious_Damage-562.html)

## **3.0 INFORMATION ASSURANCE AND SECURITY CONCEPTS AND POLICIES**

Information Assurance and Security issues ultimately involve protection of information. Information protection criteria are usually specified in policies such as confidentiality, integrity, and availability. The researchers included accountability as a separate policy even though it can be viewed as Integrity issue because it is critical for the smart grid. NIST has defined these security policies as follows.<sup>21</sup>

### **3.1. Confidentiality**

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

### **3.2. Integrity**

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Data integrity is the property that data has not been altered in an unauthorized manner. It covers data integrity covers data in storage, during processing, and while in transit and includes the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

### **3.3. Availability**

Ensuring there's timely and reliable access to and use of information.

### **3.4. Accountability**

Is the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity? This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

### **3.5. Security Concepts and Smart Grid**

With the Smart Grid's transformation of the electric system to a two-way flow of electricity and information, the Information Technology (IT) and telecommunications infrastructures have become critical to the energy sector infrastructure. Therefore, the management and protection of systems and components of these infrastructures must also be addressed by an increasingly diverse energy sector.

IT and telecommunication sectors have existing cyber security standards to address vulnerabilities and assessment programs to identify known vulnerabilities in these systems.

---

21. <http://www.nerc.com/docs/standards/Chuck-Noble-RBB-Letter.pdf>

These same vulnerabilities need to be assessed in the context of the Smart Grid. In addition, the Smart Grid has additional vulnerabilities due to its complexity, large number of stakeholders, and highly time-sensitive operational requirements.

The following definitions of cyber infrastructure and cyber security from the National Infrastructure Protection Plan (NIPP) and quoted in NISTIR7628 are included to ensure a common understanding.

- **Cyber Infrastructure:** Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.

For this document, cyber security is defined as follows:

- **Cyber Security** the protection required to ensure confidentiality, integrity and availability of the electronic information communication system.
- **Integrity** is generally considered the most critical security requirement for power system operations, and includes assurance that:
  - Data has not been modified without authorization
  - Source of data is authenticated
  - Timestamp associated with the data is known and authenticated
  - Quality of data is known and authenticated
- **Availability** is generally considered the next most critical security requirement, although the time latency associated with availability can vary:
  - 4 ms for protective relaying
  - Sub-seconds for transmission wide-area situational awareness monitoring
  - Seconds for substation and feeder SCADA data
  - Minutes for monitoring non-critical equipment and some market pricing information
  - Hours for meter reading and longer term market pricing information
  - Days/weeks/months for collecting long term data such as power quality information

- **Confidentiality** is generally the least critical for actual power system operations, although this is changing for some parts of the power system, as customer information is more easily available in cyber form:
  - Privacy of customer information is the most important
  - Electric market information has some confidential portions
  - General corporate information, such as human resources, internal decision-making, etc.

## 4.0 ADVANCED METERING INFRASTRUCTURE (AMI) SECURITY ISSUES

### 4.1. Introduction

Advanced Metering Infrastructure (AMI) refers to systems that measure, collect and analyze energy usage, from advanced devices such as electricity meters, gas meters, and/or water meters, through various communication media on request or on a pre-defined schedule. This infrastructure includes hardware, software, communications, customer associated systems and meter data management (MDM) software.<sup>22</sup>

The network between the measurement devices and business systems allows collection and distribution of information to customers, suppliers, utility companies and service providers. This enables these businesses to either participate in, or provide, demand response solutions, products and services. By providing information to customers, the system assists a change in energy usage from their normal consumption patterns, either in response to changes in price or as incentives designed to encourage lower energy usage use at times of peak-demand periods or higher wholesale prices or during periods of low operational systems reliability.

AMI systems are viewed as consisting of the following components (see also Figure 3):<sup>23</sup>

- Smart Meter – The smart meter is the source of metrological data as well as other energy-related information. These smart meters can provide interval data for customer loads as well as distributed generation.
- Customer Gateway – The customer gateway acts as an interface between the AMI network and customer systems and appliances within the customer facilities, such as a Home Area Network (HAN) or Building Management System (BMS). It may or may not co-locate with the smart meter.
- AMI Communications Network – This network provides a path for information to flow from the meter to the AMI head end.
- AMI Head End – This system manages the information exchanges between external systems, such as the Meter Data Management (MDM) system and the AMI network.

---

22. Wikipedia; Advanced Metering Infrastructure; Available [Online]:  
[http://en.wikipedia.org/wiki/Advanced\\_Metering\\_Infrastructure](http://en.wikipedia.org/wiki/Advanced_Metering_Infrastructure)

23. Open Smart Grid; Shared Documents; Available [Online]:  
<http://osgug.ucaiug.org/Shared%20Documents/Forms/AllItems.aspx>

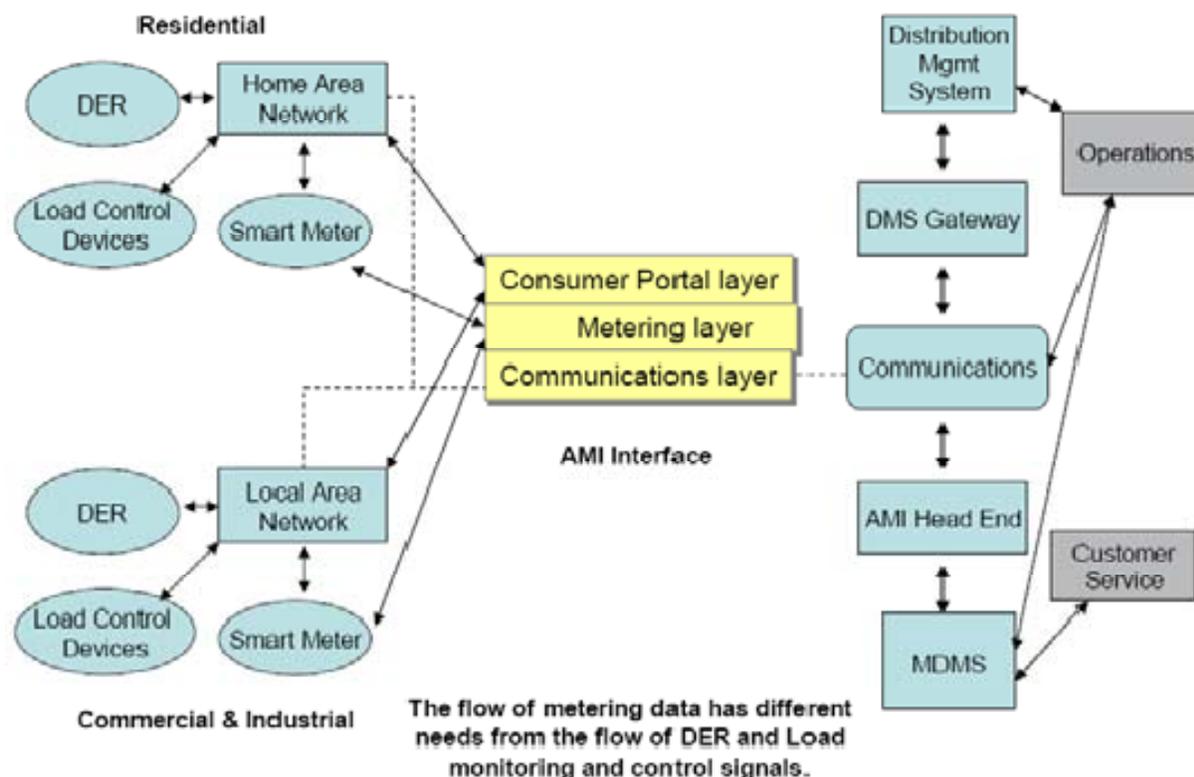


Figure 3. AMI components.

Source: Open Smart Grid; Shared Documents<sup>24</sup>

## 4.2. AMI Security Threats<sup>25</sup>

The following types of security threats are possible on AMI of Smart Grid:

- **Eavesdropping:** It is unauthorized real-time interception of a private communication.
- **Traffic Analysis:** It is the process of intercepting and examining messages in order to deduce information from patterns in communication.
- **EM/RF Interception:** Electro -Magnetic/ Radio Frequency interception to perform unauthorized interception of private communication.
- **Indiscretions by Personnel:** Lack of discretion of personnel could lead to unauthorized interception of private communication.

24. <http://osgug.ucaiug.org/Shared%20Documents/Forms/AllItems.aspx>

25. Cyber Security Issues for Advanced Metering Infrastructure (AMI); F. M. Cleveland Senior Member IEEE, IEEE T&D Conference, April 2008

Advanced Metering Infrastructure Security Considerations; Raymond C. Parks; Assurance Technologies and Assessments, SANDIA REPORT, SAND2007-7327; Sandia National Laboratories

- **Media Scavenging:** It involves rummaging through disposed magnetic media for retrieving sensitive data that is left behind on it.
- **Intercept/ Alter:** Unauthorized people may intercept and alter the AMI data.
- **Repudiation:** People, including public authorities, may modify the AMI data and thus refuse to acknowledge an action that took place.
- **Masquerade:** It is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for.
- **Bypassing Controls:** People may bypass security controls to get access to the confidential data and make unauthorized modifications.
- **Authorization Violation:** People may violate the authorization of AMI system to perform unauthorized actions.
- **Physical Intrusion:** People may physically intrude into AMI system components like Smart Meter to perform unauthorized actions.
- **Man-in-the-Middle:** It is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.
- **Integrity Violations:** Integrity is violated when someone accidentally or with malicious intent modifies the AMI interaction data.
- **Theft:** Physical theft of the AMI components could lead to unauthorized actions being performed.
- **Replay:** It is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.
- **Virus/Worms:** A computer virus is a computer program that can copy itself and infect a computer. A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention.
- **Trojan Horse:** It is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.
- **Trapdoor:** An undocumented entry point into a computer program, which is generally inserted by a programmer to allow discreet access to the program.
- **Service Spoofing:** It is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

- **Resource Exhaustion:** Hackers may use up all available facilities so no real work can be accomplished and thus AMI system resources become unavailable to the intended users.
- **Integrity Violations:** Integrity is violated when someone accidentally or with malicious intent modifies the AMI data and thus prevents intended users from using the AMI system resources.
- **Stolen/Altered:** The AMI data could be stolen or altered and that could lead to denial of action that took place or claim of an action that did not take place.
- **Repudiation:** People, including public authorities, may refuse to acknowledge an action that took place.
- **Insider Attack:** The insider attack would take advantage of access to systems at the opposite end of the AMI system from the customer endpoint. The systems that the insider may be able to access include the AMI head-end, the system from which it gets pricing information (either EMS or ICCP server to an ISO or generation entity), and the network infrastructure supporting both of those systems. Which cyber-effect an insider uses would depend upon their access to these systems.
- **Unauthorized Access from Customer Endpoint:** There is a potential for AMI to allow access to the bulk electric grid from the residential or small business customer endpoint. The adversary can suborn the customer endpoint, crack wireless communications between the AMI meter and other endpoint equipment, or crack wireless communications from the AMI meter to the local concentrator. These attacks will expose the head end equipment and systems to which the head end are connected. The exact details of this attack are greatly dependent on the implementation of AMI, particularly at the head end. Certain configurations would allow an attacker to affect the bulk electric grid.
- **Cheating Customer:** The customer at an endpoint would attack to achieve the goal of reduced cost of electric and/or natural gas use. They would use information freely available from the AMI meter vendor or a standard associated with AMI meters to reset the meter and reprogram it to report false information. If the information is not freely available, the attacker would reverse-engineer a meter to develop a way to modify it. This is very similar to the many cable modem attacks that are openly available. Either the configuration settings from the utility or the actual firmware controlling the operation of the meter would be modified in this attack.

The following table summarizes the various security threats on AMI with respect to security goals and potential threat level.

**Table 1. Security threats on AMI with respect to security goals**

Security Issue	Description	Security Goal Compromised	Security Threat Level
Listening	Unauthorized people listening to the AMI communication. <ul style="list-style-type: none"> <li>• Eavesdropping</li> <li>• Traffic Analysis</li> <li>• EM/RF Interception</li> <li>• Indiscretions by Personnel</li> <li>• Media Scavenging</li> </ul>	Confidentiality	High
Modification	Unauthorized modification of the AMI data. <ul style="list-style-type: none"> <li>• Intercept/ Alter</li> <li>• Repudiation</li> </ul>	Integrity	High
Interactions	Interactions of AMI components with the environment could lead to unauthorized access to AMI communication information, modification of AMI data, denial of service to authorized users, and non-repudiation. <ul style="list-style-type: none"> <li>• Masquerade</li> <li>• Bypassing Controls</li> <li>• Authorization Violation</li> <li>• Physical Intrusion</li> <li>• Man-in-the-Middle</li> <li>• Integrity Violations</li> <li>• Theft</li> <li>• Replay</li> </ul>	Confidentiality Integrity Availability Accountability	High
Planted in System	Malicious code/components planted in the system could lead to unauthorized access to AMI communication information, modification of AMI data, denial of service to authorized users, and non-repudiation. <ul style="list-style-type: none"> <li>• Virus/Worms</li> <li>• Trojan Horse</li> <li>• Trapdoor</li> <li>• Service Spoofing</li> </ul>	Confidentiality Integrity Availability Accountability	High

<b>Security Issue</b>	<b>Description</b>	<b>Security Goal Compromised</b>	<b>Security Threat Level</b>
Denial of Service	<p>It is an attempt to make AMI system resources unavailable to its intended users.</p> <ul style="list-style-type: none"> <li>• Resource Exhaustion</li> <li>• Integrity Violations</li> </ul>	Availability	High
After-the-Fact	<p>Denial of action that took place or Claim of the action that did not take place is covered under this category.</p> <ul style="list-style-type: none"> <li>• Stolen/Altered</li> <li>• Repudiation</li> </ul>	Accountability	Medium
Insider Attack	<p>The insider attack would take advantage of access to systems at the opposite end of the AMI system from the customer endpoint.</p>	Confidentiality Integrity Availability Accountability	Low to High
Unauthorized Access from Customer Endpoint	<p>There is a potential for AMI to allow access to the bulk electric grid from the residential or small business customer endpoint</p>	Confidentiality Integrity Availability Accountability	High
Cheating Customer	<p>The customer at an endpoint would attack to achieve the goal of reduced cost of electric and/or natural gas use.</p>	Confidentiality Integrity Availability Accountability	Low to High

## 5.0 DEMAND RESPONSE SECURITY ISSUES

### 5.1. Introduction

When electricity demand is peak, particularly in summer, utilities and other electric Independent Systems Operators (ISOs) keep electric generators on-line in order to meet high demand. This solution wastes energy and increases air pollution.<sup>26</sup> If the demand is highest in most regions and exceeds available supplies, brownouts and blackouts can happen. As a result, the electricity grids are not reliable enough. Many utilities, government, and others have been developing Demand Response (DR) to manage growth in peak electricity demands, and to provide more reliable electricity grids and more economic energy. Demand Response is "...an action taken to reduce electricity demand in response to price, monetary incentives, or utility directives so as to maintain reliable electric services or avoid high electricity prices."<sup>27</sup> During the peak hours, demand response programs or tariffs lower the energy use in return for decreasing total system costs and electric loads. Demand Response can reduce energy consumption during peak time or based on events (of which the energy prices are high), such as congestion, supply-demand balance and/or market conditions that raise the energy supply costs. Demand Response Research Center (DRRC) has been putting efforts to develop, demonstrate and deploy activities related to a framework which can enable automated demand response. The development of Open Automated Demand Response (OpenADR or Open Auto-DR) has been carried out in order to improve optimization between electric supply and demand which can improve the reliability of electronic grid and lower the total cost of overall systems. This section will mainly focus on security issues in communications and interfaces between the entities in DR system and OpenADR. OpenADR is "a set of standard, continuous, open communication signals and systems provided over the Internet to allow facilities to automate their demand and response with no human in the loop."<sup>28</sup> This report does not intend to focus on the details of how the DR and OpenADR systems operate. It may address some of Demand Response systems, but the main focus is on the security issues in the DR and OpenADR systems.

---

26. California Energy Commission's Public Interest Energy Research Program, PIER Buildings Program, "Automated Demand Response Cuts Commercial Building Energy Use and Peak Demand, Technical Brief", Public Interest Energy Research Program ,2008[online]. Available: <http://www.energy.ca.gov/2008publications/CEC-500-2008-086/CEC-500-2008-086-FS.PDF>. [Accessed October 15, 2009]

27. U.S. Federal Energy Regulatory Commission (FERC), "Assessment of Demand Response and Advanced Metering", 2007[online]. Available: <http://www.ferc.gov/legal/staff-reports/09-07-demand-response.pdf>. [Accessed October 17, 2009]

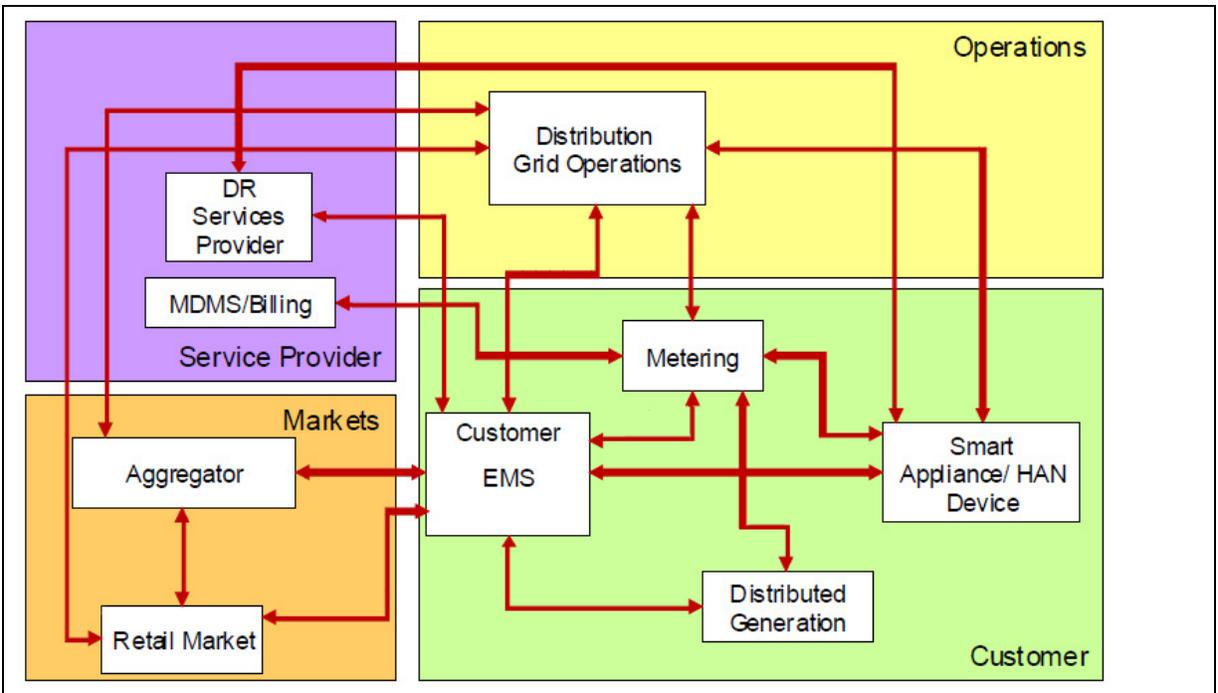
28. S. Kilicote, M.A. Piette, J.H. Dudley, Lawrence Berkeley National Laboratory (LBNL); E. Koch and D. Hennage, Akuacom, "Open Automated Demand Response for Small Commercial Buildings", Lawrence Berkeley National Laboratory ,July 2009 [online]. Available: <http://drcc.lbl.gov/pubs/lbnl-2195e.pdf>. [Accessed October 16, 2009]

## 5.2. Demand Response and Security Concerns

The primary focus on the Demand Response (DR) is to provide the customers with pricing information so that the customers or the energy-management and control system (EMCS) at the customer's sites may respond based on the demands for electricity and electricity prices during some period of time. For instance, the customer may decrease demand (or shed load) during higher priced time periods or increase demand (or shift load) during lower priced time periods. The pricing information could be real-time based, tariff-based or some combination. DR could be implemented in many different ways based on the type of pricing signals. The real-time pricing (RTP) requires computer-based response, while the fixed time-of-use pricing may be manually handled by the customer based upon the time periods and the pricing. Since the pricing information could be transmitted electronically or fixed for long period and could be accessed by the participants of the DR program the customer's security and privacy should be addressed. Also, the integrity of the pricing signal is critical because if it can be manipulated, it could lead to financial impacts on the organization or customers. Thus, most of the DR functions in the smart grid, such as load shedding, time-of-use pricing (ToU), dynamic pricing, etc. require data integrity and/or confidentiality to maintain the reliability of the grid and prevent adversaries to manipulate the information in the system. Failure to provide integrity and/or confidentiality could result in the exposure of customer's information, unauthorized modification and manipulation of the information.

Security issues are explained below by first looking at interfaces of components that affect demand response. Next Auto Demand response systems are analyzed with respect to security.

Figure 4 shows the major components of Smart Grid that affect Smart Grid and their interactions.



**Figure 4. Demand response use case shows the interfaces between each component (from NIST).**

Source: Lawrence Berkeley National Laboratory/ Akuacom<sup>29</sup>

### 5.2.1. Confidentiality

The information sent between each entity, such as control usage of the meter, pricing and metering usage and billing information, needs to be confidential and protected from unauthorized access to the information, such as eavesdropping attacks, since it can lead to the invasion of customer privacy and the leaking of the information to an adversary.

### 5.2.2. Authentication

The components in DR system, such as Home Area Network (HAN) Devices, Energy Management System (EMS), DR services provider and metering, must be authenticated in order to communicate with each other. If they fail to authenticate with the DR control services, they must not be able to connect or respond to the DR event signals in order to protect from the unauthorized devices to communicate with the DR system, such as hijacking of the meter connection.

29. A. Lee, T. Brewer, Computer Security Division, Information Technology Laboratory, National Institution of Standards and Technology (NIST) (Sept 2009). Smart Grid Cyber Strategy and Requirements (Draft NISTIR 7628). Available: <http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf>. [Accessed October 20, 2009]

### **5.2.3. Data Integrity**

Unauthorized manipulation of demand information, control signals for the EMS to manage devices and control usage of the meter or smart meter by inducing an inappropriate response, such as turning on/off electrical devices at customer sections or shutting down DR operation, could directly decrease power reliability and quality of the grid and cause financial impacts as well as annoyance on customers. Also, manipulating the pricing signal could adversely impact the customer and market sections financially.

### **5.2.4. Availability**

Pricing and metering usage information need to be confidential, accurate and available all the time; otherwise, it would affect DR control behavior. The grid may not be able to respond based on the signals and take a wrong action, leading to financial impacts on customers and markets. Real-time load use information transmitted between DR services provider and customer EMS needs to be available in a timely manner since it can affect the behavior of the grid. Legacy devices at end user and low bandwidth of communication channels may result in the loss of availability.

### **5.2.5. Accountability**

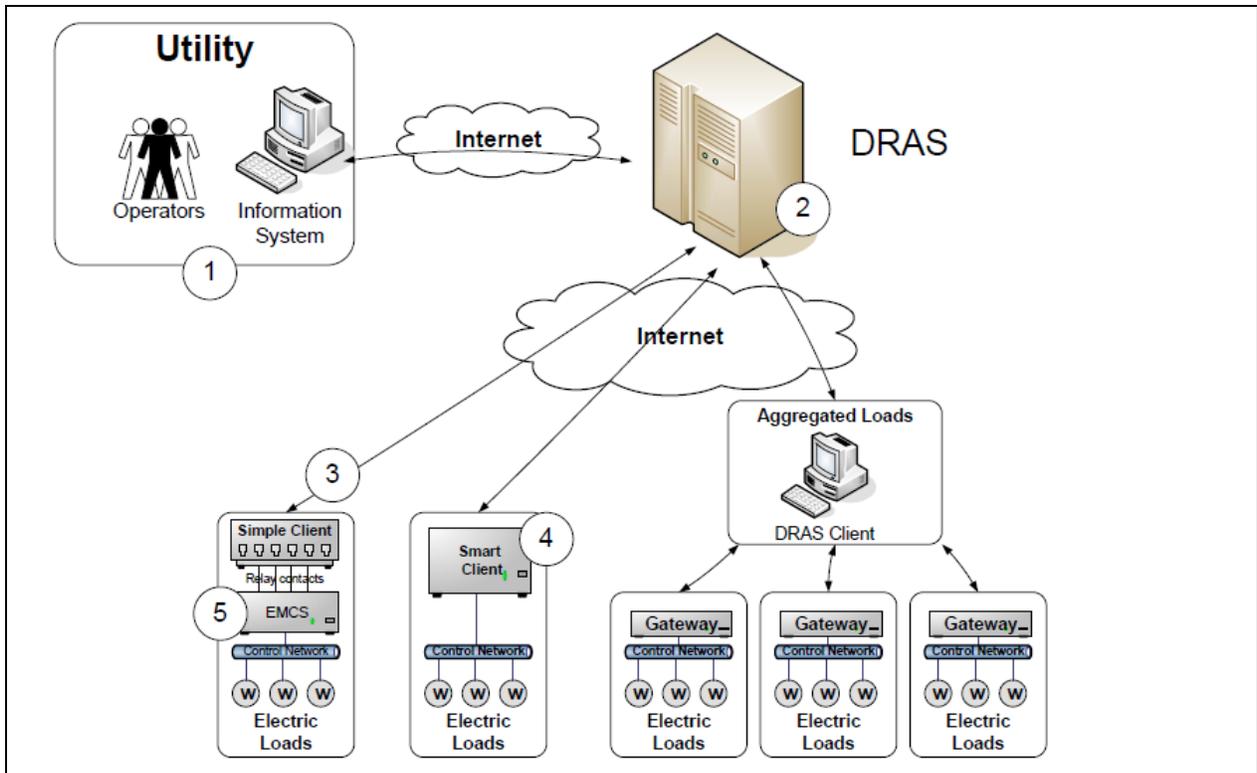
Failure to hold account of the actions taken by communicating parties because of the invalid meter, EMS, or DR services provider information would result in the dispute between parties and decrease customer confidence.

## **5.3. Open Automated Demand Response**

OpenADR is a communications data model designed to interact with Demand Response signals by automated DR actions from Energy-Management and Control System (EMCS), which are pre-programmed, at electric consumer's sites. Internet-based electricity pricing and DR signals are used with pre-programmed control strategies to optimize energy use of a site or building with no manual intervention. OpenADR is used to exchange information between a utility or Independent System Operator (ISO) and the end-point users or customer systems.

### **5.3.1. Open Automated Demand Response Communications Infrastructure**

OpenADR architecture depicted in Figure 5 consists of a Demand Response Automation Server (DRAS) and a DRAS Client. A server provides signals corresponding to DR events to notify customers and a client at the customer's site listens to the signals and automates signals to pre-programmed control systems (See Figure 5).



**Figure 5. Generic open automated demand response interface architecture.**

Source: Lawrence Berkeley National Laboratory/ Akuacom<sup>30</sup>

Information flow in the OpenADR architecture is in five steps, as follows:

- 1) The utility or ISO defines DR event and price signals that are sent to DRAS.
- 2) DR event and price services published on a DRAS.
- 3) DRAS clients, that can be a client and logic with integrated relay (CLIR) for a legacy control system or web service software for a sophisticated control system, request event information from the DRAS every minute.
- 4) Pre-programmed DR strategies determine action based on event and price.
- 5) EMCS carries out load shed based on DR events and strategies.

30. S. Kiliccote, M.A. Piette, J.H. Dudley, Lawrence Berkeley National Laboratory (LBNL); E. Koch and D. Hennage, Akuacom, "Open Automated Demand Response for Small Commercial Buildings", Lawrence Berkeley National Laboratory, July 2009 [online]. Available: <http://drcc.lbl.gov/pubs/lbnl-2195e.pdf>. [Accessed October 16, 2009]

### 5.3.2. Demand Response Automation Server (DRAS)

The DRAS is an infrastructure component in Automated Demand Response programs which are based on a client-server infrastructure. The automation server distributes and receives information among its entities, such as utilities and ISOs. The purpose of the DRAS is to automate dynamic pricing and reliable related messages and information received from utilities or ISOs to optimize the consumption of electricity during peak hours. The DRAS is an integrator between a Utility/ISO and DR participants. The major roles of DRAS are to notify the participants regarding real-time prices (RTP), DR events and DR related messages including dynamic pricing.

Figure 6 shows details of DRAS and its interface to utility and participant sites including the internet interface.

The DRAS interface can be implemented through WSDL or SOAP. XML can be used for the data model and the entities. The DRAS interface functions are divided into three groups as follows:

- 1) Utility and ISO Operator Interfaces
- 2) Participant Operator interfaces
- 3) DRAS Client Interfaces

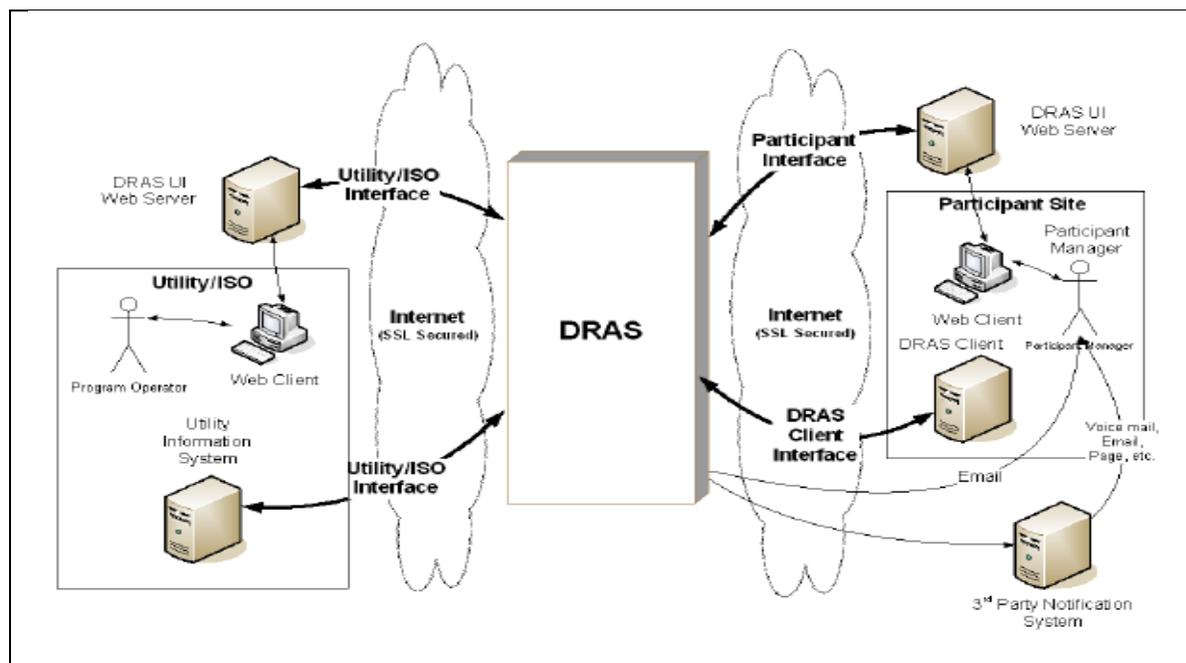


Figure 6. DRAS Interfaces.

Source: Lawrence Berkeley National Laboratory/Akuacom<sup>31</sup>

31. M.A. Piette, G. Ghatikar, S. Kiliccote, E. Koch, D. Hennage, P. Palensky, and C. McParland, "Open Automated Demand Response Communications Specification", Demand Response Research Center,

### **5.3.3. OpenADR and Security Concerns**

Since the OpenADR system is based on the Internet communication, the information transmitted in each DRAS interface must be protected and prevented from any kinds of data manipulation, such as changing pricing information and DR events. The DRAS and DRAS clients need to be authenticated in order to communicate with each other. Also, access control to each entity in the OpenADR system is needed in order to protect from unauthorized access to the system. If the security goals are breached, potentially adverse impacts could occur, such as the excessive loads in the grid leading to blackouts and the large financial impacts on both the utility and participants in DR program.

This section is focusing on the security concerns on the information transmitted between the utility/ISO, DRAS and DRAS client. Table 2 below describes possible attacks and impacts that could happen if each security goal is compromised for each of the information transmitted in the OpenADR system. The information transmitted in the OpenADR is categorized into three groups based on the DRAS interfaces.

**Table 2. Possible attacks utility/ISO operator interfaces**

Utility/ISO Operator Interfaces		
Purpose	Information Transmitted	Security Concerns
To initiate or update DR event information in DRAS	Program type, date & time of the event, date & time issued, geographic location, customer list (account numbers) and load shed event information.	<p><b>Confidentiality (L):</b> Eavesdropping on this formation is not of concern since the information may not be sent regularly. However, the information needs to be protected from unauthorized access.</p> <p><b>Integrity (H):</b> Attacker modifies configuration data in the DRAS, such as DR program data, customer list and shed event information, affecting the DR program behavior. Attacker issues false or malicious DR events in DRAS, causing blackouts and instability of the grid. Also, this may lead to the financial impacts on customers.</p> <p><b>Availability (L):</b> Failure in communication between utility and DRAS</p>
To initiate bid request in DRAS	Program type, date & time of the event, date & time issued, geographic location, customer list (account numbers), request for a bid (RFB) issue date & time, RFB close time, price offered for load reduction per time block.	<p><b>Confidentiality (H):</b> Eavesdropping on this formation could result in the leaking of bidding and also pricing information to the attacker.</p> <p><b>Integrity (H):</b> Unauthorized manipulation on this information could affect the bidding program behavior. Attacker issues false bidding information, causing the false behavior of the bidding program and the financial impacts on customer.</p> <p><b>Availability (L):</b> Failure in communication between utility and DRAS.</p>
To set accepted bids in DRAS	Participant list (account numbers), accept or reject, load reduction bids per time block (for verification)	<p><b>Confidentiality (H):</b> Eavesdropping on this formation could lead to the invasion of participant's privacy.</p> <p><b>Integrity (H):</b> Attacker modifies participant list or load reduction per time block, accepted or rejected bid, causing instability of the grid and having financial impacts on participants. Attacker issues accepted/rejected bids to DRAS clients which may make an inappropriate response, such as increase the loads, according to the false accepted or rejected bids received.</p> <p><b>Availability (L):</b> Failure in communication between utility and DRAS</p>

**Table 3. Possible attacks and impacts of DRAS client interfaces**

DRAS Client Interfaces		
Purpose	Information transmitted	Overall Impacts
<p>To send shed or event information to trigger the event client to shed or shift loads at participant sites, facilities or aggregator sites</p>	<p>Utility event information for smart DRAS clients, such as date &amp; time of the event, date &amp; time issued mode and pending signals. Mode and pending signals for simple clients. Event pending signals for simple clients.</p>	<p><b>Confidentiality (H):</b>                      Attacker intercepts information sent between DRAS and DRAS client to gain knowledge of DR events, pricing information, customer information. Loss of confidentiality on this information can lead to the exposure of customer data, unauthorized modification of information, manipulation of information, malicious attacks, etc. causing the instability of grid and financial impacts on customers.</p> <p><b>Integrity (H):</b>                      Attacker issues false/malicious DR events. Attacker may be able to turn on air conditioning or heater units in a large commercial building which can cause excessive loads to the grid and blackouts may take place, resulting in the instability of the grid and financial impacts on customers. Attacker may be able to shut down all air conditioning units which can cause annoyance and possible health concerns in some customers. Attacker issues false time synchronization, causing events to occur sooner or later than they normally would have. The signals need to be authenticated that they actually came from the DRAS. Inability to authenticate DRAS, DRAS client and UIS can lead to a number of attacks, such as authentication sniffing, denial of service (DoS), man-in-the-middle attack, etc. Attacker captures an authentic signal, prevents the required reduction in load forcing utilities to take other measures such as buying energy at higher costs, and blackouts could occur.</p> <p><b>Availability (H):</b>                      Attacker prevents the reduction of the load by disabling DRAS clients from receiving the incoming DR signals using denial of service attacks. Attacker floods the DRAS communications channel with non-DR related Internet traffic. Failure in communication between DRAS and DRAS clients.</p> <p><b>Accountability (M):</b>                      Participant denies receiving DR events.</p>

<b>DRAS Client Interfaces</b>		
<b>Purpose</b>	<b>Information transmitted</b>	<b>Overall Impacts</b>
		Participant denies receiving bidding information.
To send request for bid to participant or facility manager or aggregator	This information comes in the form of an email, phone call or page.	<b>Integrity (L):</b> An adversary may manually send an email, make a phone call or submit a page to the participant or facility manager so that the manager may respond to the adversary instead of to DRAS or the manager may take a wrong action in response to the bid request.
To notify the acceptance or rejection notification to the participant or facility manager or aggregator	This information comes in the form of an email, phone call or page.	<b>Integrity (L):</b> An adversary may manually send an email, make a phone call or submit a page to the participant or facility manager so that the manager may respond to the adversary instead of to DRAS or the manager may take a wrong action in response to the notification.

**Table 4. Possible attacks and impacts of participant interfaces**

Participant Interface		
Purpose	Information transmitted	Overall Impacts
To set, adjust or cancel standing bids in the DRAS.	Load reduction per time block (price and load amount)	<p><b>Confidentiality (M):</b> Attacker intercepts load reduction information sent from participant to the DRAS in order to gain knowledge of this information, causing the leak in the electricity usage of the customer.</p> <p><b>Integrity (H):</b> Attacker submits bids for participants, causing the financial impacts on participants.</p> <p><b>Availability (L):</b> Failure in communication between DRAS and DRAS client.</p>
To send the system load status information to DRAS from DRAS clients.	Program identifier, facility or participant identifier, date & time of the event (shed or shift), shed data in kW/kWh, load reduction end uses (HVAC, lighting, etc.), event type (Day-Ahead or Day-Of)	<p><b>Confidentiality (H):</b> Eavesdropping on this formation could invade the customer privacy.</p> <p><b>Integrity (H):</b> Unauthorized manipulation on this information could make DRAS not be able to record the actual response of the DRAS client to the DR events received. The DRAS may make an inappropriate response to the DR program according to the false system load status. This could lead to the unreliability of the grid.</p> <p><b>Availability (L):</b> Failure in communication between DRAS and DRAS client.</p>

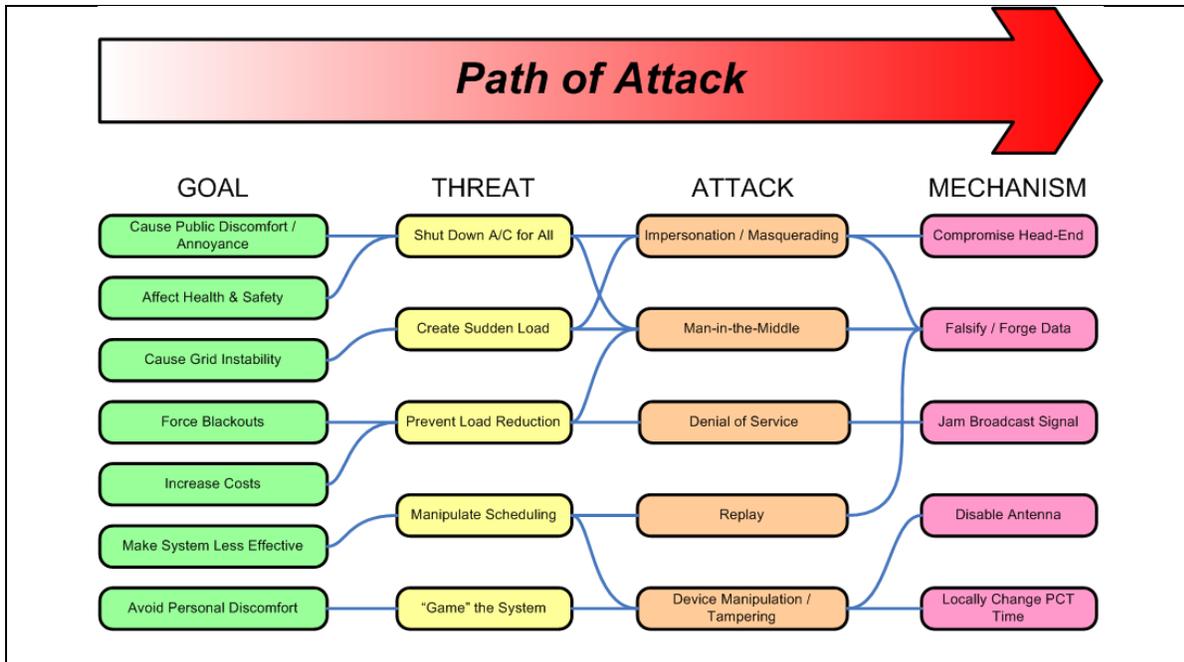
## **5.4. Demand Response at Residential Sites and Security Issues**

Demand response events arrive at the residential site from the utility to adjust the electricity price. During peak hours the price of the electricity rises; through demand response the customers can adjust their residential temperature on the basis of the demand response event received. During normal conditions the broadcast messages consisting of price signals are sent to residential whereas during emergency control signals are issued. The Programmable Communicating Thermostat (PCT) would be used in order to reduce the electric power at the residential site. Broadcast messages which will be sent out to the thermostat which causes the thermostat to update the power consumption. The PCT will be provided to the residential customers by the IOU's. The PCT will communicate with the utility through a meter. The connection is done through a wide area network. The PCT allows the customer to set the temperature for heating as well as cooling. Security issues such as confidentiality, integrity, availability and, non-repudiation come into effect for the PCT during the flow of events from the utility to the residential site. Integrity plays a crucial role in PCT. An attacker can cause annoyance, affect health and safety, grid instability by carrying out blackout, increase cost for the customer as some form of threats.

### **5.4.1. Possible Attacks in PCT**

- An attacker may attempt to shut down the A/C, prevent the load reduction, and manipulate the scheduling of events received.
- An attacker tries to tamper with the incoming signals or PCT system. The attacker carries out the attacks by carrying out masquerading and man in the middle attack by shutting or turning down the A/C units in order to cause the grid instability.
- An attacker blocks the incoming broadcast signal by carrying out denial of service attack. Replay attacks can be carried out in order to manipulate the incoming demand response signal.
- An attacker could manipulate the system by disabling the PCT antenna or changing the PCT local time.

A summary of attack patterns in PCT is shown in Figure 7.



**Figure 7. Path of attack in PCT.**

Source: Lawrence Berkeley National Laboratory/Akuacom<sup>32</sup>

32. E. W. Gunther, "Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008", March 2007 [online]. Available: [http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC\\_rev15.doc](http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc). [Accessed October 22, 2009]

# 6.0 CUSTOMER DOMAIN – HOME AREA NETWORK, GATEWAY, AND NEIGHBORHOOD AREA NETWORK SECURITY ISSUES

## 6.1. Introduction

Actors in the Customer domain enable customers to manage their energy usage and generation. Some actors also provide control and information flow between the customer and the other domains. The boundaries of the customer domain are typically considered to be the utility meter. The customer domain is electrically connected to the distribution domain. It communicates with the Distribution, Operations, Market, and Service Provider domains. The reason why this section is subdivided into HAN, gateway and Neighborhood area network is that each actor contributes to making the customer interaction with the smart grid a possibility. Therefore we will handle each of the domains in the same order

Figure 8 depicts the entire customer domain with components such as Utility, AMI-HAN interface, Gateway and multiple HAN protocols which help connect various smart appliances in the Home area network. Along with HAN, gateway there exist WNAN as well which is depicted in the figure below as communication between smart meter and the utility. The two communication standards considered in this figure are Wireless Neighborhood Area Network (WNAN) and Local Area Network (LAN).

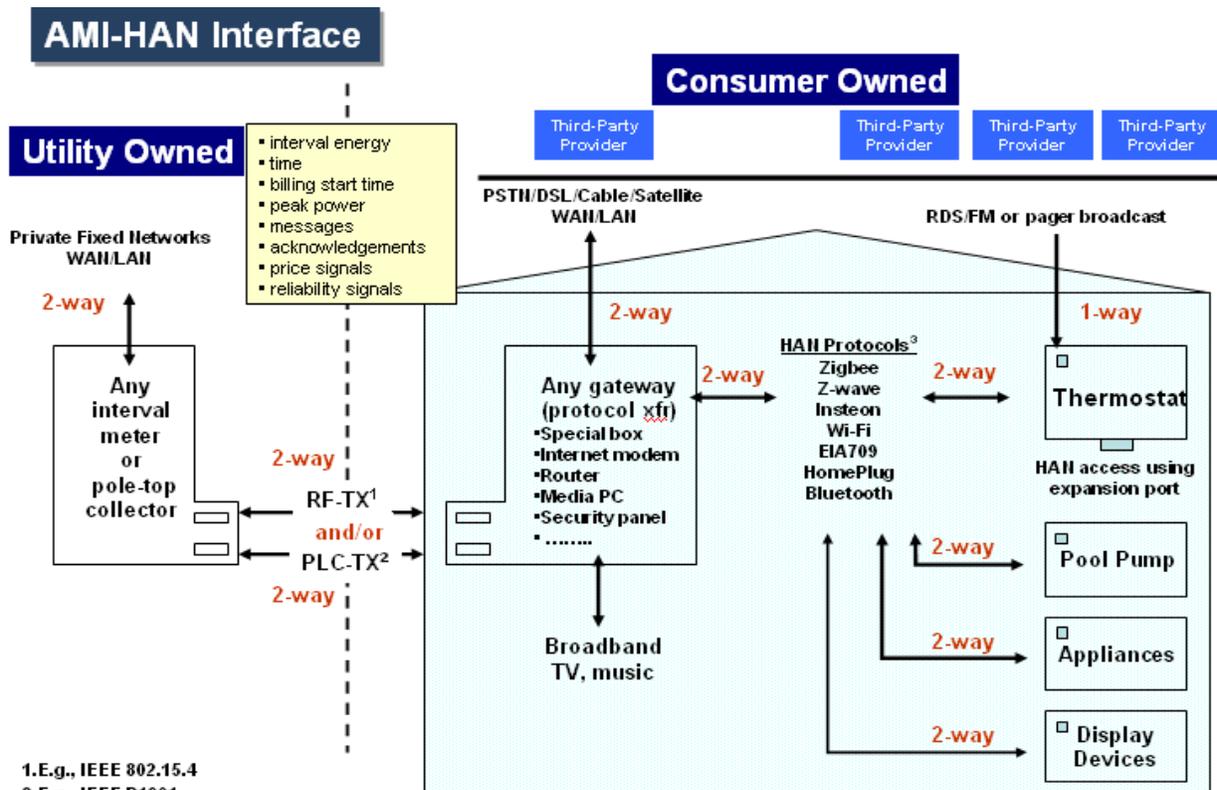


Figure 8. HAN/Gateway.

Source: From the draft document on Residential Gateway Reference Design meeting held at UC Berkeley

## 6.2. Home Area Network (HAN)

Smart Grid provides two-way communications between homeowners' premises and utility companies' back-end IT infrastructure. This is done by deploying Advanced Metering Infrastructure (AMI) systems that combine Home Area Networks (HANs) and Neighborhood Area Networks (NANs). A HAN typically connects home devices together whereas a NAN connects the home for the Utility Network. The key enabling technology for energy management products in the home are protocols such as ZigBee and Z-Wave, ultra low-power IEEE 802.15.4-based wireless networking standard that has emerged as the key to robust, reliable and secure HAN deployments. Although there are several other potential HAN Protocols, ZigBee is the only one discussed in detail, since it is the most popular open standard for HANs.

### 6.2.1. ZigBee

Following the standard OSI reference model, ZigBee's protocol stack is structured in layers. The physical and the media access layer are based on the 802.15.4 standard. The layers on top of these two layers are specific to Zigbee. They are the network layer, General Operation Framework (GOF) and the application layer. IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks. It focuses on low-cost, low-speed ubiquitous communication between devices (in contrast with other, more end user-oriented approaches, such as Wi-Fi). The emphasis is on very low cost communication of nearby devices with little to no underlying infrastructure, so as to exploit this to lower power consumption.<sup>33</sup> It is the basis for ZigBee.

ZigBee makes it practical to embed wireless communications into virtually any home/building automation/metering product without the prohibitive cost and disruption of installing hard wiring. ZigBee allows individual devices to work for long periods of time (approximately 2+ years) on battery power.<sup>34</sup>

---

33. K. Stouffer, J. Falco, K. Scarfone, Guide to Industrial Control Systems (ICS) Security, National Institution of Standards and Technology (NIST), Sept 2008 [online]. Available: [http://csrc.nist.gov/publications/drafts/800-82/draft\\_sp800-82-fpd.pdf](http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf)

34. A. Lee, T. Brewer, Computer Security Division, Information Technology Laboratory, National Institution of Standards and Technology (NIST), Smart Grid Cyber Strategy and Requirements, Draft NISTIR 7628, Sept 2009 [online]. Available: <http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf>

### **6.2.2. Z-Wave**

Z-Wave is a wireless communications proprietary standard designed for home automation, specifically to remote control applications in residential and light commercial environments. The technology, which is developed by Zensys, uses a low-power RF radio embedded or retrofitted into home electronics devices and systems, such as lighting, home access control, entertainment systems and household appliances. Since it is a proprietary standard, not much information is available on Z-Wave.<sup>35</sup>

### **6.3. Gateway Component**

Home Gateway (HG), also called Residential Gateway (RG) is a device that interconnects various home electronic devices to one another as well as connects these private home network devices to exterior public network. In the smart grid architecture the current assumption is that there is an identifiable unit performing the gateway function. But whether the gateway will be an independent functional unit or will it be a part of other smart grid component is an open possibility.

There are two implementation techniques for the gateway:

- 1) The gateway is part of the PCT (Programmable Communicating Thermostat), one such example is the U-SNAP (Utility Smart Network Access Port).<sup>36</sup> This is a hardware solution to the interoperability issues between the native AMI network and the home area network. U-SNAP card brings a Serial interface between the module that communicates with the Utility AMI network and the HAN control unit.
- 2) A gateway as an individual component. This gateway implementation technique involves hardware component which integrates ZigBee based home automation system with an external IP based network. The gateway provides two functionalities:<sup>37</sup>
  - 1) Data translation between the IP based network and the ZigBee network.
  - 2) To provide a secure environment for processing command received from the external network.

The gateway consists of Wi-Fi module, a ZigBee Microcontroller and a power supply.

### **6.4. Wireless Neighborhood Area Network (WNAN)**

The ubiquitous network requirements for Smart Grid are identified as follows: reliable, secure, power efficient, low latency, low cost, diverse path, scalable technology, ability to support burst,

---

35. E. W. Gunther, Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008 March 2007 [online]. Available: [http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC\\_rev15.doc](http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc)

36. U-SNAP Alliance Industry White Paper ENABLING THE HOME AREA NETWORK MARKET. March 20, 2009

37. Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu A ZigBee-Based Home Automation System. Loughborough University, UK 2009.

asynchronous upstream traffic to name a few. Wireless neighborhood area networks (WNAN) are a type of packet switched wireless mobile data networks. Wireless NANs are flexible packet switched networks whose geographical coverage area could be anywhere from the coverage area of a Wireless Local Area Network (WLAN), to wireless metropolitan area network (WMAN), to Wireless Wide Area Network (WWAN). In Smart Grid, WNAN has a role to play in the HOME-to-HOME or HOME-to-GRID communication. The following are the communication protocols that are under consideration for wireless neighborhood area network for Smart Grid:

- 1) **IEEE 802.11:** IEEE 802.11 is a set of standards defined for the implementation of wireless local area network computer communication, which operates in the 2.4 GHz, 3 GHz and 5 GHz frequency bands. The 802.11b operates at 2.4 GHz with a data transfer rate in the range of 5 Mbits/s to 25 Mbits/s with a maximum outdoor range of 90 meters, while 802.11g operates at 2.4 GHz as well, with a data transfer rate in the range 22 Mbits/s to 128 Mbits/s with a maximum outdoor range of 90 meters.<sup>38</sup>
- 2) **IEEE 802.15.4:** 802.15.4 defines the physical and medium access control layers for low data-rate, short-range wireless communication. The operation is defined in both sub 1 GHz and 2.4 GHz frequency bands, supporting Direct Sequence Spread Spectrum signaling with a raw data throughput of 250 kbps and can transmit point to point, ranging anywhere from tens to hundred of meters depending on the output power and receive sensitivity of the transceiver.<sup>39</sup>
- 3) **IEEE 802.16:** WiMax (Worldwide Interoperability for Microwave Access) that provides wireless transmission of data in variety of modes from a point to multi-point links. It is also called as the Last Mile Connectivity of Broadband wireless access with a range of around 50 km and a data transfer rate of up to 70Mbps with the ability to support data, voice and video. It does not require LOS (Line Of Sight) and uses public key cryptography.<sup>40</sup>

## 6.5. Potential Security Issues/Risks

### 6.5.1. ZigBee<sup>41</sup>

- 1) Power Failures – Nonce<sup>42</sup> values are initialized to a standard value, thus making the nonce a known value.
- 2) Fast Denial-of-service Attack on AES-CTR (Advanced Encryption Standard CTR mode).

---

38. [http://en.wikipedia.org/wiki/IEEE\\_802.11](http://en.wikipedia.org/wiki/IEEE_802.11)

39. Naveen Shastry, David Wagner, Security Considerations for IEEE 802.15.4 Networks. UC Berkeley. Year of Publication – 2004.

40. <http://en.wikipedia.org/wiki/WiMAX>

41. Matera: Security Issues on ZigBee Basilicata University, Italy, January 18, 2006

42. A side input to the encryption algorithm.

- 3) Acknowledges Forgery since the ACK frame returns only the DNS (Domain Name Server) value. If the attacker knows the DNS value he/she can send a false acknowledgement to the sender saying that the receiver has received the message when in fact it hasn't.
- 4) Weak Integrity Protection on AES-CTR.
- 5) Allows the use of Same Keys on multiple ACL (Access Control List) entries. Allows the use of Group Keys.

### **6.5.2. Z-Wave<sup>43</sup>**

Unsecure connection while establishment of the network and distribution of the network key is taking place. Open to sniffer attacks.

Solution: The new device and the primary controller must be less than one meter apart for set-up. Once the new device has been included on the network database it can be placed anywhere within range of the network.

### **6.5.3. Gateway**

**Medium Access Control (MAC) address spoofing:** When the U-SNAP card is plugged in for the first time it registers on the network. Since the network operates in an unlicensed frequency band any eavesdropper can listen to on-going traffic and spoof the MAC address, this MAC address the U-SNAP card uses as an ID to uniquely recognize a card. The second scenario occurs when pricing information is sent by the utility to the consumer, but as the MAC address of the card has been spoofed. In this case the utility would be sending sensitive data to an unauthorized person which is breach of confidentiality of highest security level.<sup>44</sup>

**Public Key Infrastructure security issues:** The U-SNAP card uses Public Key infrastructure as a security feature. With the use of PKI emerges the problem of distribution of public keys and the added responsibility of choosing a certifying authority to sign the keys.<sup>45</sup> This issue is a problem for any system which uses PKI and is discussed further in chapter 9.

**Virtual Home its security features and loopholes:** In a virtual home, where in the gateway has added components such as virtual home, network coordinator and device data base. Every command which is received from the external network is checked for its authenticity by the network coordinator and the device data base in the virtual home environment. Once the

---

43. Wireless security - How safe is Z-wave? -Knight, M

44. U-SNAP Alliance Industry White Paper ENABLING THE HOME AREA NETWORK MARKET. March 20, 2009.

45. John Linn, RSA Laboratories, Bedford, MA, USA Marc Branchaud, RSA Security Inc., Vancouver, BC, Canada. An Examination of Asserted PKI Issues and Pro-posed Alternatives. 2004.

command has been verified it's then implemented in the real home system. The security concerns with such a setup are as follows:<sup>46</sup>

- The gateway accepts commands even from a ZigBee based remote control and these commands are not verified in the virtual home environment. A malicious device emitting ZigBee signals could be interpreted as commands to the home environment.
- Since the gateway uses hardware components device driver updates is needed. These updates should be done in a controlled manner; otherwise virtual home which is trusted for managing the security of the home area network will be compromised.

#### **6.5.4. WLAN**

##### **IEEE 802.11<sup>47</sup>**

- **Convenient Access:** Networks announce their existence with the aid of beacon frames which are also inviting threats. Software is used by "War Drivers" to log these appearances of beacon frames and find the locations using GPS.
- **Rogue Access Points:** One of the common security risks is with the rogue access points which are easy to setup and does not even require authorization.
- **MAC Spoofing:** The management frames are not authenticated in 802.11. Every frame has a source address. The attackers take advantage of the spoofed frame to redirect the traffic and corrupt the ARP tables.
- **Denial of Service Attacks:**
  - **Physical Attacks:** Simple devices that operate in 2.4 GHz frequency band like cordless phones that support 802.11b can be used to take the network offline. This is done by reducing the signal to noise ratio of the channel to an unusable range, by inducing noise into the network.
  - **Data-link Attacks:** For devices manufactured before 2003 with wired equivalent privacy (WEP) turned on, the attacker can perform DoS attacks by accessing the user information on the link layer. Data link attacks are difficult for post 2003 devices that support WPA2.
- **Network Attacks:** An attacker can flood ICMP packets to the gateway, thereby creating a difficult time for clients associated to the same AP to send and receive packet.
- **Man-in-the-Middle (MITM) Attacks:** There are two versions MITM attack. They are
  - Eavesdropping
  - Manipulating

---

46. Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu A ZigBee-Based Home Automation System. Loughborough University, UK 2009.

47. Bob Fleck, Bruce Potter. 802.11 Security. O'Reilly Publications, December 2002, ISBN : 0-596-00290-4

**Solution:** Wi-Fi Protected Access (WPA) has an improved encryption algorithm called Temporal Key Integrity Protocol (TKIP) which uses unique key for every client and also uses longer keys that are rotated at configurable intervals. WPA also includes an encrypted message integrity check field in the packet to prevent denial-of-service and spoofing attacks.

#### **IEEE 802.15.4<sup>48</sup>**

1. **Confidentiality:** Encryption scheme must be used to prevent from message recovery. The process semantic security is to encrypt the message twice to get two cipher texts. But if the same encryption process is used, then the semantic security is violated. The technique to prevent this violation is to use a unique nonce<sup>†</sup> for each invocation of encryption process. The decryption uses this nonce at the receiver end, the nonce is sent clear in the same packet with the encrypted data and hence the security of encryption is not dependent on the nonce. The nonce is introduced to give some variations to the messages.
2. **Loss of ACL State:** Each ACL entry in the ACL table is used to store different keys and their associated nonce. There are chances of ACL table getting cleared when there is a power failure or when the device operates in a low powered state.
  - **Power Failure:** In case of power failures the ACL entries are cleared, however, the ACL table is repopulated by the software with appropriate keys. But, the issue is with the nonce states. All the nonce states are reset to a known value say 0 and there by reuse of nonce state incurred that compromises security.
  - **Low powered operation:** Again the issue is with how to retain the nonce states when the device enters the low powered state.

**Possible Fix:** Suitable fix to this problem could be saving and storing the nonce states in flash memories which incurs additional cost, power consumption and also is slow and energy inefficient.

3. **Key Management Problems:** This problem arises due to the inability in the ACL tables to support different keying models.
  - **Group Keying:** There is no support for using the same key for multiple ACL entries. If attempts are made to create separate ACL entries for each node then the reuse of nonce state problem arises.

**Possible Fix:** Fix for this could be creating a single ACL entry for a particular key. Before sending, changing the destination address associated with that ACL entry for a message would suffice to fix this issue.

- **Network Shared Keying:** The network cannot be protected from replay attacks when using a network wide shared key. In order to use the network shared keying model the application has to use the default ACL entry but a default ACL entry could be used only if there is no matching ACL entry.

---

48. Naveen Shastry, David Wagner, Security Considerations for IEEE 802.15.4 Networks. UC Berkeley. Year of Publication – 2004.

4. **Confidentiality and Integrity Protection:** Researches have proven that unauthenticated encryption modes can introduce risks of protocol level vulnerabilities compromising not only integrity but also confidentiality. An example for this could be AES-CTR which uses counter mode without a MAC.
5. **Denial of Services:** As discussed previously, the replay attacks could cause the device to reject packets.
6. **No Acknowledgement Packets Integrity:** There is an option for the sender to request for an acknowledgement from the recipient for the sent packets. But there is no confidentiality or integrity provided for the acknowledgement packets thereby attracting the attacker to forge the acknowledgement packets.

#### **IEEE 802.16<sup>49</sup>**

- **Authentication:** The drawback with WiMax is that it does not have Base Station authentication which makes it prone to Man-in-the-middle attacks exposing subscribers to confidentiality and availability attacks. Since BS does not authenticate itself, the SS cannot be protected from rouge BS.
- **Encryption:** 802.16e supports for Advanced Encryption Standard (AES) cipher providing strong confidentiality on user data. Again the drawback is with encryption not applied on the management frames thereby sufficing the attacker to gather information about the subscribers in the area and also about the network characteristics.
- **Availability:** Even though WiMax uses a licensed RF spectrum, attackers can use easily available gadgets to jam the network. This is an example for physical layer denial of service attacks whereas attackers can send legacy management frames to disconnect legitimate station, this is nothing but de-authenticate flood attacks.
- **Water Torture Attack:** This is a form of physical layer attack wherein the attacker sends a series of frames to any node to drain the battery life of the victim node.

---

49. <http://www.networkworld.com/columnists/2006/121106-wireless-security.html?page=1>

## 6.6. Comprehensive Security issues with HAN/ Gateway/ NAN

High – High Security Risk

Medium – Medium Security Risk

Low – Low Security Risk

**Table 5. HAN security issues**

Component Involved	Threat Scenario Description	Security Threat Level
U-SNAP	MAC address spoofing  Public Key Infrastructure security issues	High Confidentiality, Medium availability High Accountability High Integrity
ZigBee Gateway Module	Virtual Home its security features and loopholes	High Accountability High Integrity
ZigBee	Power Failures Fast Denial-Of-Service Attack on AES-CTR Acknowledges Forgery Weak Integrity Protection on AES-CTR Allows the use of Same Keys on multiple ACL entries	High Integrity High Availability  High Accountability
IEEE 802.11	MAC Spoofing Denial of Service Attacks Man-in-the-Middle Attacks	High Confidentiality, High Accountability High Availability
IEEE 802.16	Authentication Encryption Availability Water Torture Attack	High Confidentiality, Medium Availability Medium Integrity
IEEE 802.15.4	Confidentiality Loss of ACL State Key Management Problems Encryption Denial of Services No Acknowledgement Packets Integrity	High Confidentiality High Integrity High Availability

# 7.0 SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEM SECURITY ISSUES

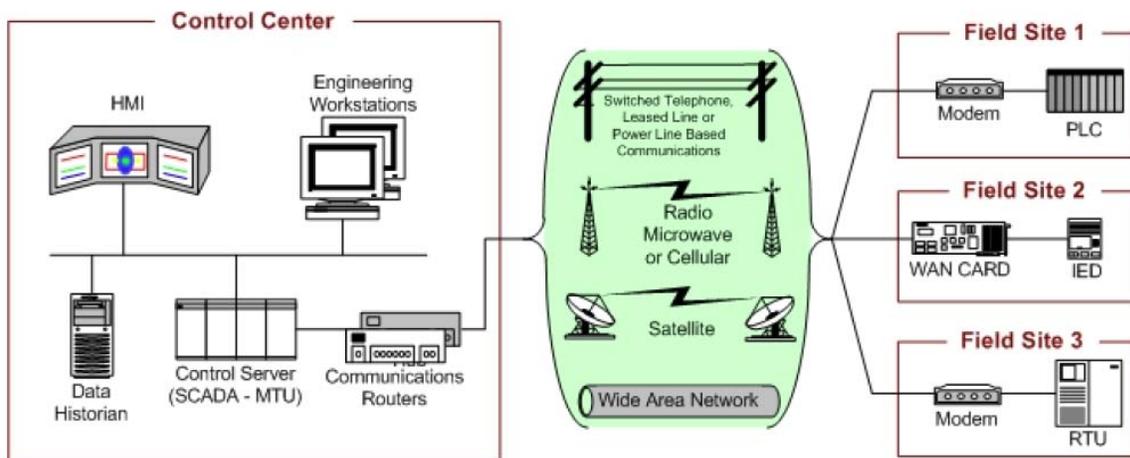
## 7.1. Introduction

SCADA systems are widely deployed in Critical Infrastructure industries where they provide remote supervisory and control. In the Smart Grid SCADA systems are used in automation.

Despite the relevant importance of SCADA security, SCADA systems are reported to be vulnerable to electronic attacks. Taking into account the wide deployment of networking technologies in SCADA and a high connectivity of SCADA networks with other networks such as the corporate intranet or even the internet, SCADA systems are exposed to electronic attacks nowadays more than ever.

This section discusses SCADA system security issues for the purpose of implementing an efficient defense of SCADA and Process Control Systems in general it is necessary to research on novel security approaches, implement them and carefully measure their suitability in terms of efficiency and overhead.

For instance, to monitor and control grid equipment such as transformers, customer equipment, generation and transmission system, etc. The general layout of a SCADA system is shown in figures 9 and 10.



**Figure 9. SCADA general layout.**

Source: Guide to Industrial Control Systems (ICS) Security, National Institute of standards and technology

The figure above gives a general layout of a SCADA (Supervisory Control and Data Acquisition) system. SCADA is a collection of systems that measure, report, and change in real-time both local and geographically remote distributed processes. The fundamental components in the above figure are the control center usually computer-based, referred to as MTU (Master Terminal Unit), RTU (Remote Terminal Unit) or also called as field site, and the communication link between them. The MTU issues commands to distant facilities and gathers data from them, interacts with other systems in the corporate intranet for administrative purposes and interfaces

with human operators. In a SCADA system it is the MTU which has full control on distributed remote processes. An operator can interface with a MTU through an interface device consisting in a video display unit, a keyboard, etc. Control commands sent by a MTU to distant facilities are triggered by programs in that MTU which are executed either manually or through a programmable built-in scheduler.

RTUs are generally based on microprocessors and are physically placed in remote locations. Their task consists of controlling and acquiring data from devices such as sensors, actuators, controllers, pulse generators, etc. An MTU communicates with one or more remote RTUs by sending requests for information that those RTUs gather from devices, or instructions to take an action such as open and close valves, turn switches on and off, etc. The communications between a MTU and RTUs follow a master-slave schema, in which the MTU is a master and RTUs are slaves, and only the MTU is allowed to initiate a transaction.<sup>50</sup>

The SCADA system is a control system which was originally designed to operate in an isolated environment. Today they are typically connected to the corporate network for business reasons. These Control Systems were also originally designed to be efficient rather than secure. Communication protocols (e.g. Distributed Network Protocol (DNP 3)) which allow remote control of the SCADA devices were designed with little security in mind. Impact of attacks on SCADA systems could be physical, economic, or societal.

The following sections discuss security issues in SCADA systems.

---

50. National Institute of Standards and Technology, US department of Commerce (September 2008). Guide to Industrial Control Systems (ICS) Security (Special Publication 800-82 FINAL PUBLIC DRAFT). Keith Stouffer, Joe Falco, Karen Scarfone.

### 7.1.1. SCADA Architecture in detail

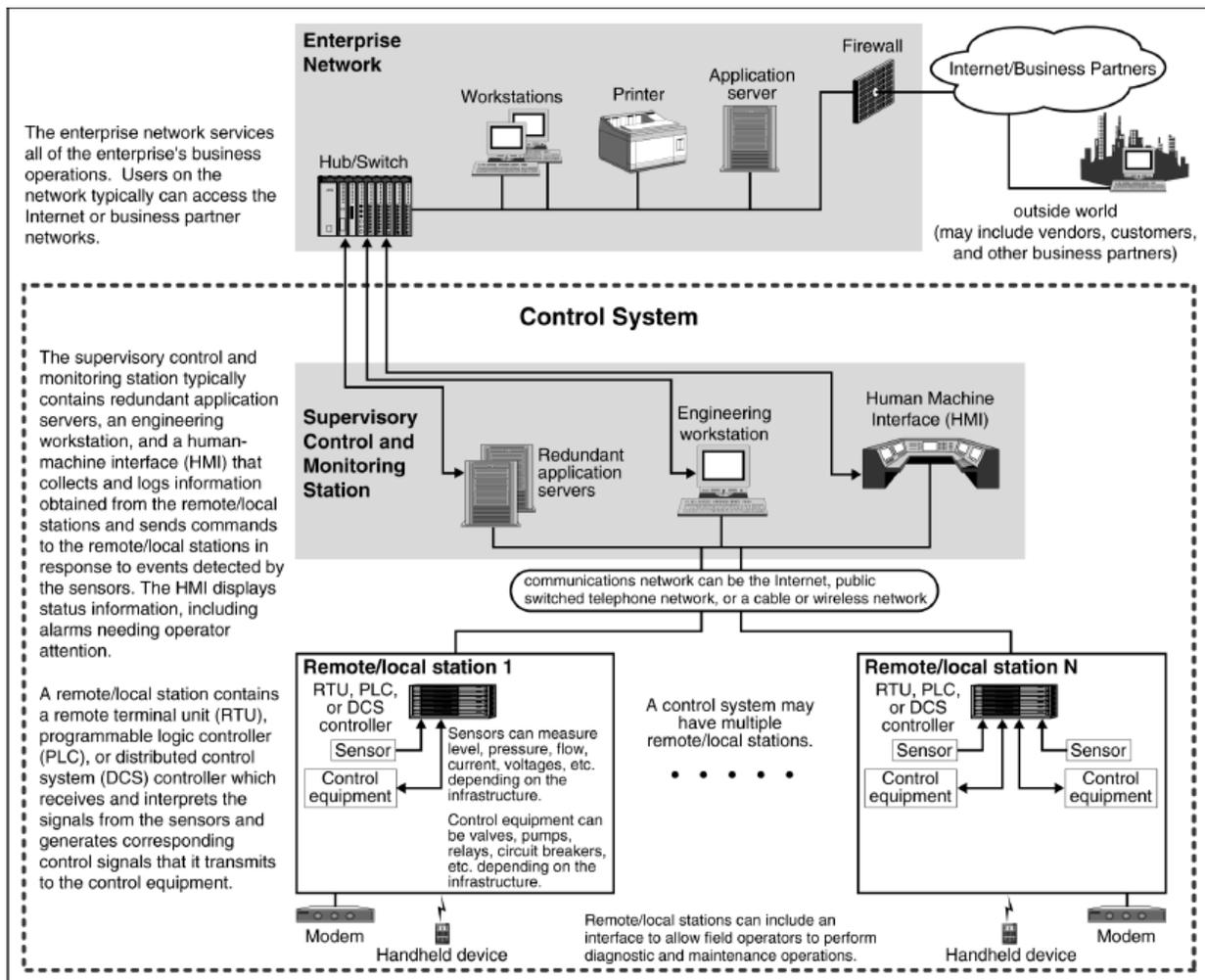


Figure 10. SCADA architecture.<sup>51</sup>

Source: Critical Infrastructure Protection, Challenges in Securing Control Systems

### 7.1.2. Security Issues In SCADA

#### Public Information Availability

Often, too much information about a utility company corporate network is easily available through routine public queries. This information can be used to initiate a more focused attack against the network. Examples of this vulnerability are listed below:<sup>52</sup>

51. East, Samuel. Butts, Jonathan. Papa, Mauricio. And Shenoi, Sujeet. (2009). A taxonomy of attacks on the DNP3 Protocol. Critical Infrastructure Protection III, IFIP AICT 311, pp. 67–81, 2009. IFIP International Federation for Information Processing.

52. Understanding SCADA System Security Vulnerabilities, Ripstech.

- Websites often provide data useful to network intruders about company structure, employee names, e-mail addresses, and even corporate network system names.
- Domain name service (DNS) servers permit “zone transfers” providing IP addresses, server names, and e-mail information.

### **Platform Configuration Vulnerabilities**

- OS and application security patches are not maintained.
- Inadequate Access controls. Poorly specified access controls can result in giving an SCADA user too many or too few privileges. The following exemplify each case: System configured with default access control settings gives operator administrative privileges, system improperly configured, results in an operator being unable to take corrective actions in an emergency situation.
- Password policies are needed to define when passwords must be used, how strong they must be, and how they must be maintained. Without a password policy, systems might not have appropriate password controls, making unauthorized access to systems more likely.<sup>53</sup>

### **Platform Software Vulnerabilities**

- **Denial of service (DoS):** SCADA software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resource or delaying system operations and functions. They could proactively exploit software bugs and other vulnerabilities in various systems, either in the corporate network or the SCADA network, to gain unauthorized access to places such as control center networks, SCADA systems, interconnections, and access links. Cyber-attacks that are based on denial of service (DoS) mechanisms, and others that spread due to viruses and worms by causing a traffic avalanche in short durations, can potentially bring down systems and cause a disruption of services and are known as Flood-based Cyber Attack Types.
- **Intrusion detection/prevention software not installed:** Incidents can result in loss of system availability; the capture, modification, and deletion of data; and incorrect execution of control commands. IDS/IPS software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected with worms. IDS/IPS software must be tested prior to deployment to determine that it does not compromise normal operation of the SCADA.<sup>54</sup>
- **Malware protection software not installed, definitions not current, implemented without exhaustive testing:** Malicious software can result in performance degradation, loss of system availability, and the capture, modification, or deletion of data. Malware protection software, such as antivirus software, is needed to prevent systems from being

---

53, 54. National Institute of Standards and Technology, US department of Commerce (September 2008). Guide to Industrial Control Systems (ICS) Security (Special Publication 800-82 FINAL PUBLIC DRAFT). Keith Stouffer, Joe Falco, Karen Scarfone.

infected by malicious software. Outdated malware protection software and definitions leave the system open to new malware threats. Malware protection software deployed without testing could impact normal operation of the SCADA.<sup>55</sup>

### ***Network Configuration Vulnerabilities***

The network architecture design is critical in offering the appropriate amount of segmentation between the Internet, the company's corporate network, and the SCADA network. Network architecture weaknesses can increase the risk that a compromise from the Internet could ultimately result in compromise of the SCADA system. Some common architectural weaknesses include the following:<sup>56</sup>

- Configuration of file transfer protocol (FTP), web, and e-mail servers sometimes inadvertently and unnecessarily provides internal corporate network access
- Network connections with corporate partners are not secured by firewall, IDS, or virtual private network (VPN) systems consistent with other networks
- Dial-up modem access is authorized unnecessarily and maintenance dial-ups often fail to implement corporate dial access policies
- Firewalls and other network access control mechanisms are not implemented internally, leaving little to no separation between different network segments

### ***Network Perimeter Vulnerabilities***<sup>57</sup>

#### Network Leak Vulnerabilities

- TCP/IP networks by their very nature promote open communications between systems and networks, unless network security measures are implemented. Improper network configuration often leads to inbound and outbound network leaks—between SCADA networks, corporate networks, business partners, regulators and outsourcers and even the Internet—which pose a significant threat to network reliability. Network leaks can allow worms, viruses or hackers direct visibility to vulnerable SCADA systems.

#### Insecure Connections Exacerbate Vulnerabilities

- Potential vulnerabilities in control systems are exacerbated by insecure connections. Organizations often leave access links—such as dial-up modems to equipment and control information—open for remote diagnostic SCADA, maintenance, and examination of system status. Such links may not be protected with authentication or encryption, which increases the risk that hackers could use these insecure connections to break into remotely controlled systems. Also, control systems often use wireless

---

55, 56, 57. National Institute of Standards and Technology, US department of Commerce (September 2008). Guide to Industrial Control Systems (ICS) Security (Special Publication 800-82 FINAL PUBLIC DRAFT). Keith Stouffer, Joe Falco, Karen Scarfone.

communications systems, which are especially vulnerable to attack, or leased lines that pass through commercial telecommunications facilities.

Firewalls nonexistent or improperly configured

- A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks. This could cause several problems, including allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping on the other network, and providing individuals with unauthorized access to systems.

### ***Network Communication (DNP 3) Vulnerabilities<sup>58</sup>***

The SCADA systems are built using public or proprietary communication protocols which are used for communicating between an MTU and one or more RTUs. The SCADA protocols provide transmission specifications to interconnect substation computers, RTUs, IEDs, and the master station. The most common protocol is DNP3 (Distributed Network Protocol Version 3.3). It was developed to achieve interoperability among systems in the electric utility.

The following list presents features of DNP3 that provide benefits to the user:

- Open standard
- Interoperability between multi-vendor devices
- A protocol that is supported by a large and increasing number of equipment manufacturers
- Layered architecture conforming to IEC enhanced performance architecture model
- Optimized for reliable and efficient SCADA communications
- Supported by comprehensive implementation testing standards
- The ability to select from multiple vendors for future system expansion and modification

Here are some attacks which exploit the protocol specifications:

- **Passive Network Reconnaissance:** An attacker with the appropriate access captures and analyzes DNP3 messages. This attack provides the attacker with information about network topology, device functionality, memory addresses and other data.
- **Baseline Response Replay:** An attacker with knowledge of normal DNP3 traffic patterns simulates responses to the master while sending fabricated messages to outstation devices.

---

58. East, Samuel. Butts, Jonathan. Papa, Mauricio. And Sheno, Sujeet. (2009). A taxonomy of attacks on the DNP3 Protocol. Critical Infrastructure Protection III, IFIP AICT 311, pp. 67–81, 2009. IFIP International Federation for Information Processing.

- Rogue Interloper: An attacker installs a “man-in-the-middle” device between the master and outstations that can read modify and fabricate DNP3 messages and/or network traffic.
- Length Overflow and DFC Flag Attack: These attacks either inserts an incorrect value in the Length field that affects message processing or sets the DFC flag, which causes an outstation device to appear busy to the master. These attacks can result in data corruption, unexpected actions and device crashes.
- Reset Function and unavailable function Attack: This attack sends a DNP3 message with Function Code 1 (reset user process) to the targeted outstation. The attack causes the targeted device to restart, rendering it unavailable for a period of time and possibly restoring it to an inconsistent state. Examples are interruption of an outstation and modification of an outstation. In unavailable function attack, the attacker sends a DNP3 message with Function Code 14 or 15, which indicates that a service is not functioning or is not implemented in an outstation device. The attack causes the master not to send requests to the targeted outstation because it assumes that the service is unavailable.
- Destination Address Alteration: By changing the destination address field, an attacker can reroute requests or replies to other devices causing unexpected results. An attacker can also use the broadcast address 0xFFFF to send erroneous requests to all the outstation devices; this attack is difficult to detect because (by default) no result messages are returned to a broadcast request.
- Fragmented Message Interruption: The FIR and FIN flags indicate the first and final frames of a fragmented message, respectively. When a message with the FIR flag arrives, all previously-received incomplete fragments are discarded. Inserting a message with the FIR flag set after the beginning of a transmission of a fragmented message causes the reassembly of a valid message to be disrupted. Inserting a message with the FIN flag set terminates message reassembly early, resulting in an error during the processing of the partially-completed message.
- Transport Sequence Modification: The Sequence field is used to ensure in-order delivery of fragmented messages. The sequence number increments with each fragment sent, so predicting the next value is trivial. An attacker who inserts fabricated messages into a sequence of fragments can inject any data and/or cause processing errors.
- Outstation Data Reset: This attack sends a DNP3 message with Function Code 15. The attack causes an outstation device to reinitialize data objects to values inconsistent with the state of the system. Examples of this attack are interruption and modification of an outstation.

Security Issues in SCADA and DNP 3 are summarized in Table 6.

**Table 6. SCADA security issues**

<b>Security Issue</b>	<b>Description</b>	<b>Security Threat Levels</b>
Public Information Availability	Information available through manuals, vendors, and through routine public queries.	Confidentiality
Policy and Procedure Vulnerabilities	Inadequate security policies, without the security architecture and design pose a threat. Lack of security audits, disaster recovery plan etc.	Integrity
Platform Configuration Vulnerabilities	OS and application security patches are not maintained. Inadequate access control to systems, inadequate password policies.	Confidentiality, Integrity, Availability
Platform Software Vulnerabilities	Buffer Overflow. Denial of Service, Intrusion detection/prevention software not installed, malware protection not provided	Confidentiality, Integrity, Availability, Accountability
Network Configuration Vulnerabilities	Weak network security architecture, data flow control not applied	Availability, Integrity
Network Perimeter Vulnerabilities	Firewalls nonexistent or improperly configured, Insecure Connections Exacerbate Vulnerabilities, Network Leak Vulnerabilities	Confidentiality, Integrity, Accountability
Network Communication Vulnerabilities	Passive Network Reconnaissance Baseline Response Replay Rogue Interloper Length Overflow and DFC Flag Attack Reset Function and unavailable function Attack Destination Address Alteration Fragmented Message Interruption Transport Sequence Modification Outstation Data Reset Outstation Application Termination	Integrity Accountability Integrity Integrity, Confidentiality Availability Availability Integrity Integrity Integrity, Availability Availability

There is a recent security extension to DNP 3 but the researchers are not aware of their widespread implementation.

## 8.0 PLUG IN ELECTRIC VEHICLES (PEV) SECURITY ISSUES

### 8.1. Introduction

Despite the current high cost of maintaining electric vehicles, they are generally cheaper to operate over the long run because they reduce dependency on oil resources which have been fluctuating in price due to political instability of the nations that supply the natural oil. Electric vehicles also produce less greenhouse emissions than gas powered vehicles which will help reduce the effects of global warming.

Many technological and economical challenges come with the continued trend of PEVs becoming more prevalent. "In particular, battery technology (e.g., battery capacity and charge time) and the infrastructure (e.g., charge stations and grid), are essential prerequisites for a massive deployment."<sup>59</sup> The Smart Grid will utilize Vehicle to Grid (V2G) which is one of the technological advances that will be used in making electric vehicles a viable mainstream option for prospective automobile customers. V2G will be a vital component for both the vehicle's owners and the energy providers because it will allow both parties to draw power from each other as needed. "Peak load leveling is a concept that allows V2G vehicles to provide power to help balance loads by "valley filling" (charging at night when demand is low) and "peak shaving" (sending power back to the grid when demand is high)."<sup>60</sup> V2G allows electric vehicle the capability to charge their fuel cells when energy demand is low while energy enables companies to draw power from the vehicles when there is a shortage of power. "Since most vehicles are parked an average of 95 percent of the time, their batteries could be used to let electricity flow from the car to the power lines and back, with a value to the utilities of up to \$4,000 per year per car."<sup>61</sup> Seeing that V2G follows the concept of peak load leveling, power consumers and providers can help each other reduce cost and improve overall effectiveness of power distribution.

Even though there has been some progress in solutions for PEV technology, other security issues associated with the technology and the data it will use remain. Some potential for security issues related to PEVs include "Secure Payment and Privacy, Smart Metering, and the Critical Infrastructure and Physical Security."<sup>62</sup>

---

59, 61. Paar, Christof, Andy Rupp, Kai Schramm, Andre Weimerskirch, and Wayne Burleson. Securing Green Cars: IT Security in Next-Generation Electric Vehicle Systems. Tech. Amherst: ECE Department, University of Massachusetts at Amherst.

60, 62. Vehicle-to-grid. Vehicle-to-grid -Wikipedia, the free encyclopedia. Wikipedia, 2 Oct. 2009.

## **8.2. Privacy of Movement**

PHEV will over load the smart grid when they are plugged-in for charging because the PHEVs move for place to place so the power requirements to the locations change. For example, there may be a city like Manhattan where more traffic flows in during peak office hours. If many PHEVs are plugged into the grid located at that point, at a time, it will overload the grid. To solve this problem the position of the PHEVs should be monitored. The constant monitoring of the PHEV location leads to privacy concerns to one's individual freedom. Additionally, if someone breaks into the monitoring system, they could get access to this information.

## **8.3. Secure Payment**

A very important element to the smart grid is a payment system which works reliably and secure, and which protects both the end-user and the provider. There are good reasons to prefer electronic payment systems over cash payments, such as reduced revenue collection costs and reduce of losses; enhance customer satisfaction, improved services and operational efficiency as well as more flexible pricing strategies. One type of solution is to use credit cards. However credit card systems do have problems as well. For example, transaction needs to be protected so that an individual's information is not revealed to third parties. Another approach would be to adopt Integrated Transportation Payment Systems (ITPS). Unfortunately, there are also examples of serious shortcomings of today's ITPS. Existing systems do not have mechanisms protecting their security and especially the privacy of their users. One problem is that some systems deploy cryptographically weak proprietary primitives. Currently e-cash protocols have been extensively studied. The study shows that it is possible to construct secure off-line payment that protect the anonymity of honest users but is nevertheless able to disclose their identities as soon as they try to cheat the system.

Potential attackers can be categorized as a small set of individuals, commercial companies, and government institutions. Typically regular individuals will attack the system to acquire private sensitive information in order to track individuals or attack the system because they are curious. On the other hand commercial companies will generate user profiles to increase their revenue. They will usually respect legal restrictions but they will also exploit legal loopholes. Finally, government institutions will have extensive power and they might even be able to define the legal environment. Therefore it is important to define a legal framework to account for companies and government institutions, and define technical solutions that account for individual attackers.

Privacy is a challenging problem, since it involves cryptographic theory, engineering, policy and sociology. In order to enable a deployment, adequate security and privacy mechanisms must be a requirement. To prevent malicious actions by attackers some form of IT security need to be introduced to systems. Such methods range from cryptographic mechanisms, to secure and privacy-preserving payment systems to a critical infrastructure interpretation of the electric car charging network. This should lead towards addressing the security problems.

## **8.4. Smart Metering**

The owner of the PEV might want to report less electricity than what was actually delivered to the PEV's batteries, and the energy provider might want to charge for more energy than what was actually delivered. Even worse than these two would be a third party or middle man, such as a charging station, which would be able to cheat both the energy providers and the owners of the PEV. This can happen if care is not taken in securing the smart meter from tampering. There are best practices that can be applied to provide protection.

## **8.5. Critical Infrastructure & Physical Security**

When PEV's becomes the norm, the link between the energy and transportation critical infrastructure will become tightly intertwined. Any malicious attack made against either one of these two critical infrastructures could potentially pose a threat to the security of these two infrastructures, specifically in the areas of traffic management, and payments for services rendered, pertaining to charging of a PEV. Since the link between these two critical infrastructures is in uncharted territory for both the energy and transportation critical infrastructure sectors, research will be needed to better understand the impacts of such a close relationship between the two sectors. If a malicious attack were to penetrate the defenses of either the energy or the transportation critical infrastructure, it would be devastation to both critical infrastructures, monetarily and physically. Many businesses will not be able to operate without the ability to charge their vehicles. Traffic management will also become a problem, and can potentially lead to physical harm to individuals. Because of the severity of the problems that can be caused by a malicious attack, the Department of Defense should be an active participant in the security of the energy and transportations sectors of the critical infrastructures.

Physical Security of the equipment is also important to the security of PEV's. If an individual is allowed to take electricity without paying for it, most of the time that individual will take the opportunity. The Smart chargers will need to be secure enough so that a potential attacker cannot hack the smart charger for a PEV to provide their PEV with free electricity. There also might be attackers that are not only looking for free electricity; but also to obtain sensitive information from the smart charging of the current owner or previous owners of the smart charging device.

Sometimes attackers are not only looking to steal information or energy; but also looking to cause physical harm to the owner of the PEV. If a battery is overcharged there is a possibility that the battery will explode and cause physical harm to anyone in the vicinity of the explosion. The solution to such a problem should be multi-faceted. The manufactures of the battery should include circuitry to not allow over charging of their batteries and the smart meter should make sure that over charging of a battery is not allowed. Another place that an attacker can cause mischief is at a charging station for a PEV's, by either skewing the amount of energy purchased or by stealing credit card numbers via card skimmers. Particular care has to taken when dealing with the physical security of the hardware that involves PEVs.

Successful integration of PEVs into the Smart Grid depends on overcoming the security challenges of “Secure Payment and Privacy, Smart Metering, and the Critical Infrastructure and Physical Security.”<sup>63</sup>

## **8.6. Communication**

The PHEVs might use cellular network for communication but there are vulnerabilities in this network that can be used as a means of getting access into the system, sending wrong information, attacking the system etc. The potential attacks that can be performed are, middle-man-attack, spoofing, etc.

---

63. Paar, Christof, Andy Rupp, Kai Schramm, Andre Weimerskirch, and Wayne Burleson. Securing Green Cars: IT Security in Next-Generation Electric Vehicle Systems. Tech. Amherst: ECE Department, University of Massachusetts at Amherst.

## **9.0 GENERIC SECURITY ISSUES OF THE SMART GRID**

### **9.1. Introduction**

These security issues are critical but they are not uniquely associated with a specific smart grid “logical” component. These issues could affect any smart grid component and refer to actual field cases. The researchers have not been able to verify these field cases with relevant California Utilities. When they do so they will document it in subsequent reports. Most of these issues addressed here can be found in NIST smart grid bottom-up security analysis of smart grid document as well as smart grid vulnerability list.

### **9.2. Authenticating and Authorizing Users (People) to Substation IEDs**

The problem is how to authenticate and authorize users (maintenance personnel) to Intelligent Electronic Devices (IEDs) in substations in such a way that access is specific to a user, authentication information (e.g. password) is specific to each user (i.e. not shared between users), and control of authentication and authorization can be centrally managed across all IEDs in the substation and across all substations belonging to the utility and updated reasonably promptly to ensure only intended users can authenticate to intended devices and perform authorized functions.

Currently many substation IEDs have a notion of “role” but no notion of “user”. Passwords are stored locally on the device and several different passwords allow different authorization levels. These role passwords are shared amongst all users of the device with the role in question, possibly including non-utility employees such as contractors and vendors. Furthermore, due to the number of devices, these passwords are often the same across all devices in the utility, and seldom changed.

Users may be utility employees, contractors, or vendor support engineers. Roles may include audit (read-only), user (read-write), administrator (add/remove/modify users), and security officer (change security parameters).

The device may be accessed locally in the sense that the user is physically present in the substation and accesses the IED from a front panel connection or wired network connection, or possibly wireless. The device may also be accessed remotely over a low-speed (dialup) or high-speed (network) connection from a different physical location.

A provision to ensure that necessary access is available in emergency situations may be important, even if it means bypassing normal access control, but with an audit trail.

### **9.3. Authenticating and Authorizing Maintenance Personnel to Smart Meters**

Like IED equipment in substations, current smart meter deployments use passwords in meters that are not associated with users. Passwords are shared between users and the same password is typically used across the entire meter deployment. The security problem is similar to IEDs.

Access may be local through the optical port of a meter, or remote through the AMI infrastructure, or remote through the HAN gateway.

Meters generally have some sort of connectivity to an AMI head end, but this connectivity may be as slow as 1200 baud, or lower (e.g. some power line carrier devices have data rates measured in millibaud).

### **9.4. Authenticating and Authorizing Users (People) to Outdoor Field Equipment (e.g. Pole-Top Device)**

Some newer pole-top and other outdoor field equipment supports 802.11 or Bluetooth for near-local user access from a maintenance truck. The problem is how to authenticate and authorize users (maintenance personnel) to such devices in such a way that access is specific to a user (person), authentication information (e.g. password) is specific to each user (not shared between users), and control of authentication and authorization can be centrally managed across the utility and updated reasonably promptly to ensure only intended users can authenticate to intended devices and perform authorized functions.

There are two problems. One is the security of the wireless channel. The second is how users are authenticated. The researchers suspect that just like IEDs and Smart Meters, there are passwords in the field device (e.g. pole top recloser) that will be the same across hundreds or thousands of devices and never changed, i.e. not specific to the user.

Access will usually be local via wired connections, or near-local via short-range radio, although some devices may support true remote access.

### **9.5. Authenticating and Authorizing Consumers to Meters**

In case meters act as home area network gateways for providing energy information to consumers and/or control for demand response programs, if consumer are authenticated to meters, authorization and access levels need to be carefully considered, i.e., a consumer capable of supplying energy to the power grid may have different access requirements than one who does not.

## **9.6. Authenticating Meters to/from AMI Head Ends (Mutual Authentication)**

It is important for a meter to authenticate any communication from an AMI head end, in order to ensure that an adversary cannot issue control commands to the meter, update firmware, etc. It is important for an AMI head end to authenticate the meter, since usage information retrieved from the meter will be used for billing, and commands must be assured of delivery to the correct meter.

## **9.7. Authenticating HAN Devices to/from HAN Gateways**

Demand response HAN devices must be securely authenticated to the HAN gateway and vice versa. It is important for a HAN device to authenticate any demand-response or commands from the DR head end to order to prevent control by an adversary. Without such authentication, coordinated falsification of control commands across many HAN devices and/or at rapid rates could lead to grid stability problems. It is important that the DR head end authenticate the HAN device both to ensure that commands are delivered to the correct device, and that responses from that device are not forged.

Should a HAN device fail to authenticate, it will presumably be unable to respond to demand response signals. It should not be possible for a broad DOS attack to cause a large number of HAN devices to fail to authenticate and thereby not respond to a DR event.

## **9.8. Securing Serial SCADA Communications**

Many substations and distribution communication systems still employ slow serial links for various purposes including SCADA communications with control centers and distribution field equipment. Furthermore, many of the serial protocols currently in use does not offer any mechanism to protect the integrity or confidentiality of messages, i.e., messages are transmitted in clear text form. Solutions that simply wrap a serial link message into protocols like SSL or IPSEC over PPP will suffer from the overhead imposed by such protocols (both in message payload size and computational requirements) and would unduly impact latency and bandwidth of communications on such connections. A solution is needed to address the security and bandwidth constraints of this environment.

## **9.9. Protection of Routing Protocols in AMI Layer 2/3 Networks**

In the AMI space, there is increasing likelihood that mesh routing protocols will be used on wireless links. Wireless suffers from several well-known and often easily exploitable attacks partly due to the lack of control to the physical medium (the radio waves). Modern mechanisms like 802.11i have worked to close some of these holes for standard wireless deployments. However, wireless mesh technology potentially opens the door to some new attacks in the form of route injection, node impersonation, L2/L3/L4 traffic injection, traffic modification, etc. Most current on-demand and link-state routing mechanisms do not specify a scheme to protect the data or the routes the data takes, primarily because of the distributed nature of the system itself. They also generally lack schemes for authorizing and providing integrity protection for adjacencies in the routing system. Without routing security, attacks such as eavesdropping,

impersonation, man-in-the-middle, and denial-of-service could be easily mounted on AMI traffic.

## **9.10. Key Management for Meters**

Where meters contain cryptographic keys for authentication, encryption, or other cryptographic operations, a key management scheme must provide for adequate protection of cryptographic materials as well as sufficient key diversity. That is, a meter, collector, or other power system device should not be subject to a break-once break-everywhere scenario due to one shared secret being used across the entire infrastructure. Each device should have unique credentials and key material such that compromise of one device does not impact other deployed devices. The key management system must also support an appropriate lifecycle of periodic re-keying and revocation.

There are existing cases of large deployed meter bases using the same symmetric key across all meters, and even in different States. In order to share network services, adjacent utilities may even share and deploy that key information throughout both utility AMI networks. Compromising a meter in one network could compromise all meters and collectors in both networks.

## **9.11. Insecure Firmware Updates**

The ability to perform firmware updates on meters in the field allows for the evolution of applications and the introduction of patches without expensive physical visits to equipment. However, it is critical to assure that firmware update mechanisms are not used to install malware. Best practices exist to deal with these issues.

## **9.12. Side Channel Attacks on Smart Grid Field Equipment**

These attacks are based on physical accessibility (Substation, Pole-Top, Smart Meters, Collectors, etc.). A side-channel attack is based on information gained from the physical implementation of a cryptosystem. Tempest attacks similarly can extract data by analysis of various types of electromagnetic radiation emitted by a CPU, display, keyboard, etc. Tempest attacks are nearly impossible to detect. Syringe attacks use a syringe needle as a probe to tap extremely fine wire traces on printed circuit boards.

Smart grid devices that are deployed in the field, such as substation equipment, pole-top equipment, smart meters and collectors, and in-home devices, are at risk of side channel attacks due to their accessibility. Extraction of encryption keys by side channel attacks from smart grid equipment could lead to compromise of usage information, personal information, passwords, etc. Extraction of authentication keys by side channel attacks could allow an attacker to impersonate smart grid devices and/or personnel, and potentially gain administrative access to smart grid systems.

## **9.13. Key Management and Public Key Infrastructure (PKI)**

Key management for Smart Grid devices that contain symmetric or asymmetric long-lived keys is essential. Standard PKI may not be appropriate since many devices will not have connectivity

to key servers, certificate authorities, OCSP servers, etc. The scale of the systems involved and their distribution is unprecedented, as it will involve millions of devices. There will also be issues of cross-certification across different domains and checking for validity of certificates within the context of this unprecedented scale.

### **9.14. Patch Management**

Specific devices such as IEDs, PLCs, Smart Meters, etc. will be deployed in a variety of environments and critical systems. Their accessibility for software upgrades or patches maybe a complex activity to undertake because of how distributed and isolated equipment can be. Also there are many unforeseen consequences that can arise from changing firmware in a device that is part of a larger engineered system. Control systems require considerable testing and qualification to maintain reliability factors.

The patch, test and deploy lifecycle is fundamentally different in the electrical sector. It can take a year or more (for good reason) to go through a qualification of a patch or upgrade. Thus there are unique challenges to be addressed in how security upgrades to firmware needs to be managed.

## GLOSSARY

ACL	Access Control List
ACM	Association for Computing Machinery (ACM)
AES-CTR	Advanced Encryption Standard – Counter Mode
AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading
ASIS	American Society for Industrial Security
Auto-DR	Automated Demand Response
BMS	Building Management System
BPL	Broadband over Power Line
CCSS	Center for Control System Security
CEC	California Energy Commission
CHP	Combined Heat and Power
C&I	Commercial and Industrial
CIA	Central Intelligence Agency
CMMS	Computer Maintenance Management System
CSO	Chief Security Officer
DA	Distribution Automation
DER	Distributed Energy Resources
DFC	Dynamic Flow Concept
DHS	US Department of Homeland Security
DLC	Direct Load Control
DNP	Distributed Network Protocol
DoE	US Department of Energy
DOS	Denial of Service
DR	Demand-Response
DRAS	Demand Response Automation Center

DRRC	Demand Response Research Center
DSPF	Distribution System Power Flow
DSM	Demand Side Management
DSSS	Direct Sequence Spread Spectrum
EI	Edison Electric Institute
EM	Electro-Magnetic
EMS	Energy Management System
EMCS	Emergency Management Control Center
EPRI	Electric Power Research Institute
HAN	Home Area Network
HG	Home Gateway
HVAC	Heating Ventilation & Air Condition
HTTP	Hyper Transfer Text Protocol
ICCP	Inter-Control center Communications Protocol
ICS	Industrial Control Systems
IDART	Information Design Assurance Red Team
IED	Intelligent Electronic Devices
IOU	Investor Owned Utility
IP	Internet Protocol
ISO	Independent System Operator
IT	Information Technology
ITPS	Integrated Transportation Payment Systems
kW	Kilowatt
kWh	Kilowatt Hour
LAN	Local Area Network
LOS	Line of Sight
LSE	Load Serving Entity
LTC	Load Tap Changer

MAC	Media Access Control
MDM	Meter Data Management
MDMS	Meter Data Management System
MTU	Master Terminal Unit
NAN	Neighborhood Area Network
NIST	National Institute of Standards and Technology
NOC	Network Operating Center
OSCP	Online Certificate Status Protocol
OpenADR	Open Automated Demand Response or Open Auto-DR
PCT	Programmable Communicating Thermostat
PEV	Plug In Electric Vehicle
PG&E	Pacific Gas & Electric
PHEV	Plug In Hybrid Electric Vehicle
PIER	Public Interest Energy Research
PKI	Public Key Infrastructure
PLA	People's Liberation Army
PLC	Programmable Logic Controllers
RCD	Residual Current Device
RD&D	Research, Development and Demonstration
RF	Radio Frequency
RFB	Request For Bids
RG	Residential Gateway
RTO	Regional Transmission Operators
RTP	Real Time Pricing
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCE	Southern California Edison
SDLC	Systems Development Life Cycle

SG	Smart Grid
SOAP	Simple Object Access Protocol
T&D	Transmission and Distribution
TDM	Time Division Multiplexing
TLS	Transport Layer Security
TOU	Time to Use
UIS	Utility Information System
USNAP	Utility Smart Network Access Port
V2G	Vehicle to Grid
WNAN	Wireless Neighborhood Area Network
Wi-Max	Worldwide Interoperability for Microwave Access
WSDL	Web Service Description Language
XML	Extensible Markup Language
XSD	XML Schema Definition

## REFERENCES

- [http://www.cisco.com/web/strategy/docs/energy/white\\_paper\\_c11\\_539161.pdf](http://www.cisco.com/web/strategy/docs/energy/white_paper_c11_539161.pdf)
- [http://carbon-pros.com/blog1/2009/08/smart\\_grid\\_security\\_vulnerabil.html](http://carbon-pros.com/blog1/2009/08/smart_grid_security_vulnerabil.html)
- <http://hardware.slashdot.org/article.pl?sid=09/03/22/082236>
- <ftp://ftp.csc.ncsu.edu/pub/tech/2009/TR-2009-5.pdf>
- [http://www.industrialdefender.com/general\\_downloads/news\\_industry/2009.07.28\\_black\\_hat\\_smart\\_meter\\_worm\\_attack\\_planned.pdf](http://www.industrialdefender.com/general_downloads/news_industry/2009.07.28_black_hat_smart_meter_worm_attack_planned.pdf)
- <http://www.cyberpunkreview.com/news-as-cyberpunk/the-cias-latest-claim-hackers-have-attacked-foreign-utilities/>
- [http://www.nationaljournal.com/njmagazine/cs\\_20080531\\_6948.php](http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php)
- <http://www.nerc.com/docs/standards/Chuck-Noble-RBB-Letter.pdf>
- [http://www.smartgridnews.com/artman/publish/News\\_Blogs\\_News/Foreign\\_Cyber-Spies\\_Inject\\_Spyware\\_into\\_U\\_S\\_Grid\\_with\\_Potential\\_for\\_Serious\\_Damage-562.html](http://www.smartgridnews.com/artman/publish/News_Blogs_News/Foreign_Cyber-Spies_Inject_Spyware_into_U_S_Grid_with_Potential_for_Serious_Damage-562.html)
- [http://www.smartgridnews.com/artman/publish/Technologies\\_Security\\_News/Smart-Security-for-a-Smart-Grid-New-Threats-on-the-Horizon-1226.html](http://www.smartgridnews.com/artman/publish/Technologies_Security_News/Smart-Security-for-a-Smart-Grid-New-Threats-on-the-Horizon-1226.html)
- <http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/index.html>
- <https://www.csoroundtable.org/knowledge/security-vulnerabilities-smart-grid>
- <http://cacm.acm.org/news/43974-smart-grid-vulnerabilities-could-cause-widespread-disruptions/fulltext>
- California Energy Commission's Public Interest Energy Research Program, PIER Buildings Program, *Automated Demand Response Cuts Commercial Building Energy Use and Peak Demand, Technical Brief*, Public Interest Energy Research Program ,2008[online]. Available: <http://www.energy.ca.gov/2008publications/CEC-500-2008-086/CEC-500-2008-086-FS.PDF>
- U.S. Federal Energy Regulatory Commission (FERC), *Assessment of Demand Response and Advanced Metering*, 2007[online]. Available: [http://www.ferc.gov/legal/staff\\_reports/09-07-demand-response.pdf](http://www.ferc.gov/legal/staff_reports/09-07-demand-response.pdf)
- S. Kiliccote, M.A. Piette, J.H. Dudley, Lawrence Berkeley National Laboratory (LBNL); E. Koch and D. Hennage, Akuacom, *Open Automated Demand Response for Small Commercial Buildings*, Lawrence Berkeley National Laboratory ,July 2009 [online]. Available: <http://drrc.lbl.gov/pubs/lbnl-2195e.pdf>

- M.A. Piette, G. Ghatikar, S. Kiliccote, E. Koch, D. Hennage, P. Palensky, and C. McParland, *Open Automated Demand Response Communications Specification*, Demand Response Research Center, April 2009 [online]. Available: <http://drcc.lbl.gov/openadr/pdf/cec-500-2009-063.pdf>
- E. Koch, Akuacom; M.A. Piette, Lawrence Berkeley National Laboratory (LBNL), *Architecture Concepts and Technical Issues for an Open, Interoperable Automate Demand Response Infrastructure*, 2007 [online]. Available: [http://www.gridwiseac.org/pdfs/forum\\_papers/104\\_paper\\_final.pdf](http://www.gridwiseac.org/pdfs/forum_papers/104_paper_final.pdf)
- A. Lee, T. Brewer, Computer Security Division, Information Technology Laboratory, National Institution of Standards and Technology (NIST), *Smart Grid Cyber Strategy and Requirements*, Draft NISTIR 7628, Sept 2009 [online]. Available: <http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf>
- K. Stouffer, J. Falco, K. Scarfone, *Guide to Industrial Control Systems (ICS) Security*, National Institution of Standards and Technology (NIST), Sept 2008 [online]. Available: [http://csrc.nist.gov/publications/drafts/800-82/draft\\_sp800-82-fpd.pdf](http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf)
- E. W. Gunther, *Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008*, March 2007 [online]. Available: [http://drcc.lbl.gov/pct/docs/ReferenceDesignTitle24PC\\_rev15.doc](http://drcc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc)
- R. Ramesh, *CSCTG Demand Response Interfaces NISTIR*, Aug 2008 [online]. Available: [http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGDR/CSCTG-DR-Draft\\_082809.doc](http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGDR/CSCTG-DR-Draft_082809.doc)
- Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu *A ZigBee-Based Home Automation System*. Loughborough University, UK 2009.  
<http://www.usnap.org/technical.aspx>
- Matera: *Security Issues on ZigBee* Basilicata University, Italy, January 18, 2006
- Ken Masica, *Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments*, Lawrence Livermore National Laboratory  
[http://en.wikipedia.org/wiki/IEEE\\_802.15.4-2003](http://en.wikipedia.org/wiki/IEEE_802.15.4-2003)  
<http://en.wikipedia.org/wiki/Z-Wave>  
[http://en.wikipedia.org/wiki/IEEE\\_802.11](http://en.wikipedia.org/wiki/IEEE_802.11)  
<http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html>  
<http://en.wikipedia.org/wiki/WiMAX>
- Bob Fleck, Bruce Potter. *802.11 Security*. O'Reilly Publications, December 2002, ISBN : 0-596-00290-4

Naveen Shastry, David Wagner, *Security Considerations for IEEE 802.15.4 Networks*. UC Berkeley. Year of Publication – 2004.

Keith Stouffer Joe Falco, Karen Scarfone .*Guide to Industrial Control Systems (ICS) Security* (Special Publication 800-82 FINAL PUBLIC DRAFT). National Institute of Standards and Technology, US department of Commerce.

East, Samuel. Butts, Jonathan. Papa, Mauricio. And Sheno, Sujeet. *A taxonomy of attacks on the DNP3 Protocol*. Critical Infrastructure Protection III, IFIP AICT 311, pp. 67–81, 2009. IFIP International Federation for Information Processing (2009).

Robert F. Dacey, Director, Information Security Issues. *Critical Infrastructure Protection, Challenges in Securing Control*. US Government Accountability Office, United States General Accounting Office October 2003.

Chikuni, Edward and Dondo, Maxwell. *Investigating the security of Electrical Power Systems SCADA*. (2007).

Paar, Christof, Andy Rupp, Kai Schramm, Andre Weimerskirch, and Wayne Burleson. *Securing Green Cars: IT Security in Next-Generation Electric Vehicle Systems*. Tech. Amherst: ECE Department, University of Massachusetts at Amherst. Print [PEV-2] Vehicle-to-grid. *Vehicle-to-grid* -Wikipedia, the free encyclopedia. Wikipedia, 2 Oct. 2009.

## APPENDIX A

### 1. Key Power System Use Cases and Cyber Security Requirements

The following Use Cases were obtained from the NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements (Sept 2009) presented a full set of Use Cases taken from many sources, including the following:

- IntelliGrid Use Cases, only the power system operations Use Cases and Demand Response/AMI ones are of particular interest for security. The EPRI IntelliGrid project developed the complete list of Use Cases (700 cases).
- AMI Business Functions which were extracted from Appendix B of the AMI-SEC Security Requirements Specification.
- Benefits and Challenges of Distribution Automation – Use Case Scenarios extracted from CEC document which has 82 Use Cases.
- EPRI Use Case Repository, compilation of IntelliGrid and SCE Use Cases, plus others.
- SCE Use Cases developed by Southern California Edison (SCE) with the assistance of EnerNex.

The Use Cases has been grouped in categories that follow and they represent a good summary of most of the information discussed in this report.

#### 1.1. Category: AMI

**Scenario 1:** Meter Reading Services (Periodic Meter Reading, On-Demand Meter Reading, Net Metering for DER and PEV, Feed-In Tariff Metering for DER and PEV, Bill - Paycheck Matching)

##### **Cyber Security Requirements:**

Integrity of meter data is important, but the impact of incorrect data is not large.

Availability of meter data is not critical in real-time.

Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database, to avoid serious breaches of privacy and potential legal repercussions.

**Scenario 2:** Pre-Paid Metering (Limited Energy Usage and Limited Demand)

##### **Cyber Security Requirements:**

Integrity of meter data is critical, to avoid unwarranted disconnections due to perceived lack of pre-payment. Security compromises could have a large impact on the customer and could cause legal repercussions

Availability to turn meter back on after payment is important, but could be handled by a truck roll if necessary.

Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database

**Scenario 3:** Revenue Protection (Tamper Detection, Anomalous Readings, Meter Status and Suspicious Meter)

**Cyber Security Requirements:**

Integrity of meter data is important, but if tampering is not detected or if unwarranted indications of tampering are detected, there is no power system impact, just revenue impact.

Availability to turn meter back on after payment is important.

Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database is important.

**Scenario 4:** Remote Connect/Disconnect of Meter (Remote Connect for Move-In, Remote Connect for Reinstatement on Payment, Remote Disconnect for Move-Out, Remote Disconnect for Non-Payment, Remote Disconnect for Emergency Load Control and Unsolicited Connect / Disconnect Event)

**Cyber Security Requirements:**

Integrity of control commands to the RCD switch is critical to avoid unwarranted disconnections or dangerous/unsafe connections. The impact of invalid switching could be very large if many meters are involved.

Availability to turn meter back on when needed is important.

Confidentiality requirements of the RCD command is generally not very important, except related to non-payment.

**Scenario 5:** Outage Detection and Restoration (Smart meters report one or more power losses e.g. "last gasp", Outage management system collects meter outage reports and customer trouble calls, Outage management system determines location of outage and generates outage trouble tickets, Work management system schedules work crews to resolve outage, Interactive utility-customer systems inform the customers about the progress of events and Trouble tickets are used for statistical analysis of outages)

**Cyber Security Requirements:**

Integrity is important to ensure outages are reported correctly.

Availability is important to ensure outages are reported in a timely manner (a few seconds).

Confidentiality is not very important.

**Scenario 6:** Meter Maintenance (Connectivity validation, Geo-location of meter and Smart meter battery management)

### **Cyber Security Requirements:**

Integrity of meter maintenance repairs and updates are essential to prevent malicious intrusions.

Availability is important, but only in terms of hours or maybe days.

Confidentiality is not important unless some maintenance activity involves personal information.

### **Scenario 7: Meter Detect Removal**

This scenario discusses the AMI meter's functionality to detect and report unauthorized removal and similar physical tampering. AMI meters require additional capability over traditional meters to prevent theft and tampering due to the elimination of regular visual inspection provided by meter reading.

#### **Objective/ Requirements:**

Reduce energy theft. Prevent theft/compromise of passwords and key material. Prevent installation of malware.

### **Scenario 8: Utilities detects Probable meter Bypass**

AMI meters eliminate the possibility of some forms of theft (i.e. meter reversal). Other types of theft will be more difficult to detect due to the elimination of regular physical inspection provided by meter reading. This scenario discusses the analysis of meter data to discover potential theft occurrences.

#### **Objective/ Requirements:**

Reduce theft. Protect integrity of reporting. Maintain availability for reporting and billing.

## **1.2. Category: Demand Response**

### **Scenario 1: Real Time Pricing (RTP) for Customer Load and DER/PEV**

Use of Real Time Pricing for electricity is common for very large customers, affording them an ability to determine when to use power and minimize the costs of energy for their business. The extension of real time pricing to smaller industrial and commercial customers and even residential customers is possible with smart metering and in-home displays. Aggregators or customer energy management systems must be used for these smaller consumers due to the complexity and 24x7 nature of managing power consumption. Pricing signals may be sent via an AMI system, the Internet, or other data channels.

#### **Cyber Security Requirements:**

Integrity, including non-repudiation, of pricing information is critical, since there could be large financial and possibly legal implications.

Availability, including non-repudiation, for pricing signals is critical because of the large financial and possibly legal implications.

Confidentiality is important mostly for the responses that any customer might make to the pricing signals.

### **Scenario 2: Time of Use (TOU) Pricing**

Time of use pricing creates blocks of time and seasonal differences that allow smaller customers with less time to manage power consumption to gain some of the benefits of real time pricing. This is the favored regulatory method in most of the world for dealing with global warming

Although Real Time Pricing is more flexible than Time of Use, it is likely that TOU will still provide many customers will all of the benefits that they can profitably use or manage.

#### **Cyber Security Requirements:**

Integrity is not critical since TOU pricing is fixed for long periods and is not generally transmitted electronically.

Availability is not an issue.

Confidentiality is not an issue, except with respect to meter reading.

### **Scenario 3: Net Metering for DER and PEV**

When customers have the ability to generate or store power as well as consume power, net metering is installed to measure not only the flow of power in each direction, but also when the net power flows occurred. Often Time of Use (TOU) tariffs are employed.

Today larger C&I customers and an increasing number of residential and smaller C&I customers have net metering installed for their photovoltaic systems, wind turbines, combined heat and power (CHP), and other DER devices. As plug-in electric vehicles (PEVs) become available, net metering will increasingly be implemented in homes and small businesses, even parking lots.

#### **Cyber Security Requirements:**

Integrity is not very critical since net metering pricing is fixed for long periods and is not generally transmitted electronically.

Availability is not an issue.

Confidentiality is not an issue, except with respect to meter reading.

### **Scenario 4: Feed-In Tariff Pricing for DER and PEV**

Feed-in tariff pricing is similar to net metering except that generation from customer DER/PEV has a different tariff rate than the customer load tariff rate during specific time periods.

#### **Cyber Security Requirements:**

Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically.

Availability is not an issue.

Confidentiality is not an issue, except with respect to meter reading.

#### **Scenario 5: Critical Peak Pricing**

Critical Peak Pricing builds on Time of Use Pricing by selecting a small number of days each year where the electric delivery system will be heavily stressed and increasing the peak (and sometime shoulder peak) prices by up to 10 times the normal peak price. This is intended to reduce the stress on the system during these days.

#### **Cyber Security Requirements:**

Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically.

Availability is not an issue.

Confidentiality is not an issue, except with respect to meter reading.

#### **Scenario 6: Mobile Plug-In Electric Vehicle (PEV) Functions**

Customer connects PEV at another home. Customer connects PEV outside home territory.

Customer connects PEV at public location. Customer charges the PEV.

#### **Cyber Security Requirements:**

Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically.

Availability is not an issue.

Confidentiality is not an issue, except with respect to meter reading.

### **1.3. Category: Customer Interfaces**

**Scenario 1:** Customer's In Home Device is Provisioned to Communicate with the Utility.

Configure customer's device to receive and send data to utility systems. The device could be an information display, communicating thermostat, load control device or smart appliance.

#### **Objective/Requirements:**

Protect passwords. Protect key material. Authenticate with other devices on the AMI system.

**Scenario 2:** Customer Views Pricing or Energy Data on Their In Home Device

The information available to customers on their in home devices.

Multiple communication paths and device functions will be considered.

**Objective/Requirements:**

To validate that information is trustworthy (integrity).

**Scenario 3:** In Home Device Troubleshooting

The resolution of communication or other types of errors that could occur within home devices. The roles of the customer, device vendor and utility will be discussed.

**Objective/Requirements:**

Avoid disclosing customer information. Avoid disclosing key material and/or passwords

**Scenario 4:** Customer Views Pricing or Energy Data via the Internet

The information that should be available to the customer using the internet and some possible uses for the data.

**Objective/Requirements:**

Protect customer's information (privacy). Provide accurate information

**Scenario 5:** Utility Notifies Customers of Outage

When an outage occurs the utility can notify affected customers and provide estimated restoration times and report when power has been restored. Smart grid technologies can improve the utility's accuracy for determination of affected area and restoration progress.

**Objective/Requirements:**

Validate that the notification is legitimate. Customer's information is kept private.

**Scenario 6:** Customer Access to Energy-Related Information

Access to real-time (or near real-time) energy and demand usage and billing information

Requesting energy services such as move-in/move-out requests, pre-paying for electricity, changing energy plans (if such tariffs become available), etc.

Access to energy pricing information.

Access to their own DER generation/storage status.

Access to their own PEV charging/discharging status.

Establishing thermostat settings for demand response pricing levels.

Although different types of energy-related information access is involved, the security requirements are similar.

**Cyber Security Requirements:**

Integrity, including non-repudiation, is critical since energy and pricing data will have financial impacts

Availability is important to the individual customer, but will not have wide-spread impacts  
Confidentiality is critical because of customer privacy issues

## **1.4. Category: Electricity Market**

### **Scenario 1: Bulk Power Electricity Market**

The bulk power market varies from region to region, and is conducted primarily through Regional Transmission Operators (RTO) and Independent System Operators (ISO). The market is handled independently from actual operations, although the bids into the market obviously affect which generators are used for what time periods and which functions (base load, regulation, reserve, etc.).

Therefore there are no direct operational security impacts, but there are definitely financial security impacts.

#### **Cyber Security Requirements:**

Integrity for pricing and generation information is critical

Availability for pricing and generation information is important within minutes to hours

Confidentiality for pricing and generation information is critical

### **Scenario 2: Retail Power Electricity Market**

The retail power electricity market is still minor, but growing, compared to the bulk power market, but typically involves aggregators and energy service providers bidding customer-owned generation or load control into both energy and ancillary services. Again it is handled independently from actual power system operations. Therefore there are no direct operational security impacts, but there are definitely financial security impacts.

#### **Cyber Security Requirements:**

Integrity for pricing and generation information is critical

Availability for pricing and generation information is important within minutes to hours

Confidentiality for pricing and generation information is critical

### **Scenario 3: Carbon Trading Market**

The carbon trading market does not exist yet, but the security requirements will probably be similar to the retail electricity market.

#### **Cyber Security Requirements:**

Integrity for pricing and generation information is critical

Availability for pricing and generation information is important within minutes to hours

Confidentiality for pricing and generation information is critical

## 1.5. Category: Distribution Automation

### Scenario 1: Distribution Automation (DA) within Substations

Distribution SCADA System Monitors Distribution Equipment in Substations

Supervisory Control on Substation Distribution Equipment

Substation Protection Equipment Performs System Protection Actions

Reclosers in Substations

#### Cyber Security Requirements:

Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently

Availability for control is critical, while monitoring individual equipment is less critical

Confidentiality is not very important

### Scenario 2: Distribution Automation (DA) Using Local Automation

Local Automated Switch Management

Local Volt/Var Control

Local Field Crew Communications to Underground Network Equipment

#### Cyber Security Requirements:

Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently.

Availability for control is critical, while monitoring individual equipment is less critical.

Confidentiality is not very important.

### Scenario 3: Distribution Automation (DA) Monitoring and Controlling Feeder Equipment

<ul style="list-style-type: none"> <li>Remotely open or close automated switches</li> </ul>	<ul style="list-style-type: none"> <li>Remotely switch capacitor banks in and out</li> </ul>
<ul style="list-style-type: none"> <li>Remotely raise or lower voltage regulators</li> </ul>	<ul style="list-style-type: none"> <li>Block local automated actions</li> </ul>
<ul style="list-style-type: none"> <li>Automation of Emergency Response</li> </ul>	<ul style="list-style-type: none"> <li>Dynamic Rating of Feeders</li> </ul>
<ul style="list-style-type: none"> <li>Send updated parameters to feeder equipment</li> </ul>	<ul style="list-style-type: none"> <li>Interact with equipment in underground distribution vaults</li> </ul>
<ul style="list-style-type: none"> <li>Retrieve power system information from Smart Meters</li> </ul>	<ul style="list-style-type: none"> <li></li> </ul>

### **Cyber Security Requirements:**

Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently.

Availability for control is critical, while monitoring individual equipment is less critical.

Confidentiality is not very important.

### **Scenario 4: Fault Detection, Isolation, and Restoration**

- The automated fault location, isolation, and service restoration function uses the combination of the power system model with the SCADA data from the field on real-time conditions to determine where a fault is probably located, by undertaking the following steps:
  - Determines the faults cleared by controllable protective devices
  - Determines the faulted sections based on SCADA fault indications and protection lockout signals
  - Estimates the probable fault locations, based on SCADA fault current measurements and real-time fault analysis
  - Determines the fault-clearing non-monitored protective device
  - Uses closed-loop or advisory methods to isolate the faulted segment
  - Once the fault is isolated, it determines how best to restore service to unfaulted segments through feeder reconfiguration

### **Cyber Security Requirements:**

Integrity of outage information is critical.

Availability to detect large scale outages usually involve multiple sources of information

Confidentiality is not very important.

### **Scenario 5: Load Management**

Load management provides active and passive control by the utility of customer appliances (e.g. cycling of air conditioner, water heaters, and pool pumps) and certain C&I customer systems (e.g. plenum pre-cooling, heat storage management).

- Direct load control and load shedding
- Demand side management
- Load shift scheduling
- Curtailment planning
- Selective load management through Home Area Networks

### **Cyber Security Requirements:**

Integrity of load control commands is critical to avoid unwarranted outages

Availability for load control is important – in aggregate (e.g. > 300 MW), it can be critical.

Confidentiality is not very important.

#### **Scenario 6:** Distribution Analysis using Distribution Power Flow Models

The brains behind the monitoring and controlling of field devices are the DA analysis software applications. These applications generally use models of the power system to validate the raw data, assess real-time and future conditions, and issue the appropriate actions. The applications may be distributed and located in the field equipment for local assessments and control, and/or may be centralized in a Distribution Management System for global assessment and control.

Local peer-to-peer interactions between equipment.

Normal distribution operations using the Distribution System Power Flow (DSPF) model.

Emergency distribution operations using the DSPF model.

Study-Mode Distribution System Power Flow (DSPF) model.

DSPF /DER Model of distribution operations with significant DER generation/storage.

#### **Cyber Security Requirements:**

Integrity is critical to operate the distribution power system reliably, efficiently, and safely.

Availability is critical to operate the distribution power system reliably, efficiently, and safely.

Confidentiality is not important.

#### **Scenario 7:** Distributed Energy Resource (DER) Management - Distribution Operations

In the future, more and more of generation and storage resources will be connected to the distribution network and will significantly increase the complexity and sensitivity of distribution operations. Therefore, the management of DER generation will become increasingly important in the overall management of the distribution system, including load forecasts, real-time monitoring, feeder reconfiguration, virtual and logical microgrids, and distribution planning.

Direct monitoring and control of DER.

Shut-down or islanding verification for DER.

Plug-in Hybrid Vehicle (PEV) management, as load, storage, and generation resource.

Electric storage fill/draw management.

Renewable energy DER with variable generation.

Small fossil resource management, such as backup generators to be used for peak shifting.

**Cyber Security Requirements:**

Integrity is critical for any management/control of generation and storage.

Availability requirements may vary depending on the size (individual or aggregate) of the DER plant.

Confidentiality may involve some privacy issues with customer-owned DER.

**Scenario 8:** Distributed Energy Resource (DER) Management – Control Centers

Distribution planning typically uses engineering systems with access only to processed power system data that is available from the control center. It is therefore relatively self-contained.

• Operational planning	• Assessing Planned Outages
• Storm Condition Planning	• Short-term distribution planning
• Short-Term Load Forecast	• Short-Term DER Generation and Storage Impact Studies
• Long-term distribution planning	• Long-Term Load Forecasts by Area
• Distribution Financial Planners	• Distribution System Upgrades and Extension
• Optimal Placements of Switches, Capacitors, Regulators, and DER	

**Cyber Security Requirements:**

Integrity not critical due to multiple sources of data.

Availability is not important.

Confidentiality is not important.

**1.6. Category: Plug In Hybrid Electric Vehicles (PHEV)**

**Scenario 1:** Customer Connects Plug in Hybrid Electric Vehicle to Energy Portal

A customer plugging in an electric vehicle at their premise to charge its battery. Variations of this scenario will be considered that add complexity: a customer charging their vehicle at another location and providing payment or charging at another location where the premise owner pays.

**Objective/Requirements:**

The customer’s information is kept private. Billing information is accurate

**Scenario 2:** Customer Connects Plug in Hybrid Electric Vehicle to Energy Portal and Participates in ‘Smart’ (Optimized) Charging

In addition to simply plugging in an electric vehicle for charging, in this scenario the electric vehicle charging is optimized to take advantage of lower rates or help prevent excessive load peaks on the electrical system.

**Objective/Requirements:**

Customer information is kept private.

**Scenario 3:** Plug In Hybrid Electric Vehicle or Customer Receives and Responds to Discrete Demand Response Events

- An advanced scenario for electric vehicles is the use of the vehicle to provide energy stored in its battery back to the electrical system. Customers could participate in demand response programs where they are provided an incentive to allow the utility to request power from the vehicle at times of high system load.

**Objective/Requirements:**

- Improved system stability and availability. To keep customer information private.

To insure DR messages are accurate and trustworthy

**Scenario 4:** Plug In Hybrid Electric Vehicle or Customer Receives and Responds to Utility Price Signals

The electric vehicle is able to receive and act on electricity pricing data sent from the utility. The use of pricing data for charging is primarily covered in another scenario. The pricing data can also be used in support of a distributed resource program where the customer allows the vehicle to provide power to the electric grid based on market conditions.

**Objective/Requirements:**

Improved system stability and availability. Pricing signals are accurate and trustworthy.

Customer information is kept private.

**1.7. Category: Distributed Resources**

**Scenario 1:** Customer Provides Distributed Resource

The process of connecting a distributed resource to the electric power system and the requirements of net metering.

**Objective/Requirements:**

Customer information is kept private. Net metering is accurate and timely.

**Scenario 2:** Utility Controls Customer’s Distributed Resource

Distributed generation and storage can be used as a demand response resource where the utility can request or control devices to provide energy back to the electrical system. Customers enroll in utility programs that allow their distributed resource to be used for load support or to assist in maintaining power quality. The utility programs can be based on direct control signals or pricing information.

-

**Objective/Requirements:**

Commands are trustworthy and accurate. Customer's information is kept private.

DR messages are received timely.

**1.8. Category: Transmission Operations**

**Scenario 1:** Real-time Normal Transmission Operations Using EMS Applications and SCADA Data

Transmission normal real-time operations involve monitoring and controlling the transmission system using the SCADA and Energy Management System. The types of information exchanged include:

Monitored equipment states (open/close), alarms (overheat, overload, battery level, capacity), and measurements (current, voltage, frequency, energy) Operator command and control actions, such as supervisory control of switching operations, setup/options of EMS functions, and preparation for storm conditions.

Closed-loop actions, such as protective relaying tripping circuit breakers upon power system anomalies.

Automation system controls voltage, var and power flow based on algorithms, real-time data, and network linked capacitive and reactive components.

**Cyber Security Requirements:**

Integrity is vital to the safety and reliability of the transmission system.

Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g. one second).

Confidentiality is not important.

**Scenario 2:** EMS Network Analysis Based on Transmission Power Flow Models

Energy Management Systems (EMS) assesses the state of the transmission power system using the transmission power system analysis models and the SCADA data from the transmission substations.

EMS performs model update, state estimation, bus load forecast.

EMS performs contingency analysis, recommends preventive and corrective actions.

EMS performs optimal power flow analysis, recommends optimization actions.

EMS or planners perform stability study of network.

Exchange power system model information with RTOs/ISOs and/or other utilities.

**Cyber Security Requirements:**

Integrity is vital to the reliability of the transmission system.

Availability is critical to react to contingency situations via operator commands (e.g. one second).

Confidentiality is not important.

### **Scenario 3: Real-Time Emergency Transmission Operations**

During emergencies, the power system takes some automated actions and the operators can also take actions:

Power System Protection: Emergency operations handles under-frequency load/generation shedding, under-voltage load shedding, LTC control/blocking, shunt control, series compensation control, system separation detection, and wide area real time instability recovery.

Operators manage emergency alarms.

SCADA system responds to emergencies by running key applications such as disturbance monitoring analysis (including fault location), dynamic limit calculations for transformers and breakers based on real time data from equipment monitors, and pre-arming of fast acting emergency automation SCADA/EMS generates signals for emergency support by distribution utilities (according to the T&D contracts):

Operators perform system restorations based on system restoration plans prepared (authorized) by operation management.

### **Cyber Security Requirements:**

Integrity is vital to the safety and reliability of the transmission system.

Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g. one second).

Confidentiality is not important.

### **Scenario 4: Wide Area Synchro-Phasor System**

The Wide Area Synchro-Phasor system provides synchronized and time-tagged voltage and current phasor measurements to any protection, control, or monitoring function that requires measurements taken from several locations, whose phase angles are measured against a common, system wide reference. Present day implementation of many protection, control, or monitoring functions is hobbled by not having access to the phase angles between local and remote measurements. With system wide phase angle information, they can be improved and extended. The essential concept behind this system is the system wide synchronization of measurement sampling clocks to a common time reference.

### **Cyber Security Requirements:**

Integrity is vital to the safety and reliability of the transmission system.

Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g. one second).

Confidentiality is not important.

### **1.9. Category: RTO/ISO Operations**

**Scenario 1:** RTO/ISO Management of Central and DER Generators and Storage

RTOs and ISOs manage the scheduling and dispatch of central and distributed generation and storage.

These functions include:

Real time scheduling with the RTO/ISO (for non-market generation/storage)

Real time commitment to RTO/ISO

Real time dispatching by RTO/ISO for energy and ancillary services

Real time plant operations in response to RTO/ISO dispatch commands

Real time contingency and emergency operations.

Black Start (system restoration after blackout).

Emissions monitoring and control.

### **Cyber Security Requirements:**

Integrity is vital to the safety and reliability of the transmission system.

Availability is critical to operator commands (e.g. one second).

Confidentiality is not important.

### **1.10. Category: Asset Management**

**Scenario 1:** Utility gathers circuit and/or transformer load profiles

Load profile data is important for the utility planning staff and is also used by the asset management team that is monitoring the utilization of the assets and by the SCADA/EMS and system operations team. This scenario involves the use of field devices that measure loading, the communications network that delivers the data, the historian database and the load profile application and display capability that is either separate or an integrated part of the SCADA/EMS.

Load profile data may also be used by automatic switching applications that use load data to ensure new system configurations do not cause overloads.

-

**Objective/Requirements:**

Data is accurate (integrity).

Data is provided timely.

Customer data is kept private.

**Scenario 2:** Utility makes decisions on asset replacement based on a range of inputs including comprehensive off line and on line condition data and analysis applications.

When decisions on asset replacement become necessary the system operator, asset management, apparatus engineering and maintenance engineering staff work closely together with the objective of maximizing the life and utilization of the asset while avoiding an unplanned outage and damage to the equipment.

This scenario involves the use of on-line condition monitoring devices for the range of assets monitored, off line test results, mobile work force technologies, the communications equipment used to collect the on-line data, data marts (historian databases) to store and trend data as well as condition analysis applications, CMMS applications, display applications and SCADA/EMS.

**Objective/Requirements:**

Data provided is accurate and trustworthy.

Data is provided timely.

**Scenario 3:** Utility performs localized load reduction to relieve circuit and/or transformer overloads

Transmission capacity can become constrained due to a number of system level scenarios and result in an overload situation on lines and substation equipment. Circuit and/or transformer overloads at the distribution level can occur when higher than anticipated customer loads are placed on a circuit or when operator or automatic switching actions are implemented to change the network configuration. Traditional load reduction systems are used to address generation shortfalls and other system wide issues. Localized load reduction can be a key tool enabling the operator to temporarily curtail the load in a specific area to reduce the impact on specific equipment. This scenario describes the integrated use of the AMI system, the demand response system, other load reduction systems and the SCADA/EMS to achieve this goal.

**Objective/Requirements:**

Load reduction messages are accurate and trustworthy.

Customer's information is kept private.

DR messages are received and processed timely.

**Scenario 4:** Utility system operator determines level of severity for an impending asset failure and takes corrective action

When pending asset failure can be anticipated the system operator, asset management, apparatus engineering and maintenance engineering staff work closely together with the objective of avoiding an unplanned outage while avoiding further damage to the equipment.

This scenario involves the use of on-line condition monitoring devices for the range of assets monitored, off line test results, mobile work force technologies, the communications equipment used to collect the on-line data, data marts (historian databases) to store and trend data as well as condition analysis applications, CMMS applications, display applications and SCADA/EMS.

**Objective/Requirements:**

Asset information provided is accurate and trustworthy.

Asset information is provided timely.