SANDIA REPORT
SAND2007-7327
Unlimited Release
Printed November 2007

Advanced Metering Infrastructure Security Considerations

Raymond C. Parks

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND200X-XXXX
Unlimited Release
Printed Month Year

Advanced Metering Infrastructure Security Considerations

Raymond C. Parks
Assurance Technologies and Assessments
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS0671

Abstract

The purpose of this report is to provide utilities implementing Advanced Metering Infrastructure (AMI) with the knowledge necessary to secure that implementation appropriately. We intend that utilities use this report to guide their planning, procurement, roll-out, and assessment of the security of Advanced Metering Infrastructure.

This report discusses threats to the AMI, the likely sources of threat, damage mechanisms, and attack consequences. A high-level assessment of risk due to AMI exploitation is given. The report concludes with an outline strategy and specific recommendations for reducing risk. A utility implementing the recommendations contained in this report as it installs AMI technology will be positioned to detect and withstand attacks that attempt to exploit the vulnerabilities of the AMI.

Acknowledgements

I would like to thank EPRI and AMI vendors for their assistance with the content of this report, and Bob Hutchinson and Roxie Jansma for their assistance with the format of the report. I would also like to acknowledge that the work that produced the results presented in this paper was funded by the U.S. Department of Energy/Office of Electricity Delivery and Energy Reliability (DOE/OE) as part of the National SCADA Test Bed (NSTB) Program.

Executive Summary

The purpose of this report is to provide utilities implementing Advanced Metering Infrastructure (AMI) with the knowledge necessary to secure that implementation appropriately. We intend that utilities use this report to guide their planning, procurement, roll-out, and assessment of the security of Advanced Metering Infrastructure.

The national risk of harm to the economy, public health, trust in government, public safety, and environmental integrity is low to moderate based on the consequences of AMI attack. Another factor that reduces risk, at this time, is the low penetration of AMI into the electric infrastructure. That factor is about to change, however, as California utilities fulfill the requirements of the California Energy Commission that will enable them to deploy AMI, and other states follow the California lead.

The threats to AMI range from the cheating customer to the foreign nation state with a side trip through various types of insiders. AMI faces three primary threats: customer attacks, insider attacks, and terrorist or nation-state attacks. These threats could cause cyber effects such as loss of integrity and availability to the AMI system or to the bulk electric grid controls. System impacts range from increased peak usage up to widespread outages. AMI attacks could cause low to moderate local and regional consequences as a result of the system impacts. The risk of national harm is low to moderate but will increase as AMI market penetration increases.

In order of capability, customers, insiders, terrorists, and nation-states are the primary agencies that could threaten the AMI. There are effective measures against all of these.

Customer threat should be the easiest to mitigate but the solutions could prove to be difficult because of political reasons. The AMI industry and operators could mount an effective defense against abusive customers by using a data transmission standard for AMI data and investigating abnormal usage patterns.

Effective defense against the insider threat requires that abnormal insider activity be detected with high probability, since individual insider threats are negated by discovery. Publicizing the improved detection capability also reduces risk by deterring insider activity. Background checks and audits, authentication, intrusion detection, and software integrity checking are all relevant in this role.

The terrorist and nation-state threats are mitigated by all of the above because they make the target less attractive. Additional effective approaches to protecting against this threat are router access lists, firewalls, protected communication between the AMI network and other networks, strong communication authentication, and detection and halting of rapid market fluctuations.

A utility implementing the recommendations contained in this report as it installs AMI technology will be positioned to detect and withstand attacks that attempt to exploit the vulnerabilities of the AMI.

Table of Contents

1 Introduction 9
1.1 Background 9
1.1.1 Description 9
1.1.2 Historical Information 9
1.1.3 Signifigance 9
1.1.4 Literature Review 9
1.2 Purpose 9
1.2.1 Reason for investigation 9
1.2.2 Roadmap Challenges 10
1.2.3 Audience 10
1.2.4 Desired Response 10
1.3 Scope 10
1.3.1 Extent and Limits of Investigation 10
1.3.2 Goals 10
1.3.3 Objectives 10
1.4 How to use this report 10

2 Approach 12
2.1 Methods 12
2.2 Assumptions 13
2.3 Procedures 13

3 Results and Discussion 14
3.1 Risks Summary 14
3.2 Threat to Risk Analysis 14
3.2.1 Threats 14
3.2.2 Cyber Effects 16
3.2.3 Electric System Impacts 19
3.2.4 Consequence 19
3.2.5 Risk 20
3.3 Plausible Threat Scenario 21

4 Conclusions 23

5 Recommendations 24

Appendix A: References 26

Appendix B: Description of AMI 27

Appendix C: Acronyms, Symbols, Abbreviations 32

Appendix D: For More Information 33

Table of Figures

Figure 1: Threat to Risk Methodology 10
Figure 2: Sustainable Security 11

Figure B1: Typical AMI Architecture.....29
Figure B2: Control System Reference Model 30

1 Introduction

1.1 Background

1.1.1 Description

The Advanced Metering Infrastructure (AMI) is not in widespread use today, but its use is increasing. Since the technology is new and provides significant advantage to utilities, ther is the potential for widespread adoption to occur before best security practices have been established.

1.1.2 Historical Information

DOE/OE directed Sandia National Laboratories' (SNL) Center for Control System Security (C2S2) to investigate potential vulnerabilities of the bulk electric grid due to the introduction of new technology called the Advanced Metering Infrastructure (AMI), as part of the FY06 National SCADA Test Bed (NSTB) program. This request was particularly timely after an electric utility had asked SNL to help scope a security assessment of their planned AMI implementation and electric industry representatives had asked SNL about the state of security analysis of AMI at the Spring 2006 SANS SCADA Summit.

1.1.3 Signifigance

The benefits and relatively low expense of installing AMI make it attractive to utilities. Unless best practices and standards are established and followed, potential for significant vulnerability exposure because of the expected widespread use of AMI over the next decade or so. This report exposes the AMI's vulnerabilities and risks and outlines a defensive strategy for mitigating the most relevant threats.

1.1.4 Literature Review

Threats of concern are described with reference to the characteristics of cyber threat models in *Generic Threat Profiles* [1]. An attacker wishing to attach the AMI infrastructure itself would reverse-engineer a meter to develop a way to modify it. This is similar to the many cable-modem attacks that are openly available, for instance as discussed in [2] and [3]. Tools to modify advanced meters are beginning to go commercial [4] and will provide an easy opening for agencies wishing to attack the AMI.

1.2 Purpose

The purpose of this report is to provide utilities implementing AMI with the knowledge necessary to secure that implementation appropriately.

1.2.1 Reason for investigation

The AMI is only beginning to take hold, but is inspected to grow quickly as its advantages become apparent based on the experience of early adopters and vendors, recognizing a new relatively untapped market, grows to make available better and cheaper version of the necessary devices and software. This document is an attempt to get out in front of the general tendency of security to lag the introduction and use of new technology.

1.2.2 Roadmap Challenges

The *Roadmap to Secure Control Systems in the Energy Sector* [5] says "Despite the diverse range of legacy systems throughout the energy sector, the industry would benefit from a collection of best practices for managing control systems throughout their life cycles. Such best practices should address extending the fleet of existing legacy systems to new functionality, incorporating advanced components, and migrating to fully advanced systems." This document supplies a best-practice core for the Advanced Metering Infrastructure.

1.2.3 Audience

The intended audience for this report is electric power generation utilities, which are sometimes called load-serving entities (LSEs).

1.2.4 Desired Response

We intend that LSEs use this report to guide the planning, procurement, roll-out, and assessment of the security of their Advanced Metering Infrastructure technlogy.

1.3 Scope

1.3.1 Extent and Limits of Investigation

This report is limited to AMI as implemented by load-serving entities (LSEs) with connections to the bulk electric grid. Although many AMI roll-outs seem to include gas metering infrastructure as well as electric, the natural gas distribution system is outside the scope of this document, although AMI elements used there could be an attack starting point.

1.3.2 Goals

The purpose of this report is to provide utilities implementing AMI with the knowledge necessary to secure that implementation appropriately.

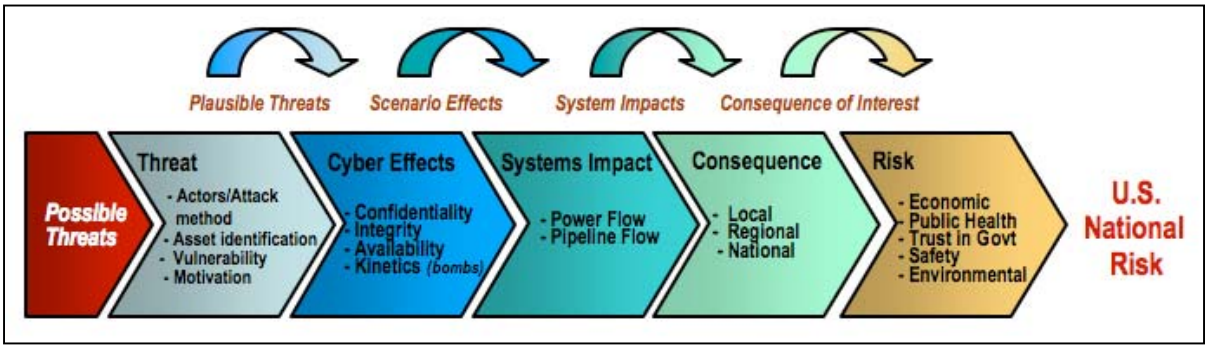
1.3.3 Objectives

We intend that utilities use this report to guide their planning, procurement, roll-out, and assessment of the security of Advanced Metering Infrastructure. Some parts may be applicable to other aspects of demand response and automated metering, but that is not guaranteed.

1.4 How to use this report

The report structure includes a summary of the risks associated with AMI, an analysis supporting those risks based on Sandia's Threat to Risk Analysis Method in Figure 1, a description of a high risk attack, and the mitigations we recommend. The Threat to Risk Analysis framework elements are described in Appendix B for reference, but understanding of them is not necessary to use this report.

All mitigations are stated in terms of Sustainable Security as shown in Figure 2. Sustainable Security is the best possible security that can be consistently maintained while meeting business objectives with available resources.



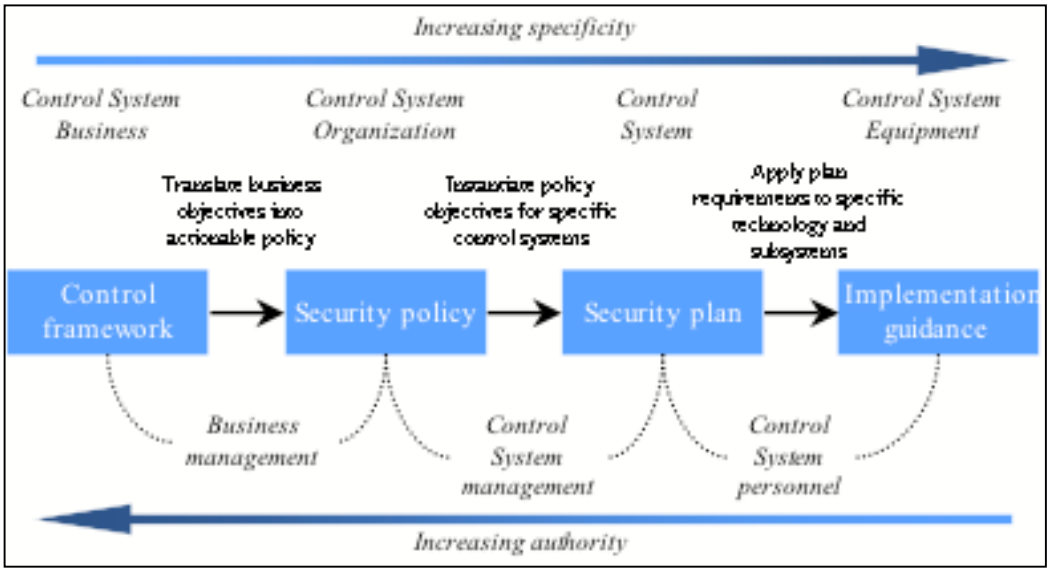


Figure 1: Threat to Risk Methodology

Figure 2: Sustainable Security

The driving requirement behind any security in AMI should be to fulfill the business objectives of the utility. The justification for AMI to regulators is usually based on cost savings and efficiencies that can be achieved by AMI. That means AMI security measures should center on preserving those cost savings and efficiencies. In addition, when AMI shares infrastructure with other utility systems, AMI inherits the requirement to implement security that fulfills the business objectives of those systems. For example, if AMI uses a communication link in common with a transmission operation's energy management system (EMS), the AMI security must meet the EMS business objective of preventing damage to equipment. Sustainable Security translates business objectives into security policy that uses security primitives in plans that are then implemented with specific security software and hardware.

2 Approach

2.1 Methods

For this work task, the Center for Control System Security used the Information Design Assurance Red Team (IDART) methodology. IDART allows a red team to tailor a mature, repeatable assessment framework to the needs of a customer and budgetary and scheduling realities of a project. We accept that complete understanding of a highly complex system is impractical for most projects and we use the IDART process to generate meaningful assumptions and realistic simplifying representations for the target system. This allows us to capture the principal features and generate custom viewpoints that are used to assist in understanding processes, interactions, and identify critical interfaces and components. Combining this understanding with domain expert knowledge, we can then identify system and subsystem vulnerabilities and postulate their effect on both system components and the system as a whole.

It should be noted that the maturity of the target system affects the applicability of the IDART process. A system must have a reasonable level of maturity, be it in the operational or design phase, in order to support an IDART methodology assessment.

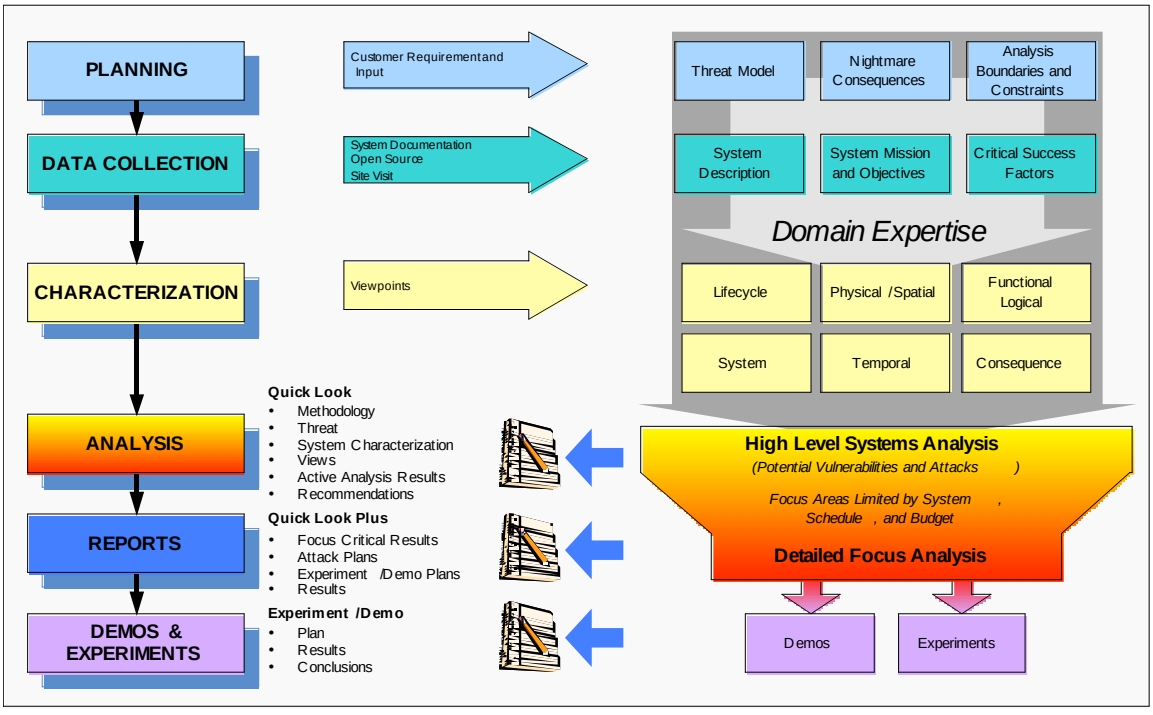


Figure 3 – IDART Methodology

2.1.1 Planning

Figure 3 shows the IDART methodology. In the "Planning" phase, the Red Team identifies the adversary and capabilities that will be modeled, the worst case scenarios for system failure, and any constraints that will be placed on the analysis or on the Red Team. The results of this phase are based on customer requirements and are usually produced by a joint

Red Team/customer team, though sometimes the Red Team develops recommendations which are submitted to the customer for approval.

2.1.2 Data Collection

The second phase involves data collection. In this phase, the Red Team reviews all available system documentation, collects open source material relevant to the target system, and visits an operational customer site if it is available. This phase serves to provide the Red Team with the appropriate background information to model the adversaries identified in the Threat Model. The Red Team develops a detailed description along with the mission and objectives of the target system. The Red Team also identifies its critical success factors, a list of objectives that will serve as indicators of Red Team success. The subsequent system characterization and analysis phases are very dependent on the accuracy and completeness of the system description generated in this step.

2.1.3 Analysis

The Analysis phase is highly variable depending on the projects budget and schedule, the Threat Model and any constraints identified during the Planning phase. This phase can range from a Quick Look overview, which simply identifies potential vulnerabilities and attacks with little or no verification to a detailed analysis in which the system or portions of it are subjected to a deep analysis with full attack development, validation, and countermeasure generation.

2.1.4 Reports and Demos & Experiments

The Report and Demo/Experiment phases are dependent on the Analysis phase for their level of detail. The higher the level of analysis, the greater the detail in the report and the more complex and advanced the demonstrations and/or experiments.

2.2 Assumptions

The CCSS assumed that while AMI was the primary subject of this analysis, related forms of demand-response could be considered.

2.3 Procedures

The CCSS used a two-phase process, using the IDART process in both. The initial phase involved an examination of AMI to determine whether the technology could cause adverse affects to the bulk electric grid. The second phase, which did not take place, would have involved using the IDART process to develop likely attacks from which the team could develop mitigations.

3 Results and Discussion

3.1 Risks Summary

The national risk of harm to the economy, public health, trust in government, public safety, and environmental integrity is low to moderate based on the consequences of AMI attack. Another factor that reduces risk, at this time, is the low penetration of AMI into the electric infrastructure. That factor is about to change, however, as California utilities fulfill the requirements of the California Energy Commission and other states follow the California lead.

The risk of economic harm is low, at this time, but could rise to moderate with the widespread use of AMI. The risk of harm to public health is very low. The risk of harm to trust in government is moderate in those cases where there is a clear conflict between regulators and utilities and when residential customer rates are increased. The risk of harm to public safety is low as there would need to be a "perfect storm" of effects outside of the electric grid for the consequences of attack to harm public safety. The risk of environmental harm is low as the only reasonable connection between attacks on AMI and the environment are through increased pollution from increased generation.

3.2 Threat to Risk Analysis

3.2.1 Threats

The threats to AMI range from the cheating customer to the foreign nation state with a side trip through various types of insiders. Threats of concern are described with reference to the characteristics of cyber threat models in *Generic Threat Profiles* [1]. The lowest level, highest probability threat to AMI implementations is the cheating customer. Next highest in probability is the insider whose motivation is financial. Beyond these threats are the high-level, low-probability threats of nation-state or terrorist groups.

3.2.1.1 Cheating customer threat

Current interest in security among utilities implementing AMI centers on the familiar threat of cheating customers. This is evident in discussions and workshops as well as requests for help in evaluating the security of AMI roll-outs. This limited concern is understandable but could leave AMI implementations vulnerable to the more sophisticated threats.

The cheating customer threat has low levels of funding, moderate commitment to achieving their goal, can tolerate some risk of exposure, have extended physical access only to the meter on their premises, have a range of cyber skills from low to high, has months to years to achieve their goals, and will initially work in small numbers. There may be some attempt to perform the types of physical attacks that have been used in the past against conventional meters, but these will be quickly detected through monitoring of electric use in real-time. The more likely attacks against advanced meters will be similar to the attacks against broadband modems. These will include accessing the AM configuration through cyber means as

described in [2] and even modification of the AM firmware as described in [3]. Just as in the cable modem un-capper world described in the references, the threat will arise from small groups who combine talents and knowledge to develop tools to modify advanced meters for consumers. The problem arises when these tools go commercial [4] and customers who would not or could not develop the tools themselves are able to purchase them.

3.2.1.2 Insider threat

Some utilities have expressed concern with insider threats in other systems, such as distribution or energy management. The insider threat to AMI is also of concern.

AMI is intended to manipulate the load to reduce peak usage in order to minimize the cost of energy to the utility and end-customer (see Appendix B: Description of AMI). An insider in collusion with a generation provider could use an AMI to make money. The insider will use the AMI to increase peak usage, thereby creating increased demand for generation power, possibly via the spot market, but certainly at a higher price point than would otherwise occur. Thus the colluding generation provider will make more money that they can share with the insider. The insider in this case would be described as having low funding (they want to make money, not spend it), low goal intensity (they can't spend the money in prison), high stealth (insiders require stealth to succeed and to avoid being caught), high physical access (they are insiders, after all), low cyber skills (they are far more likely to misuse the system than to develop cyber attacks), an implementation time in months, and a cyber organization size in ones. The insider may have access from one or more of several points in the system. The insider could be someone who controls the AMI head-end system, in which case they would have access to that system and associated networks. The insider may be someone who works with the EMS from which the AMI head-end gets pricing information, with access to that EMS and associated networks as well as potential access to the AMI head-end. The insider may be someone who works with the balancing authority, ISO, or other entity from which the pricing information flows. The insider need not be an operator or controller of a control system – the insider may have access through administration of computers or networks used in the AMI head-end or EMS. One side note about the insider threat is that utilities may need to exercise due diligence to show that insiders are not cooperating with generation divisions within the same energy company.

3.2.1.3 Nation-state or terrorist threat

Although utilities cannot counter nation-state or terrorist threats on their own, their security improvements for other threats can help the US government in countering these threats. The high-level threat is best described as either category I or II in the Generic Threat Models document. These threats would attack AMI with intent to cause effects outside of the AMI system, probably effects centered on the bulk electric grid. The high-level threat will have all of the access of the customer and insider threat, so defenses against these would help counter the high-level threat. In addition, the high-level threat may have access in ways different from those threats discussed earlier.

3.2.2 Cyber Effects

3.2.2.1 Cyber Effects of Customer attack

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. Of the few examples we have seen of actual AMI meters, the configuration is controlled remotely by the utility through the external interface of the meter. Just as some cable modems initially allowed control from both the broadband and the local network interfaces, we would expect that some AMI meters will be susceptible to configuration attacks through the communication interfaces to the customer's appliance control equipment. This type of vulnerability will be found and corrected quickly, but there will still remain the possibility that the utility-side configuration interface will remain. Since the meter is physically accessible to the customer, the customer will be able to access this utility configuration interface and use the same methods as the utility to reconfigure the meter. Just as with cable modems, eventually the meters will be protected from this type of attack through various means which will leave the reverse-engineering attack. This attack will not be feasible for the average customer, but with a sufficiently large install base, the probability of a customer with the capability to perform the reverse engineering attack and the will to conduct it will approach one. Just as with the broadband modem uncapping movement, the first attackers will eventually find a way to make their attack usable by less technical customers and potentially sell it to those customers. The primary cyber effect will be that AMI meters at customer endpoints will under-report electric usage. A secondary cyber effect would be under-reporting of ancillary services such as natural gas usage. Another secondary, and probably unintended, cyber effect could be failure to report correct status or outage information.

In those few cases where the utility offers (and probably uses) broadband over power line (BPL), the AMI meter will probably have even more of the aspects of the broadband modem. In those cases, the customer attack might have the goal of uncapping upstream bandwidth, just as broadband modem users attack now. The method of attack would be the same as described in the previous paragraph but the cyber effect would be different. The effect would be to flood communications within the BPL network. This contention for bandwidth would not only affect other BPL customers but it would affect any communications of the utility over the same media as the publicly accessible BPL. In particular, the AMI meters would have difficulty communicating status and usage information as well as receiving pricing information.

3.2.2.2 Cyber Effects of Insider attack

The insider attack would take advantage of access to systems at the opposite end of the AMI system from the customer endpoint. Systems 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.

An insider with access to the AMI head-end as an operator or engineer could modify its function to change pricing information sent to customer end-points. This is problematic without further research into actual head-end implementations. There may be no operator or engineer interface function that allows the user to modify pricing information as it flows through the system. If the interface function exists, the insider need not have a great deal of technical knowledge to perform this attack. Alternately, this type of insider would have either physical access to the systems involved or administrator access to either systems or networks.

An insider with physical access to the AMI head-end system, the EMS, ICCP server, or the network infrastructure supporting these systems can perform attacks at either the computer or network level. This insider can modify software or settings on any of the systems so that the pricing information is changed as it flows through that system. This requires knowledge of the software and the supporting systems or protocols.

An insider who has administrator or root access to the AMI head-end system, the EMS, ICCP Server, or the network infrastructure supporting these systems can perform attacks virtually on the computers or networks.

3.2.2.3 Cyber Effects of Nation-state or terrorist attack

3.2.2.3.1 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 is 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.

This attack is enabled by the AMI connectivity, the trust relationships between the various systems involved, and the commodity hardware and software that these systems use. An AMI system provides connectivity from the balancing authority or ISO all the way down to the individual meter at the residential and small business customer. The ISO trusts the utility to which it is connected via ICCP. The utility trusts its EMS to connect to its DMS. The DMS trusts the AMI head-end system. The AMI head-end trusts the meters.

Our research shows that the meter is built for the functional capability to connect other meters and customer equipment to the AMI network. Like cable-modems, these meters use standard, embedded operating systems. There are whole communities of hobbyists who have developed open-source firmware for certain cable modems. This shows that the technical capability to take over the meter function and gain the connection to the AMI network is perfectly feasible.

Head end or AMI Host systems available through commercial channels seem to use Microsoft Windows Advanced Server 2003 on standard hardware. This combination has had vulnerabilities that can be exploited in the past in the basic platform package. The additional software that provides the AMI functionality may also have vulnerabilities. Unless these systems are patched quickly for newly disclosed vulnerabilities, standard exploits will be available to crack into them. In addition, sophisticated adversaries with the right connections into the black-hat world may be able to exploit vulnerabilities that are not yet disclosed and for which no patch exists – the so-called zero-day exploits.

The AMI is inherently connected to some source of pricing information, whether that is directly from the ISO or through the utility EMS from the ISO. The adversary could use that connection to gain access to the EMS or, via ICCP, the ISO. Once the attacker has this access, they can affect the bulk electric grid.

3.2.2.3.2 Interference with Utility Telecommunications

Since the AMI communication network will frequently share some or all hops with other utility communication networks, there is a potential for an attack that takes advantage of poor separation of channels. Bypassing that separation could lead to access to the EMS and, therefore, access to attacks on the bulk electric grid.

This attack depends upon the AMI connectivity in the "cloud" that current vendors treat as a functional and not security problem. As mentioned above, there are myriad solutions in the AMI world to the telecommunications problem and the vulnerability of an AMI network depends upon the vulnerabilities in the communications technologies it uses.

3.2.2.3.3 Mass Load Manipulation

Utilities plan to use AMI for many purposes including reduction of peak loading, real-time dynamic load modeling, fault detection and reporting and at least four others. Most of these actual uses of AMI are not relevant to the bulk electric grid as they primarily serve the load-serving entity. The one use which could affect the bulk electric grid is reduction of peak loading. This is the primary purpose of AMI as a demand-response system. Clearly, the utilities rolling out AMI expect to achieve a reduction in peak loads and an overall lessening of electric usage during peak periods. This is very similar to previous systems such as Demand Side Management (DSM) or Direct Load Control (DLC).

Sandia discovered a possible attack on the bulk electric grid using DSM or DLC in 1997. The discovery was fortuitous in that our research happened to discover that a popular system for communication in DSM was also a system we had assessed for other uses. Sandia had discovered a vulnerability in the communication system that would allow an attacker with physical access to a node to send messages to all the other nodes. Putting that together with existing DSM systems of tens of thousands of residential customers led to the concept of attacking the DSM through the communications system. An attacker could use the DSM to send messages turning off all controllable customer equipment. Once a long enough time had elapsed to guarantee most of the equipment would turn on when allowed, the attacker could send the turn-on permission message. This would cause the maximum possible peak load to develop very quickly, which would affect the bulk electric grid.

This attack carries over into AMI, but with some differences. Since AMI depends upon the customer equipment to respond to market price fluctuations, there is no direct control of the load. Instead, the attacker would have to publish a price to the AMI that would drive most of the customer equipment off-line. Once the load dropped and stabilized, the attacker could publish a new price that would drive that same customer equipment to start up, again.

Sandia has not modeled the exact effects of a sudden peak load on the bulk electric grid. Clearly, there would be effects. Utilities and regulatory agencies would not be interested in AMI if it couldn't have a positive effect on the bulk electric grid. However, that doesn't automatically mean that AMI could have negative effects, if misused.

3.2.3 Electric System Impacts

The electric system impacts due to the cyber effects of customer and insider attacks are low to moderate. The electric system impacts of high-level threats could be more severe.

The electric system impacts of customer attacks will include higher peak usage of electricity (and concomitant higher prices of electricity to utilities and consumers), under-reporting of usage in local areas that could affect planning, and potential loss of outage information. This could vary from a negligible impact if only a few customers modify their meters to significant impacts if meter hacking becomes readily available and widespread. A major consideration that regulates the severity of impact is how widespread the customer attack becomes. If the attack becomes readily available to customers with moderate technical skills and enough customers modify their local meters, the severity will increase. The sheer numbers in this case would obfuscate the extent of the effects.

The electric system impacts of insider attack will include higher peak usage of electricity and artificially high usage reporting for planning.

The system impacts of terrorist or nation-state attacks could include instability of the bulk electric grid, widespread outages, and equipment damage.

3.2.4 Consequence

Just as the systems impacts of customer and insider cyber attacks are low to moderate, the consequences beyond the local level are low to moderate. The consequences of cyber attack by high-level threats are by definition moderate to severe at the local and possibly regional level.

Customer attacks will have low to moderate local consequences with the potential, in case of disaster, of moderate regional consequence. The immediate economic consequence of customer attacks will be decreased profitability of investor-owned utilities and increased operating costs of publicly owned utilities. Longer-term, utilities may not plan infrastructure that will meet loads because the data shows the loads as less than actual. During large outages due to weather or ground fault conditions, utilities expecting to send crews to pinpoint problems could find that customer-hacked meters don't provide them with the information they need. At a minimum this could increase operating costs for utilities. However, at least one current user of AMI reported using the outage information to manage recovery from hurricanes. If the detailed outage information from AMI had not been present,

the crews trying to restore service after that disaster would have had to localize outages before correcting the problems.

Insider attacks that cause higher peak usage of electricity would have low to moderate consequence at the local level and low consequence at the regional level. Unlike the customer attack, the consequence of insider attack will not be decreased profitability of investor-owned utilities if they may simply pass artificially high electric costs on to the consumer. However, regulation could prevent passing on the costs and investor-owned utilities could find themselves operating at a loss if they pay more for generation than they can charge their customers. Publicly owned utilities will have similar problems as their rates are set by their franchising government. Co-ops could suffer internal conflict. An additional consequence that could ensue from an insider attack is customer dissatisfaction that could result in regulation if none is present. The insider attack, if discovered, would be cause for investigation for code of conduct and information conduit violations in utilities that participate in the power market. These consequences could result in bankruptcy or restructuring of utilities that cannot operate within the economic parameters resulting from an insider attack. While it is unlikely that any customers would go without service, these economic disruptions will reduce the level of service and increase the probability of other forms of disruption. Reliability activities may be the first cost centers to be cut in the case of economic disruption of a utility. One of the first reliability activities to be cut in economically stressed utilities is tree-trimming. Tree-trimming sounds unimportant, but lack of tree-trimming led to the August 2003 blackout.

Terrorist or nation-state attacks which disrupt the bulk electric grid, cause widespread outages, or damage vital equipment could achieve severe local consequences and moderate to severe regional consequences.

3.2.5 Risk

The national risk of harm to the economy, public health, trust in government, public safety, and environmental integrity is low to moderate based on the consequences of AMI attack. Another factor that reduces risk, at this time, is the low penetration of AMI into the electric infrastructure. That factor is about to change, however, as California utilities fulfill the requirements of the California Energy Commission and other states follow the California lead.

The risk of economic harm is low, at this time, but could rise to moderate with the widespread use of AMI. Economic harm could result from the economic consequences to the electric utilities spreading into local economies and from higher prices for electricity affecting commercial and industrial electric users, all of which would affect residential electric users. Economic harm from disruption of the electric grid, widespread outages, and equipment damage are more direct but could affect other critical infrastructures as well as general business.

The risk of harm to public health is very low. Although electric power is necessary to activities that affect public health such as water and sewage treatment, the duration of any outage caused by the most advanced adversary through AMI would not last long enough for public health to be affected.

The risk of harm to trust in government is moderate in those cases where there is a clear conflict between regulators and utilities and when residential customer rates are increased.

The risk of harm to public safety is low as there would need to be a "perfect storm" of effects outside of the electric grid for the consequences of attack to harm public safety. That said, terrorist or nation-state adversaries could use AMI attacks that disrupt the bulk electric grid as an effects multiplier of other attacks on other critical infrastructures.

The risk of environmental harm is low as the only reasonable connection between attacks on AMI and the environment are through increased pollution from increased generation.

3.3 Plausible Threat Scenario

As an example of the how an adversary that should concern utilities could attack AMI, we look at the Insider Threat Scenario.

The AMI installation at ElecNet (Electric Networks, Inc.) includes redundant Windows 2003 Server systems running the head-end software that communicates with the customer endpoints. The AMI server software includes the capability to adjust pricing information received from the Independent Systems Operator (ISO) via the Energy Management System (EMS). The ISO sends pricing data calculated on a quarter-hourly basis from the latest hourly generation bids provided to the ISO through the regional market. The EMS gets the pricing feed via Inter Control Center Protocol (ICCP) links to the ISO servers. The EMS splits the pricing information into two streams, one that feeds the brokers and one that feeds the AMI.

The adversary is Bob Williams, a system administrator for the head-end servers of the AMI system, who has a gambling problem and desperately needs funds to maintain his lifestyle. Representatives of GensR'Us, a genco which supplies electricity to ElecNet, approach Bob with an offer to provide him with enough money to keep him gambling. All they ask him to do is modify the pricing calculation software in the head-end server with a library they supply. Bob agrees to do so – he's desperate. Bob takes the compact disk provided by the GensR'Us representative, inserts it into the Windows 2003 Server system, and executes the installation program on the CD. GensR'Us had previously paid a cyber-criminal to reverse engineer the AMI software and change certain static variables by small amounts. The modified library is almost identical to the real library. Once Bob has installed the library, the pricing information sent to the customer endpoints of the AMI system is consistently low by about 2% – not so much as to cause the customers to complain but enough for the demand to remain higher than it would be if the correct pricing information were provided. ElecNet buys more electricity from their generation sources, including GensR'Us, and GensR'Us pays Bob a small percentage of the extra money they make selling to ElecNet.

This attack would be easy to perform and difficult to detect without the appropriate countermeasures. The cost to GensR'Us would be approximately four weeks of the cyber-criminal's time, the purchase price of the AMI software (if they can't get a demo copy), and the payment to Bob. Even if the change is discovered, there will be no possibility of attribution to GensR'Us or even Bob. Certainly, if the software is discovered to be changed,

Bob would be a prime suspect, but there would not be sufficient proof to pin the deed on him. Since all of the generation companies from which ElecNet buys have benefited, there is no way of knowing which, if any, is behind the modification. Other possible candidates could be energy market speculators. What's worse, ElecNet could itself be held liable by regulators for the extra costs to customers.

4 Conclusions

Risk in general based on Advanced Metering Infrastructure (AMI) an adversary exploitation is low to moderate at the time of this writing. This is due primarily to the fact that there is very little installed AMI. This is likely to change as more AMI is installed due to its attractive features. Even with an extended AMI in place, risk to the environment and public health and safety remain low.

The primary consequences of an AMI attack are economic through disruption and falsification of metering information. Theft of power through falsified meter data, manipulation of the power market, and higher prices are the general consequences. A more capable threat would cause consequences of greater magnitude affecting a larger area.

In order of capability, customers, insiders, terrorists, and nation-states are the primary agencies that could threaten the AMI. There are effective measures against all of these.

Customer threat should be the easiest to mitigate but the solutions could prove to be difficult because of political reasons. The AMI industry and operators could mount an effective defense against abusive customers by using a data transmission standard for AMI data and investigating abnormal usage patterns.

Effective defense against the insider threat requires that abnormal insider activity be detected with high probability, since individual insider threats are negated by discovery. Publicizing the improved detection capability also reduces risk by deterring insider activity. Background checks and audits, authentication, intrusion detection, and software integrity checking are all relevant in this role.

The terrorist and nation-state threats are mitigated by all of the above because they make the target less attractive. Additional effective approaches to protecting against this threat are router access lists, firewalls, protected communication between the AMI network and other networks, strong communication authentication, and detection and halting of rapid market fluctuations.

A utility implementing the recommendations contained in this report as it installs AMI technology will be positioned to detect and withstand attacks that attempt to exploit the vulnerabilities of the AMI.

5 Recommendations

The customer threat should be the easiest to mitigate but the solutions could prove to be difficult because of political reasons. Essentially, the AMI vendors and operator industry should adopt a standard similar to DOCSIS [6] and rigidly enforce that standard. The experience of the broadband industry shows that enforcement is the key step: nearly all the reported vulnerabilities in broadband modems stem from failure to follow the standard. This will require purchaser pressure on vendors to move from their proprietary market models to an industry model such as OpenAMI and to add security requirements to the standard. No standard, however strict and widespread, will prevent determined fraud, so the industry should consider mitigation by shifting risk through increased rates to cover losses. Another mitigation strategy would be to detect anomalies in electric use among customers (referent to usage history or peers) and investigate those anomalies. Such investigation would involve checking the configuration and firmware of the meters of suspected cheaters. This can be automated for minimal expense to the utility and maximum chance of detecting unauthorized modifications.

The insider threat is sensitive to being caught (low goal intensity) so the best defenses against insiders are those that increase the deterrent effect by increased chance of detecting the activity. First, all communication from the head-end to the customer endpoint should be treated as control traffic. As such, authentication of commands should be put in place. Good authentication will prevent man-in-the-middle and spoofing attacks by insiders with access to the AMI communication network. While the head-end systems are clearly not critical cyber assets in the sense of NERC CIP-002, the utility may want to treat them as such and implement personnel and system security management. Measures such as background checks and auditing will deter insiders who attack through physical access to AMI or related systems. Host-based intrusion detection with software integrity checking of the head-end systems will detect changes to the systems by insiders. Utilities should conduct frequent, irregular audits of head-end output compared against input to ensure that they match. All user commands and actions in the head-end systems should be accountable, which will require logging and strong user authentication.

All of the defenses mentioned above will help to mitigate the terrorist or nation-state threat. Any of them could be overcome by this type of threat, but having them in place will make AMI a less attractive target to achieve the effects this threat will want to achieve. This is analogous to making one’s house less attractive to burglars so they move on to someone else’s house. In addition, utilities should consider implementing specific defenses against the three attacks discussed above. The first attack, using the customer endpoint as access to exploit the AMI network, can be prevented by implementing network control defenses such as router access lists and firewalls within the AMI network. When doing so, the utility will need to consider each of the points at which the communication changes networks to ensure that attackers can’t bypass defenses by jumping into the middle of the network. Some AMI architectures call for several transitions from one communication network to another, including wireless communication at points upstream from the customer endpoint. The second attack can be prevented by protecting communications between the electronic

security perimeters of components of networks that are collocated with the AMI network. The third attack can be prevented by implementing strong authentication of communication from the head-end to the customer endpoints and safety systems that look for and stop rapid changes in pricing information. The latter defense may also serve to prevent market fluctuations due to computer control of the market.

In summary, the recommendations are:

1. Adopt an open reference standard for security of advanced meters.
2. Enforce full implementation of the security standard by advanced meter vendors.
3. Authenticate all commands from the head-end to the customer endpoint.
4. Authenticate all reporting from the customer endpoint to the head-end.
5. Protect head-end systems as if they were critical cyber assets in the sense of NERC CIP-002.
6. Implement host-based intrusion detection with software integrity checking of the head-end systems.
7. Perform frequent, irregularly scheduled audits of head-end outputs to ensure they reflect inputs.
8. Use strong user authentication on all head-end systems and log all user actions.
9. Implement network separation, strong firewalls, and limited router access control lists in the AMI network.
10. Implement strong separation between the AMI network and the electronic security perimeters of other systems such as EMS.
11. Implement safety logic to prevent rapid changes in pricing information sent from the head-end to the customer endpoint.

Appendix A: References

[1] Duggan, David P.; *Generic Threat Profiles*; Sandia Report SAND2005-5411; Sandia National Laboratories, July 2005.

[2] McWilliams, Brian; "Cable Modem Hacking Tricks Uncapped Online"; *Security Focus* web site; March 2002. http://www.securityfocus.com/news/353

[3] Poulsen, Kevin; *Cable Modem Hackers Conquer the Co-Ax*; *Security Focus* web site; February 2002. http://www.securityfocus.com/news/7977

[4] TCN-ISO web-site. http://www.tcniso.net/

[5] *Roadmap to Secure Control Systems in the Energy Sector*, Sponsored by the U.S. Department of Energy and the U.S. Department of Homeland Security, prepared by Energetics Incorporated, January 2006.

[6] *CableLabs* web-site. http://www.cablemodem.com/

[7] *Assessment of Demand Response and Advance Metering*, Staff Report Docket Number: AD-06-2-000; Federal Energy Regulatory Commission; August 2006.

Appendix B: Description of AMI

Introduction to Advanced Metering Infrastructure (AMI)

Since the NSTB program scope includes the bulk electric grid and not the distribution systems with which AMI is normally associated, SNL first needed to determine if there could be effects on the bulk electric grid from attacks on AMI. SNL had already begun investigation of AMI and has a history of analysis of other, similar technologies. The first task SNL undertook was to organize the knowledge of AMI already gathered. SNL supplemented this with information from the Federal Energy Regulatory Commission Staff Report, Assessment of Demand Response and Advanced Metering when that became available in August of 2006.

The key concept behind AMI, specifically, and demand response, is that electric usage is not consistent over time. In particular, usage peaks for certain hours of the day during certain seasons, is much smaller at other specific times, and varies in between these peaks and valleys. The electric system, from generation through transmission to distribution, must either be built to support peak demand or find a way to limit peak demand to the level the grid can support.

Demand Response

Demand response refers to changes in electric usage by end-use customers from their normal consumption patterns in response to changes in the price of electricity over time, or to incentive payments designed to induce lower electricity use at times of high wholesale market prices or when system reliability is jeopardized. Methods to achieve the goal of demand response include incentive-based demand programs and time-based demand response programs.

Incentive-based demand response programs include direct load control (also referred to as demand-side management or DSM), interruptible/curtailable rates, demand bidding/buyback programs, emergency demand response programs, capacity market programs, and ancillary-service market programs ([7], p 45). For purposes of analyzing AMI, the only one of these programs that is of interest is DSM. The others do provide evidence that large load customers will respond to incentives to reduce usage. However, to be effective, the other demand response programs require a minimum load size in excess of typical residential and small business.

Time-based demand response programs vary according to the time period and the method of feedback to the customer. Most customers are exposed to time-based demand response in the form of seasonal variations in the cost of energy. Simple forms of time-based demand response are based on time of use with several variants among utilities as to peak pricing hours and differences in price between peak, average, and off-peak. Two forms of time-based demand response, critical peak pricing and real-time pricing, connect the wholesale market more directly to the retail customer. Other than seasonal changes in price, all of the time-

based demand response programs require special metering technology to enable them. At a minimum, the meters need to be aware of time of day. The most technologically sophisticated systems provide pricing information to customer control systems, e.g. smart thermostats.

AMI, AMR, DSM

Advanced Metering Infrastructure is a term that is not easily defined. The FERC report states that the commission staff define "advanced metering" as a metering system that records customer consumption [and possibly other parameters] hourly or more frequently and that provides for daily or more frequent transmittal of measurements over a communication network to a central collection point. This definition includes Automated Meter Reading (AMR) as well as some aspects of AMI. For this report, SNL defines AMI as a metering system that records customer consumption hourly or more frequently, provides for transmittal to a central collection point at an equivalent useful frequency, and provides electric costs to the customer to guide electricity usage at an equivalent frequency.

Both definitions fail to specify anything about the means of communication between the customer meter (usually called an endpoint) and the central collection point (sometimes called head end). The sheer variety of solutions that utilities have implemented precludes any standard definition. The next section will go into more detail on this subject.

DSM has long been used by utilities to control peak loads, usually with incentives to the customer whose load is being controlled. The author of this report first came across DSM implemented in a small municipal utility by his father in the late '80s in Texas. The technology has evolved since that time, but the concepts are the same. The customer agrees to let the utility directly control major load-inducing appliances within the customer's establishment. In residential and small commercial establishments, this usually encompasses air conditioners, electric water heaters, and, occasionally, smaller appliances. These are selected for their contribution to the variability of electric usage. The customer is usually compensated for any possible inconvenience by reduced electric rates. DSM achieves the reduction of peak loads by cycling the major appliances in fractional groups. Even on a hot summer day, residential air conditioners usually don't run all the time in a 100% duty cycle. A DSM system such as the one the author observed in Texas will turn off one-quarter of the air-conditioners for 15 minutes, then allow those to turn back on after turning off a different quarter of the units. Each system is allowed to run at a 75% duty cycle, but no more than 75% are running at a time. The peak load should be reduced by 25% of the load contribution from air-conditioners, which can mean considerable savings in the wholesale market as well as reducing the required infrastructure capacity.

AMI is the logical conjunction of AMR and demand-side management or direct load control. DSM provides the forward path from the utility to the endpoint. AMR provides the return path from the endpoint to the utility. With the addition of a connection to the source of electricity costs, AMI can provide the customer with near real-time information on which to decide electricity usage.

AMI Architecture

AMI is typically pictured as in Figure B1: as the meters and the AMI host connected together by a communication cloud and connecting to external systems. This explains the concept, but the real security issues are hidden in the cloud and the arrows. The great variety of possible implementations of the data collection network as well as connections to external systems would be the subject of the AMI Secure Implementation Guide.

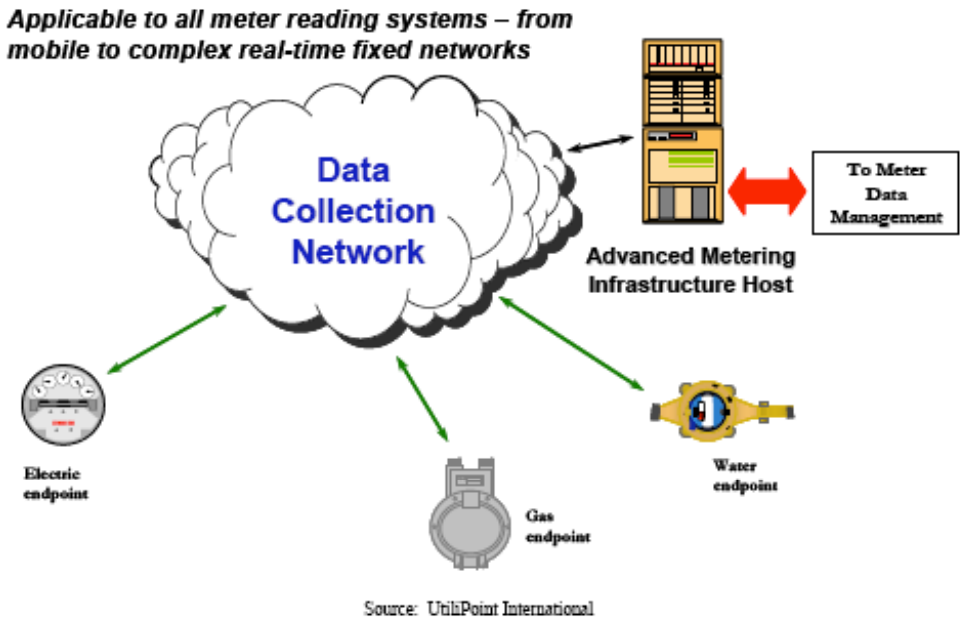


Figure B1: Typical AMI Architecture

AMI is an amalgamation of two technologies and one process. The two technologies, DSM and AMR, join with time-based demand response to enable small retail customers to control their electricity usage according to the real price of electricity, passed on from the wholesale market. This involves two systems that are, in effect, control systems.

At the customer end of AMI, the customer owns one or more systems that control appliances and systems within the customer's home or business. This system receives information from the AMI system, which itself is a control system. In some cases, the AMI also acts as a control system for other processes than electricity delivery such as gas delivery or water delivery.

The advanced meter, itself, encompasses all of the elements of infrastructure equipment and field equipment in the Control Systems Reference Model (Figure B2). It clearly has sensors equipped to detect the flow of electricity. It has an actuator that will switch off that flow upon command. It has some form of IO controller with which to communicate with other meters and the customer control system. The only role in those two areas which may not be present is local control. The AMI system includes many of the objects in the control center portion of the CSRM and also has external connections.

The customer system includes all of the elements of field equipment and infrastructure equipment. The advanced meter fulfills the Field IO role as well as IO Controller role.

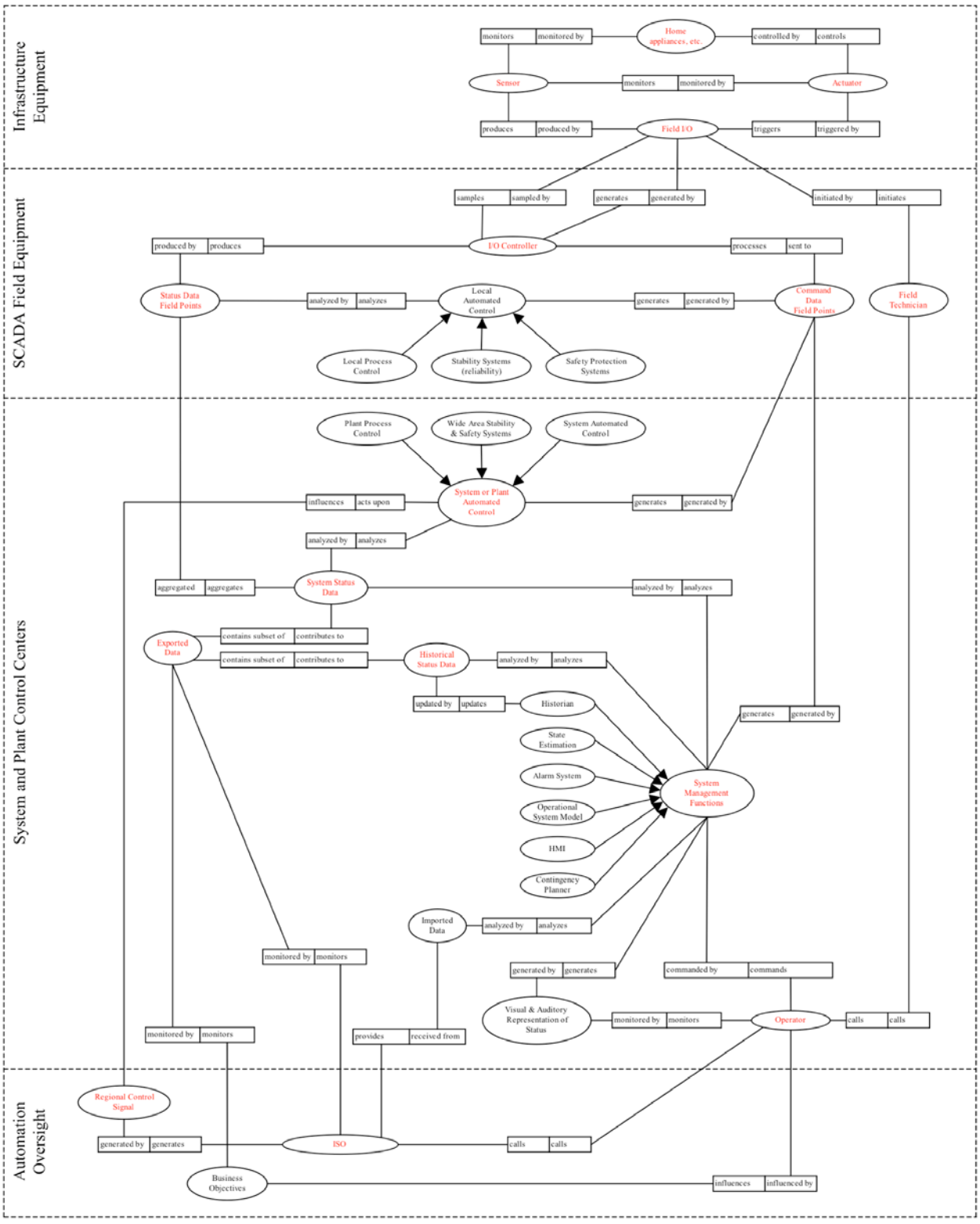


Figure B2: Control System Reference Model

Data Collection Network

The data collection network (the “cloud” in the center of Figure B1) can be implemented in many ways with correspondingly variant security risks. All of the methods rely on a hierarchical, star architecture from the customer endpoint to the head-end. Various levels of concentration eventually lead to a standard Ethernet connection to the AMI Host or head-end system. Each hop between nodes may use the same or different technologies for communication. Some of the technologies mentioned in various sources include wireless (802.11, 802.15, proprietary), wired (serial, high-speed serial, Ethernet), and power line carrier (broadband and lesser). A particular AMI implementation will normally use several different technologies on different hops for different purposes. It is possible to use a single technology for the entire communication network but that seems to be the exception rather than the rule. Another factor that enters into the equation is existing communications. Communication is a valuable resource, and most implementations seem to depend upon re-use of an existing network, frequently one already used for control. The industry contacts we have made indicate their intention of re-using existing systems put in place for commercial and industrial customers or re-using power-line-carrier systems that support SCADA.

Appendix C: Acronyms, Symbols, Abbreviations

AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading
BPL	Broadband Over Power line
C2S2	Center for Control System Security
DLC	Direct Load Control
DSM	Demand Side Management
EMS	Energy Management System
ICCP	Inter-Control center Communications Protocol
ISO	Independent System Operator
LSE	Load-Serving Entity

Appendix D: For More Information

Ray Parks	(505) 844-4024, rcparks@sandia.gov
Jennifer Depoy, manager	(505) 844-0891, jdepoy@sandia.gov

Distribution List

1 Mr. Hank Kenchington
US Dept of Energy
OE-10
1000 Independence Ave SW
Washington, DC 20585

1 MS 0671 Raymond C. Parks, Dept 05627

2 MS 9018 Central Technical Files, Dept 8945-1

2 MS 0899 Technical Library, Dept 4536