SANDIA REPORT

SAND2008-0947 P
Unlimited Release
Printed February 2008

Renewable Systems Interconnection Study:

Cyber Security Analysis

Annie McIntyre

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

SAND2008-0947 P
Unlimited Release
Printed February 2008

Renewable Systems Interconnection Study:

Cyber Security Analysis

Annie McIntyre,
Energy Systems Analysis Department
Sandia National Laboratories
PO Box 5800
Albuquerque, New Mexico 87185-0619

Abstract

To facilitate more extensive adoption of renewable distributed electric generation, the U.S. Department of Energy launched the Renewable Systems Interconnection (RSI) study during the spring of 2007. The study addressed the technical and analytical challenges that must be addressed to enable high penetration levels of distributed renewable energy technologies. The RSI project includes a Security Analysis Task designed to address the cyber security issues that may be associated with increased PV penetration. This task examines the current and future architectures that facilitate this larger penetration, identifying components and critical areas that may expose cyber vulnerabilities. This introductory review also identifies areas—such as protocol, inverter, and meter designs—that require further consideration as designs evolve and penetration increases throughout the life cycle.

Preface

Now is the time to plan for the integration of significant quantities of distributed renewable energy into the electricity grid. Concerns about climate change, the adoption of state-level renewable portfolio standards and incentives, and accelerated cost reductions are driving steep growth in U.S. renewable energy technologies. The number of distributed solar photovoltaic (PV) installations, in particular, is growing rapidly. As distributed PV and other renewable energy technologies mature, they can provide a significant share of our nation's electricity demand. However, as their market share grows, concerns about potential impacts on the stability and operation of the electricity grid may create barriers to their future expansion.

To facilitate more extensive adoption of renewable distributed electric generation, the U.S. Department of Energy launched the Renewable Systems Interconnection (RSI) study during the spring of 2007. This study addresses the technical and analytical challenges that must be addressed to enable high penetration levels of distributed renewable energy technologies. Because integration-related issues at the distribution system are likely to emerge first for PV technology, the RSI study focuses on this area. A key goal of the RSI study is to identify the research and development needed to build the foundation for a high-penetration renewable energy future while enhancing the operation of the electricity grid.

The RSI study consists of 15 reports that address a variety of issues related to distributed systems technology development; advanced distribution systems integration; system-level tests and demonstrations; technical and market analysis; resource assessment; and codes, standards, and regulatory implementation. The RSI reports are:

- *Renewable Systems Interconnection: Executive Summary*
- *Distributed Photovoltaic Systems Design and Technology Requirements*
- *Advanced Grid Planning and Operation*
- *Utility Models, Analysis, and Simulation Tools*
- *Cyber Security Analysis*
- *Power System Planning: Emerging Practices Suitable for Evaluating the Impact of High-Penetration Photovoltaics*
- *Distribution System Voltage Performance Analysis for High-Penetration Photovoltaics*
- *Enhanced Reliability of Photovoltaic Systems with Energy Storage and Controls*
- *Transmission System Performance Analysis for High-Penetration Photovoltaics*
- *Solar Resource Assessment*
- *Test and Demonstration Program Definition*
- *Photovoltaics Value Analysis*
- *Photovoltaics Business Models*

- *Production Cost Modeling for High Levels of Photovoltaic Penetration*
- *Rooftop Photovoltaics Market Penetration Scenarios.*

Addressing grid-integration issues is a necessary prerequisite for the long-term viability of the distributed renewable energy industry, in general, and the distributed PV industry, in particular. The RSI study is one step on this path. The Department of Energy is also working with stakeholders to develop a research and development plan aimed at making this vision a reality.

Acknowledgments

The author wishes to thank the following project team members and colleagues at Sandia National Laboratories, who contributed to the technical analysis and content of this report.

David Brown, Sacramento Municipal Utility District (SMUD)

Jeff Goh, Pacific Gas and Electric Company (PG&E)

Mark McGranaghan, Electric Power Research Institute (EPRI)

Tom Ortmeyer, EPRI

Mike Ropp, Institute of Electrical and Electronics Engineers

Chuck Whitaker, BEW Engineering

Randall Wetherington, Oak Ridge National Laboratory (ORNL)

Ward Bower, Sandia

David Duggan, Sandia

Glenn Kuswa, Sandia

Jason Stamp, Sandia

Juan Torres, Sandia

Executive Summary

Integration of renewable energy into the U.S. critical power-generation infrastructure will likely continue to increase throughout the next decade. Incorporating PV energy into the existing bulk power distribution grid requires consideration of potential effects associated with that integration. Cyber security issues are among these potential effects. Addressing cyber security now affords the opportunity to optimize design and build a more secure, cost-efficient solution up front. Secure operations are beneficial in that they protect both the energy consumer and the provider, ensuring continued availability and creating greater economic stability.

The RSI project includes a Security Analysis Task designed to address the cyber security issues that may be associated with increased PV penetration. This task examines the current and future architectures that facilitate this larger penetration, identifying components and critical areas that may expose cyber vulnerabilities. The aspects of cyber security for critical infrastructure, although built on information security principles, are customized for operational environments. Integrated PV aligns with operational objectives, focusing on availability and accuracy. This report defines risk in terms of threat, vulnerability, and consequence. It also presents an introductory review of cyber security in PV integration designs as it applies to power levels of 15 kV and below by defining the architecture, separating it into workable security domains, and addressing critical components. Crucial points in the architecture, such as inverters, meters, and communication pathways, require a secure design focus. These points are identified here and sample mitigation strategies are discussed. This introductory review also identifies areas—such as protocol, inverter, and meter designs—that require further consideration as designs evolve and penetration increases throughout the life cycle.

Reviewing these critical areas as penetration increases constitutes a proactive approach to ensuring reliability. By applying security controls at critical points within the architecture that facilitate continued service and stability, a balance can be struck between generation and distribution objectives and secure operations. Risks can be mitigated by employing security controls that facilitate operations and result in minimal impacts to overall architecture cost and development objectives.

Table of Contents

List of Figures

1.0 Introduction

Renewable energy technologies are being increasingly integrated into the nation's critical infrastructure, and this trend is expected to continue throughout the next decade. Incorporating photovoltaic (PV) energy into the existing bulk power distribution grid necessitates consideration of potential effects associated with that integration. Among these are cyber security issues, which are now included during reviews of energy and infrastructure systems. Traditionally, many critical infrastructure systems, which include telecommunications, economics, health care, transportation, and energy, were not designed with cyber security as a primary objective. Given global events, considerable emphasis has been placed on this topic in the past several years, and securing our critical infrastructure from cyber attack has become a primary objective. To meet this objective, legacy systems must be evaluated and designs for new systems must be optimized to ensure maximum operability and security. As PV penetrates further into the distribution system, aspects of its use will become attractive adversary targets. Addressing cyber security now affords the opportunity to optimize designs and build a more secure, cost-efficient solution from the ground up. Secure operations protect energy consumers and providers, and lead to continued power availability and greater economic stability.

The Renewable Systems Interconnection (RSI) study project includes a Security Analysis Task designed to tackle cyber security issues that may arise from increased PV penetration. This task examines the current and future architectures that facilitate greater penetration, identifying components and critical areas that may prove vulnerable to cyber attack. These areas might include hardware, software applications, communication paths and protocols, or data processes. Because cyber and physical security are closely coupled, physical access control is also considered. Assessing the risk to the infrastructure as a result of PV penetration should be an ongoing effort to ensure that defenses are maintained as new designs evolve.

The aspects of cyber security for critical infrastructure are built on information security principles. Here, they are customized for operational environments. For example, the objectives of a financial institution in securing their operations differ from those of an oil refinery. Integrated PV will align more with operational objectives, focusing on availability and accuracy. Examples of security concerns in that environment might include

- Communication paths and protocols
- Access control (both cyber and physical)
- Data in storage and transit
- Standards
- Areas of control
- Situational awareness

This report contains an introductory review of cyber security in PV integration designs with power levels of 15 kV and below. The review begins by defining the architecture, separating it into workable security domains, and addressing critical components. Critical areas that require a secure design focus are then identified, followed by a discussion of sample mitigations. Finally, areas that require further technical study are enumerated.

2.0 Current Status of Existing Research

Cyber security as it relates to critical infrastructure is an expanding area of study. Research results exist that detail cyber security issues within the bulk power distribution grid. Renewable energy integration, however, is an area in which limited research on cyber security has been done. Just as distribution grid designs are evaluated, the increasing connectivity associated with renewable integration requires consideration. Much of the material on the security of PV was written before the shift in characterizing threat that followed September 11, 2001. For example, Chowdhury investigates the integration of PV into power systems and studies the flow and system behavior in a journal article[1] and a paper in a proceedings,[2] but these studies were conducted in 1990. Although these studies do not address cyber security specifically, they do suggest operational impacts of integration. The dated results, however, require that consideration be given to existing and future designs.

Recent research on security in PV integration, which focuses primarily on physical security, is limited. Physical security is important, and students evaluating the performance of PV utilization in an international environment touch on the subject in a report titled *2006 Student Research Projects, Photovoltaic Security.* [3] No studies of cyber security as it relates to PV integration from a critical infrastructure protection standpoint have been done. Several research initiatives have assessed bulk power generation and transport. As discussed later in this report, an Automation Systems Reference Model (ASRM) was developed under a project for the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability. That project was designed to address cyber security issues in a control systems environment.

Other projects that are exploring control system security and critical infrastructure protection include the National SCADA (Supervisory Control and Data Acquisition) Test Bed, the Institute for Infrastructure Information Protection (I3P), and the Control System Security Program. Although many current efforts are evaluating interdependencies and vulnerabilities and characterizing risks, they do not readily include PV in the analysis phase. The National SCADA Test Bed, for example, has been focused primarily on electricity transmission security instead of distribution system security. As renewable energy technologies like PV come to be a larger part of our overall critical infrastructure, a review of cyber security for PV integration—ultimately aimed at ensuring the stability and availability of the grid—is necessary.

3.0 Project Approach

The Security Analysis Task maintains the elementary approach of defining the problem, investigating and analyzing it, and presenting a technical summary. The following steps, then, are included in the basic approach:

- Define the architecture and future PV trends
- Identify critical areas for further analysis and research
- Enumerate potential security hazards based on the design
- Suggest mitigations or recommend further study.

The following sections present the rationale for the various aspects of the cyber security analysis.

3.1 Background for Security Discussion

It is important to enumerate the foundational cyber security aspects that guide this analysis. Historically, information security is well defined, and various research initiatives and industry forums continue to enhance the applicability of those aspects to the operational world. The analysis phase of this task requires that key security aspects be defined as they relate to the energy sector. These are described in the following subsections.

3.1.1 Elements of Security

Many different terms exist within cyber security, including "computer security," "information security," and "information assurance." The *Free Dictionary* defines information security as

> The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. [4]

The same source defines information assurance, a term often used by the federal government that is now coming into use in industry, as

> Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.[5]

For the purposes of this study, all aspects of the previous definitions have been considered. Availability, integrity, authentication, confidentiality, and nonrepudiation issues are overarching topics that guide the PV integration analysis. Again, it is important to consider how these terms relate to operational and control system environments, highlighting the objectives of critical infrastructure and energy sectors.

3.1.2 Definition of Risk

Independent of sector or environment, risk is often defined the same way, in terms of threat, vulnerability, and consequence. Numerous methodologies have been created in the past several decades to assess and measure risk, both qualitatively and quantitatively. In a control system or system of systems environment, selected processes to characterize risks can be optimized to yield more accurate results. Sandia National Laboratories performed one characterization of risk under the I3P project. That process included characterizing risk from an operational standpoint that required consideration of mission and organizational priorities such as safety and reliability. [6,7] Reports from that effort are summarized here to build a foundational view of risks to control systems and critical infrastructure.

Figure 1. Components of risk [6]

3.1.2.1 Threats

Threats can exist in numerous forms, and they can be anthropogenic or environmental. These are classed as normal, abnormal, or malevolent threats. [8] Malevolent cyber threats often suggest a person or attacker with some intent to harm. Even though this can be true, one must also consider unintentional threats, such as accidents caused by humans or weather events such as hurricanes that down power lines. Threat assessments are often performed to identify potential causes of harm to an architecture or system. Threats to control systems can be assessed by [6]

- Identifying known and potential adversaries
- Analyzing each adversary's motivations, goals, and capabilities
- Assessing the threat posed by each adversary to critical system assets.

Malevolent threats or adversaries can be characterized by their level of access, motivations, and capabilities. The *I3P Risk Characterization Report* describes an adversarial threat.[6]

> A threat implies that an individual or group has the ability and access to carry out a process that creates damage to a system or exploits the system for a specific gain. Threats to control systems can come from both insiders and outsiders. For example, a disgruntled employee sympathetic to a terrorist cause will have more direct access to the control systems than a corresponding outsider.
>
> Threats can vary in capability. Capability is a function of resources such as time, money, computing power, technical knowledge, and intelligence resources. Threats and their capabilities are often divided into several specific categories such as nation-state, international terrorists, domestic terrorists, organized crime, or hackers. Although individual hackers may have malicious intent and technical knowledge, organized cyber-terrorist groups may possess the resources necessary to carry out an effective, distributed attack that produces severe consequences.

Attributes that can affect a threat's success include

- Commitment
    - Intensity
    - Stealth
    - Time
- Resources
    - Technical personnel
    - Knowledge
    - Access.

Detailed threat attributes and success factors are defined in the Sandia report entitled *Categorizing Threat: Building and Using a Generic Threat Matrix.*[8]

3.1.2.2 Vulnerabilities

A vulnerability is a weakness in a system, network, application, or process that can be exploited by a threat to create an adverse effect. [6] Vulnerabilities, which can be technical or physical in nature, can be identified through assessment activities and continual situational awareness. An unpatched vulnerability presents an opportunity for exploitation by a threat. Physical vulnerabilities, such as unlocked doors and open gates, are easily spotted. Identifying cyber vulnerabilities, such as open ports, unpatched software, and the absence of intrusion detection systems, is a more difficult task. Until a vulnerability is discovered, a system is seemingly secure. A system does not degrade over time but can become insecure instantaneously once a vulnerability is found. Locating and mitigating vulnerabilities in the design phase is a critical step. Continual situational awareness and security evaluation, however, remain necessary because threats become more sophisticated every day.

In PV integration, an example of a physical vulnerability might be the ability to easily access a circuit board in an inverter. Likewise, a cyber vulnerability might be the ability to access and alter digital usage data in a smart meter. Although some vulnerabilities appear more serious than others, it is the consequence value that allows an asset owner to make important decisions about mitigation and design.

3.1.2.3 Consequences

When defining risk, it may be consequence that gains the most attention and is heavily weighted in the equation. Consequence is the loss, damage, or impact resulting from a threat successfully exploiting a vulnerability, and can include data access and alteration, service disruption, system destruction, and public safety effects.[6]

The placement of bulk power distribution systems in publicly accessible areas creates a need to consider safety and security over a wide system area. Defining the threat and mitigating vulnerabilities is important, but understanding potential consequences and using that understanding to make solid decisions about protection and design may be most critical. Potential consequences should be considered from an operational standpoint, including both cyber and physical aspects. Interdependencies within the system and within the national

critical infrastructure should be evaluated. Stamp categorized potential consequences at the 2005 I3P Workshop as[9]

- Physical impacts that encompass the set of direct consequences of control system malfunction. This includes injury or loss of life, environmental damage, and loss of property.
- Economic impacts are the resulting side effects of the physical impacts ensuing from an attack. This includes equipment or site damage, personnel compensation, and other impacts that could negatively affect the local, regional, national, or possibly global economy.
- Social impacts or "quality of life," including a loss of national or public confidence in an organization or industry, which can often lead to economic impacts as well.
- Impact on national critical infrastructure, including other dependent infrastructures such as water, agriculture, telecommunications, health care, and other energy sectors.

The technical effects resulting from a threat exploiting a vulnerability lead directly to these consequences. For example, a threat that takes advantage of an unprotected port on a system can alter system data that affect billing and load analysis. This can lead to economic impacts to the utility. Although this may be a low-impact consequence, one must also consider the possibility of access to a system that alters load, resulting in a more serious consequence. Consideration of consequences associated with vulnerabilities is crucial to ensuring that the correct levels of protection are applied in the system.

3.1.3 Domains

When addressing cyber security, it is common to break apart an architecture or set of processes into manageable layers or "domains." Evaluating domains creates a manageable approach to applying security and generally ensures that no gaps exist in the architecture. Because security controls can be dependent on one another, it is important to consider all aspects of the architecture or process set, making sure that one application of security does not make another process vulnerable.

As discussed later in this report, the bulk power grid has been analyzed from a cyber security perspective. Although some issues exist throughout the entire design, this analysis focuses on power levels of 15 kV and below.

Figure 2 depicts a simplistic view of the domains identified in this effort. Each domain drills down to a more detailed view of the components. Domain 1, which is the top level of this effort, contains the distribution substation, distribution grid, transformers, distribution buses, and house tap. Domain 2 drills down at the house level and includes the transformer and devices that interface with the distribution grid. Logically, this domain considers the movement of energy to and from the house and the associated data. Domains 3 and 4 address specific devices—the meter and the inverter, respectively. This analysis includes current designs for these devices, but proposed designs and future capabilities were also considered. As these devices evolve, future assessments should include advanced capability, potential communication functions, and accessibility.

Risk assessment was performed under the context of these domains, leading to suggestions for applying security to this effort.

3.1.4 Control Systems Security Research

Under programs funded by DOE and the Department of Homeland Security (DHS), research has been conducted that addresses security in control system environments. The consequences of a cyber event to systems within the critical infrastructure have been theorized, offering insight into needed security applications in specific operational areas. This research can be leveraged, but each new energy application should be evaluated from a security perspective. An assessment early in the design phase often reduces added costs later during implementation. With evolving technologies and applications, though, it is important to continually revisit security and consider protection levels.

Previous research indicated that potential consequences can range from insignificant to major during and after a cyber event. Although total security is difficult to attain and costly, programs such as I3P are viewing survivability and recovery as part of inherent security, equally important as prevention. Although bulk power and control system issues are reflected in this analysis, a specific view of PV integration is needed to ensure that operational objectives are met without cyber security issues.

3.2 Security Model

A project conducted at Sandia National Laboratories for the DOE Office of Electricity Delivery and Energy Reliability produced the ASRM, a logical model of control systems in an operational environment.[10] The ASRM is highly detailed, but Figure 3 illustrates an adaptation. Although this model primarily considered the electric sector, it can actually be applied across control system environments such as oil, gas, and chemicals. In 2006, the model was used as a basis for applying security metrics in an operational environment under a project for the National SCADA Test Bed.[11] This effort produced guidance to assist asset owners in tailoring the model to their architecture and applying controls to needed areas to meet their security objectives.

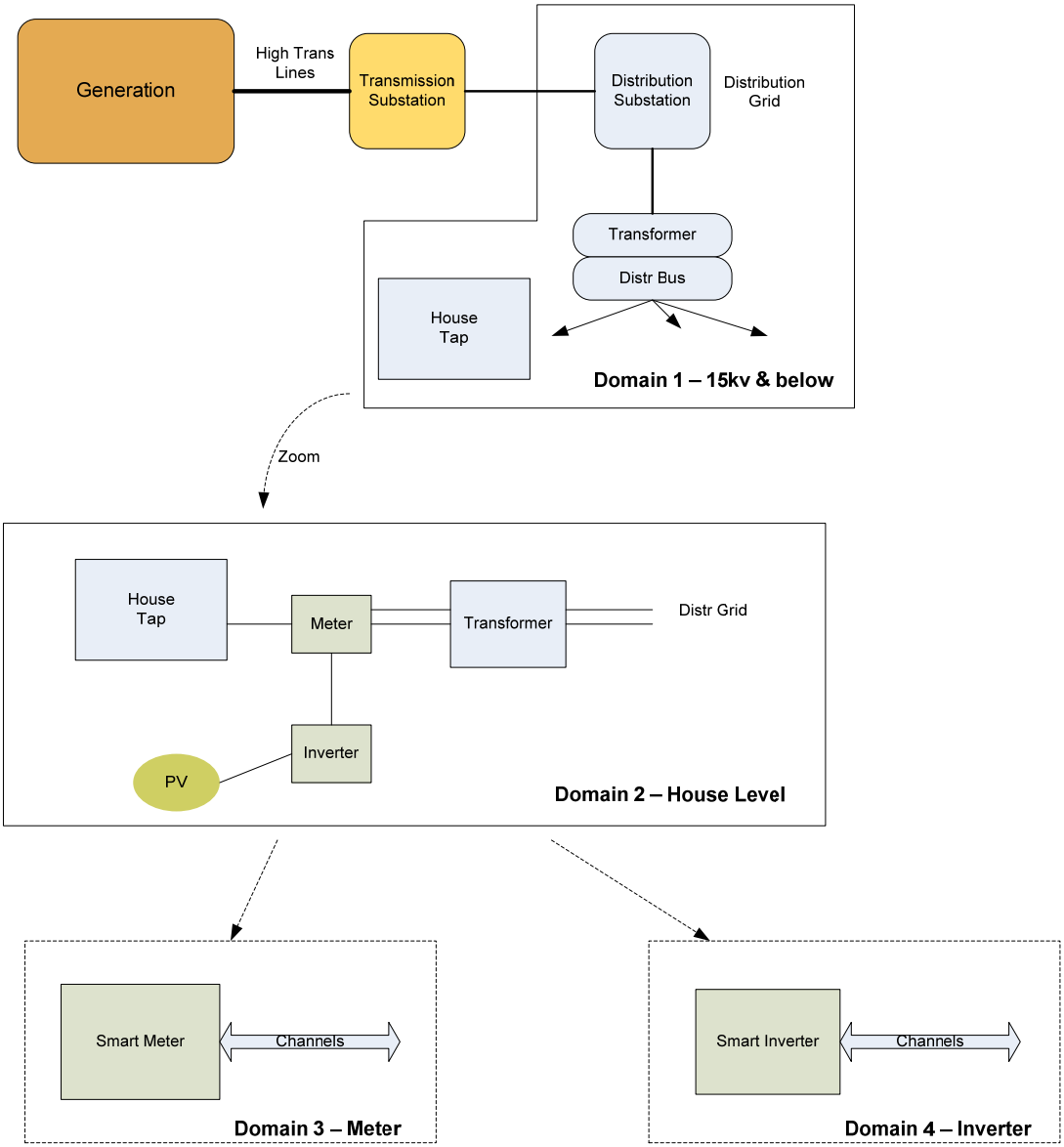


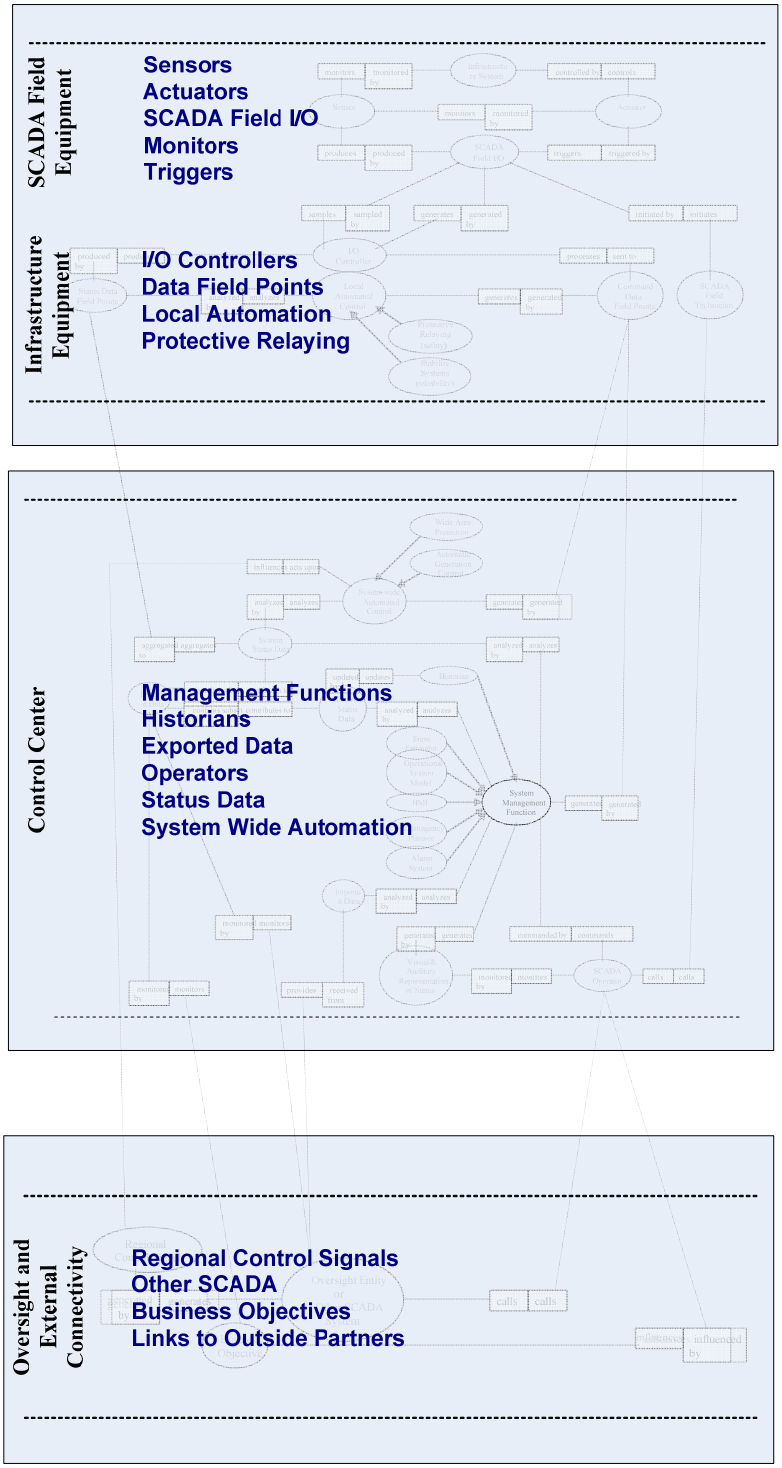
Figure 2. PV integration domains

At the utility control center and downstream, the ASRM can be used to identify areas that require security controls, such as access control and encryption. Industry guidelines exist that assist in identifying these controls. These include the North American Electric Reliability (NERC) Critical Infrastructure Protection Committee (CIPC), the National Institute of Standards and Technology (NIST) Special Publications (800 series), and the Institute of Electronics & Electrical Engineers (IEEE) standards.*

* See http://www.nerc.com/~filez/cip.html for the NERC CIP, http://csrc.nist.gov/publications/PubsSPs.html for the NIST 800 series, and http://ieeexplore.ieee.org/Xplore/dynhome.jsp for the IEEE standards.

It is important to note that although this analysis focuses on power levels of 15 kV and below, the distribution grid is a complex system. Data flow and consumption at lower levels directly relate to the larger grid and affect overall utility performance. Data movement throughout the system and back to a utility, for example, is subject to the security controls identified by standards and guidelines and applied by the utility. Security at the level of 15 kV and below means that one must fully consider security at higher levels and the ultimate destination and purpose of the data in transit.

In this study, all tiers of the ASRM were considered. For example, field and infrastructure systems are included in the distribution grid. Protection mechanisms were considered for the systems and data flow at these tiers. A control center or subset of control systems that require equal consideration can also be located within the distribution grid. Automation oversight often relates to systems that link back to business systems or billing. In the case of PV, and the sale of power to and from the grid, these systems are of particular interest. As described later in this report, the future may include centralized energy management systems (EMS) that define complex connectivity between energy control and administrative systems.



Note: I/O = input/output

Figure 3. Automation systems reference model (adapted)[10]

4.0 Preliminary Analysis

Key questions in the preliminary analysis include the following:

- What devices/components in the PV integration design should be evaluated?
- What processes in the PV integration design should be considered?
- Do vulnerabilities exist and where?
- Are there any critical points of failure?
- What is the cyber risk to the PV design?
- What are the typical threats and consequences?

These questions provided the foundation for research on potential critical cyber security issues inherent in the integration of PV. Results of this analysis are outlined in the following sections.

4.1 Description of the Issues

Integration of PV presents new challenges in both technology and operations. Effective PV integration and an increase in penetration levels will likely be reliant on the use of advanced technology. This will result in the use of components that require two-way communication, such as inverters and meters. The flow of data and control will require that potential cyber events be considered.

Likewise, a dependence on standard and off-the-shelf technologies could present security challenges. Analyzing the design and addressing any potential security concerns now will create a more cost-effective solution for the future. Manufacturers of PV components that integrate secure solutions and processes will definitely benefit the user community. Implementing those changes early in the life cycle fosters a more secure evolution, increased stability, and eventually increased penetration.

4.2 Results of Task Research

Each concept of risk, as described in the following sections, was considered in this analysis.

4.2.1 Threats

Given the global realization that cyber incidents have become a part of daily risk to both individuals and organizations, it is important to consider the entire spectrum of threat. An infrastructure in any sector should be protected from all possible threats, normal, abnormal, and malevolent. These threats range from the inexperienced malicious hacker through organized crime to large, well-planned and -funded terrorist efforts. Although the threat can be analyzed in terms of resources and in conjunction with physical threats, it is difficult to predict an event or assume with complete certainty that one is protected from each possible threat. In terms of PV integration, it is important to look at likely threats, potential motivators, and the attractiveness of the distribution grid as a target.

Likely threats to power levels of 15-kV and below include those threats that plan to use the house or neighborhood system as an entry point to the distribution grid. A threat might find

these entry points more attractive and accessible than a larger asset upstream that may have monitoring or access control. With physical and cyber controls in place at points upstream, however, it is unlikely that entering a single house could cause a large-scale incident. Several access points, such as multiple inverters in the neighborhood, may be more attractive starting points.

Details of potential consequences are outlined in upcoming sections. From this standpoint, it is important to consider a threat with physical or remote accessibility to the PV systems at the house or neighborhood level. This threat could include the curious homeowner or an individual threat performing reconnaissance to see how much control he or she could gain over the system. Although these threats do not generally have the resources or motivation to do significant harm, a poorly configured or secured system can open the door to a cyber incident.

Although it may seem unlikely that a well-funded, well-organized, and highly motivated threat would create an incident from a "shock and awe" perspective, it is still important to consider this threat from the perspective of a coordinated effort. For example, a coordinated effort might be used to produce multiple effects. Hypothetically, imagine coordinating a loss of service to strategic areas to reduce or halt communications from public media such as television and radio. This might take place to assist with a larger effort while other infrastructures are targeted. Although this simplistic example might be temporary, or easily mitigated by using a backup generator, disruptions could still occur. As a result, the potential for a coordinated attack, even if minimal, must be considered.

Whether a limited or sophisticated threat is active, the same PV components are addressed in this analysis. A detailed threat assessment should be conducted during a full vulnerability assessment of new architectures and implementations. As PV penetration evolves, standard implementations become more visible targets. Information availability on designs, especially when implemented at the house level, will increase and more data will be available to the threat. Although this cannot be stopped, vulnerabilities within components of PV can be mitigated.

4.2.2 Critical Elements and Vulnerabilities

Considering a physical perspective, domains 1, 2, 3, and 4 in Figure 2 are the primary focus of this analysis. A logical perspective includes consideration of the entire ASRM and all critical processes, along with the flow of data. Identifying the critical components requires definition of hardware, software, and processes within these views. Although focused on cyber aspects of each domain, it is important to consider physical accessibility as well. The separation between cyber and physical aspects of security is becoming increasingly less clear. The dependency between these two aspects requires the underlying consideration of physical security throughout the analysis.

It should also be noted that complex systems, such as those in electricity delivery, are evolving to facilitate optimized service. This includes delivering data to the needed recipient and fostering good decision making that leads to effective operations. This creates increased interconnectivity among systems, domains, and large-scale architectures. Interconnectivity generally creates increased risk. It is understood, however, that the trend to connect domains

will likely continue and may be necessary to achieve objectives. Therefore, the result of this analysis is not to suggest disconnection, but to mitigate risks created by connection points.

Another underlying consideration in this analysis is the use of standard interfaces and a shift toward information technology (IT)-centric solutions. A movement toward standard interfaces is similar to interconnectivity. It is likely to continue to evolve to meet overall objectives, provide a cost benefit, and promote increased penetration. Standardization, however, also generally increases the availability of system details and can contribute to making the system a more attractive and accessible target. This requires forward thinking about future designs to ensure that mitigations are in place.

The following sections describe each of the critical elements, starting at the lowest level, and their potential areas of concern.

4.2.2.1 Inverter

Common inverters in use today typically have limited functionality. Advanced or "smart" inverters have been identified, however, as necessary components of future PV design. This analysis considers elements suggested for future PV designs. The main purpose of the inverter is to convert DC to AC energy, creating usable solar energy. Future PV designs are likely to include much more functionality. This could include data generation, data movement, and communication pathways. In fact, it has been stated that

> The effects of high penetration will need additional studies and inverter/controller equipment tied to the electrical distribution systems must be in communications, have intelligence to make decisions on operations, and include energy management and possible energy storage to improve the stability of the integrated grid system.[12]

Increased intelligence and smart" devices directly offer optimization, increased availability, and better decision making.[12] Considering this move forward, cyber threats can utilize data pathways as roads into the system for exploitation. Two-way communications are a valuable piece of new inverter designs, providing data for energy management.[12]

Sensors within future inverters may generate data that are useful to both the homeowner and the utility. It may be beneficial to a threat to access and alter these data, allowing the threat to change flow, alter billing, or contribute to another coordinated event. The absence of cyber and physical access controls on the data produced by the inverter may pose a vulnerability. The ability to access a physical port on the system or to obtain access through a centralized home EMS or through open wireless protocols provides an entry for a threat. Altering the load would likely only affect the home or neighborhood. A coordinated event, though, could create service availability issues across an area. Upstream changes or larger outages are unlikely but may not be completely impossible. Mitigation includes hardened physical and cyber inverter access control and upstream validity checks of the data. Monitoring for anomalies or changes in data beyond reasonable sets helps to mitigate both short- and long-term cyber events. Altered data produced at the inverter could be used to change the load, creating instability and reliance on other controls to avoid a localized trip.

Dependency on the data from a smart inverter means that altered data could affect results at various areas within the overall distribution system. Relays that prevent damage to lines may utilize this data as well as supervisory systems and EMS at various levels. It is suggested that future homes may contain a central EMS. Altered data could affect not only existing load, but could also contribute to inaccuracies in optimization, trending, and demand. Hardware and software controls to prevent unauthorized access to data production on the inverter should be considered in future designs.

4.2.2.2 Meter

Metering is one aspect that has gained notice and evolved more rapidly. Countless studies of advanced or smart metering have been performed. Many advantages to smart meters benefit both the utility and the consumer. Smart meters are being rolled out in both the United States and in parts of Europe, including rural areas. A cyber incident involving the meter may not produce a consequence that alters energy flow. But data produced at the meter can suffer economic consequences, making it an attractive target. The ability to alter usage data at the meter and hide or change consumption and production rates could result in billing inaccuracies. For example, this could give the appearance that more energy was sold back the grid than was actually returned, or that very little energy was consumed. It is assumed that a utility would detect a large anomaly. Stealthy, moderate changes to data over a long period of time, however, could result in significant economic benefit to the threat carrying out the cyber incident.

Data produced at the meter move along standard communication pathways to administrative systems at the utility. These data are used for billing as well as aggregated in trending and usage analyses. A series of cyber events that altered meter data could have the potential to significantly modify these analyses over a period of time. Although security and safety are often the primary objectives of utility companies, economic accuracy is definitely a concern as well. Like the inverter, the smart meter must have physical and cyber access control. If a centralized EMS is employed at the house level, controls on the ability to “write: or change meter data are necessary. These controls may not require significantly new technology, but considering their structure during the design phase will definitely save costs to upgrade after implementation.

4.2.2.3 Communications

At the component level, it can be concluded that control of data is most valuable. Advanced smart components clearly rely on the ability to move data to specific destinations. It can be said, then, that the communications pathways included in the PV integration system may be the most critical and valuable pieces of the implementation.

It is first necessary to consider where communications exist within the integrated architecture. Figure 4 illustrates one example of logical communications within an architecture.

It can be assumed that smart components might use two-way communications in the following functions:

- Energy production and usage data moving to and from the inverter
- Energy usage data moving from the meter.

Data can move to various places, including an EMS that could be off site or in house. The EMS would interface with smart appliances and then travel off site. The data can also move to the utility for load adjustment. This could occur at a control center, an intelligent relay at a substation, or onto a system or historian for trending analysis. Data can also move directly to the utility for billing and trending analysis, which normally occurs on the utility's administrative network.

Data movement presents challenges. One benefit to the two-way communications design is the interactive capability. Moving data directly to where a utility requires the information, when the utility requires it, creates more effective and stable operations. Increased interactive capability, though, also presents an increased number of access points and a greater opportunity for altered data. Senate Bill S.1115 suggests secure, dependable communications, and the smart grid will rely on these communications to perform critical functions.[12] Communication protocols and mechanisms that have been suggested as possible standards include[12]

- Protocols:
    - BACnet
    - TheLonTalk
- Mechanisms:
    - TCP/IP Ethernet
    - Wireless such as Bluetooth and WiFi
    - BPL/Broadband over power line

These protocols and mechanisms are currently in use in some architectures. Standard protocols and mechanisms are required for increased interoperability and ease of implementation, but often create easier, more visible targets. The use of TCP/IP in two-way communications for PV integration, for example, opens the architecture to many existing TCP/IP vulnerabilities. Generally, the longer a mechanism or protocol is in use, the more available configuration and implementation details become across Web sites and within documentation. If security is not evolving at that same rate of availability, the standard becomes vulnerable. An inevitable shift toward commercial IT products may also be likely, posing inherent risks by potentially introducing common vulnerabilities. Physical and cyber access control on ports, routers, and other networking equipment that facilitate communications is important and must be considered throughout the life cycle.

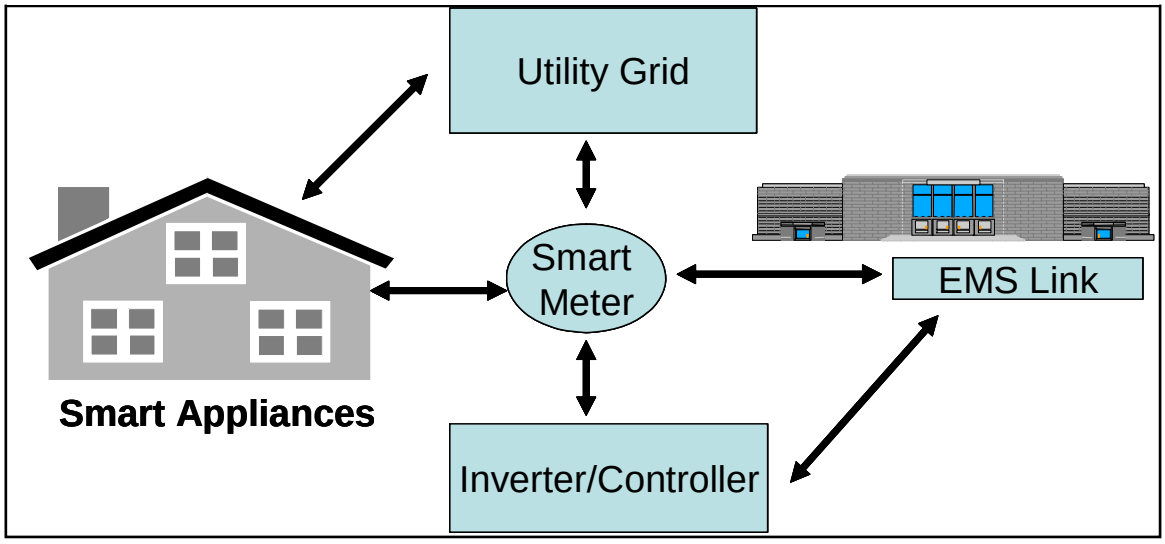


Figure 4. Smart components and logical communications[12]

Once data are in transit, the information is subject to the same risks that standard mechanisms present across a large physical area. In addition to access control, an encryption mechanism may be useful in protecting the integrity of the data in transit. Likewise, signature mechanisms to ensure the authentication of the data produced may be useful. This would also assist in preventing data alteration resulting from a "man-in-the-middle" attack, which is certainly possible when utilizing a standard mechanism such as a TCP/IP network. Data moving to control centers, administrative systems, or historians should be protected at those locations as well. These sites have been analyzed in other control system research projects and the results apply across sectors.

The value of transit, sensor, load, or billing data should be protected at levels according to the priorities and values assigned by the utility. Monitoring and validity checks on the data assist in determining whether data have been altered significantly. This, as well as signed or authenticated data, can double as a static intrusion detection system that alerts the utility to an event that produced altered data.

As in all control system and operational environments, standard IT protective mechanisms are not easily applied. Virus protection software, off-the-shelf access controls, and real-time intrusion detection and prevention systems are not readily available or easily implemented. Unfortunately, increased PV penetration will likely increase motivations by threats that seek to exploit any existing vulnerabilities. In many instances, protocols and communication mechanisms are leased by utilities from commercial entities. Utilities may not have sufficient control over implementation of security controls within the communication backbone. If a utility has the option to own and manage its own communication infrastructure, though, it has complete control of security.

There are still many positive reasons to include a communications layer in PV architectures, such as, for example, stability and reliability of the grid. Communications provide[13]

- Monitoring capability
- Demand management and automated decisions
- Advanced metering
- Coordinated control
- Distributed generation, integration, and storage
- Real-time analysis
- Pricing controls
- Protective mechanisms.

As the trend of utilizing two-way communications continues, standardized IT functionality may become increasingly present in PV architectures. This could include interfaces with smart appliances and home-level management and monitoring systems. As the industry considers standard implementations to facilitate these functions, security must also be taken into account in the design to mitigate emerging risks. Overall reliability and efficiency can clearly be increased by using two-way communications. A recommended model for approaching security in operational layers, however, would be beneficial to ensure that mitigations are applied accordingly and that potential consequences are contained. Standard approaches such as the IEEE guidelines represent the future; currently, utilities are using disparate configurations to meet data requirements.[14] Increased communications facilitate added functionality and can increase survivability during a cyber incident through situational awareness and response. Overall operational objectives can be met securely by achieving a balance between security and functionality.

4.2.2.4 Upstream Distribution Substations

When evaluating a design of 15 kV and below, security at the distribution substation level should also be considered. Any control system, EMS, digital sensor, or data aggregation point at a substation should be protected using applicable security mechanisms. These mechanisms should include a combination of physical and cyber access controls. A layered approach to securing the perimeter and then protecting systems with cyber access control will prevent tampering, data alteration, and service disruptions resulting from cyber-based effects. Disruptions caused by physical damage are extremely difficult to prevent over widespread geographic areas. Mitigating data loss in those instances requires redundancies at data storage and aggregation points, such as backup systems and archives. Substations provide a location for those systems, but protective mechanisms are needed to ensure that access is controlled, data integrity is maintained, and monitoring is in place to detect intrusion. Conventional data management systems and networking equipment at these locations may be sufficiently protected with standard IT controls. Operationally focused security mechanisms can assist in protecting control systems at these locations. Such security mechanisms are being identified by industry forums and research projects and are becoming increasingly available in the form of guidelines and recommendations for control system environments.

4.2.3 Potential Consequences

As mentioned in the previous sections, potential consequences can be derived from scenarios developed by investigating possible designs. One scenario, altered data at the inverter, could affect load balancing and faulting, which could disrupt service on a localized level, such as a neighborhood or a microgrid service area. Local hardware damage is also possible. Large, cascading failures are unlikely, but cannot be completely disregarded. Coordinated localized outages could result in widespread effects, especially if carried out by a well-motivated threat that places emphasis on interdependent infrastructures. Altered data at the meter results in billing and trending inaccuracies. Although this may have little effect on delivery, over time, the utility could experience financial consequences. Communication backbones provide added functionality and stability to the grid. These lines of communication facilitate the following benefits to the consumer and the utility:

- Service stability and reliability
- Improved delivery
- Accurate usage measurement and prediction
- Distributed generation
- Accurate pricing.

Protective mechanisms at each layer are necessary to ensure that data integrity is preserved and data flow is maintained. An approach to security should include mechanisms that address the following aspects:

- **Prevention** entails hardening the systems and process structure to make sure defenses are in place to maintain proper function. Redundant architectures should be employed to facilitate operations.
- **Awareness and reaction** includes the ability to detect a cyber anomaly that results in an impact. This includes information management that supports decision making during a cyber event and fosters reactions that end the event with minimal impact.
- **Recovery** means that when or if a cyber event occurs, a structure is in place that supports redundant capability or backup data, mitigating the lasting effects of the event.

Hardware, software, and design solutions can serve as protective mechanisms, ensuring that these steps are accomplished. Digital data, the primary subject of protection, must be controlled to make sure that energy generation, distribution, and consumption are maintained at necessary levels. Data integrity, authentication, and encryption technologies can be used to protect these data during production and transport.

A complete denial of service to an area can be accomplished by inflicting physical damage to areas of the distribution grid. A common assumption is that this event is more likely and easier to carry out than a cyber event. Although that conclusion may be true in some cases, specific objectives may prompt a cyber-focused event launched by a threat with a specific intent. The stealth capabilities of a cyber event often foster long-lasting effects, and if detected, require time and resources by the utility to troubleshoot. Without monitoring and

detection in place, cyber events may go unnoticed for long time periods, allowing a threat to carry out more reconnaissance and produce targeted, lasting consequences.

Distributed architecture and increased functionality also create the possibility of unintentional consequences. Curious homeowners or operator errors at the component level can also produce negative consequences. Hardware- and software-based access controls, in addition to well-configured house-level EMS, can prevent accidental disruption and physical damage.

To ensure that the overarching objectives of PV integration are met, protocols, data transport mechanisms, and overall implementation activities must be standardized. Because standard implementations often create more visible targets, security should be applied at each significant area of the architecture and accompanying security guidelines are recommended.

A first step toward identifying and mitigating vulnerabilities, thereby reducing consequences, is an assessment of the architecture. “Red teaming” is an assessment process that can be customized and performed on an architecture at various levels of maturity. A red team assessment or a risk assessment can be a paper-based or hands-on evaluation that identifies and analyzes critical processes, access points, potential failure points, and possible vulnerabilities. An example of red teaming in the design phase can be reviewed at http://www.idart.sandia.gov, which illustrates how even notional architectures can be assessed.

5.0 Recommendations for Future Research

Considering cyber security and potential consequences early in the design life cycle is more cost effective and generally offers more comprehensive protective mechanisms than “bolt-on” solutions addressing systems that have already been implemented. As standard designs and implementations evolve, specific areas that can represent critical points of failure or significant vulnerabilities should be evaluated from a security perspective. Based on the objectives of distributed functionality and interconnected systems, each valuable component of the system should be evaluated, along with the communication pathways. System components can include

- Standard protocols and mechanisms (such as broadband over power line), any associated vulnerabilities, existing threats, and potential mitigations
- Advanced metering designs
- Advanced inverter designs
- Evolving EMS
- Digital sensors
- Secure wireless for reliability

Evaluating designs from an access control perspective is recommended. Protecting access to the component’s configuration as well as the data it produces is paramount. Cost analyses of advanced components for security can also be helpful. A balance between implementation and security can be found, especially if evaluated early in the life cycle. A review of both the ramifications and benefits of standard implementations is suggested. An accompanying set of security guidelines and desired protective mechanisms during implementation assists in mitigating risks.

Finally, continued review of consequences associated with increased penetration is recommended. A specific example is the potential for any coordinated events that may create a cascading failure. This requires a review of interdependent infrastructures and potential threat scenarios.

6.0 Conclusions

Increased PV penetration and distribution capabilities can enhance grid stability. Distribution fosters evolving ways to manage energy from generation through distribution to consumption. Advanced designs of critical components facilitate the capabilities of new energy management methods. These smart components utilize digital controls and communication pathways to supply data to specific locations within the architecture. Movement and management of these data affects load balancing and fault tolerance, as well as administrative functions such as billing. The distributed architecture and cyber capabilities create potential vulnerable access points. Data generated at inverters and meters must be authentic and protected during generation and transit. Standardized implementations and common communication protocols are necessary to increase PV penetration and ensure stability. Standard implementations, however, create attractive targets and must be protected through security controls. A blend of physical and cyber access controls, monitoring, intrusion prevention, encryption, and signature technologies can help mitigate the risks of altered data. Data alteration could have consequences for load, hardware, and administrative information. Even though widespread denial of service as a result of exploiting a single component is unlikely, coordinated cyber events should be considered, including other interdependent infrastructures.

Information technology security has evolved extensively, but readily available security technologies are not easily applied in operational or control system environments. As components and critical processes evolve in future architectures, a risk assessment that includes a review of threat, vulnerabilities, and potential consequences is recommended. Implementing security controls as the system designs evolve easier and more cost effective than retrofitting existing designs.

Given the importance of the distribution grid and our national critical infrastructure, security should be considered as all new energy systems adapt to provide new capabilities. A balance between generation and distribution objectives and secure operations can be met by applying security controls at critical points within the architecture. These controls will facilitate continued service and stability. Risks can be mitigated by employing security controls that promote operations and present minimal impacts to overall architecture cost and development objectives.

7.0 References

1. Chowdhury, B.H. “Optimizing the Integration of Photovoltaic Systems with Electric Utilities.” *IEEE Transactions on Energy Convergence*; Vol. 7, No. 1, March 1992.

2. Chowdhury, B.H. “Effect of Central Station Photovoltaic Plants on Power System Security.” *Proceedings of the 21st IEEE Photovoltaic Specialist Conference.* Kissimmee, FL, May 1990.

3. Hightower, A. “2006 Student Research Projects, Photovoltaic Security.” *Occidental College Renewable Energy Education Fund 2006 Annual Report.* Los Angeles, CA: Occidental College, March 2007.

4. “Information Security.” *Dictionary of Military and Associated Terms.* 2005. U.S. Department of Defense. http://www.thefreedictionary.com/information+security. Accessed August 29, 2007.

5. “Information Assurance.” *Dictionary of Military and Associated Terms.* 2005. U.S. Department of Defense. http://www.thefreedictionary.com/information+assurance. Accessed August 29, 2007.

6. McIntyre, A.; Stamp, J.; Cook, B.K. *I3P Risk Characterization Report.* Research Report No. 9. Hanover, NH: Institute for Infrastructure Information Protection (I3P), May 2007. http://www.thei3p.org/repository/researchrepo9.pdf.

7. McIntyre, A.; Stamp, J.; Cook, B.K.; Lanzone, A. “Workshops Identify Threats to Process Control Systems.” *Oil and Gas Journal*; Vol. 104, Issue 38, October 9, 2006; pg. 44-50.

8. Duggan, D.; Thomas, S.; Veitch, C.; Woodard, L. *Categorizing Threat: Building and Using a Generic Threat Matrix.* SAND2007-5791. Albuquerque, NM: Sandia National Laboratories, September 2007.

9. Stamp, J. “Drivers and Concerns for SCADA Security.” Presented at the I3P 2005 Workshop. Houston, TX, June 2, 2005.

10. Stamp, J.; Berg, M.; Baca, M. *Reference Model for Control and Automation Systems in Electric Power.* SAND2005-6286P. Albuquerque, NM: Sandia National Laboratories, November 2005.

11. McIntyre, A.; Becker, B.; Halbgewachs, R.; Tejani, B. “Security Metrics Taxonomy for Control Systems.” Presented at the Process Control Systems Forum (PCSF) 2007 Annual Meeting. Atlanta, GA, March 6-8, 2007.

12. U.S. Department of Energy (DOE), Office of Energy Efficiency and Renewable Energy. *Advanced Integrated Inverters/Controller and Energy Management Systems Program.* Washington, DC: DOE, July 2007.

13. McGranaghan, M.; Ortmeyer, T.; Key, T.; Barker, P.; Smith, J.; Crudele, D.; Roth, T. "Study Area 1: Grid Issues and Research Needs." Presented at the RSI Status Meeting, Washington, DC, July 26, 2007.

14. "Power System Communications Committee (PSCC)." IEEE Power Engineering Society. http://www.ewh.ieee.org/soc/pes/pscc/index.html. Accessed September 2007.

Distribution

1	MS1104	Margie Tatro, 6200
1	MS1104	Rush Robinett, 6330
1	MS1033	Charlie Hanley, 6335
1	MS1110	Jeff Nelson, 6337
1	MS1124	Jose Zayas, 6333
1	MS1108	Juan Torres, 6332
1	MS1033	Doug Blankenship, 6331
1	MS0734	Ellen Stechel, 6338
1	MS1108	Jason Stamp, 6332
1	MS1108	David Wilson, 6332
1	MS1108	Jaci Hernandez, 6332
1	MS1108	Michael Baca, 6332
1	MS0455	Shannon Spires, 6332
1	MS1108	Steven Goldsmith, 6332
1	MS1108	Jeff Carlson, 6332
1	MS 0899	Technical Library, 9536 (electronic copy)