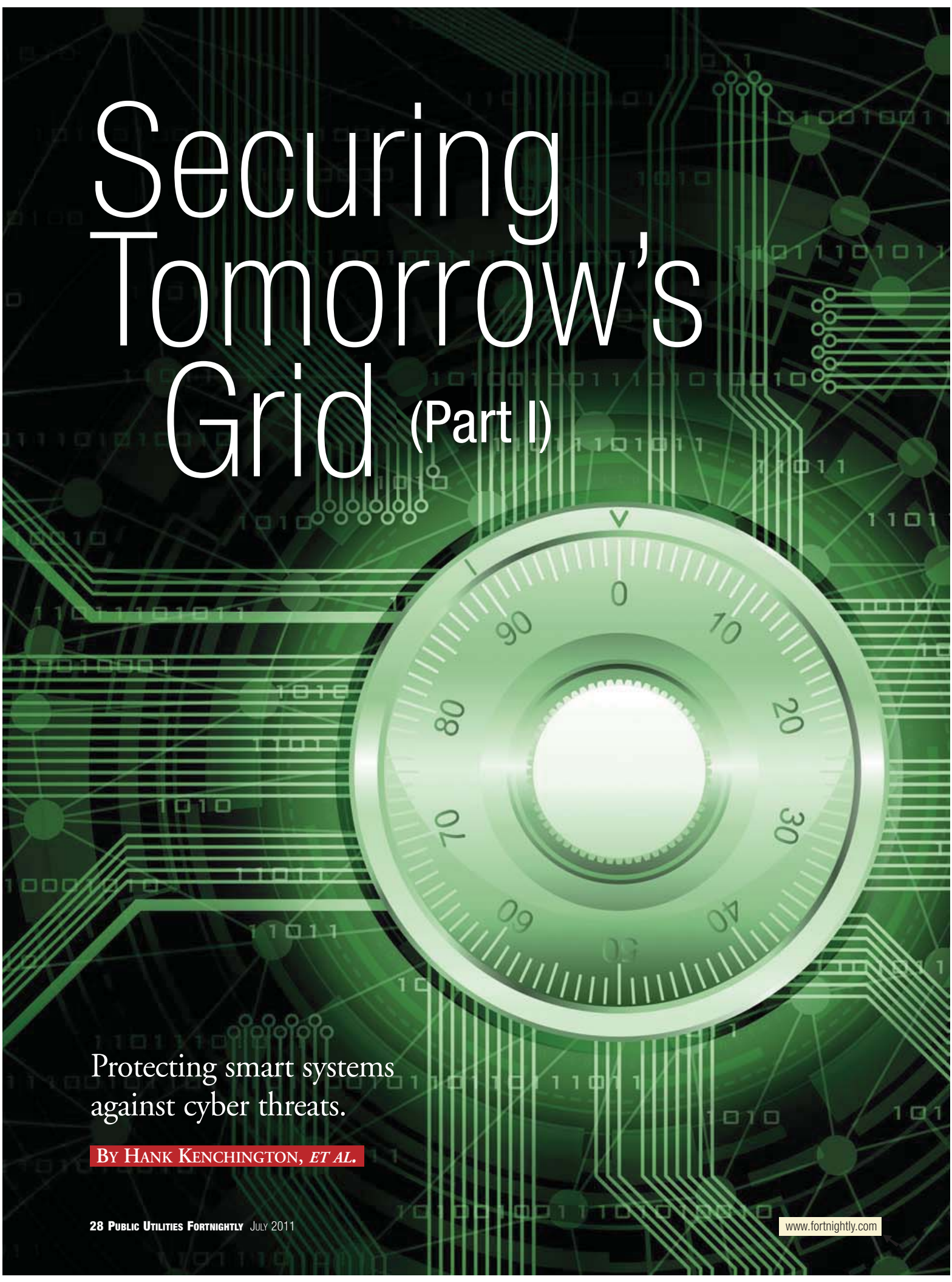
Securing Tomorrow's Grid (Part I)



Protecting smart systems against cyber threats.

By Hank Kenchington, *et al.*

The electric sector has steadily expanded the use of electronic controls and automation technologies during recent decades. But the widespread implementation of smart grid technologies will mark a notable shift in the U.S. electric grid, changing the way it operates, communicates, and ultimately delivers power. Millions of digital devices interconnected through complex public and private communication networks will collect a large amount of data to better understand the behavior of the power grid, enable greater automation to reduce system outages, improve system efficiency and resilience, and provide information for customers to better manage their electricity use. But these benefits will also be accompanied by a host of new cyber security challenges. Of the seven smart grid domains—as defined by the National Institute of Standards & Technology (NIST)[1] (*See Figure 1*)—the transmission, distribution, and customer realms will see the greatest changes.

Smart grid technologies enable utilities to operate complex systems that collect data from hundreds of advanced sensors throughout the transmission system and from thousands more sensors throughout the distribution system. Utilities will gather and distribute data across jurisdictional and organizational boundaries to communicate with third-party service providers, other energy providers, distributed renewable energy devices, and customer systems. The smart grid will change power T&D system operations by making operational data available in greater quantities with higher quality, and by using this data to improve and further automate grid operations. These changes will give operators more visibility into the real-time behavior of the electric grid, but they will also increase the importance of protecting the availability and integrity of system data, since access to this detailed operational data can be valuable to hackers interested in monitoring the grid or spoofing system data to induce instability. More frequent and detailed information will allow operators to operate the grid more efficiently and closer to limits, but also creates a corresponding reduction in margin for error, and therefore an increased dependence on data security.

Historically, distribution systems passed limited information from the utility to the customer—high-level pricing and usage data in each monthly bill—and little to no information was passed in the other direction, from the customer back to the utility. The smart grid will use two-way communications systems to provide more extensive and detailed information in both directions.

Utilities must not allow smart grid technologies to be used as a conduit for attacks—or to amplify their effects.

With a smart grid, residential, commercial, building and industrial customers each have an energy services interface (ESI) that communicates upstream to the utility through the advanced metering infrastructure (AMI) or through the Internet using customer-selected third-party service providers. The two-way flow of information allows utilities, customers and even third-party service providers to actively participate in energy markets. For example, dynamic price signals sent to customers' smart meters through a utility's advanced metering infrastructure (AMI) will empower electricity consumers to better manage their electricity use or even approve utility-initiated changes to energy usage, often in return for a better electric rate. In turn, this information exchange will help the utility hold costs down by extending the life of its transmission infrastructure and reducing the use of inefficient peak generation capacity.

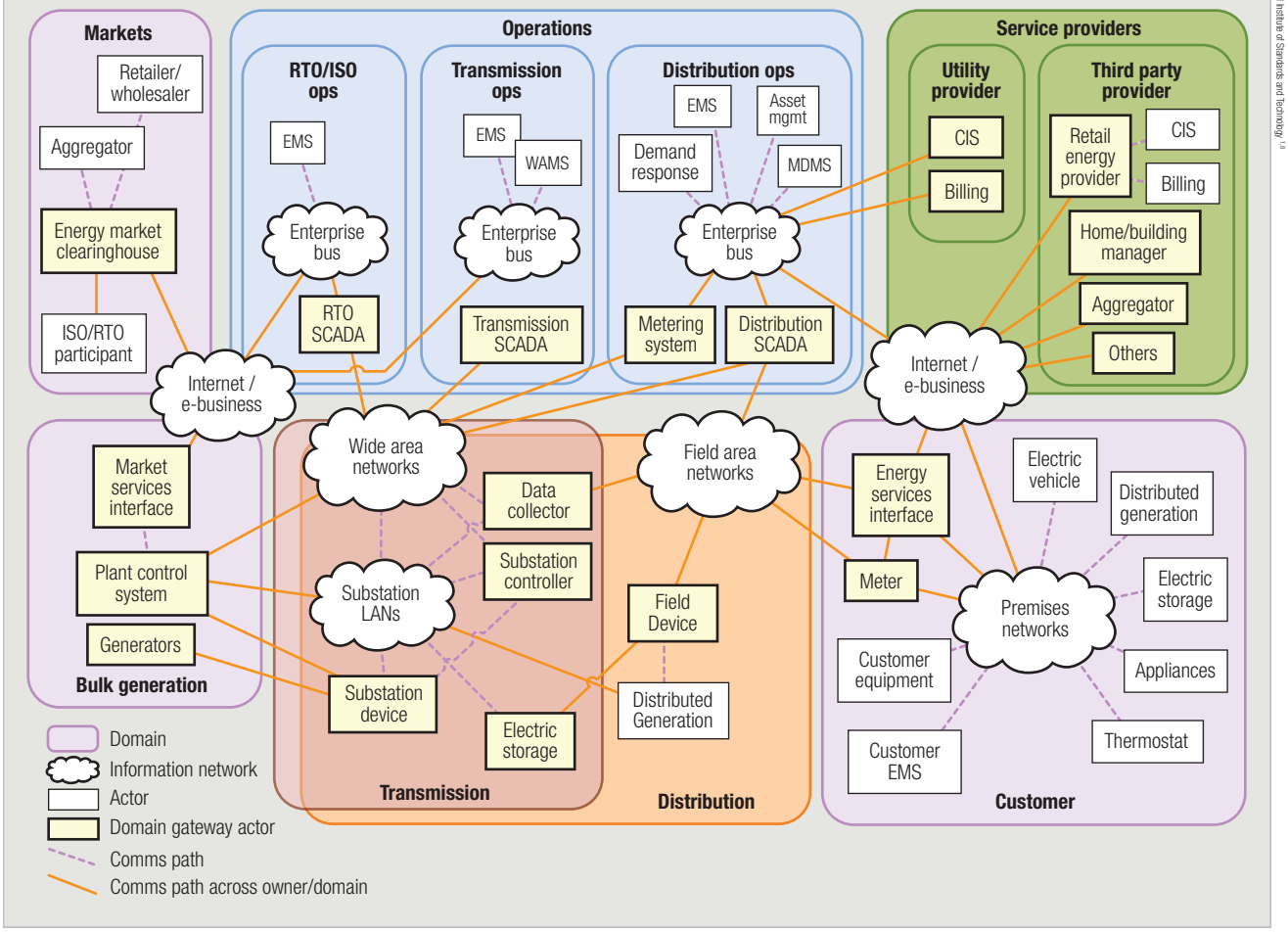
However, this detailed, two-way information exchange presents new cyber security challenges to protect data security and customer privacy. Cyber security protections are needed not only to ensure the privacy of detailed customer data, but also to protect against malicious load manipulation that could lead to a disruption in the delivery of electricity.

Today, collaborations of utilities, vendors, academic institutions, national laboratories and government representatives are actively working to systematically address smart grid cyber security issues and provide actionable information and best practices to those designing, manufacturing, and implementing smart grid technologies and architectures.

Henry S. (Hank) Kenchington is deputy assistant secretary at the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability. **Carol Hawk** is a program manager in the office. **Darren R. Highfill** is founder of UtiliSec, an independent utility security consultancy. **Jack Eisenhauer** is president and CEO of consulting firm Nexight Group LLC, and **Lindsay Kishter** is a communications specialist with the firm.

This is the first of a two-part article edited from the authors' report, Cyber Security for the Smart Grid, scheduled for publication on Fortnightly.com (www.fortnightly.com/whitepapers.cfm). The second part will be published in *Fortnightly's* August 2011 issue.

Fig. 1 **High-Level Smart Grid Domains**



Source: National Institute of Standards and Technology [18]

Smart Security Goals

The electricity industry needs cyber security solutions and smart grid security implementations that achieve the following objectives:[2]

- Protect all smart grid services from malicious attack and unintended adverse cyber and physical events that interrupt critical functions.
- Protect the electrical system, the people that work on it, and the people that are served by it, as well as stakeholders and their own services and assets—including networks and other technology—from harm caused by security events associated with smart grid services.
- Don't allow smart grid services, networks, or technologies to be used as a stepping stone or conduit for attacks—or to amplify the effects of attacks—on other smart grid services, end users, external service providers (*e.g.*, cell phone networks, ISPs), or other interconnected entities. The same should be true for natural disasters and human error.
- Ensure that sufficient information about a security event is available when and where it's needed to support tactical decisions, such as preventing or minimizing disruption to the mission of the affected smart grid service. This includes the collection and delivery of the real-time data needed for situational awareness as well as the collection and protection of forensics data needed for post-mortem analysis.
- Ensure the integrity and availability of services and mechanisms required for system security and survivability. System security mechanisms shouldn't provide an attack vector themselves, nor should they incorrectly respond to either malicious or benign commands in a manner that would create or worsen a security event.

As smart grid technologies are being deployed, the electric sector is collaboratively developing and demonstrating various cyber security solutions. Current case study examples illustrate how cyber security solutions are being applied in the T&D and customer domains. Specifically, home area networks help customers better understand and control their energy usage. Cyber security controls must restrict unwanted access to customers' information and protect their privacy. Synchrophasor technology, including phasor measurement units (PMU) integrated with real-time software applications, provides high-quality, system-wide visibility for grid operators. Cyber security measures

Fig. 2 **Home Area Network Vulnerabilities**

Threat	Potential Impact
Attacker compromises one HAN (local)	Inadequate protection of cryptographic material and inadequate network security design result in attacker gaining access to the meter or AMI network.
Attacker compromises multiple HANs (remote, neighborhood scale)	(All of the above, plus…)
	Visibility (*i.e.*, surveillance) of energy usage betrays sensitive information about others' behavior.
	Manipulation of pricing signals causes undesired behavior in smart energy devices.
Attacker compromises multiple HANs (remote, regional, or greater scale)	(All of the above, plus…)
	Manipulation of pricing signals causes undesired load ramping.
	Simultaneous operation of load control causes grid instability.

Source: Authors' analysis

are needed to ensure grid operators can depend on the integrity and accuracy of PMU readings as well as ensure the timely delivery of operator control signals. Finally, AMI facilitates the exchange of information between the utility and its customers. Cyber security measures are needed to protect against undesired access through this new utility-customer interface.

Customer Domain: Home Area Network

The home area network (HAN) includes a home's intelligent appliances—those that can connect to and communicate with the utility—along with any local generation, storage, and communication devices that better enable customers to understand and control their energy usage. Intelligent appliances typically include large energy devices such as air conditioners and refrigerators with built-in digital devices designed for two-way communication with the electric service provider through the HAN. That communication enables the utility or another value-added third-party service provider to measure the appliance's usage data and communicate it back to the customer—often through an Internet- or interactive TV-based energy management system (EMS), or even a programmable communicating thermostat (PCT). An advanced meter that has a HAN interface can also communicate pricing data back to the consumer in real time, allowing the consumer (or the networked appliance) to choose to use energy when its cost is low rather than at peak. The HAN might also enable the utility, with customer approval, to temporarily reduce a customer's power consumption during periods of peak load regardless of price in order to avoid overloading transmission systems operating near capacity.

The HAN also connects distributed energy resources (DER), such as household-scale generators or energy storage devices, and could enable those devices to coordinate with the utility to control generation, storage, and distribution of energy back onto the grid for re-sale or intentional islanding. As the market develops, the HAN will also enable plug-in electric vehicles to re-charge at the home and might even bring a host of other functions that stem from its potential to serve as a mobile DER.

Leading HAN communication technologies include: Zigbee (a wireless mesh topology); Homeplug (which carries information over the actual power line or electric wires in a house); and wi-fi (the same technology used in laptop computers and other devices for wireless Internet). With two-way communication capabilities, smart meters and intelligent appliances become access points to the smart grid network. These devices lie outside of the service provider's physical control, leaving hobbyist hackers free to purchase, then disassemble, and attempt to reverse-engineer or re-engineer them in an effort to access the meter or utility network. To manage the security of these components cost effectively, smart meters and other smart devices must be remotely upgradeable—but pushing out firmware updates over the wire or over the air means these devices must be capable of authenticating and authorizing changes from the utility, while rejecting malicious traffic from hackers or viruses. This level of processing, interaction, and updating can be a challenge for these devices, many of which are highly resource constrained and are expected to perform for many years without significant upgrades, unlike such consumer electronics as personal computers. Plus the broadcast range of neighboring HANs might overlap, making it difficult to bind electronic devices to a specific customer. The potential for neighbors to see or control each other's smart energy devices must be prevented by appropriate cyber security measures.

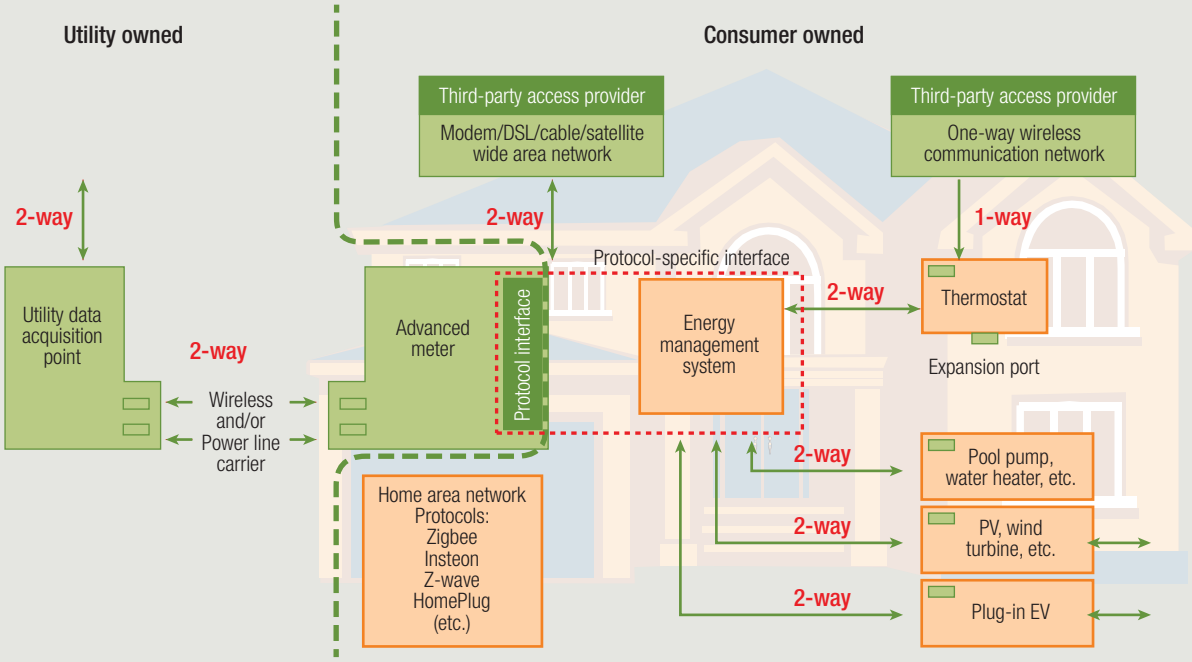
The low threshold to maliciously attack home area networks encourages the nuisance hacker.

The low equipment and investment threshold required to maliciously access HANs encourages the nuisance hacker—looking for fame, entertainment, or merely a challenge—to attempt to observe or manipulate a network. Figure 2 outlines the potential impacts of a successful hack attempt.

Securing the Home Network

By applying best practices for cyber security, utilities and other companies in the electricity industry can protect against many

Fig. 3 **General HAN Communication Architecture**



Source: Electric Power Research Institute (with slight author modification)

current attack vectors. At present these mitigations aren't uniformly adopted, or in some cases not adopted at all, often because of cost or resource constraints associated with incorporating them into the technology or network:

- Validate that all HAN input data is within expected numeric ranges, character sets, and field lengths at the earliest possible point in the communications chain, such as HAN gateways and AMI meters.
- Drop all communications that don't conform to behavior as specified in the UCAIug HAN System Requirement Specification v2.0.[3]
- Require that all remote access requests to a HAN device (*i.e.*, from outside the home) be authenticated against a list of homeowner-approved service providers and validated against a list of homeowner-approved access and actions for explicitly defined data.
- Audit all remote access requests that come through the energy service interface.
- Require all service providers offering energy pricing information or load control commands to register with the state public service commission (PSC).
- Require independent security review by a PSC-approved entity of all service provider methods for presentation of energy pricing information or load control commands.

A complete list of recommendations appears in the UCAIug HAN System Requirement Specification v2.0.

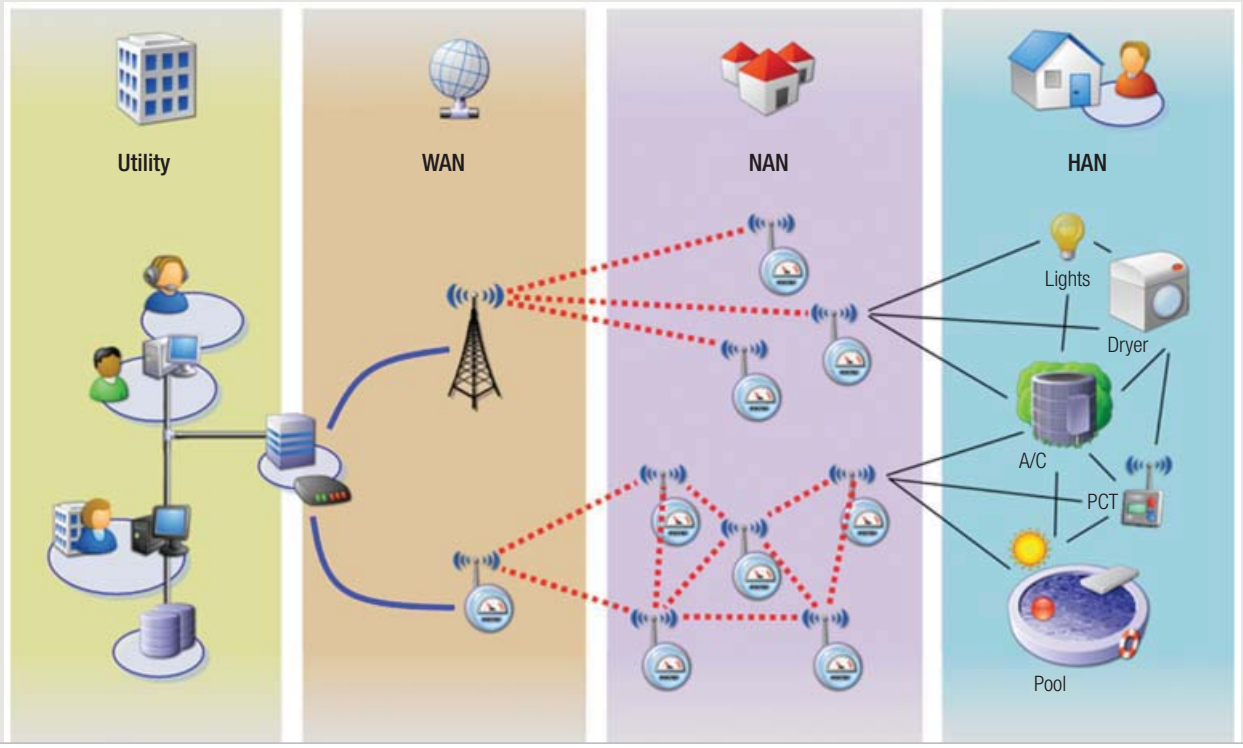
Utilities providing an interface from the AMI into the HAN must consider system architectural issues, such as who owns what device and where specific communication protocols are used. As Figure 3 illustrates, the ownership boundary for the utility includes the advanced meter and the interface to the customer-owned EMS. In this example, the EMS serves as a proxy for the smart energy devices in the home. The utility might choose to limit the depth of interactions to the EMS and delegate responsibility for secure communications with endpoints, or it might choose to require a secure channel all the way to the endpoints as might be the case for functions like direct load control. Additionally, third-party service providers might interact with devices in the HAN, creating the need for clear delineation of homeowner choices with respect to binding of device behavior to pricing and control signals.

Distribution Domain: Metering

The distribution-level AMI provides for advanced bi-directional communications between the home and the utility that enable many of the smart grid's flagship capabilities, such as remote meter reading, demand response programs, and load control. This infrastructure includes an advanced meter that facilitates two-way communication with the utility, but might also interface with the customer's HAN. Meters communicate with the utility by sending data to an aggregation point through a field-area network (FAN), also sometimes called a neighborhood-area network (NAN). The aggregation point then collects information from multiple meters in a region and sends it across the utility's wide-area network (WAN) to the utility's back office systems. There, a front-end processor (FEP), usually called a "head end," assembles the data, resolves addressing, and secures or validates the information using encryption or decryp-

Fig. 4 **AMI Topology: Mesh and Star**

AMI = Advanced metering infrastructure; WAN = Wide area network; NAN = Neighborhood area network; HAN = Home area network; PCT = Programmable communicating thermostat.



tion respectively. The FEP sends the raw information to a data store—the utility's meter data management system (MDMS)—which processes raw data, parses energy usage and other relevant data, associates the information with a utility customer, and makes the information available for other utility applications such as billing, customer information, outage management, and distribution management.

The AMI communications network can use a variety of technologies and both proprietary and standardized communications protocols. The FAN—which operates between the individual meters and the data aggregation point—currently uses predominantly proprietary communications technologies, although standardization efforts are under way. Three primary network topologies are used for the FAN; the most common in the United States is a wireless mesh network. Mesh networks (*see Figure 4*) use radio nodes embedded within meters that can each act as an end-point or serve to relay or route information to other points in the network. They are usually self-organizing and can sometimes offer redundant communication paths depending on implementation and deployment. Other topologies include a tower network—sometimes called a star network, in which a physical tower or high-mount antenna communicates directly with end-points—and power line, which carries information across power lines by modulating the AC waveform. Power line topologies in particular can be effective at combatting radio frequency (RF) interference in densely populated areas, but can also require expensive equipment to carry the information long distances or across transformers.

Once meter data reaches the aggregation point through one of these FAN topologies, aggregated data from hundreds of meters travels to the utility over the WAN, which typically uses standardized wide-area communication technologies such as cellular, fiber, or microwave—sometimes from a third-party service provider and potentially shared with other non-utility infrastructure networks.

As with traditional metering, AMI places smart meters in public areas where they are vulnerable to physical tampering. Smart meters, capable of accessing utility networks, are installed on customer property and offer limited physical protections—the hobbyist hacker may have direct access in their own home. Because meters are produced, shipped, and installed in great quantities, numerous opportunities exist for an interested adversary to obtain a functional meter for analysis. If the meter has a wireless interface, the FAN with which it communicates will be visible to anyone with an adequate antenna and wireless network application; many networks might even be visible to off-the-shelf laptops with wireless LAN cards. Additionally, advanced wireless communications analysis tools are widely available for a nominal investment. The proprietary communi-

FIG. 5 METERING VULNERABILITIES

Threat	Potential Impact
Attacker compromises one meter (local)	Compromised usage measurement results in loss of revenue.
	Inadequate protection of cryptographic material and inadequate network security design result in attacker gaining access to multiple meters and/or the aggregation point.
	Improper operation of disconnect switch causes property damage, personal injury, or death.
Attacker compromises multiple meters (remote)	(All of the above, plus…)
	Visibility (*i.e.*, surveillance) of energy usage betrays sensitive information about others' behavior.
	Manipulation of pricing signals causes undesired behavior in smart energy devices.
	Remote operation of disconnect switches causes a localized outage.
Attacker compromises multiple aggregation points	(All of the above, plus …)
	Manipulation of pricing signals causes undesired load ramping.
	Remote operation of disconnect switches causes widespread outage and grid instability.
Attacker compromises head end or MDMS	(All of the above, plus …)
	Potential access to other utility operational or business systems.

Source: Authors' analysis

cation networks used in FANs are also difficult to evaluate and prove secure; many early technologies and protocols had insufficient security and were easily hacked, while others today still haven't received substantial scrutiny.

Compromising AMI networks is attractive to a host of attackers: from hobbyist hackers with similar motivations to those mentioned for the HAN; to homeowners attempting to control their energy bill; and more ominously to malicious actors intending to create fear or distrust of the technology, or to extort money.

Secure Metering

Ensuring meter security over the equipment's long deployment life (10 to 20 years) becomes increasingly difficult as vulnerabilities grow over time with hacker capabilities. In particular, mesh networks are targeted by hackers because this architecture, if not properly secured, is inherently susceptible to worm-style (*i.e.*, self-propagating) attacks. Residential meters tend to be highly resource-constrained, with low processing power and small amounts of memory that make firmware updates challenging. Pushing firmware updates out over the wire or the air also presents bandwidth challenges due to the large number of devices, and challenges in ensuring that the meter only authenticates and authorizes changes from the utility.

Figure 5 summarizes potential impacts of a successful cyber attack against metering systems. The following mitigation practices would address many known attack vectors.

- Remote status and alarm for meter tamper-detection mechanisms.
- Cryptographic hardware modules such as trusted platform modules (TPM) that perform all encryption, decryption, and digital signing operations including key storage, so that cryptographic keys are never exposed to other hardware components such as the microprocessor, RAM, or flash memory.
- Auditing and unique credentials for each technician connecting to the meter in the field via optical port or wireless handheld equipment.
- Unique keys for each meter, ensuring compromise of one key doesn't compromise more than one meter. This is applicable for both optical port communication and wireless communication with the head end.
- Cryptographic signing and validation of software and firmware upgrades upon receipt from the head end and during each boot process.
- Compartmentalized field-area network design such that individual meters are assigned to a small and finite number of potential aggregation points and network devices.
- No decryption of payload data at aggregation points or any other points between the meter and the head end.
- Cryptographic signing of all data in transit and encryption of all data deemed sensitive (*i.e.*, firmware).

Meter security becomes increasingly difficult over the equipment's long life span.

A complete list of recommendations presented in a systematic approach can be found in the UCAIug *AMI Security Profile v2.0*.[4] The *AMI Security Profile* uses a security domain analysis approach to tailor controls from the DHS *Catalog of Control Systems Security*[5] to AMI components. These controls are currently being re-evaluated by the AMI security subgroup within the NIST cyber security working group to drive them to a level that may be independently tested and certified.

Fig. 6 Phasor Measurement Unit Vulnerabilities

Threat	Potential Impact
Attacker compromises one PMU	Loss of individual data stream
	Inaccurate (*i.e.*, spoofed) data falsely indicates problem, causing expenditure of resources in investigation.
Attacker compromises multiple PMUs, individual field PDC, or phasor gateway	(All of the above, plus …)
	Aggregate system information reveals sensitive perspective of system state.
	Inaccurate (*i.e.*, spoofed) data falsely indicates problem, causing incorrect operator or system choices, with the potential to invoke partial system segmentation/isolation or load shed event.
Attacker compromises primary/central PDC	(All of the above, plus …)
	Complete loss of system functionality.
Attacker compromises phasor application	(All of the above, plus…)
	Comprehensive misrepresentation of system state, potentially causing destabilization of the grid through incorrect operator or system choices.
Attacker compromises data store	Loss of system analysis/forensics capability.
	Incorrect system analysis/forensics conclusions.
Attacker compromises environmental data interface	Loss of ability to correlate system trends/events with environmental circumstances.
	Inaccurate (*i.e.*, spoofed) data falsely indicates problem, causing expenditure of resources in investigation.
Attacker compromises registry	Loss of ability to look up/find available phasor data streams.
	Inaccurate (*i.e.*, spoofed) data falsely indicates availability or non-availability of phasor data stream, causing expenditure of resources in investigation.

PMU = Phasor measurement unit PDC = Phasor data concentrator

Source: Authors' analysis

Transmission Domain: Phasor Measurement

Existing situational awareness tools such as state estimators extrapolate transmission-level data from SCADA-based systems to produce a periodic estimate of the state of the transmission system. In contrast, advanced measurement technologies, such as PMUs, capture GPS time-synchronized transmission-level data at a much faster rate (typically 20 samples per second) across an entire grid interconnect, providing operators a real-time, high-quality view of transmission system state. PMUs accurately measure parameters such as voltage timing (phase angle) differences across the transmission network that reveal areas of strain and potentially dangerous anomalies such as oscillations, and clarify the current state of the grid in ways that aren't available from traditional sensors.

Phasor data concentrators (PDCs) collect data from multiple PMUs across wide regions of the grid. The data is then analyzed and used to inform advanced decision support systems, enabling operators to pinpoint problems on the grid and quickly receive actionable information to manage grid operations, identify potentially unstable conditions, and restore the system after an outage. Phasor applications may also collect other external environmental data (such as weather or traffic data) to provide a more complete picture of system disturbances. Because PMUs are widely distributed throughout a region or interconnect, utilities can share data across organizations through implementation of a phasor gateway. With this fast, accurate, wide-area system data, operators can monitor stability and grid dynamics over a broad area in real time, and operate the power system closer to its limits, which increases asset utilization and reduces congestion costs.

Phasor data information flow is continuous and time sensitive—it must reach the point-of-use typically within two seconds. Late-arriving data is either discarded or passed on to a data store where it has benefits beyond real-time use: analysis of PMU data stores can improve future state estimation and aid in system or event analysis after the fact. Depending on how and where they're deployed and used, many PMUs might be considered a critical cyber asset under North American Electric Reliability Corp. (NERC) critical infrastructure protection standards.

A critical component of PMU technology is the use of GPS signals for time-synchronization. Yet GPS signals can be jammed or spoofed by a hacker with moderate expertise and resources. Because PMU data must arrive at the point-of-use within one to two seconds to be relevant, cyber security solutions that protect PMU data communications must not introduce any delay in transmission. PMU data is shared between many entities and across geographical boundaries, making security measures at connecting gateways critical. The aggregated system information that passes through connecting gateways would be highly valuable to electricity market participants, also making it an attractive target for malicious actors.

Case Study: Synchrophasor Security Architecture

One example of an approach to synchrophasor security architecture is Southern California Edison's (SCE) Wide-Area Situational Awareness System (WASAS). In this case, the architecture is primarily based on synchronized phasor measurement technology, but will also utilize other wide-area information input, such as energy management system (EMS) SCADA data and external data to provide additional information for system operators. The WASAS spans a complex trust environment, and therefore must ensure that it provides trusted data to system operators. WASAS is designed so that essential functions are preserved even if some data sources are deemed untrustworthy and consequently excluded from consideration.

The WASAS interfaces with four different sets of systems—two internal to SCE but outside of the WASAS, and two from outside the utility. Externally, the WASAS will pull weather, traffic, fire, and earthquake data from public sources and phasor measurement data from utilities across the country. From inside SCE, the WASAS will interface with systems in both the enterprise and the grid control center.

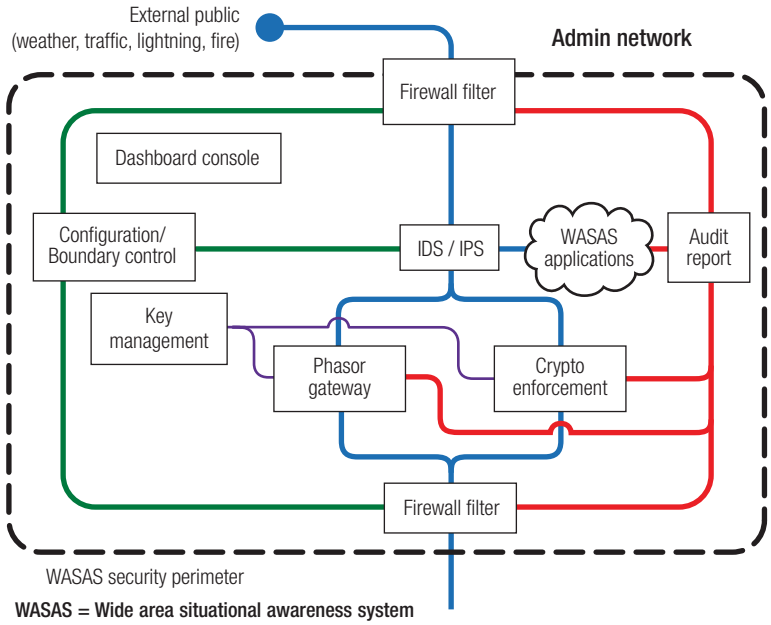
The WASAS breaks down the approach for cyber security into two domains: central security services and edge security services. The central security services domain provides automated security services to all elements of the system as well as management capability for each of the automated services. The edge security services domain provides the field component counterparts for corresponding services in the central security services domain. For example, the central security services domain provides a management interface to control cryptographic functions such as generating and distributing cryptographic key material, as well as controlling key material expiration and replacement; while the edge security service domain responds to these functions by accepting, storing, purging, or replacing the key materials in use in the actual field device. Both domains use physical access controls together with electronic controls to provide comprehensive security.

Figure 7 illustrates the low-level logical architecture for central security services. The architecture is designed to automate cryptography enforcement, integrity enforcement, and audit enforcement. Cryptography enforcement provides fast cryptographic services such as encryption, decryption, signing, and validation to meet the low-latency demands of synchrophasor data. Integrity enforcement provides all of the services involved in ensuring any form of tampering or malicious attack is quickly detected, and enables rapid response to adverse cyber security events. Audit enforcement provides the means to validate proper operation of the system and produce trails of evidence that support forensic analysis for cyber security events.–***HK et al.***

Fig. 7 Synchrophasor Security Example

Source: Southern California Edison

Synchrophasor central security low-level logical architecture: Blue lines indicate primary business data flow. Red lines indicate audit and reporting support. Green lines indicate security configuration and boundary control support. Purple lines indicate key management support.



WASAS = Wide area situational awareness system

The potential to compromise the data and cause system instability could further motivate malicious actors interested in creating fear or leveraging their access to extort money.

Figure 6 outlines potential impacts of a successful cyber attack against PMU technology used for wide area monitoring of the transmission system.

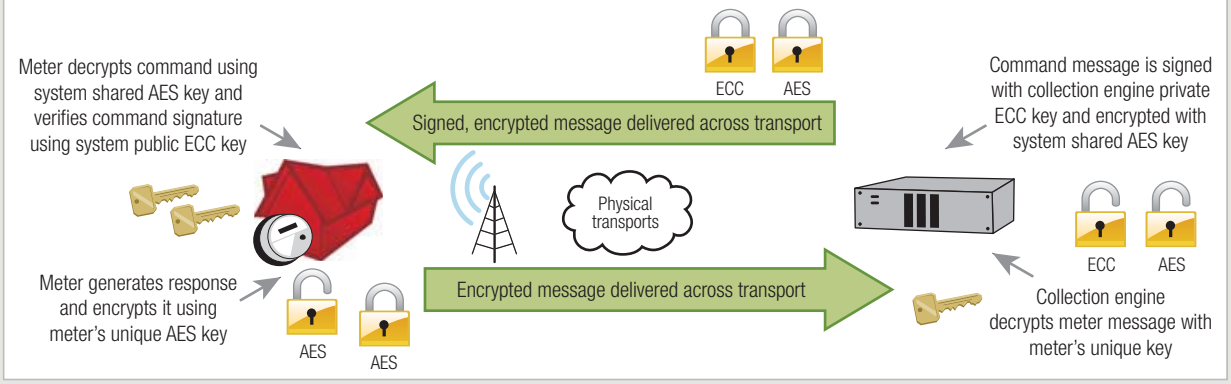
Protecting Transmission

The following mitigations are selected examples of good practices for security of wide-area situational awareness systems operating on the transmission network—*i.e.*, synchrophasors:

- Security controls should have minimal impact on the synchrophasor system, and in no way prevent its primary mission.
- Security controls should minimize the impact of adverse events on the quality of service for synchrophasor communications and functions.
- No external entity should have direct access to a utility's PMU.

Case Study: Smart Meter Security Architecture

Fig. 8 AMI Security in OpenWay

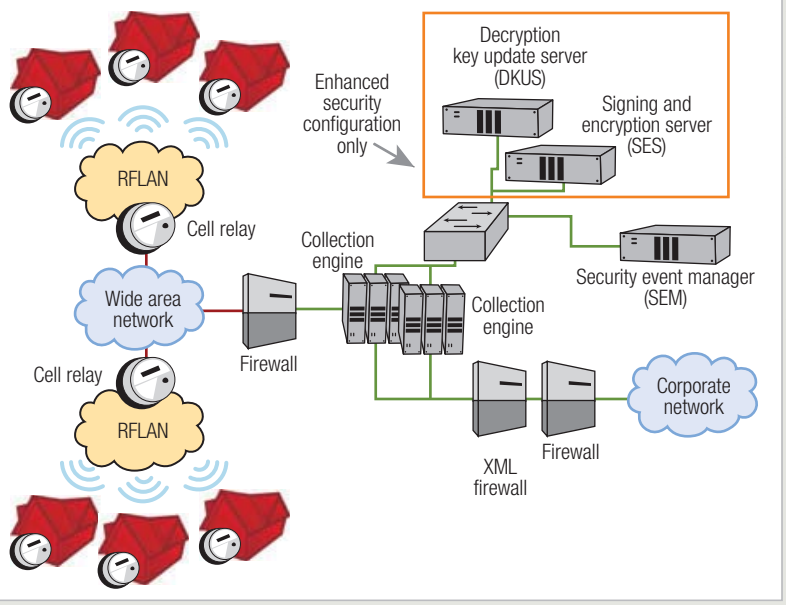


Source: Palmquist, Scott and Ido Dubrawsky, OpenWay Security Overview, Itron white paper (2011)

Security vendor Itron introduced its OpenWay advanced metering infrastructure (AMI) security architecture, designed to provide flexibility and robust security in an infrastructure using a radio frequency-based local-area network (RFLAN). Its security solution leverages both public key cryptography and symmetric key cryptography to serve different functions in securing the communication between the collection engine and the meter endpoint (*See Figure 8*).

Itron uses a specific and efficient type of asymmetric (or public key) cryptography to ensure the integrity and non-repudiation of all messages between the Itron collection engine (or "head end") and the OpenWay meter. All messages in both directions are signed using the elliptic curve digital signature algorithm (ECDSA) that meets NIST federal information processing standard (FIPS) 186-3. This signature ensures that no one may alter or tamper with the message without introducing an error in validation, while the use of public key cryptography means that the signatures may be validated without ever exposing the private key used to generate the signature.

Fig. 9 AMI Security in OpenWay



Source: Palmquist, Scott and Ido Dubrawsky, OpenWay Security Overview, Itron white paper (2011)

Additionally, Itron uses the 128-bit version of the advanced encryption standard (AES) that meets NIST FIPS 197 to encrypt all messages between the collection engine and the OpenWay meter (*see Figure 9*). The use of a symmetric algorithm means that the same key may be used across the system, facilitating broadcast and multicast communications and thereby allowing the collection engine to direct behavior for a large number of meters simultaneously (as in sending out pricing information) or to send an individual command to a particular meter (as in a remote connect or disconnect). The fact that both ends of the communication channel are capable of asymmetric cryptography also helps ensure that symmetric key updates may be handled while minimizing risk of a malicious actor taking control.–***HK et al.***

■ All synchrophasor systems and components should restrict logical and physical access to authenticated and authorized systems and personnel.

■ Only authenticated and authorized configuration changes (*e.g.*, firmware, settings) should be processed by synchrophasor systems.

■ All configuration changes and access requests to synchrophasor systems should be auditable.

■ Synchrophasor applications should validate the authenticity and integrity of all data acquired.

■ Asset owners shouldn't rely exclusively on security measures outside their direct observation and control.

■ The introduction or integration of synchrophasor systems shouldn't expose other utility systems to unauthorized access or attack.

■ Utility systems should be able to continue essential functions in the absence of PMU data.

■ Authorized operators should have the ability to disable automated protection and control associated with synchrophasor systems while maintaining monitoring functionality.

■ Essential synchrophasor functionality shouldn't have single points of failure.

A complete list of recommendations presented in a systematic approach can be found in the UCAIug *Security Profile for Wide-Area Monitoring, Protection, and Control (Synchrophasor)*, developed by the advanced security acceleration project for the smart grid team.[6] The synchrophasor security profile uses a failure analysis approach to define controls for an explicit set of use cases, and validates this set of controls for completeness against the controls in NIST IR 7628, "Guidelines for Smart Grid Cyber Security."[7]

Advancing Cyber Security

Securing the smart grid, from transmission systems to home area networks, will require coordination among many stakeholders, including owners and operators, vendors, technology developers, systems integrators, government agencies, and researchers at national laboratories and universities. By coordinating their activities and building on the work of others, industry and government can work together to deliver secure next-generation technologies; practical, actionable implementation guidance for utilities; and security standards and testing requirements for smart grid components and systems. F

[*Editor's note: In the second of two articles, scheduled for publication in August 2011, the authors discuss plans and recommendations for implementing cyber security standards for smart grid technologies.*]

Endnotes:

1. Smart grid domains are defined in: National Institute of Standards and Technology, The Smart Grid Interoperability Panel—Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security*, NISTIR 7628 NIST, August 2010.
2. The objectives are taken directly from: Howard Lipson and James Ivers, *Advanced Metering Infrastructure Security and Survivability: Risks, Challenges, and Progress*, Draft v0.1, Carnegie Mellon University Software Engineering Institute, Sept. 29, 2008.
3. OpenHAN Task Force, UCAIug Home Area Network System Requirements Specification, Version 2.0, (UCAIug, August 30, 2010).
4. Advanced Security Acceleration Project for the Smart Grid, *Security Profile for Advance Metering Infrastructure*, Version 2.0 (AMI-SEC Task Force and NIST Cyber Security Coordination Task Group, June 22, 2010.
5. Department of Homeland Security Control Systems Security Program, National Cyber Security Division, *Catalog of Control Systems Security: Recommendations for Standards Developers*, DHS, September 2009.
6. Advanced Security Acceleration Project for the Smart Grid, *Security Profile for Wide-Area Monitoring, Protection, and Control*, UCAIug Smart Grid Security Working Group, draft May 16, 2011.
7. National Institute of Standards and Technology, The Smart Grid Interoperability Panel – Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security*, NISTIR 7628, NIST, August 2010.