

White Paper

Ensuring reliable end-to-end communications and data integrity for AMI networks

Communications networks represent a partial paradox. The very openness and ubiquity that make them powerful can also present a weakness. Worms, viruses, malware, hackers, disgruntled employees and innocent mistakes... all of the risks faced by enterprise networks and the Internet could be considerations for utility networks as well.

“Threats to electric utilities do not just come from potshots at transmission towers or downed line,” warns the Utilities Telecom Council (*The Utility Spectrum Crisis: A Critical Need to Enable Smart Grids*, January 2009). “Some of the greatest vulnerabilities in electric utility networks come within the cyber-based systems that ensure continuous operation and electric reliability. ... While the power industry has avoided mandates in the past, the protection of utilities’ cyber assets has changed from being taken for granted to being investigated thoroughly, upgraded and tested.”

New Expectations for Utility Communications

As utilities move forward with for Advanced Metering Infrastructure (AMI) deployments, they will find themselves responsible for two-way communication networks that reach every customer site and every monitoring point in the power distribution and metering architecture. This represents a far-reaching network with many elements to be safeguarded, to ensure the integrity of the critical utility infrastructure.

There are no specific requirement documents or standards that apply directly to security for AMI systems. However, there are standards and documents that provide relevant guidance. For example, in May 2009, the National Institute of Standards and Technology (NIST) released a set of standards and reference documents for interoperability and cyber security that it considered as broadly applicable to Smart Grid initiatives. Even as standards evolve, utilities can take a lead from the enterprise network world and apply proven methods for multi-layered security, from physical

controls to encryption to virtual private networking and more.

Network Security101—Multiple Tactics for Multi-layered Security

The goals of a security strategy are to protect all points of entry to the network, make reconnaissance difficult from the inside, limit points of vulnerability, and thwart attempts to misuse or compromise the network and the data it transmits. The good news is that network developers and operators have a broad range of techniques and best practices to apply to achieve these aims. Using multiple security approaches in tandem, organizations can create a multi-layered security scheme appropriate for the critical nature of AMI communications.

Here is a snapshot look at some of the most prevalent methods used in the most critical enterprise networks, which are equally applicable for securing utility communications networks.

Firewall devices permit or deny data transmissions into a company’s network based on rules and other criteria. All

messages entering or leaving the controlled network (such as the regional network interface) must pass through the firewall, which examines each message and blocks those that do not meet specified security criteria.

An **intrusion detection system (IDS)** monitors the events occurring in the network, identifies activities that are potentially malicious or in violation of security policy—such as an unauthorized attempt to alter smart meter firmware—and reports to a management station.

Intrusion prevention systems can also react in real-time to block or prevent certain activities, such as dropping unauthorized data packets while allowing legitimate traffic to pass through.

A **demilitarized zone (DMZ)** combines firewall and intrusion prevention system to tightly regulate traffic entering the company’s servers, usually at the regional network interface and head end. When a DMZ is in use, there are no common communication ports between the outside world and the internal controlled zone.

Anti-virus software detects, prevents and removes damaging code from a computer, such as worms, viruses and Trojan horses. Servers that support utility applications—such as the Sensus FlexNet™ Network Controller, Web Server, Stats Server and Maps Server—should have anti-virus software for local protection from such threats.

Virtual private networks (VPNs) encapsulate the data being transmitted, much like a pipe within a pipe, and authenticate both endpoints of a communication to prevent unauthorized users from accessing or reading the data. In a FlexNet network, for instance, all backhaul network interactions from the tower gateway base station to the regional network interface (the head end) are transmitted via VPN tunnels.

VPNs use **Transport Layer Security (TLS)** or its predecessor, **Secure Socket Layer (SSL)** to encrypt transmissions at the transport layer, and use the **Secure Shell (SSH)** network protocol to establish a secure channel between devices for data exchange.

Encryption is achieved by an algorithm that makes data unreadable except to a device that has the key to decrypt the message. *Symmetric* encryption uses the same key for both encryption and decryption. *Asymmetric* encryption uses a public key and a very highly protected private key, so anyone can send an encrypted communication but only the intended recipient can decrypt it.

The longer the encryption *key*, the stronger the encryption. In symmetric encryption systems, 128-bit keys are commonly used and are considered very strong. Sensus goes beyond that, encrypting FlexNet communications with 256-bit keys. The encryption method changes dynamically over time based on time and packet sequencing, preventing packet replay and pattern detection.

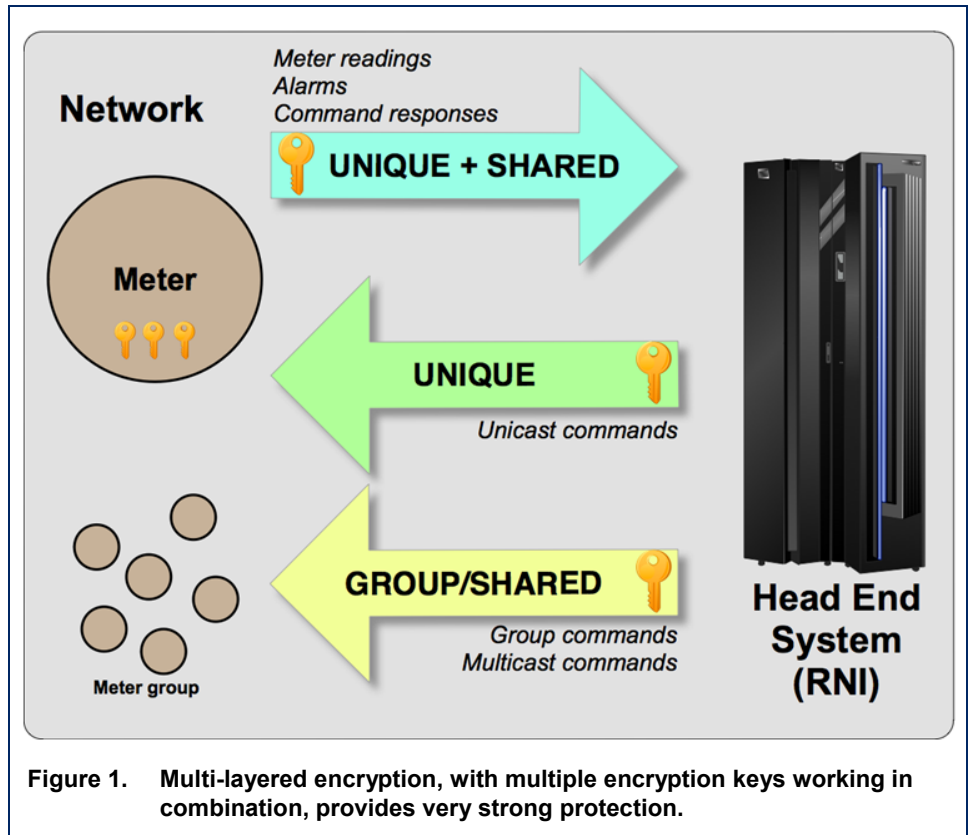
Furthermore, the proprietary Sensus 7-FSK (frequency shift keying) modulation scheme is not public domain. This scheme is not commonly recognizable by a spectrum analyzer, and no off-the-shelf equipment can be purchased to demodulate it.

Multilayer encryption combines several encryption keys for even more robust protection. In a FlexNet system, for instance, each meter has a *unique key* that was assigned during manufacturing. The regional network interface (RNI) can automatically distribute a *shared key*

traffic. The RNI automatically rotates shared keys. With this encryption scheme, a compromise to one meter cannot affect other meters or components in the network.

Strong **encryption key management** techniques keep these keys secret. In FlexNet systems, every endpoint has a unique key that is injected during manufacturing but can only be enabled by the customer. A central key server securely manages the system's encryption keys.

Even the keys themselves are encrypted



to all meters on the network. And each meter group can be assigned a unique *group key*.

The unique meter key and/or group key can be used in conjunction with the shared key to encrypt all meter-to-RNI

with a master key before being stored in the key database. Access to the master key is securely managed to the strongest possible Federal Information Processing Standardization 140 (FIPS) standards.

Authentication establishes or verifies a user or endpoint as authentic, such as through passwords entered by authorized users or digital signatures supplied by devices or computer programs. In the FlexNet system, both ends of the communication are authenticated.

Once the identity of a user or device has been validated, **authorization** processes grant access to network resources as permitted. For instance, under a sound security policy of separation of duties, an administrator may have permission to access certain utility network functions or commands but not others.

Tamper prevention and detection techniques protect against unauthorized physical access to devices, particularly those in insecure locations, such as at customer sites. The endpoint device can have a lock, seal and other tamper-resistant mechanisms. Tampering with the devices will trigger an alarm to the network management system.

A wireless network based on **licensed spectrum** provides intrinsic security advantages. For one, since this is not a technology that an individual can order through the Internet and plug in at home, it is not a target for casual intruders. Furthermore, by law only the authorized license holder can access the licensed channel. It is illegal to infringe on this channel either by sending or intercepting transmissions. In the U.S. this protection is enforced by the Federal Communications Commission.

Time-windowed commands add yet another layer of defense to limit the risk of replay attacks and other types of malicious activities. For critical actions, such as configuration changes or firmware updates to remote devices, the system first sends a “notification of action” message to the device. The subsequent “action” message must be received within a designated window of time, and

it must contain elements that match those in the notification message, or else the action is rejected.

In the network security context, **entropy** refers to a degree of built-in uncertainty in how security provisions are applied. When security features are less predictable, they are harder to crack. The FlexNet Security Architecture introduces random information elements into the methods by which it processes commands and other information, which makes it far more difficult to compromise the system.

Pass-through devices extend the connectivity of an AMI network without adding risk. For example, Sensus smart meters can operate in buddy mode to help an out-of-range endpoint reach the tower, and vice versa. In buddy mode, the meter simply forwards the encrypted communication; it does not have the means to decrypt or re-encrypt the messages.

Behavior auditing monitors activity on the network, looking for suspicious activities or deviations from policy. For example, any attempt to tamper with a secured device or update its firmware would trigger an alarm, alert notifications to appropriate personnel and an audit log entry.

Naturally, these technology-based security tactics must be backed with strong organizational **security policies** as well, such as division of responsibility, physical access control, secure storage of hardcopy information and disaster recovery plans.

Security in the FlexNet Network

Many existing utility communication networks have just one or two layers of security—insufficient for emerging AMI and Smart Grid requirements. Others rely on third-party security measures that

are generic and not customized for each customer.

In contrast, the FlexNet solution provides its own, built-in, multi-layered security shield—in which *all* layers are active all the time to protect data at rest and in transmission. Layering security, wrapping one security layer upon another, takes the FlexNet system to thresholds unattainable elsewhere.

FlexNet hardens the basic system, uses multi-layered encryption methods with entropy, and strengthens this protection through access control, authorization and authentication—all based on licensed spectrum for wireless communications and VPN tunnels for wired connections.

Ultimately, the utility has control over the final elements of network security—attributes such as which TGB firewall filters to activate or how encryption keys are used. As a result, every FlexNet security system is unique, which provides even further protection.

At the customer site...

Smart meters and home area network (HAN) devices are equipped with locks, security tags and seals, and secure physical mounts (non-exposed fasteners, etc.). Attempted breaches trigger alert notifications.

A unique, 256-bit AES (Advanced Encryption Standard) key is injected into the endpoint device during manufacture; this key works with shared keys issued by the regional network interface to encrypt and decrypt all transmissions. An endpoint can support up to eight keys—unique, shared, and primary or secondary group keys. The keys themselves are stored in encrypted form.

If encryption is not used, at minimum the transmissions are obfuscated via Viterbi optimization algorithms and FSK transmission.

At the tower gateway basestation (TGB)...

Additional security measures are applied. Data is stored for only the period of time needed to ensure accurate pass-through of data between endpoints and the regional network interface. All communications occur over secure, encrypted channels. Backhaul communications to the RNI travel over VPN tunnels. No data is ever sent over any network—public or private—in the clear. Encryption keys are never stored on the same device as the data.

Tower gateway basestations also have a built-in firewall with preconfigured filters. Customers can choose to turn on any or all of these filters to meet the needs of their enterprise security policy.

For physical security, TGBs are generally installed in hardened facilities established for wireless telecom or paging. All equipment is located inside areas that have been highly secured by the primary owner of the tower site to protect all their customers' high-value services.

For tower facilities with buildings, the FlexNet TGB hardware sits in a locked, hardened, rack-mount enclosure. For tower sites without buildings, FlexNet provides an environmentally secure, hardened enclosure with locks. All cabinets (interior and exterior mount) have door switch sensors that generate an alarm at the operations center when the door is opened. All cabinets and enclosures comply with National Marine Electronics Association (NMEA) standards for weatherproofing.

FlexNet offers a unique security advantage because it operates over licensed wireless spectrum, which enables a range of 20 miles or more between network elements. As a result, the network does not require hundreds or thousands of home or pole-top mounted collectors,

which can often attract vandalism. Instead, there are far fewer intermediate network nodes, and they are always located at highly secured tower sites.

At the regional network interface (RNI)...

Additional security measures prevent unauthorized users from accessing FlexNet servers: the Network Controller, Web Server, Stats Server and Maps Server.

Sensus provides a broad range of security options for this network control center but does not dictate which practices to employ. Utilities have the choice of determining exactly which local operational and security practices are appropriate for each location.

Security measures can include additional hardening of the system, access control, secure VPN administrator access, time-windowed commands, customized encryption key management, physical security and more.

Secure communications between FlexNet servers and tower gateway base stations are strongly recommended. If outside connectivity is required, the layered security of a DMZ is also recommended.

Benefits of the Sensus Approach to Security

Working together in a security scheme customized and owned by the utility, FlexNet security features effectively prevent the system from being compromised from within or outside.

For example:

Endpoint firmware and software cannot be modified without authorization.

- Modifications are only considered if they originate from the head-end

system at the regional network interface.

- Modifications must be transmitted by an authentic source that knows the unique or private key for the endpoint, or the endpoint cannot decrypt the commands or modifications.
- All modifications are automatically monitored and logged by the system.

A compromise to any endpoint would not affect the network or other endpoints.

- Transmission from endpoints cannot cause the head-end to take any actions.
- False data sent from potentially compromised endpoints would be identified by business logic within the head-end system.
- False or corrupted data or transmissions from any compromised endpoint could not spread to other endpoints, because the compromised endpoint would not know the unique or private key of any other uncompromised endpoints.

Data confidentiality, integrity and authenticity are preserved throughout the network.

- Transmissions are all encrypted using strong AES-256 encryption with multiple keys and secure key management with an incorrect key, the endpoint cannot decrypt the command and will not take action on the unauthorized command.
- In transmissions from RNI to endpoints, only the RNI and the endpoint know the unique key (or private key in an asymmetric

- model). If commands are encrypted with an incorrect key, the endpoint cannot decrypt the command and will not take action on the unauthorized command.
- Entropy and time windowing prevent replay attacks and pattern detection.
- VPN tunneling further protects transmissions between the head-end and tower gateway basestations.

Closing Thoughts

In a two-way AMI system, every deployed endpoint could potentially be used to try to exploit the network or other networks that use the same technology. Logically layered security for authentication, access control and data transmission address those risks, establishing multiple barriers against unauthorized or accidental misuse of the network.

Sensus takes seriously the requirement to keep pace with evolving security threats, especially as Smart Grid deployments place more critical data on communication networks. To that end, we are::

- Collaborating with customers to continue to develop and expand FlexNet security measures
- Commissioning regular third-party testing of FlexNet security and making summary results available to customers
- Providing our security expertise to customers to help them develop their own security programs
- Encouraging continued development of security system standards among regulatory authorities and industry partners, as well as adhering to those system standards by the industry

Contact us for more information about multi-layered security for FlexNet communication networks.

About Sensus

Sensus leads in innovative and evolving technology solutions that enable intelligent use and conservation of critical energy and water resources. Sensus has led the discovery, development, and implementation of technologies for the energy and water industries for more than a century. Water, gas, and electric utility customers around the world benefit from the company's open, flexible products and solutions to help them optimize their resources – today and tomorrow. Headquartered in Raleigh, N.C., USA, Sensus serves customers from locations throughout the Americas, Europe, Africa and Asia. For more information, visit www.sensus.com.

© 2010 Sensus USA Inc. All rights reserved.
FlexNet is a trademark of Sensus USA Inc.