

# AMI security considerations

Jeff McCullough

## Introduction

Many electric utilities are deploying or planning to deploy smart grid technologies. For smart grid deployments, advanced metering infrastructure (AMI) is a new technology that enables radical changes in the operation of the distribution grid. Given the new levels of automation and extended access to the grid enabled by AMI, issues have been raised concerning the potential of security gaps within smart grid deployments, with some concerns pertaining specifically to existing and new AMI solution offerings.

This paper examines some of the security concerns related to AMI systems and describes key preventive measures that can be taken against cyber security issues.

## Basic AMI components

The AMI network comprises various networks for communication as well as software and hardware components, such as the following:

- An element and/or system management application (also called the “head end”) operating on the utility network
- A wide area network (WAN) (also called the “backhaul”) providing communications from the utility head end out to the field
- Field access or collection points on the edge of the WAN providing connections and/or consolidation for metering data access, and
- A mesh network known as a local area network (LAN) or neighborhood area network (NAN) providing sub-networks of meters, extending the reach to a larger meter population.

Home area networks (HAN) are also being introduced to provide interfaces into the home to support consumer awareness of energy consumption and to extend support for demand response functionality.



## Securing the LAN

As with existing wire-line or wireless networks, the primary concern revolves around the security protections for easily accessible devices such as the meters and the associated communications hardware.

### Reverse engineering of LAN devices to attack the grid

One key concern is the presumed ability of a hacker to reverse engineer a stolen or purchased field device such as a meter.

To greatly reduce the risk of a hacker evading device security in the AMI system, the manufacturer can lock the microcontrollers containing the firmware. This prevents intruders from reading the firmware from the device.

This approach still allows the firmware to be written (key to enabling highly efficient remote upgrades) but still protecting against unauthorized changes as follows:

- One section of firmware (known as the boot loader) is locked and cannot be overwritten
- Regardless of whether one section or the entire firmware image is written, the boot loader verifies the new downloaded section as well as the entire image. A hacker would have to satisfy all security requirements expected by the boot loader. In addition, the hacker would need detailed knowledge of the complete firmware image in order to attempt to modify or load a new image that would meet the boot loader's verification standards.
- The meter (exercising its distributed intelligence) will not attempt to switch to a new firmware image until the new image is validated by the meter's boot loader.

In summary, because the firmware cannot be read, any would-be reverse engineer is operating "blind." Partial or complete modifications written to the firmware must exactly match all expected characteristics to be validated for use by a meter.

[Elster Solutions EnergyAxis meters and network interface cards currently provide these key characteristics.](#)

## Secure remote OTA upgrades

In the event of a potential security risk or breach on remote assets, it is critical those devices can be remotely managed and upgraded to patch the threat. Remote upgrade capability must apply to not only the radio firmware, but more importantly, the metrology firmware. This capability adds the required flexibility to future proof the system and enables new functionality or parameters to be provided as well as keep up with evolving security threats.

The manufacturer can encrypt the firmware to increase the security of the transfer and download into the device. This secures the new firmware from the point of origin and allows only the intelligent device to successfully decrypt prior to performing validation. The encryption of the firmware should be completed with a unique encryption key different than that used for encrypted communications. All communications should also be encrypted (for example, using AES-128 bit) to provide additional remote security strength.

[EnergyAxis release 7.0 provides all of these required characteristics.](#)

## LAN endpoint behavior monitoring

Behavior monitoring is based on the premise that observing past behavior enables one to predict future behavior. Would-be hackers can monitor meter communications to learn network messaging behaviors that would subsequently enable the attacker to send other (disruptive) messages to a device.

This risk is reduced by minimizing the amount of messaging (reducing the chatter) and providing few examples of valid messages or behavior.

For example, in the LAN an endpoint device is programmed to originate only event messages. An endpoint device will not volunteer any other communication task unless such task is initiated by a secure communication from a collection device. Metering data is never sent and control messages are only acted upon unless requested by a collection device (for example, firmware within endpoint devices is incapable of initiating control messages to other network devices).

[EnergyAxis release 7.0 provides all of these required characteristics.](#)

## LAN communication attack prevention

There are various preventive measures that can be deployed in parallel to further strengthen the security of overall LAN communications.

Technical expertise in both metering and low bandwidth networks are needed to successfully implement enhanced security within the resource and often bandwidth constrained components comprising the AMI LAN. Factors such as radio interference, battery operated devices and optimized messaging must be accommodated when designing and implementing the LAN security solutions.

Some field proven means to enhance LAN security are listed as follows:

- Select an intrinsically more secure type of radio communications. For example, the US military uses frequency hopping spread spectrum (FHSS) communications (which can be used on the LAN) because it provides an inherent level of security not found in single channel systems. Because FHSS uses multiple channels in a random hop sequence for data transmission, it is very difficult to eavesdrop and intercept complete messages. Each device uses a different hop sequence and timing, so even if a hacker manages to penetrate a single device, it is impossible to extrapolate to any other device in the system.
- Sessionless LAN communications between the access point and each endpoint offer stronger security because each communication must be authenticated before it can be acted upon
- Encrypted LAN communication (for example, AES-128 bit) provides an additional layer of confidentiality for each message between the access point and endpoint
- Additional checks should be provided to add data integrity checks (to confirm the data has not been tampered with prior to arrival)
- Use of unique encryption keys per LAN device further increase the strength and decrease the capability to infiltrate LAN communications
- To defend against future threats, or just meet utility security policies, it is critical to be able to manage and change the crypto keys remotely
- To defend against imminent or active threats it is also critical to be able to manage or change keys quickly and easily across a large AMI system network
- To help identify attempts to breach LAN elements, host (device) based intrusion detection (tamper alerts) logging on the LAN assets can be added.

Some critics have implied that an attack could be initiated through a meter or other LAN devices. The scenario imagines that LAN messages can be sent to change device behavior or control a device causing (for example) a mass disconnect of residential home power.

If designed correctly (that is, to support a parent-to-child configuration), a WAN access point (parent device) will not accept a command message (from a LAN child device). In hierarchical system architecture, control over a single endpoint cannot be extrapolated to control over a multitude of endpoints.

Restricting how system communications are processed further secures LAN communications. One example is to limit the metering endpoint to spontaneously sending only system exception data and events such as tamper alerts or outage notifications. The meter gathers and holds register and interval data until it is retrieved using a request and response communications session with the data collector.

This approach greatly increases the protection against spoofing a meter and allowing false data to be presented to the system. The addition of encrypted LAN communications provides confidentiality of the data to further secure the network and prevent potential spoofing.

[EnergyAxis release 7.0/7.5 provides all of these required characteristics.](#)

## Spoof-proof meters?

Given the meter is an exposed component in the network (not only to the natural elements but to physical attackers as well), there is reasonable concern over the cyber security of these edge devices to prevent reverse engineering or meter spoofing. Each of the items discussed above (parent-child architecture, FHSS, tamper notification, authentication, encryption, unique crypto keys, etc.) all provide protection, but additional preventative measures can be taken within the design of the meter to help prevent spoofing or manipulation.

To spoof a meter, an attacker would have to know intricate details about the microcontrollers within the meter as well as the firmware. Attackers (or security consultants) create unique probes or monitoring devices with one goal in mind: to monitor or access information on the physical device itself with the objective of manipulating or modifying the meter (for example, change billing data, cause the device to disconnect, cause the device to broadcast out to other devices, etc.)

Microcontrollers contain the meter firmware that controls the metrology and its communications. By using microcontrollers that can be locked, the manufacturer can prevent the firmware from being read from a meter when probed, thus preventing an attacker from directly accessing and reading or downloading the firmware. Locking foils a hacker's ability to analyze or manipulate and re-install firmware.

The ability to write (or overwrite) the firmware is required to allow the remote devices to be field upgraded as additional changes and meter technology evolve (future proofing). The next level in security is to prevent the firmware from being overwritten by either corrupted or unauthorized firmware.

Given this need, one method to prevent the overwriting of firmware is to have any and all new firmware validated for integrity and authenticated upon installation. Both validation and authentication must be complete before the firmware is placed into the runtime environment (that is, the boot loader). This approach prevents spoofing and blocks insertion of worms and viruses.

In addition to these preventative measures, the entire firmware images can be encrypted by the vendor's design team. Encryption provides confidentiality and helps maintain the integrity of the new firmware images by enabling secure transport through the utility network into the metering devices, where it is then decrypted.

Assuming all of these preventative meter security measures are in place, and assuming that an attacker is able to successfully...

- obtain or modify a firmware image
- crack the authentication and validation mechanism in the image
- install the new image
- decrypt and/or encrypt firmware images
- find or break the unique crypto keys for communication encryption

...what can the utility and consumers expect?

Having broken through all of these layers of security, the attacker is able to reach a single meter/account. In addition, the breach will trigger an automatic alert to the utility which then can take action to investigate and quickly update or replace the meter if deemed necessary.

[EnergyAxis release 7.0 provides all of these required characteristics.](#)

## Securing the WAN

The wide area network (WAN) infrastructure may be utility owned or public access. Utility owned options such as WiMax, licensed frequency, or fiber may be used for utility automation as well as for AMI. Public wireless is another option for a WAN.

Because it is rare for a single technology to support all utility communication requirements, the AMI system should be designed to operate securely using a variety of WAN technologies. Regardless of the WAN technology selected, a secure solution must be provided.

[EnergyAxis release 7.0 provides all of these required characteristics.](#)

## WAN communications

Industry standards for WAN communications exist and are actively deployed and used today, providing various levels of security. Two of the most important are ANSI C12.21 and ANSI C12.22.

ANSI C12.21 provides WAN access two-way authentication using DES encryption of a randomly generated token. Given C12.21 protocol is session-based, a timeout can be implemented to release the session and reduce the potential threat of denial of service through session exhaustion.

ANSI C12.21 encryption is commonly provided by communication carriers when the data is transmitted over the WAN (GPRS/EDGE/HSDPA, CDMA/1xRTT/EVDO, etc).

ANSI C12.22, if provided by the system vendor, adds another layer of security by providing WAN access authentication and data encryption using AES-128 bit (per ANSI C12.22 standards). ANSI C12.22 provides sessionless communications; each communication must be authenticated before it can be acted upon.

To increase the level of security, each WAN access point or end device should have a unique cryptographic key for WAN encrypted communications. Encryption key management must support utility security policies and be implemented to expedite key changes in the event of an identified potential threat.

[EnergyAxis release 7.0 provides all of these required characteristics.](#)

## WAN encryption attributes

When providing WAN encryption solutions, many vendors do not take into account the added cost and complexity of providing a key management solution (typically the most difficult component to provide in an AMI network).

Given the nature of the AMI system, existing IT network security solutions are not an exact fit for the need. A variety of solutions are being proposed and implemented by various vendors. When evaluating the various offerings, the utility should look for the following:

- The ability to change keys (re-keying) on the AMI network (as required by utility security policies)
- Unique re-keying key (different than the data crypto key) used on a per device basis to encrypt the new key, adding an additional layer of security
- Minimal system and device performance impacts related to encryption, decryption, and re-keying functions
- Minimal (optimally no) system and device costs related to providing encryption and key management

[EnergyAxis release 7.0 provides all of these required characteristics.](#)

## WAN network provider security

For wireless WANs, telecommunication companies use private networks and encryption to provide secure data transmissions. If used, wireless WAN modems should provide password protection. Wireless WAN modems should also support custom access point nodes (APNs) which make the modem's IP address inaccessible from outside the corporate network (that is, private and not exposed to the public Internet).

[EnergyAxis currently supports all of these vendor characteristics, and continually assesses new versions and modems.](#)

## Head-end system security

The AMI head-end system resides within the utility network. As such, it must be integrated into the existing enterprise network and provide needed security solutions. Basic security attributes to consider are:

- Access authentication
- Co-existence within the utility's firewall
- User password management with optional access to centralized security servers (that is, LDAP)
- Authorization - role-based access level controls
- Event thresholds and alerts
- Auditing - system user monitoring and audit reports
- Secure network interfaces
- Secure data transfer for network applications

These security considerations are well understood by experienced IT professionals and should be included and applied to the head-end system of any AMI solution.

[EnergyAxis release 7.0 provides all of these required characteristics.](#)

## Securing the HAN

Some home area network (HAN) devices currently require data from the AMI system. When this network connection is required, maintaining a secure communication channel will prevent potential access or manipulation of the AMI system. Attributes to evaluate the security of the HAN offerings should include:

- The WAN access or collection point should not allow in-premise devices (HAN) direct connection
- HAN devices should connect using an electric meter to limit/reduce potential system threat impacts (that is, single point compared to potential thousands on a WAN access point)
- HAN devices are limited to communicating only with a HAN manager application within the meter, not directly with the metrology application (to restrict HAN data access)
- Write access from the HAN device into the meter HAN manager should be restricted to designated locations
- The HAN manager function should not be capable of writing configuration tables in the meter
- Meters can communicate only with HAN devices provisioned and authenticated from the head end
- HAN data and message integrity checking, and authentication are needed to validate communications

The ZigBee Alliance and other interested groups are evolving security standards for HAN communications and devices. A secure AMI solution will implement these or other similarly comprehensive standards.

[EnergyAxis release 7.0 provides all of these required characteristics.](#)

## Summary

As utilities evaluate AMI systems, the industry's basic security requirements should be considered and the selected AMI system should provide superior security.

By design, the AMI system must be designed and implemented with security in mind. Security should not simply be applying third party solutions as an overlay (that is, security should be built in and not bolted on). To be successful, this will require vendors and utilities alike to possess not only security, communications, and networking expertise but also detailed expertise and working knowledge of the AMI components to allow them to successfully integrate these together into a secure AMI system solution. The Elster EnergyAxis System solution is designed and implemented with the secure attributes defined above, providing a secure AMI offering to meet these demanding requirements.

[EnergyAxis release 7.0 provides a secure AMI solution.](#)

## About the author

Jeff D. McCullough is Director of IP Communications, Systems Tools and System Test at Elster Solutions in Raleigh, NC. In this role Mr. McCullough is responsible for IP communications development evolution, EnergyAxis System verification, EnergyAxis System Tools development, and EnergyAxis Security solutions.

Mr. McCullough's 25 years of experience include extensive work in telecommunications, including network management solutions, evolution and introduction of new technologies, secure system offerings and federal government system solutions.

Mr. McCullough sees the technical evolution of the smart grid as having many parallels to the profound changes of the telecommunication industry in the 1990s. He is excited to have the opportunity to assist in the development of smart grid technology.

ALPHA, ALPHA Plus, REX, REX2, REX2-EA, EnergyAxis, Metercat, and AlphaPlus trademarks and/or registered trademarks of Elster. Other products and company names mentioned herein may be the trademarks and/or registered trademarks of their respective owners.

Elster  
208 S Rogers Lane  
Raleigh, NC 27610-2144  
United States

T +1 800 338 5251 (US toll free)  
T +1 905 634 4895 (Canada)  
F +1 919 212 4801

[www.elster.com](http://www.elster.com)

© 2010 by Elster. All rights reserved.

Information contained herein is subject to change without notice. Product specifications may change. Contact your Elster representative for the most current product information. Printed in the United States.