Deterrent and detection of smart grid meter tampering and theft of electricity, water, or gas

Jeff McCullough

Introduction

This white paper was inspired by real concerns regarding "smart grid electric meters being altered to steal electricity." There are often reports of meters being exploited to under-report consumption. This paper examines some of the concerns raised and describes measures currently provided by Elster meters and the Elster EnergyAxis® System to detect and/or prevent theft, tamper and loss of electricity, water, or gas.

Threat: alteration of meters to steal electricity, water, or gas

Since the day the first meter was deployed, unscrupulous people have attempted to alter meters to steal utility-provided resources. Some approaches are simplistic; others are sophisticated. What is certain is that as security technology evolves so does the inventiveness and sophistication of the criminals.

Remote reading of smart meters has eliminated the monthly physical visit by utility technicians to read the meter and visually inspect it. The use of electronic smart meters (intelligent electronic devices as opposed to mechanical meters), also introduces the threat of a cyber attack or alteration.

Energy thieves are inventive and persistent; realistically, as long as there is product worth stealing, there will be theft. Utilities and vendors must continue to provide stronger preventative and detective methods to deter these efforts and/or identify and prosecute the fraudulent act.

Meter and system characteristics that prevent theft and tamper

The primary concerns revolve around the security protections for smart grid meters that can be physically accessed. It is obviously cost prohibitive to the utility to physically secure all meters from individuals who are intent on theft, but meters and systems can be armed with safeguards—alerting utilities to physical tamper, providing law enforcement with clear identification and documentation of the theft, and preventing cyber tampering.

Elster meters and the EnergyAxis System AMI solution currently provide functionality to help deter both physical and cyber tampering. Key attributes include the following:

- **Layered security and multiple passwords protect Elster EnergyAxis-enabled meters from unauthorized access over the local optical port.** Field (and bench) configuration and testing are accomplished using a local optical port connection. Password authentication is required to establish successful connection to the meter via the optical port. Assuming that this single layer is breached, the would-be thief now has "read-only" access to the meter data (this does not include account data). An additional level of authentication is required before the meter will accept changes to any power consumption configuration settings (this authentication is used during the manufacturing process to set the utility-designated configuration prior to shipment, and the capability is not supported in field tools). The last level requires that the thief possess extensive and detailed knowledge of the data table structures that contain the configuration data.

  To successfully implement configuration changes to Elster meters, a rogue application would therefore need to overcome three levels of complexity—1) optical password authentication, 2) configuration access password authentication, and 3) accurate use of low level table structures containing the configuration data. The optical password could be found at the utility or in Elster field tools used by that utility. The configuration access password is only used within Elster manufacturing tools which are not available to the utility. Per Elster's development and manufacturing processes, only authorized internal Elster primes have access to configuration settings and passwords; general manufacturing employees do not. Meter configuration settings are established during the manufacture utilizing specific internal tools designed for this purpose. Elster field tools (for example, Metercat) lack the ability to accept the configuration password and/or write configuration changes to a meter.

  In the unlikely event all three of these preventative measures are compromised, a detection log would be generated and reported. The detection log captures the date and time of the last configuration table write, providing the forensic data needed to show a change after installation. It is worth noting as well, that an authenticated and authorized userid and password are required to launch and access the Elster field tools (for example, Metercat).

- **Elster electric meters provide both tilt warnings and outage notifications to alert the utility of possible physical tampering with the devices.** Meters that show a pattern of power outages that do not match neighboring meters cue the utility to schedule a site visit or look for other evidence of theft. Elster gas modules also provide tilt warnings. Water and gas modules are battery powered devices, so outage notifications do not apply. Other means exist for water and gas utilities with EnergyAxis to detect leaks or inappropriate use (such as illegal water use during drought restrictions).

- **It is nearly impossible to pierce an Elster meter enclosure to access the serial port without setting off either the tilt or the outage notifications.** In the event (theoretically) an individual were able to open a meter without removing or tilting it, that person would have to possess a detailed expert knowledge level of the specific device (as not all meters are the same) to enable successful connection to a serial port without damaging a laptop (or injuring themselves).

  If such access were gained, the serial port grants read only permission, the same as the successful authenticated access using the optical port. Attempting to modify meter data by penetrating the meter itself would be extremely dangerous and require far more detailed knowledge of the physical construction of the meter, as well as the internal firmware operation and data structures.

- **Elster electric meters provide host-based intrusion detection logging to detect and log all potential remote meter access attempts.** Utilities can quickly respond to cyber security threats to the meters in the field. The EnergyAxis-enabled meters provide the following:

  - Count of the number of invalid optical port access attempts (access attempts with an invalid optical port password)
  - Count of the number of invalid radio access attempts over the EA_NIC (access attempts with an invalid LAN encryption key)

- Access warning status flag if either the optical port or radio invalid access attempt counts exceed a configurable threshold. The EA_NIC can be configured to immediately transmit an exception message when this status flag is set
- A status flag to indicate a configuration table was written. The EA_NIC can be configured to immediately transmit an exception message when this status flag is set
- The date and time of the last configuration table write

In the event of a potential security threat 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.

Elster encrypts the meter firmware to further 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 EnergyAxis System completes the encryption of the firmware with a unique encryption key which is different than that used for encrypted communications. The EnergyAxis system solution provides Wide Area Network (WAN) and Local Area Network (LAN) encrypted communications (using NIST approved AES-128) to provide additional security strength during transport. Each device utilizes a unique crypto key to encrypt the communications (differing from other crypto keys used for re-keying or firmware decryption). EnergyAxis System release 7.0 currently provides all of these required characteristics.

In additional to technologically based security, organizations involved in Smart Grid systems must also apply internal security policies and procedures to safeguard and limit personnel access to mission critical information. Elster employs such personnel security safeguards as:

- Employee background checks
- Access control, monitoring and logging to:
  - physical locations (for example, buildings, labs, equipment, etc.)
  - sensitive internal documents and data
  - released product images (firmware and software)
  - encryption techniques and crypto keys
  - utility specific configuration data
  - utility remote networks
- System verification and testing of secure solutions

Remote theft detection and revenue protection

Utility security personnel currently rely on tips from employees and the public to find electricity theft. Following up on those tips is a labor-intensive process that, unfortunately, involves investigating many false leads along with the productive ones.

Detection techniques internal to the revenue meter itself, such as the outage or blink count, have limitations. Blink counts infer theft by detecting that a meter has been de-energized more often than its neighboring meters, thereby implying that the customer has removed the meter to tamper with it or to install jumpers around the meter base. A limitation of blink counts is that they cannot detect a common theft technique involving live tapping of the customer service drop wires ahead of the meter.

Remote detection and measurement of electricity theft is one of the challenges that inspired Elster to develop transformer meters such as the Elster Low Voltage (LV) transformer AGInode™ device. The LV AGInode device is designed for secondary outputs of pole- and pad-mounted distribution transformers. These types of devices have been especially effective in detecting theft associated with marijuana-growing operations in residential premises. For some electric utilities, such operations account for 99 percent of electricity theft.

This more definitive theft detection technique uses such devices as the AGInode to measure the full energy output of a distribution transformer and then compare that metric to the sum of the energy consumption registered in the meters supplied from that transformer. After factoring in secondary distribution line losses and any unmetered loads, such as streetlights, the full output of the transformer should roughly equal the consumption of customer meters. Missing energy is direct proof that one or more customers are stealing.

With transformer meters and energy inventorying, theft can be positively identified and isolated down to the distribution transformer serving the offending customer. Regardless of how the theft is attempted — meter tampering, meter inverting, jumpers around the meter, tapping in ahead of the meter — transformer measuring will detect the missing energy that represents theft. By comparing location data with other incidental evidence

such as blink counts or unusual consumption patterns, the utility can easily narrow down the list of accounts to be investigated before sending a technician into the field. Data from EA_Water or EA_Gas modules can be aggregated to track leaks or theft of water or gas.

Utilities can also move monitoring nodes onto the feeder, such as installing Elster's MV overhead line AGInode device. These devices, which measure the flow of energy through a point on a medium-voltage line, can be placed at regular intervals, and utility engineers can choose the number of customers between them. The difference between readings of two MV overhead line AGInode devices represents the energy consumed in that section of the feeder. The energy-consumption number should match the sum of the energy consumption recorded by customer meters that are between the two MV devices. If it does not, then the circumstances call for additional investigation.

Reference material

There are many facets to securing the AMI solution. Given the various access points (for example, WAN, LAN, HAN), it is no longer enough to just provide a secure meter. To provide a secure solution, the entire security offering must be examined to review and confirm a complete system solution is in place to provide the preventative measures required.

For additional details on how to provide a secure AMI system, refer to the white paper "AMI Security Considerations", also by the Author. For additional information on Elster's Advanced Grid Infrastructure (AGI) Initiative and how this solution provides extensive theft and loss detection and revenue protection, please reference the white paper "Applications of transformer and feeder monitoring with AGInodes".

EnergyAxis white papers can be downloaded at http://www.energyaxis.com/ea-inf-white-papers.asp

Summary

As utilities evaluate AMI systems, the industry's basic security requirements should be considered and the selected AMI system should provide superior security. Security is not a constant, but an evolving technology. Elster continues to operate in this mode, by researching and implementing enhancements to further secure our AMI offering.

The AMI system must be designed and implemented with security in mind. Applying third party security solutions as an overlay is not as effective; that is, security should be built in and not bolted on. To be successful, vendors and utilities alike must 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 into a secure AMI system solution. Additionally, an AMI system can reap significant benefits from deploying monitoring sensors such as the Elster LV and MV AGInode device to detect theft of electricity. The Elster meters and EnergyAxis System solution are designed and implemented with the secure attributes described herein, providing a secure AMI offering to meet these demanding requirements, while also providing solutions to detect theft and protect utility revenue.

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.

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

WP42-1010A