EnergyAxis System: Security for the Smart Grid

elster

NOTICE

The information contained in this document is subject to change without notice. Product specifications cited are those in effect at time of publication.

Elster shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Elster expressly disclaims all responsibility and liability for the installation, use, performance, maintenance and support of third party products. Customers are advised to make their own independent evaluation of such products.

Document number: WP42-1007A

Contents

Overview

As the smart grid evolves, so will the standards to allow inter-operability and defined security solutions. Many industry consultants have raised concerns around the potential of security gaps or holes within smart grid deployments, with some concerns pertaining to existing advanced metering infrastructure (AMI) solution offerings. This paper is intended to address the security concerns related to AMI systems and how the Elster EnergyAxis® System is architected to provide preventative measures against cyber security issues by examining each element of the system in detail. It is important to understand the EnergyAxis AMI network is comprised minimally of the EnergyAxis Management System (EA_MS), the wide area network (EA_WAN), EA_Gatekeepers, the local area network (EA_LAN), and meters (that is, REX2™ and A3 ALPHA®).

Below are several of the key concerns raised in the market place about security with a summary of the secure offerings provided by EnergyAxis to prevent these starting with the home and progressing back to the head-end control system:

- reverse engineering of the EA_LAN devices
- EA_LAN endpoint behavior monitoring
- EA_LAN attack prevention
- EA_Gatekeeper-to-endpoint communications
- EA_WAN communications
- EA_WAN security
- Head-end system security

EnergyAxis System security

Reverse engineering

In the EnergyAxis System, microcontrollers containing the firmware are locked such that the firmware cannot be read from the device. Firmware can be written, but:

- Internal to the device is a section of firmware known as the boot loader that cannot be overwritten
- Regardless of whether one section or the entire firmware image is written, the boot loader verifies the new downloaded section, *and* the entire image is validated. In addition to satisfying all security requirements, one would have to have knowledge of the complete firmware image in order to attempt to modify or load a new image.
- The meter will not attempt to switch to a new firmware image until the new image is validated.

LAN endpoint behavior monitoring

Experts are concerned that by monitoring LAN endpoint messaging behaviors, rogue devices could mimic network messaging patterns and send disruptive messages to other devices in the utility's AMI network. In the EnergyAxis System, an endpoint device, when energized, will autonomously send only event messages (for example, a power restoration message) and time request messages. An endpoint device will not perform any other communication task unless such task is securely initiated by a gatekeeper. Metering data is never sent unless requested by another device, and firmware within endpoint devices never initiates control messages to other network devices.

LAN attack prevention

The EA_LAN uses frequency hopping spread spectrum (FHSS) communications, which provides an inherent level of security not found in single channel systems. The FHSS technique is often used for military communications due to inherent security features of FHSS communications. FHSS uses multiple channels in a random hop sequence for data transmission making it difficult to eavesdrop and intercept messages. In the EnergyAxis System, the hop sequence is per device (not common to all devices), increasing the difficulty to predict the channel for the next packet in a communication sequence. All EA_LAN communication is checked and authenticated and beginning with EA_MS Release 7.0, AES-128 encryption will provide a security layer on top of FHSS.

In addition to the security techniques designed to prevent unauthorized access, Elster's REX2 meter endpoint provides host based intrusion detection logging to identify attempts to breach the endpoint and include:

- 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 (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 endpoint can be configured to immediately transmit an exception message when this status flag is set.
- A status flag to indicate a table write

  The endpoint can be configured to immediately transmit an exception message when this status flag is set
- The date and time of the last table write
- A tilt warning if the meter is removed from the installation site

  The endpoint transmits this information in the outage message to differentiate an outage from a tamper event

Some security consultants have implied that LAN messages can be sent to change device behavior or control a device. In the EnergyAxis System, this is *not* possible. Gatekeepers do not accept LAN requests that cause them to perform control or configuration operations to devices in the LAN. For example, a gatekeeper will not accept a LAN message that would cause it to open a service control switch on a LAN device.

In the EnergyAxis System, exception data and events are pushed from the endpoint device; but meter register and interval data are retrieved by the gatekeeper through a request and response communications session with endpoints. This makes it practically impossible to spoof a meter and present false data to the system. With the introduction of encrypted LAN communications in EA_MS Release 7.0 and later, the endpoint must be able to decrypt requests and encrypt responses to allow for communications over the EA_LAN.

EA_Gatekeepers are typically accessed remotely over the EA_WAN, but they can also be accessed locally over the optical port. Local access using the optical port requires an optical port password, which is set at the factory using the customer provided Metercat™ program. Optical port passwords can be changed using Metercat (changed locally over optical port or remotely using the WAN), and it is recommended that the utility maintain a policy of disclosing passwords for meter access on an as-needed basis.

Gatekeeper-to-endpoint communications

In the EnergyAxis System, messaging between the gatekeeper and endpoint is transmitted over the EnergyAxis protocol using ANSI C12 protocol for table read, writes, and function executions. Gatekeepers are the masters of the LAN communication sessions, and each message is authenticated for validity.

EnergyAxis commands (that is, functions) to an endpoint can only be initiated through the WAN interface. A LAN message received by the gatekeeper cannot cause the gatekeeper to issue a control command to a meter.

EnergyAxis endpoints only initiate communications to a gatekeeper to report an event or alarm condition (C12 “Report Exceptions” function). The gatekeeper stores the data from the function and sends an acknowledgement to the device to clear the event.

EA_LAN communications between the gatekeeper and endpoint are sessionless, and each communication must be authenticated for it to be acted upon.

With EA_MS release 7.0, gatekeeper firmware version 6.0, and REX2 meter firmware version 3.0, AES-128 encrypted LAN communication is provided. AES-128 encryption provides the additional integrity verification of each message between the Gatekeeper and meter. Unique AES encryption keys per LAN device further increase the strength and decrease the capability to infiltrate LAN communications.

Gatekeeper WAN communications

EA_Gatekeepers use ANSI C12.21-based security. The gatekeeper's WAN access is authenticated (2-way authentication) using DES encryption of a randomly generated token. Given C12.21 protocol is session-based, the EA_WAN sessions (EA_MS-to-gatekeeper) have a timeout to release the session if not kept open by communications (that is, EA_MS requested action), reducing the potential threat of session exhaustion. Encryption of the C12.21 data transmitted between the gatekeeper and EA_MS is dependent on the underlying WAN (GPRS/EDGE/HSDPA, CDMA/1xRTT/EVDO, etc.), which is commonly provided by communication carriers.

With the introduction of WAN interface cards (WICs) in EnergyAxis System release 7.0, additional security is provided with the inclusion of ANSI C12.22. WAN access is authenticated and data is encrypted using AES-128 encryption per ANSI C12.22 standards. Each gatekeeper has a unique crypto key used for WAN encrypted communications.

Communications between EA_MS and Gatekeepers is sessionless, per ANSI C12.22, and each communication must be authenticated for it to be acted upon.

EnergyAxis System release 7.0 also provides an infrastructure to manage WAN security keys. When keys are changed on the EnergyAxis network (as required by utility security policies), a unique re-keying key (different than the data crypto key) is used on a per gatekeeper basis to encrypt the communication, adding an additional layer of security.

WAN network provider security

For wireless WANs, telecommunication companies use private networks and encryption to secure data transmissions between gatekeepers and EA_MS. The wireless WAN modem in the gatekeeper has password protection and supports custom access point nodes (APNs) making the modem's IP address private and not exposed to the public Internet. Also, GPRS devices can be set up on custom APNs and made to appear as if they are from within the utility intranet so that the IP address is inaccessible from outside the corporate intranet.

Head-end system security

The EnergyAxis Management System (EA_MS) has a number of security mechanisms built in to ensure system security.

Access/Authentication

Each EA_MS user is authenticated using a built-in user name and password mechanism. Passwords can be forced to expire periodically by the system administrator. If necessary, user authentication, access control, and identity management can be tied to an enterprise LDAP directory or other central scheme. The EA_MS resides within the corporate intranet, and thus all security mechanisms that the utility has in place for its enterprise security are the primary mechanisms for securing access to the EA_MS.

Authorization

EA_MS provides role-based access control for each user: system administrator, meter services user, billing and cis user, and report only user. Each user obtains access to the system via a unique username/password, with access to system functions limited by the assigned role.

Auditing

The audit report and activity monitor enables the system administrator to:

- View logs of each user's activities
- View specific meter, account etc. that were involved in the transaction and the parameters sent

Every operation executed by a user from the web application, along with timestamps and user IDs is logged and can be reported. Programmatic interfaces and batch operations are also logged in a similar fashion.

Data transfer

When needed, data transferred between the EA_MS and other enterprise systems can be encrypted using either symmetric or asymmetric encryption algorithms. Elster currently utilizes RSA with OAEP (RSA/OAEP) for the asymmetric cipher algorithm and triple DES (DESede) for the symmetric cipher algorithm for data being exported from the EA_MS.

EnergyAxis Security Enhancements

Release 7.0

With the delivery of EnergyAxis System release 7.0, further security enhancements are included increasing the overall network strength, while reducing the complexities to manage it. The following is a high-level summary of these attributes:

- Research, analysis and implementation of many industry standards meeting NIST stringent guidelines were utilized in the architecture and design of the EnergyAxis system

  Examples of these include FIPS 140-2, FIPS 197, ANSI C12.22, NIST SP 800-57, Smart Energy (SE) 1.0/1.x, OpenSG AMI-SEC, etc.

- ANSI C12.22 protocol support with the introduction of the Elster WAN Interface Card (WIC)
- C12.22 WAN sessions are authenticated and encrypted using AES-128 per ANSI C12.22 standards

  Note: AES-128 was chosen given its characteristics to best meet low power, low resource device needs, while (via NIST) providing a 20+ year system roadmap to meet security needs)

- EnergyAxis LAN sessions are authenticated and encrypted using AES-128
- Each C12.22 WAN based gatekeeper has a unique crypto key utilized to encrypt data (no single or common shared network key)
- Each EnergyAxis LAN endpoint (REX2 meter, A3 ALPHA meter) has a unique crypto key utilized to encrypt data (no single or common shared network key)
- EA_MS 7.0 will provide an infrastructure (Security Manager with restricted access to only the Security Administrator) to manage WAN security keys, allowing WAN keys to be changed to meet utility security policy needs (either automatically generated or manually entered 16-byte value)
- WAN key generation is provided in part by a NIST approved cryptographically secure random number generator at the Security Manager (that is. RSA X9.31 PRNG (Pseudo-Random Number Generator))
- Unique re-keying encryption keys are utilized per gatekeeper to encrypt new seed values communicated from the EA_MS to each gatekeeper (keys are never transmitted over the communications network, and seeds are never transmitted in the clear)

- Two levels of secure C12.22 communication are provided in EnergyAxis: authentication with plain-text sessions; authentication with encrypted sessions
- Ability to enable and disable WAN security at the security manager on a per gatekeeper basis (as well as across all)
- Ability to enable and disable LAN security (key management will follow in an upcoming release)

Planned security enhancements

In future EA_MS releases, additional security enhancements will be provided to further increase the system level security strength. Enhancements planned include the following:

- Security Manager GUI enhancement to manage LAN security keys and allow LAN keys to be changed to meet utility security policy needs (either automatically generated or manually entered 16 byte value)
- LAN key generation is provided in part by a NIST approved cryptographically secure random number generator at the Security Manager (i.e. RSA X9.31 PRNG (Pseudo-Random Number Generator))
- Unique re-keying encryption keys are utilized per meter to encrypt new seed values communicated from EA_MS through the gatekeeper to each meter (keys are never transmitted over the communications network, and seeds are never transmitted in the clear)
- Metercat support for WAN C12.22 AES-128 encrypted communications
- EA Inspector support for EA LAN AES-128 encrypted communications
- EA Inspector and Metercat secure synchronization with EA_MS when LAN or WAN security keys are changed/managed
- EA Inspector and Metercat added security audit logs and upload to EA_MS for auditing

Conclusion

In conclusion, the Elster EnergyAxis AMI system provides superior security. By design, the EnergyAxis System was designed and implemented with security in mind, not simply applying third party solutions as an overlay (that is, built in and not bolted on) as is the case with certain competitive offerings.


elster