> Itron white paper

OpenWay® Security Overview

Scott Palmquist
Sr. Product Manager

Ido Dubrawsky
Sr. Principal Systems Engineer

Introduction

The smart grid represents an evolution transformation in the way electricity is delivered from suppliers and the way it is used by consumers. With a smart grid, electricity is controlled throughout the delivery system via a two-way digital communication channel to appliances within a consumer's premise to save energy, shift peak load, reduce costs and increase reliability. To that end, smart meters play a key role as a communication, monitoring and control device in the overall evolution of the power distribution system. With this evolution comes significant challenges in ensuring that the smart grid is both secure and reliable.

Smart grid and smart metering systems promise to deliver on a wide variety of capabilities, including dynamic pricing by electric service providers (ESPs); increased customer control of their energy usage and ESP rates; fine-grained demand-response by ESPs in conjunction with customers; and improved reliability of the electric grid. A well-designed security architecture is an absolute requirement in order to provide these capabilities. Threats to smart grid systems come from a wide range of sources, or "threat agents." These include unethical customers, curious and motivated eavesdroppers as well as active and passive attackers (LeMay, Gross, Gunter, & Garg, 2007). The motivations of these threat agents vary from publicity seekers to those with a focused and directed agenda. Regardless of the specific attacker's motives, threats can include unauthorized access to communications; interruption of service; and injection of commands into the system to gain access and control either core systems or meters.

The ultimate concern, from a national security perspective, is one where a rogue or enemy state or a terrorist organization cripples the electric power grid during a conflict or as part of an organized attack. To address these concerns, smart grid vendors are developing secure, resilient architectures that are designed to withstand both casual and focused attacks. These architectures require strong authentication and encryption to protect both core systems as well as meters from both amateur and sophisticated adversaries.

The electric grid has changed dramatically over the past 20 years and will change even more in the years ahead. In the past, the standard meter on the grid was a very simple device measuring monthly electricity usage that required manual, visual readings by meter readers. Over time, meters became more sophisticated to include a radio broadcast capability where the meter can be read without physically approaching it. More recently, automated meter reading (AMR) has evolved into advanced metering and smart grid initiatives where meters can now receive commands as well as requests for meter readings over a radio-based local area network (RFLAN), as well as provide data at regular intervals to the utility billing system. These capabilities are necessary as the power generation grid evolves to include a larger portfolio of renewable and/or distributed energy generation sources such as solar and wind.

Regulatory and Industry Drivers

As smart grid and smart metering initiatives have gained momentum, and utilities look to deploy these technologies more broadly, an obvious concern turns toward the security of these systems. One of the key factors that drive this concern is the North American Electric Reliability Corporation (NERC), which has been chartered by the Federal Energy Regulatory Commission (FERC) to develop and drive critical infrastructure protection (CIP) requirements for the electric grid. The NERC CIP requirements cover a wide range of topics—from sabotage reporting to cyber security and critical cyber system identification to cyber security to personnel training, as well as other topics. These requirements are written in a broad enough fashion to allow the energy providers the ability to tailor their cyber security policies in order to be in compliance.

While the NERC CIP guidelines do not explicitly state what is or what is not a critical cyber asset (CCA), it does provide sufficient guidelines that could include most smart grid deployments as CCAs. NERC CIP-002 provides the criteria for determining whether something is or isn't a critical cyber asset. These criteria include:

- Control and backup control centers
- Transmission substations
- Generation resources
- Systems and facilities critical to system restoration.
- Systems and facilities capable of shedding 300 MW or more.
- Any additional assets that support the reliable operation of the Bulk Electric System (North American Electric Reliability Corporation, 2009)

In addition to NERC, other organizations have been developing guidelines for smart grid security. These include the National Institute of Standards and Technology (NIST) and the AMI-SEC Task Force (TF). NIST published NIST IR 7628 in September of 2010 covering smart grid security guidelines. This work covers both an overall smart grid security strategy as well as privacy concerns in a smart grid. The AMI-SEC Task Force published version 2.0 of the AMI Security Profile in June of 2010.

NISTIR 7628

The NISTIR 7628 – Guidelines for Smart Grid Cyber Security – is divided into three volumes. Volume one covers smart grid security strategy, architecture and high-level requirements; volume two covers privacy in the smart grid; volume three provides supportive analyses and references for the overall work. One key aspect that must be considered when evaluating the information in the NISTIR document is that the information in the report is written to provide organizations planning a smart grid deployment with guidelines. The NISTIR does not prescribe particular solutions but rather requires organizations to leverage the information in the documents and develop their own cyber security approach as well as a risk assessment methodology for the smart grid. It is essential that any

utility looking to deploy their own smart grid infrastructure should leverage the information in the NISTIR 7628 documents in order to develop their cyber security policies with respect to smart grid and AMI.

NERC Critical Infrastructure Protection

NERC CIP is currently divided into a series of nine documents – NERC CIP-001 to NERC CIP-002. These NERC CIP standards specify requirements that are policy and process focused rather than technology focused. The key NERC CIP documents that apply most directly to a smart grid or AMI deployment include the following:

- NERC CIP-002 – Critical Cyber Security Asset Identification
- NERC CIP-003 – Security Management Controls
- NERC CIP-005 – Electronic Security Perimeters
- NERC CIP-006 – Physical Security of Critical Cyber Assets
- NERC CIP-007 – Systems Security Management
- NERC CIP-008 – Cyber Security – Incident Reporting and Response Planning

It is important to note that the requirements in the NERC CIP standards do not speak to a specific technology directly but rather help drive the necessary technology standards.

Smart Grid Threats

A smart grid deployment presents significant challenges to the security architect in providing a defense against a wide variety of threats. The majority of the smart grid components—the smart meters themselves—are located *at* the end user's facility (either home or business), and are considered to be in an extremely hostile environment. Theoretically, an attacker can have nearly 24/7 access to the component in order to identify a vulnerability or devise an attack. In addition to environmental and physical threats, smart grid components must also contend with a wide variety of electronic threats such as hacking and denial of service. Given the nature of the smart grid, there are several general categories of attack against it. These threats are shown in Figure 1 and pertain to the following smart grid/AMI system components:

- The smart meters
- The RFLAN
- The wireless devices bridging the RFLAN to the wide area network (WAN)
- The WAN providing backhaul for the RFLAN
- The collection system head-end

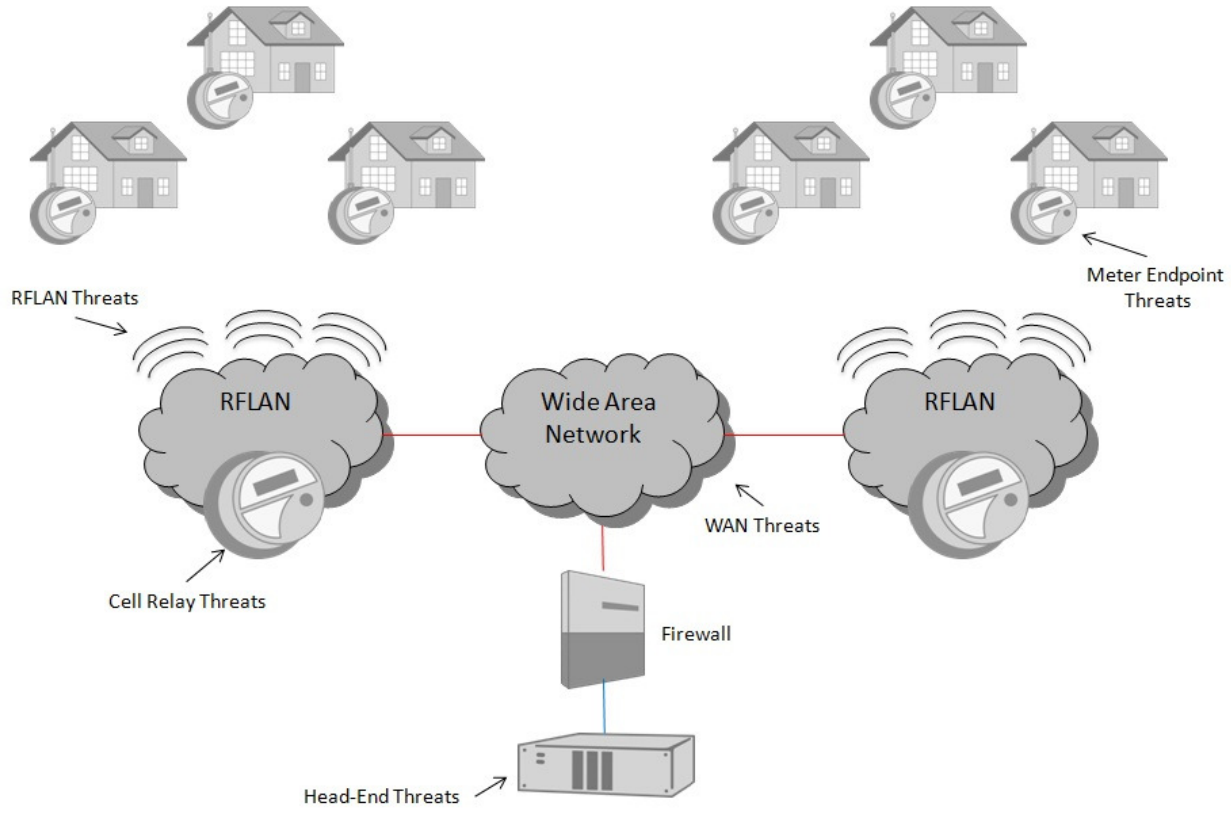

Figure 1 – Potential Threat Points in an AMI Deployment

Given the unique nature of smart grid deployments operating in an exposed and actively hostile environment, it is critical that the security of the components be comprehensive and of the highest caliber and scrutinized in detail. To address these threats and needs, smart grid components must leverage strong software and hardware development processes that include threat modeling, a software development lifecycle and security testing to identify potential, undiscovered vulnerabilities and to remediate them before the components are released to the market.

OpenWay Architecture

The OpenWay architecture is designed to provide flexibility as well as robust security in a smart grid deployment. AMI systems could be classified as CCAs according to NERC CIP-002-3, as they often comprise systems capable of automatic load shedding of 300MW or more (R1.2.5) *and* because they utilize a routable protocol to communicate outside the Electronic Security Perimeter (R3.1) (North American Electric Reliability Corporation, 2009). Itron's OpenWay architecture is designed to address the specific security requirements of a smart grid deployment.

The OpenWay solution consists of several primary components: OpenWay CENTRON® meters, OpenWay Cell Relays and a head-end system known as the OpenWay Collection Engine. Figure 2 shows the OpenWay architecture's Enhanced Security Configuration. Together, all of these components play in integral part in securing a deployment and these components and associated security measures are discussed in more detail below.

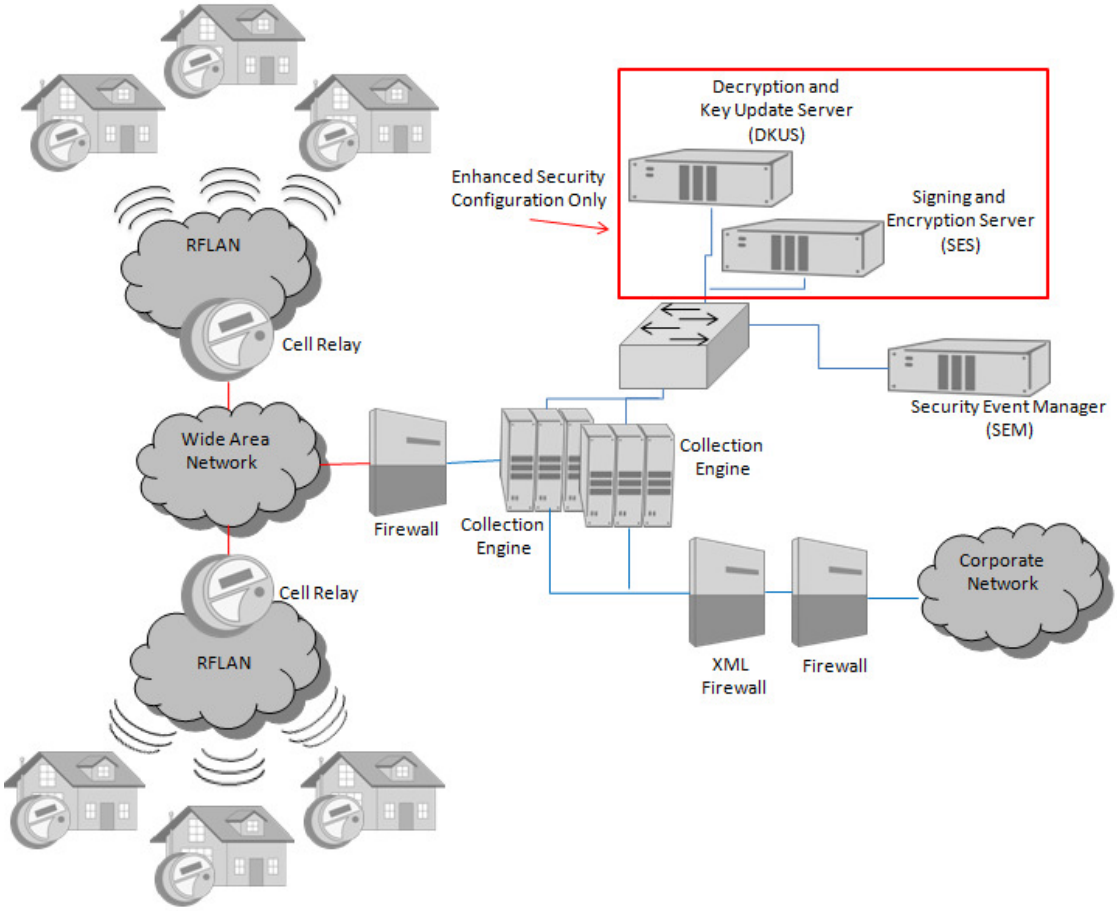

Figure 2 – Itron's OpenWay Smart Grid Architecture Enhanced Security Configuration

Collection Engine

The OpenWay collection engine is the core of the OpenWay solution. Built upon the Windows .NET framework, the collection engine provides both inbound data collection services from the infrastructure as well as outbound meter command and key management. The Collection Engine is responsible for supporting the integrity of the system.

RFLAN and Cell Relay Communications

The OpenWay radio frequency LAN (RFLAN) is a frequency-hopping RF network that utilizes the 900 MHz ISM band. Messages are transmitted in accordance with the ANSI C12.22 protocol, and are encrypted using 128-bit AES keys. The command messages are also signed using ECC public/private keys.

The Collection Engine interfaces with meters through Cell Relays. Firewalls are recommended between portions of the system; however, the OpenWay architecture requires full two-way communication between the Collection Engine and the Cell Relay. The Collection Engine can be placed behind a firewall and allow traffic on port 1153 (C12.22) to pass through. The Collection Engine needs to be able to access its database as well as the enterprise management system and the meter data management (MDM) application. These applications may be behind additional firewalls, or they may be on the same network as the Collection Engine itself, provided that the Collection Engine has full two-way access to the appropriate ports for data transfer. This initial communication is done using TCP/IP. As either the Collection Engine or the Cell Relay can initiate communications, both products must accept incoming C12.22 messages on TCP/IP port 1153. The Collection Engine listens on port 1153 for C12.22 communication and monitors the network for Web services calls.

OpenWay CENTRON Meters

The C12.22 architecture plays an important role regarding the implementation of security. The major benefit of the design of a C12.22 network is that the Collection Engine interfaces at an application level protocol layer, enabling both session- and sessionless-based communication directly to the meter register. Unlike designs tied to a single communications network, with OpenWay the security architecture does not need to change if the communication architecture changes. OpenWay Security protects the entire communication from the head-end-system into the processor in the meter, giving the utility flexibility to select an underlying communications' infrastructure appropriate to the utilities strategic needs.

OpenWay also benefits from the ability to perform broadcast and multicast communications to meters, minimizing the amount of messages that require encryption and processing, as opposed to sending multiple messages point to point to meters.

Security Event Manager

As with any deployed IT system security, events must be monitored and evaluated in order to determine if a potential security breach has occurred, and if so, how to appropriately respond to it. One of the key features of a security event manager (SEM) in a smart grid deployment is the ability to accurately identify a developing or ongoing attack against the system. Attacks can vary considerably but include such threats as:

- An attacker attempting to shut off a population of meters
- An attacker trying to obtain key material from the system

- An attacker attempting to execute a denial of service attack against a population of meters
- An attempt to hijack or spoof on or more trusted systems
- Attempts to recover key material from endpoints
- Attempts to modify an endpoint to change metrology or other parameters

The above events represent a sample of possible events that should be monitored by a security event manager.

A SEM is deployed to collect, correlate and analyze audit events in order to detect intrusions and attacks. Examples of audit events in OpenWay include but are not limited to: endpoint reprogramming, endpoint authentication failure, signature verification failure, message decryption failure, home area network (HAN) traffic rate exceeding threshold, device firmware upgrade and spurious HAN and local area network (LAN) messages. These events are primarily generated at the meter or from wide area network (WAN) devices and sent to the OpenWay Collection Engine, which then sends the events to the security event monitor.

OpenWay Security

OpenWay Enhanced Security provides for both the confidentiality of data and commands, and also provides data integrity and non-repudiation for commands from the Collection Engine to the endpoints. New threats and looming regulatory requirements have driven the need for a higher level of security. To fulfill that need, OpenWay provides a strong security layer in a smart grid deployment known as Enhanced Security. Enhanced Security leverages public key cryptography in addition to symmetric key cryptography to secure the communication between the Collection Engine and the meter endpoint. Asymmetric cryptography is used to provide digital signatures for command verification and symmetric cryptography is used to provide data confidentiality. OpenWay also supports the following security standards for security controls and functions:

- NIST FIPS 197 approved encryption algorithms (AES)
- NIST FIPS 186-3 approved signature algorithms (ECDSA)
- NIST FIPS 180-2 approved hashing algorithms (HMAC-SHA-1,HMAC-SHA-256)

Collection Engine with Enhanced Security

The Collection Engine is responsible for supporting the integrity of the control of the system. As a result, asymmetric cryptography is supported for command and control messages. Every node in the system has a set of asymmetric keys that are used for authentication and non-repudiation functions. Initial meter registration involves a key exchange process that establishes mutual authentication. When sending out messages, the C12.22 payload is signed and encrypted before being wrapped it in the C12.22 protocol. This is accomplished by the integrated Signing and Encryption appliance. As control over this operation is absolutely critical to ensuring control over the system, the Signing and Encryption Server will never expose the signing key. When the meter communicates information

upstream to the Collection Engine, the C12.22 messages are encrypted to protect the confidentiality of data and decrypted by the DKUS appliance. An overview of this exchange is depicted in Figure 3.

Enhanced Security with OpenWay CENTRON Meters

With OpenWay Enhanced Security, cryptographic processing at the meter is done using algorithms recommended by the National Security Agency under their "Suite B" recommendations for commercial security. Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. Leveraging enhanced security provides not just confidentiality for the information flow between the Collection Engine and the meter but also message integrity. This makes it considerably more difficult for an attacker to inject falsified messages into the system either from the Collection Engine to the meter or from the meter to the Collection Engine. Each OpenWay CENTRON meter has a unique private key, which is used to validate digitally signed commands received from the Collection Engine and to authenticate the meter to the Collection Engine during initial meter registration.

Messages from the Collection Engine to the Meter

Messages from the Collection Engine to the meter are encrypted using an AES-128 bit key and signed using an ECC-283 bit key as shown in Figure 3. The OpenWay security architecture allows for broadcast and multicast communications, where a single message from the Collection Engine can direct behavior for a large number, potentially millions, of meters simultaneously as well as for unicast communications. Signature verification and decryption is pushed out to the meters in a distributed fashion. The meter processes these security functions in milliseconds once the command is received. Thus, while each meter will need to validate the signature on the message to ensure its authenticity, those validations occur in parallel resulting in very little latency being added to a group operation no matter how many meters are involved. At the collection engine, the system can easily sign and encrypt 200 operations per second.

Messages from the Meter to the Collection Engine

Messages from the meter to the Collection Engine are encrypted using an AES-128 bit key to provide customer data confidentiality as shown in Figure 3. The OpenWay architecture is optimized such that an IP load balancer shapes the incoming traffic and distributing it equally among the Collection Engine subcomponents for processing. The Collection Engine removes the network portion of the packet and passes the payload to the OpenWay Decryption and Key Update Server for processing. This appliance is scaled to decrypt 20,000 messages per second, which maps out to over a million meters per minute processing.

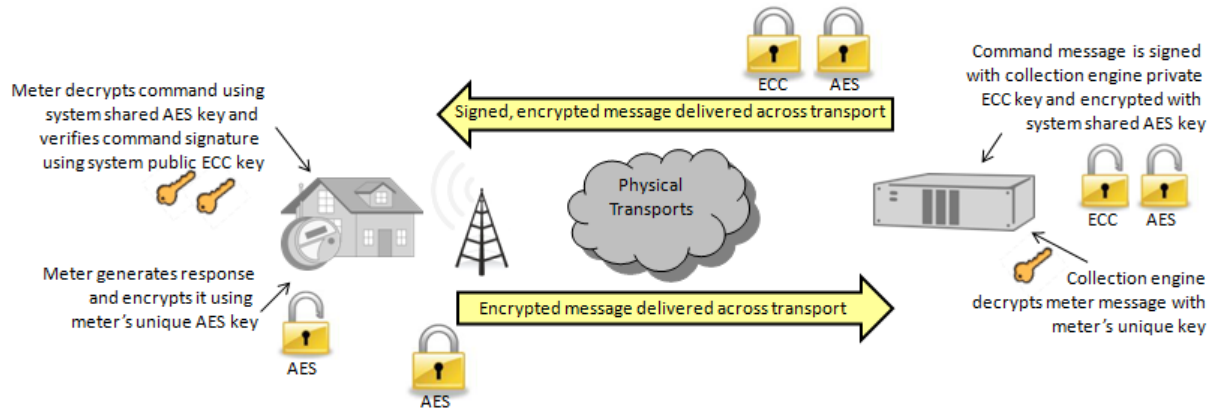

Figure 3 – Enhanced Security in OpenWay

The security architecture was designed specifically for OpenWay operational use cases centered on performing multiple functions such as meter data collection, demand response and remote disconnects simultaneously for 10 million meters or more. It is important to note that while command and control messages are signed all command, control and data messages are encrypted. In addition, the OpenWay SES and DKUS security appliances are designed so one appliance pair can handle the message traffic of a system with 10 million devices. Customers need only install additional appliances for high availability and disaster recovery, not performance.

Signing and Encryption Server (SES)

The Signing and Encryption Server is responsible for securing command messages being sent from the Collection Engine to the meters. As a result, the number of keys managed for these messages is quite small, potentially as little as two keys that need active control. However, these keys must be very tightly controlled to ensure that the system is not compromised. The private signing key of the Collection Engine is never exposed in raw form, though there are facilities to back it up. To protect the keys, the Signing and Encryption Server includes an integral hardware security module (HSM). The HSM is FIPS 140-2 level 3 compliant, meaning that it is meets the government guidelines to protect the keys it contains against both physical and electronic attacks.

Decryption and Key Update Server (DKUS)

This component provides rapid message decryption and comprehensive key management. Messages coming from the meters to the Collection Engine need to be quickly decrypted. In a large-scale OpenWay implementation, the system can decrypt more than 20,000 messages a second, each with its own unique key. While the messages are small, over the course of several hours, the system may need to decrypt messages using between 5 and 10 million unique AES keys. The solution must be able to quickly handle accessing millions of keys, decrypting thousands of messages and passing them on to the Collection Engine.

System Security

The OpenWay Collection Engine uses role-based security for authenticated users. Administrators can be assigned different levels of privileges with each administrator using an individual password. Administrators can also be integrated into Microsoft's Active Directory. Administrator web access to the Collection Engine is protected using X.509 certificates and TLS for session encryption. In addition, the Collection Engine is always installed in the utility's data center behind its firewall and intrusion prevention systems.

Data Management programs, such as a Meter Data Management System (MDMS), which access the Collection Engine to instruct the collection engine to issue a command to the meter endpoint, are authenticated through X.509 Certificates and the communications is kept confidential through the use of TLS. The Collection Engine's data management interface can also use Secure Assertion Markup Language (SAML) or Kerberos if these techniques are supported by the MDM.

Conclusion

In summary, OpenWay's security architecture is designed specifically for key security functions, without sacrificing the performance requirements that are needed for two-way command and control for AMI and smart grid network operations. The OpenWay security architecture provides customers the ability to comply with applicable NERC and FIPS requirements to protect their smart grid network. In addition, OpenWay security supports the operational requirements of OpenWay to support up to 10 million meters without impacting the system's performance managing upstream and downstream message processing. OpenWay's architecture also reduces the complexity around security through the use of C12.22 and node-to-node communication between the Collection Engine and the meter register.

Itron Inc.

At Itron, we're dedicated to delivering end-to-end smart grid and smart distribution solutions to electric, gas and water utilities around the globe. Our company is the world's leading provider of smart metering, data collection and utility software systems, with nearly 8,000 utilities worldwide relying on our technology to optimize the delivery and use of energy and water. Our offerings include electricity, gas, water and heat meters; network communication technology; collection systems and related software applications; and professional services. To realize your smarter energy and water future, start here: **www.itron.com**.

Itron Inc.
Corporate Headquarters
2111 North Molter Road
Liberty Lake, Washington 99019
U.S.A.
Tel.: 1.800.635.5461
Fax: 1.509.891.3355

Publication 100933WP-042/11