Solving the HAN Firmware Distribution Problem

Where we are today and where we must go

By Marcia Martin
October 2009

(303) 453-8380
info@greenenergycorp.com
www.greenenergycorp.com/smartenergy

Table of Contents

Abstract

Energy utilities are beginning to consider the deployment of consumer home-area networks that operate in conjunction with the Advanced Metering Infrastructure to enable consumers to actively and selectively monitor and control their energy consumption and participate in partnership with the utilities in demand management programs. As these deployments reach the millions of households in number, a network-based mechanism for distributing firmware updates and managing device compatibility must be found.

Many issues must be settled to accomplish this in a way that ensures the behavior of the entire HAN, in the presence of a device upgrade, is predictable. Standards and institutions must be established to preserve consumer autonomy while ensuring the security and availability of the Smart Grid. This whitepaper surveys the problem space and provides the reader with a basis for further investigation.

Why Worry about Firmware Distribution?

Providing the ability to remotely upgrade Home Area Network (HAN) devices used for energy management is a critical need for the Smart Grid. Why? – HANs were originally something of an adult toy, providing the means for homeowners to centrally and remotely control their high-end home video, audio, and lighting equipment. Home automation devices contained firmware, but it was supported by the AV reseller and the consumer Devices were upgraded, if at all, at the discretion of the consumer. Typically, they worked as installed for the life of the system.

Today, however, the same home automation technology is being put to a much more serious use – opening up a two-way channel of communication between the consumer and the public utility. This will enable consumers to better control their energy costs, and become the utility's partner in the crucial task of managing energy consumption to create a more stable, sustainable grid.

What can Energy Management HANs do?

An Energy Management HAN connects individual devices in the home to the Advanced Metering Infrastructure or AMI network. Utilities are deploying AMIs in major cities around the United States already. The AMI data communications network connects the utility meter on every house in the utility service area with the utility's data center, providing a two-way communications channel. The utility collects data about the home's energy consumption in more detail than has ever been possible. The utility can also transmit commands and information to the "smart" meter. However, the meter alone can't do much to affect the household's energy consumption. The smartest of smart meters have the ability to communicate with home-area networked devices inside the home. Connecting the smart meter to the HAN opens up a world of possibilities for home energy management. This energy management strategy can:

- Collect data about not only how much power the whole house is using, but determine which devices in the house are consuming, and when
- Display information to the homeowner about current rates, so that consumers can make informed decisions about when to perform high-consumption activities
- Alert consumers about upcoming maintenance events, anticipated peak consumption periods, and so on.
- Most importantly, communicate directly with individual smart devices in the home to remotely modify the home's energy consumption. This is called Demand Management. It will become an increasingly important tool for utilities in keeping the energy grid stable and available, and in controlling cost to consumers.

Managing the HAN as Critical Infrastructure

Now that the Home Area Network is playing a critical role not only in the household but in the community, it has to be managed in a different way from when it was just a toy. These are the three main differences to consider:

- **Security** — There was little motivation for anyone to "hack" a HAN when gaining access could, at worst, allow the hacker to turn the home's stereo on and off. But an Energy Management HAN could be collecting and transmitting data that consumers might wish to keep private between themselves and the utility. Worse, spoofing demand-response commands to many households at once could actually destabilize or damage the grid.
- **Availability** — As soon as consumers become dependent on the enhanced service levels they can enjoy with the Smart Grid, then they will consider it a service failure, for example, if their electric bill jumps because the devices in their home have failed to carry out their energy management policies. They will hold the utility responsible.
- **Currency** — Utilities will need to be able to manage households uniformly in order to maintain the security and availability of the energy management network. This problem becomes more complex if many versions of the several communications protocols they employ must be supported. Just as with the software on your business's desktops, everything works better when everyone's up-to-date.

Requirements on the Smart Grid

The critical need to maintain HAN Security, Availability, and Currency in the firmware on HAN devices imposes some requirements on the way utilities and energy service providers must deploy the data communications portion of the Smart Grid that enables connectivity between Home Area Networks and the utilities' or Energy Service Provider's network operations center (NOC).

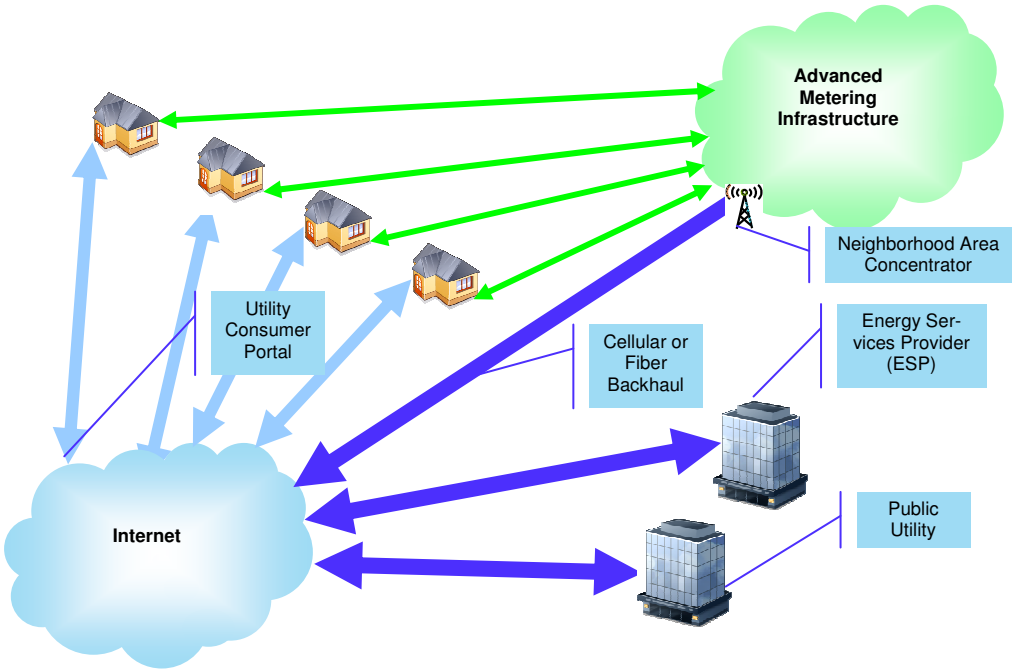
Enabling Firmware Distribution
What mechanisms need to be put in place to make it happen?

Need	Requirements	State of the Art
Standards	• HAN devices need to support a standard protocol for accepting a code load and restarting the device. • If NEMA SG-AMI 1-2009 requirements regarding code loads were applied by analogy to HAN devices, it would facilitate safe firmware upgrades.	• NEMA SG-AMI 1-2009 defines requirements for commanding smart meters to accept a network code load, but does not define a standard protocol. • Device vendors have proprietary methods. • Many HAN devices deployed today do not meet the analogous requirements.
Testing	• Nothing forces consumers to deploy only devices approved by their utility So industry-wide interoperability testing and certification is a must.	• Smart Energy Profile (SEP) is an emerging de facto standard for energy HANs. • On 9/14/2009 Landis+Gyr announced a HAN device interoperability certification program to SEP 1.0. • SEP 1.0 does not specify any code-load protocol.
Network	• All energy management HANs must be connected to a network that can support the load from firmware updates and its normal workload. • Two candidate networks are the Internet and the AMI network.	• Connecting HANs to the internet is expensive. • AMI infrastructures today are proprietary and diverse Most can support networked firmware updates, but some need careful management to do so.
Owner	• Some entity must control distribution of firmware updates to maintain Security, Availability, and Currency in the utility service area.	• "Who owns the HAN?" • Homeowners feel they do. • Utilities want easy support. • Manufacturers want control. • NEMA SG-AMI 1-2009 implies central distribution center.

Emerging Deployment Model

A workable combined model for maintaining energy management HANs consistently within a utility service area seems to be emerging.

HAN support deployment model
The public utility, commercial Energy Service Providers, and consumers will be partners in maintaining the home delivery segments of the Smart Grid, including smart devices inside the home.



In this picture, the home area networks in these homes are connected to the Advanced Metering Infrastructure via the utility meters on their houses. AMI networks lack the uniformity and transparency we've become used to on the World Wide Web. A number of different vendors are competing to supply utilities with network infrastructure for their Smart meters. Several different physical architectures have already been deployed in the United States and Europe. In the US, a plurality of vendors favors the RF Mesh architecture. This has the lowest deployment cost, and poses relatively few technical and regulatory issues because the RF signal used is in the unregulated 900 MHz band, the same frequency band used by older cordless home telephones.

Emerging Deployment Model *(continued)*

The table below summarizes the leading AMI network architectural models. RF Mesh AMI networks are of most concern it they are to be used for firmware distribution, because of their low effective bandwidth compared to the other models. If each firmware load is broadcast to all meters, regardless of whether the household served contains a device to receive it, then perhaps RF Mesh AMIs can be used for this purpose. However, using connection-oriented download strategies to target individual devices within the household, and to control the order in which devices are updated, is much more problematic, because it would be easy to overrun the network. A carefully chosen distribution strategy taking advantage of detailed knowledge of the network topology would be required.

Comparing AMI Network Types

Network Architecture	Characteristics	Vendors
RF Mesh	• Most common in the USA • Lowest effective bandwidth of any AMI architecture • 900 Mhz RF band • One “concentrator” tower for every 50 -5000 meters • Maximum raw bandwidth meter to meter is about 20 kbps, or only 2000 characters per second • Effective bandwidth is much less in a busy network	• Itron • Landis+Gyr • Silver Springs • Trilliant • Elster
Cellular	• More popular in Europe • Some RF Mesh solutions in the US use Cellular backhaul • 3G data rates exceeding 36MB/sec	• Echelon • Smart Synch
Power Line (PLC)	• Bandwidth can be comparable to broadband internet • Expensive devices to modulate signal on power line • Can cause RF interference • Good for rural areas	• Echelon • Enel

Emerging Deployment Model *(continued)*

To date, utilities have not attempted to develop their own software to manage the data collected by the AMI infrastructure, whether or not it includes HAN extensions. Commercial entities that do this in partnership with utilities are termed Energy Service Providers (ESPs). Some AMI networking vendors also provide the energy management software services, and so are also ESPs. Other ESPs, like Tendril, do not manufacture or deploy AMI networks or devices, but work in partnership with the hardware vendors. Regardless of the supply model, it is the ESP which ultimately has the closest working relationship with the utility.

Data collected from HAN devices is transmitted over the AMI network, which is connected to the Internet backbone by means of some sort of concentrator . The concentrator may reach the Internet either via a cellular wireless connection or have a direct Ethernet connection to the fiber backbone. The data is collected at a Network Operations Center run by the ESP The ESP carries out energy management policies set on the one hand by utilities (rates, demand management advisories) and on the other hand by consumers (home energy policies such as acceptable temperature ranges for the home, times of day when the utility may shut off some devices such as HVAC, or goals for energy savings). Because of this, the ESP is emerging as the likeliest candidate for controlling firmware distribution to intelligent energy-management devices in the home.

Consider the logistical advantages that the ESP has over other possible candidates for managing software distribution:

- The ESP's NOC is an appropriate repository for firmware images ready to be distributed.
- The ESP must already have good information about what devices are present in each household it services.
- The ESP already has relationships with the primary device vendors.
- The ESP can serve as "gatekeeper" to decide whether to admit third-party devices into the energy-management HAN.
- Because the ESP serves multiple utilities, the effort of interoperability testing, making deployment decisions, etc. is reusable. It would be too much effort for each utility to perform this testing independently.
- Because ESPs are participants in standards organizations, they receive early warning about changes and can benefit from the interoperability testing performed by standards bodies, vendors, and industry associations.

Conclusions

Because all AMI/HAN deployments by public utilities are in their infancy, the firmware distribution problem has not yet been well tested .In the rush to be first to market, this problem, which inherently arises in the second generation, has not been the top priority for ESPs or their utility partners. Today, however, as important regulatory agencies such as NIST, FERC and the Department of Homeland Security are focusing on AMI deployments and insisting that strong security be built into these networks from the beginning, the firmware distribution issue is moving up the list. A secure network cannot be maintained without a secure reliable method of updating the nodes in the network. The energy industry can profit from the experience gained in the 1980s and 1990s with wide area networks. The costs of failing to build security into any networking solution from the beginning are now well understood.

As the Smart Grid leaves the prototype era and becomes a firm reality, software architecture and the ability to develop software to exacting compliance with published standards will become increasingly important to new energy startups, to utilities, and to the large traditional players in the energy management space. Green Energy Corp has been solving problems of this nature in the communications arena since 2001. Our growing Smart Energy practice applies this critical know-how to this exciting new field of endeavor. To date, we have provided software services and consulting to HAN device manufacturers, ESPs, business-area-network providers, and industry/academic consortia.

Abbreviations and Acronyms

The primary acronyms and abbreviations used in this publication are listed here:

Acronym	Definition
AMI	Advanced Metering Infrastructure
ESP	Energy Service Provider
HAN	Home Area Network
NEMA	National Electrical Manufacturers' Association
NOC	Network Operations Center
PLC	Power Line Carrier
SEP	Smart Energy Profile

About Green Energy Corp

Green Energy Corp is a leading technology company that provides software solutions and software engineering services to communications, utilities and energy companies. Our team includes senior business leaders and top industry experts with deep experience managing technology companies and building energy and communications solutions.

Our customers include established and emerging leaders in the communications, smart energy and utility segments. Our management team has the commitment, experience and depth to execute. Our employees bring exceptional 'been there, done that' skills and knowledge. Our partners are like-minded and architecturally complementary. Our engineering and project endeavors are oriented toward long-term solutions delivered via contracts with meaningful returns. We are well positioned to fulfill our mission to take a leading and sustainable role in the transformation to the smart grid at the national and global level.

Green Energy Corp Headquarters

12050 N Pecos St., Suite 210
Denver, Colorado 80234

Contact Us

303–453–8381
info@greenenergycorp.com

For more information, visit us on the web at **www.greenenergycorp.com**

Rev. 08/2012