Xanthus
Consulting International

White Paper for NIST CSWG: Cyber Security Requirements for Business Processes Involving Home Area Networks (HAN)

(Extracts from an EPRI-sponsored project developed by Frances Cleveland, Xanthus Consulting International)

Table of Contents

1. Overview

This report "*Home Area Network (HAN) Security Requirements*" identifies and discusses the key cyber security requirements for different interfaces of HAN-based systems. These cyber security requirements for HAN interfaces are derived from the DHS "*Catalog of Control Systems Security*", which provides an excellent checklist of general security requirements.

Although these cyber security requirements are focused on the HAN environment, it is nonetheless recognized that different systems, technologies, and environments will ultimately dictate the specific security solutions. One size cannot fit all.

1.1 Background of HAN

As Smart Grid requirements drive the development new technologies and the deployment of new systems, more and more new and existing Business Functions are becoming stakeholders in Smart Grid systems. The Home Area Network (HAN) is a prime example of these new Smart Grid functions and the technologies that are needed to support them. Figure 1 shows examples of some of the customer appliances and equipment that the HAN will need to support.

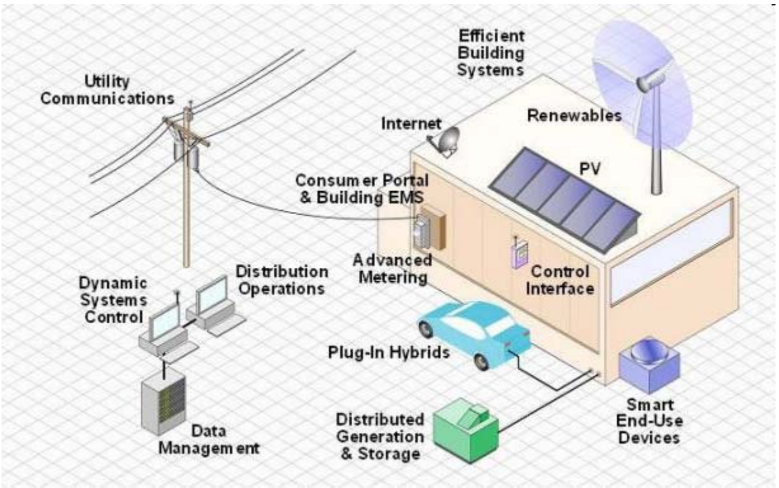


Figure 1: Home Area Network (HAN) Appliances and Equipment *(credit EPRI)*

However, HAN systems are still a work in process: many ideas are being explored as to which functions could potentially be absolutely required, or needed for special situations, or beneficial to certain types of customers. In addition, there will inevitably be business functions which are not yet foreseen that will suddenly become viable, or somewhat profitable, or "the HAN killer app".

1.2 Security Requirements Procedure

The HAN security requirements are derived through a clearly defined procedure:

- **Identified HAN-related business processes.** Key business processes that utilize the HAN were identified. These were derived from utility business process that have been identified in Use Cases including those mentioned in the AMI-SEC "*UtilityAMI 2008 Home Area Network System Requirements Specification*" document released in August 2008.
- **Identified actors and interfaces for each HAN-related business process.** Using an expanded HAN-centric version of the AMI System diagram developed by the EPRI team as one of the FERC4+2 diagrams for the National Institute of Standards and Technology

(NIST) for the NIST Smart Grid Roadmap, the actors and "logical" interfaces used by each HAN-related business process were identified.

- **Assessed the basic CIA security requirements for these business processes.** Simplified Use Cases were then developed to identify the types of information flows between the actors across these logical interfaces, plus an assessment of the basic security requirements of confidentiality/privacy, integrity, and availability (CIA). At this stage, no configurations, types of equipment, or networking technologies were assumed for the logical interactions.
- **Categorized HAN interfaces by their characteristics.** A set of Interface Categories, originally developed for NIST CSCTG security requirements, was refined for HAN-based interfaces. These Interface Categories are defined by the characteristics of their "typical" technological constraints and known security issues that could affect the types of security vulnerabilities and security measures. Each interface was then assigned to one of these categories.
- **Identified security requirements for each Interface Category as it applies to the HAN environment, using the DHS "*Catalog of Control System Security*" as a checklist.** Based on the characteristics of each category and assuming the most stringent security CIA requirements identified for any interface in a particular category, security requirements were identified for each category using the security controls in the Department of Homeland Security (DHS) "*Catalog of Control System Security*" document as a checklist.

1.3 Business Processes (Functions) involving HAN Systems

The key energy-related business processes involving the Home Area Network (HAN), the Building Area Network (BAN), the Neighborhood Area Network (NAN), and in general the customer-site energy-related systems, include:

- HAN business processes involving utility energy management requirements
- HAN business processes involving customer energy management
- HAN business processes involving third party remote access

About 40 different business processes were identified. These business processes may be implemented differently by different customers and may be designed with different types of equipment and communication networks by different vendors, but nonetheless the information flows generally involve the same logical interfaces between systems.

1.4 Characteristics-Based Interface Categories for Defining Security Requirements

At the most basic level, ***security requirements*** for exchanging information among different systems for different business processes (as seen in Section 0) are stated as the need for confidentiality, integrity, and availability (CIA). But translating these basic requirements into feasibility and cost-effectiveness ***security measures*** must take into account the technical constraints, the environments, organizational issues, and primary security requirements of the interfaces. Therefore the interfaces that are used to exchange information need to be defined according to these constraints and issues.

For this reason, the interfaces related to HAN systems were identified and then categorized according to their major characteristics. These Interface Categories were then assessed against the DHS "*Catalog of Control System Security*" to provide guidelines for developing the appropriate security measures.

These security-related categories can be helpful as examples, guidelines, and/or checklists of security requirements to help utilities specify security requirements and to assist vendors and integrators as they design, implement, and maintain secure systems but in the end, actual security measures must reflect the real-world security requirements of specific implementations.

1.5 Key Interface Categories for HAN-based Systems

Out of the 18 Interface Categories identified during work performed for National Institute of Standards and Technology (NIST)'s Cyber Security Coordination Task Group (CSCTG), five (5) Interface Categories were identified as key for HAN-based business processes:

- **Interface Category 1b:** Interface to private networks of **energy service providers** (including utilities) who are directly (tightly-coupled, immediate controls) managing DER and/or load at the customer site. The focus of this interface category is on the security requirements for *power system reliability*.
- **Interface Category 10:** Interface to the **AMI network** that connects to the utility, used primarily for accessing information related to metering, DER devices, and distribution automation devices. The focus of this interface category is on *revenue metering integrity* to ensure customer billing is accurate, and on *customer confidentiality and privacy,* since some customer data may be transmitted across the AMI network.
- **Interface Category 11:** Interfaces **within the HAN networks** to customer appliances, to DER generation and storage, to PEVs, to customer EMS, and to other systems and applications. The focus of this interface category is on *power system reliability involving distributed energy resources* (generation, storage, and load), as well as on *customer confidentiality,* since so many stakeholders have some degree of access to the HAN.
- **Interface Category 12:** Interface through an **ESI/HAN Gateway** to the public and/or private networks, such as the public Internet, private intranets, community networks, GPRS connections, etc., who interact (loosely-coupled signals and settings) with HAN systems, devices, and applications. The focus of this interface category is on *customer confidentiality and privacy,* since so many stakeholders can interact with the HAN.
- **Interface Category 14: Metering interactions** including sub-metering and use of the AMI network for providing metering data to the utility for billing. Included are also local laptop or maintenance tool connections by field installers and maintenance crews to meters and certain HAN appliances.

2. Business Processes Involving HAN Systems

The following sections describe the key energy-related business processes involving the Home Area Network (HAN), the Building Area Network (BAN), the Neighborhood Area Network (NAN), and in general the customer-site energy-related systems. These business processes may be implemented differently by different customers and may be designed with different types of equipment and communication networks by different vendors, but nonetheless the information flows generally involve the same logical interfaces between systems.

In addition to the brief description of the business process, each function identifies the “Actors” and the “Logical Interfaces” from the HAN diagram, and indicates the types of information which flow across them. These can be viewed as “security-focused Use Cases” since they are focused only on the HAN interfaces and only expanded enough to identify the security requirements.

The main purpose for describing these HAN-related business processes is to determine the security requirements of the information exchanges across the interfaces. Although there may ultimately be hundreds of interfaces between devices within the HAN, HANs have four primary interfaces to the outside, between the home and external parties:

- Interface to the AMI network that connects to the utility, used primarily for metering and related functions
- Interface to private networks of energy service providers (including utilities) who are directly (tightly-coupled, immediate controls) managing DER and/or load at the customer site.
- Interface through an ESI/HAN Gateway to the public and/or private networks, such as the public Internet, private intranets, community networks, GPRS connections, etc., who interact (loosely-coupled signals and settings) with HAN systems, devices, and applications.
- Local laptop or maintenance tool connections by field installers and maintenance crews to meters and certain HAN appliances.

Therefore, the primary emphasis is to determine the security requirements at these external interfaces, while still identifying the security requirements internally to the HAN. So for each business function, the basic security requirements (confidentiality/privacy, integrity, and availability) are assessed as high or low for these actors and logical interfaces. These basic security requirements, which are too high level to be directly useful for deriving specific security measures, nonetheless provide a rough assessment of the security focus, and are used in the next step of the security assessment procedure to help identify the key security requirements.

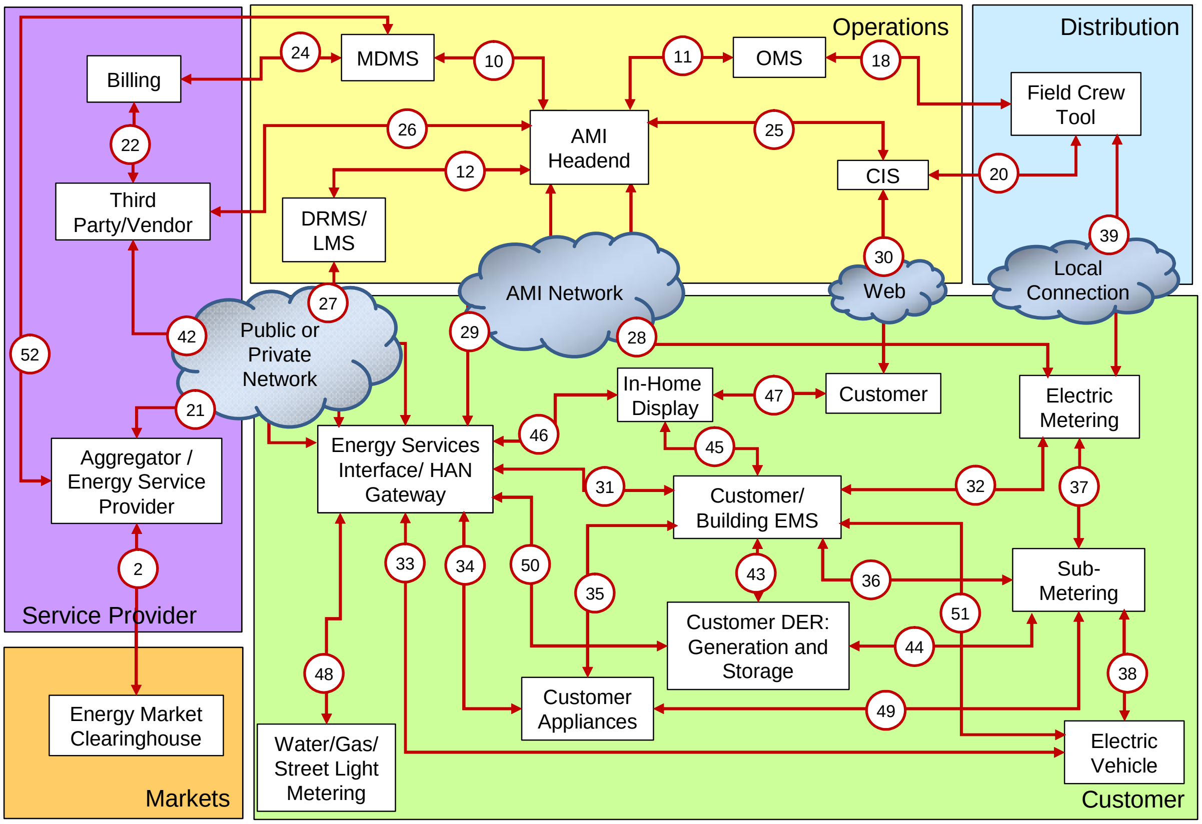
In order to protect this critical infrastructure, end-to-end security must be provided at the HAN boundaries, across the HAN communications systems, and within the customer systems and appliances. (see **Error! Reference source not found.**). HAN systems consist of the hardware, software, communication equipment, and associated system and data management applications that create a communications network at customer premises. The main components of HAN systems are:

- **Home Area Network**: The HAN is a network (or networks) within a customer premise. The HAN is typically defined as focused on residential customer premises and small commercial sites, although many of the same functions, issues, and security requirements can apply to larger building management systems and industrial management systems.
- **Interface to the AMI Network**: The AMI network provides a communications path for information to flow from the meter (and other special "registered" devices) to the AMI headend. It typically consists of a wide area backbone network to data concentrators which communicate over "last mile" links to the customer site (smart meter and/or customer gateway).
- **Interface to Public and/or Private Networks**: Public or private networks can include the public Internet, community or campus Intranets, GPRS cellphone systems, and any other special networks.
- **Smart Meter**: The smart meter is the source of metrological data as well as other energy-related information. These smart meters can provide interval data for customer loads as well as for customer distributed energy resources (generation and storage) and plug-in electric vehicles.
- **Registered HAN Devices**: Registered HAN devices are a select set of appliances and/or equipment that is under the direct management of the utility. These could include Programmable Communicating Thermostats (PCTs) and equipment used for direct load control, such as controllers for cycling air conditioners and pool pumps.
- **Energy Services Interface / HAN Gateway:** The ESI /HAN gateway acts as an interface between external networks (e.g. the AMI network and a public or private network) and the non-registered HAN customer systems and appliances within the customer facilities. It acts as one of the primary security firewalls between the utility-owned AMI equipment, the customer appliances, and all external interfaces. It may or may not co-located with the smart meter.
- **Customer Appliances and Equipment**: Customer appliances and equipment range from smart HVAC systems, to smart refrigerators, to DER generation and storage systems, to Plug-in Electric Vehicles (PEV), to home entertainment systems, down to smart toasters.
- **(Optionally) Neighborhood Area Network (NAN)**: Some Smart Grid experts include NANs in with HANs. However, in this report, these are not explicitly covered.

2.1 HAN Interfaces

2.1.1 HAN Logical Interfaces Extrapolated from NIST Roadmap

The HAN/BAN Use Case diagram of Actors, Logical Interfaces, and Networks (see was derived from the DR, H2G, I2G, and AMI Systems diagram of the FERC4+2 diagrams developed by the EPRI team for the NIST Phase 1 project. This HAN diagram captures the key interfaces used by the business processes described in the following section.



HAN/BAN Use Cases: Actors, Logical Interfaces, and Networks

DRMS: Demand Response Management System
LMS: Load Management System
CIS: Customer Information System
OMS: Outage Management System

HAN: Home Area Network
DER: Distributed Energy Resources
MDMS: Meter Data Management System
EMS: Energy Management System

Figure 2: HAN/BAN Actors, Logical Interfaces, and Networks

2.1.2 HAN List of System Actors and Logical Interfaces

The following is a list of the HAN logical interfaces between actors:

- HAN-2: Energy Market Clearinghouse – Aggregator/Retail Energy Service Provider
- HAN-10: MDMS – AMI Headend
- HAN-11: OMS – AMI Headend
- HAN-12: LMS/DRMS – AMI Headend
- HAN-15: LMS/DRMS – CIS

- HAN-18: OMS – Field Crew Tool
- HAN-20: CIS – Field Crew Tool
- HAN-21: Aggregator/Retail Energy Service Provider – ESI/HAN Gateway
- HAN-22: Third Party/ Vendor – Billing
- HAN-24: Billing – MDMS
- HAN-25: CIS – AMI Headend
- HAN-26: Third Party – AMI Headend
- HAN-27: AMI Headend – ESI/HAN Gateway
- HAN-28: AMI Headend – Metering
- HAN-29: LMS/DRMS – ESI/ HAN Gateway
- HAN-30: Customer – CIS
- HAN-31: ESI/HAN Gateway – Customer EMS
- HAN-32: Customer EMS – Metering
- HAN-33: ESI/HAN Gateway – Electric Vehicle
- HAN-34: ESI/HAN Gateway – Customer Appliances
- HAN-35: Customer EMS – Customer Appliances
- HAN-36: Customer EMS – Sub-metering
- HAN-37: Meter – Sub-metering
- HAN-38: Electric Vehicle – Sub-metering
- HAN-39: Field Crew Tool – Metering
- HAN-42: Third Party – ESI/HAN Gateway
- HAN-43: Customer EMS – Customer DER
- HAN-44: Customer DER – Sub-metering
- HAN-45: Customer – Customer EMS
- HAN-46: AMI Headend – In Home Display
- HAN-47: In Home Display – Customer
- HAN-48: ESI/HAN Gateway – Water/Gas/Street Light Metering
- HAN-49: Customer Appliance – Sub-metering
- HAN-50: ESI/HAN Gateway – Customer DER
- HAN-51: Customer EMS – Electric Vehicle
- HAN-52: MDMS – Aggregator/ Retail Energy Service Provider

2.2 HAN Business Processes Involving Utility Energy Management Requirements

2.2.1 Demand Response (DR) for Customer Energy Management

Demand response (DR) signals can support utilities by providing customers with near-real-time energy costs and power system reliability indices, and can thus help customers voluntarily manage their energy needs based on this information.

DR prices may be fixed as pre-established Time of Use (TOU) and feed-in tariff rates or could be scheduled with advanced notice (24 hrs) or could be near real-time (within an hour or even within seconds). The incentive for such a voluntary response could be for the customer to minimize energy usage or maximize generation during high price times, and/or to provide more sophisticated ancillary services to utilities, such as load following by using electric storage to respond rapidly to changing frequency.

One key benefit of HAN-based devices at the customer site is that they can automatically react to DR signals. Some HAN devices can provide key energy information to the customer in a timely manner: instantaneous kWh electricity pricing, consumption, projected costs, rate tiers, and voluntary load reduction program events.

DR signals may be focused on immediate needs (e.g. a power system emergency) or on longer term needs (e.g. expectation of high energy prices on a hot summer afternoon). These “demand response” signals may actually request more than responses of demand, but could include any or all of the following:

- Energy reduction for peak shifting (e.g. raise thermostat level) for a specific length of time, such as during on-peak times (demand reduction)
- Immediate emergency demand reduction (e.g. shed all unnecessary loads immediately) due to an emergency situation. Release from the load shedding could be within minutes or hours.
- Suggested energy increases (e.g. pre-cool building now in anticipation of higher prices later)
- Power quality (e.g. provide var support, use storage to level-out voltage fluctuations)
- Ancillary services (e.g. “frequency following” by using energy storage devices (including plug-in electric vehicles) to respond rapidly in order to counteract frequency deviations due to renewable generation fluctuations and/or rapid load changes).
- Microgrid procedure (e.g. set the Point of Common Coupling (PCC) to zero, so that internal generation matches internal load). This could apply to a home or hospital with an uninterruptible power supply (UPS), or could involve a community of multiple customers.

All demand response scenarios assume that the customer is in charge of responding to the DR signal, but the tariffs between utilities and their customers could vary depending upon regulatory rules and utility agreements with their customers. For instance, some demand response actions could be completely voluntary, with the metering and billing reflecting the customer choices. Other demand response actions might include mandatory responses, say to emergency conditions, and the customer would incur a penalty fee if they did not respond appropriately.

For the utility to receive the desired consumer response, it must provide timely pricing, event, and usage information, and must be able to accurately meter the responses by the customer, and include accurately time-stamped event logs.

It is expected that demand response interactions will take place through generic "DR-enabled controllers" which range from the extremely simple to the very complex, including:

- Visual pricing indicators, such as Energy Orb lights that turn red, yellow, or green depending on the current price of energy, as well as In-Home Displays (IHD)
- Programmable communicating thermostats (PCTs) that respond to pricing signals by changing settings within pre-specified limits
- Controllers for individual appliances that can respond to pricing signals by managing the energy usage of their appliance
- Controllers for individual distributed energy resources (DER) generation and storage units that can respond to pricing signals by increasing generation from generators or discharging stored energy, and/or by charging energy storage (and thus increasing the load)
- Customer computer systems that coordinate the responses to pricing signals across multiple appliances, generation, and storage devices within the customer site.
- External energy service providers that coordinate the responses across multiple customers and issues specific commands to appliances and devices at these customer sites.

DR signals may be initiated by:

- Utilities through their Demand Response Management System (DRMS) and/or Load Management System (LMS)
- Aggregators or Energy Services Providers, based on information from an Energy Market Clearinghouse

With respect to cyber security, DR signals are expected to be broadcast widely to all applicable customers, and therefore are not considered confidential. These DR signals are also expected to be responded to by less than 100% of customers for a variety of reasons, so that availability is not critical for the utilities, but may be important to individual customers who expect to be able to minimize their electric bills. The integrity or accuracy of the signal is important, but generally not critical. What might be critical are requests to shed load, so the integrity of these demand response requests must be high.

2.2.1.1 DR Signals from Utilities to Customer Sites

Utilities can broadcast to all customers (or multi-cast to selected customers) their DR signals via their AMI systems or via external public or private networks. All of these signals will be validated by the Energy Services Interface at the HAN gateway – they will not use the metering channel that will be dedicated only to metering.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-12	DRMS/LMS	AMI Headend	DR signal (price, urgency, level) List of HAN addresses	Acknowledgment of receipt of DR signal	C – Low I – Medium A - Low
HAN-29	AMI Headend	ESI/HAN Gateway	DR signal (price, urgency, level)	Acknowledgment of receipt of DR signal	C – Low I – Medium A - Low
HAN-27 (non-AMI alternative to HAN-12/ HAN-29)	DRMS/LMS	ESI/HAN Gateway	DR signal (price, urgency, level)	Acknowledgment of receipt of DR signal	C – Low I – Medium A - Low

2.2.1.2 DR Signals from Aggregators/ESPs to Customer Sites

Energy service providers, such as aggregators as well as special divisions of utilities, can broadcast to all customers (or multi-cast to selected customers) their DR signals via external private or public network systems. For instance, these signals could be transmitted via GPRS cellphone networks, DSL over telephone networks, cable networks, or potentially by broadband powerline carrier. Regardless of the type of external network, these DR signals will be validated by the Energy Services Interface at the HAN gateway.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-1	Energy Market Clearinghouse	Aggregator/ ESP	DR signal (price)	Acknowledgment of receipt of DR signal	C – Low I – Medium A - Low
HAN-21	Aggregator/ ESP	ESI/HAN Gateway	DR signal (price)	Acknowledgment of receipt of DR signal	C – Low I – Medium A - Low

2.2.1.3 DR Signals from ESI/HAN Gateway to Visual Pricing Indicators

DR signals can be shown to customers visually via in-home displays (IHD) or via special devices such as the Energy Orb. The customer then makes decisions on the used of their appliances based on these visual indications. No other automation is involved.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-46	ESI/HAN Gateway	In-Home Display	DR signal (price, urgency, level)	Acknowledgment of receipt of DR signal	C – Low I – Medium A - Low
HAN-47	In-Home Display	Customer	Visual indication of DR signal	Acknowledgment of receipt of DR signal	C – Low I – Medium A - Low

2.2.1.4 DR Signals from ESI/HAN Gateway to Programmable Communicating Thermostats

DR signals can be sent to programmable communicating thermostats (PCTs) that respond to pricing signals by changing the thermostat settings within pre-specified limits. For instance, on hot days the PCT could be set to move progressively from the normal 72°F up to the limit of 82°F for increasing price signals. The reverse could be set for cold days. An emergency load shedding signal could tell the PCT to turn off the air conditioner or heating system, respectively. In any of these situations, the customer could override the PCT settings and responses.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-34	ESI/HAN Gateway	PCT (as a special Customer Appliance)	DR signal (price, urgency, level)	Acknowledgment of receipt of DR signal	C – Low I – Medium A - Low

2.2.1.5 DR Signals from ESI/HAN Gateway to Individual Appliance Controllers

In addition to PCTs, DR signals could be sent directly to individual appliance controllers. For instance, these signals could be sent to pool pumps and/or to electric water heaters to advise them of the current energy prices and then let them determine a pre-programmed response.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-34	ESI/HAN Gateway	Customer Appliance	DR signal (price, urgency, level)	Acknowledgment of receipt of DR signal	C – Low I – Medium A - Low

2.2.1.6 DR Signals from ESI/HAN Gateway to Individual DER Controllers

DR signals to Distributed Energy Resource (DER) controllers would permit these controllers to take local actions in response. For instance, a PV inverter could stop charging locally connected batteries and start exporting to the grid. Or an electric vehicle could slow down its charging rate or even start discharging.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-33	ESI/HAN Gateway	Electric vehicle	DR signal (price, urgency, level)	Acknowledgment of receipt of DR signal	C – Low I – Medium A - Low
HAN-50	ESI/HAN Gateway	DER generation and storage	DR signal (price, urgency, level)	Acknowledgment of receipt of DR signal	C – Low I – Medium A - Low

2.2.1.7 DR Signals from ESI/HAN Gateway to Customer EMS

The most beneficial approach to handling DR signals is the use of a "Customer Energy Management System (EMS)" which can analyze the current status of all DR-enabled equipment on the HAN, the level, type, and urgency of the DR signal, the preset customer limits, and other factors to determine the best schedule of responses, possibly using a multi-pronged approach.

A customer EMS receives DR signals, assesses the energy usage of appliances on the HAN, and initiates appropriate signals (on-off, cycle on-off time, don't start, change energy usage level, etc.) to these appliances based on the type and value of the DR signal. The assumptions are:

- The customer EMS is aware of or can retrieve the types of HAN devices and the status of those devices connected to the HAN upon registration or change-out. (e.g., refrigerator on/off, air conditioning cycling, pool pump status, and electric vehicle charging status).
- The customer EMS controls production, consumption, and storage of these HAN devices (e.g. controls PV inverter on/off state, controls charging/discharging rates of an electric vehicle).
- The customer EMS can include selected load shedding capability if a serious reliability event is signaled.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-31	ESI/HAN Gateway	Customer EMS	DR signal (price, urgency, level)	Acknowledgment of receipt of DR signal	C – Low I – Medium A - Medium

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-35	Customer EMS	Customer appliances	Direct commands over time or a schedule of actions for the appliances	Acknowledgment of receipt of control commands or schedule Updated status and alarms	C – Low I – Medium A - Medium
HAN-43	Customer EMS	DER generation and storage	Direct commands over time or a schedule of actions for the appliances	Acknowledgment of receipt of control commands or schedule Updated status and alarms	C – Low I – Medium A - Medium
HAN-51	Customer EMS	Electric vehicles	Direct commands over time or a schedule of actions for the appliances	Acknowledgment of receipt of control commands or schedule Updated status and alarms	C – Low I – Medium A - Medium

2.2.2 Direct Load, Generation, and Storage Control for Utility Energy Management

Direct load control provides active control by the utility of customer appliances (e.g. cycling of air conditioner, water heaters, and pool pumps) and certain C&I customer systems (e.g. plenum pre-cooling, heat storage management). Direct load control is thus a callable and schedulable resource, and, within limits, can be used in place of operational reserves in generation scheduling. The limits reflect how much load is actually available to be controlled – if an air conditioner is not on, it cannot be cycled.

In the future, more distributed energy resources (DER), comprising both generation and electric storage, will be connected to the distribution network. The integration of DER, particularly renewable DER, adds both complexity as well as opportunity for managing the power system. The complexity is the result of two-way flows of energy and in the variability of some of these sources of energy. The opportunity stems from the ability to control these resources in a planned and coordinated manner in order to manage the power system more efficiently and reliably.

2.2.2.1 Direct Load Control by Utilities

Direct load control is a well-proven and well-established technology for broadcast (multi-cast) signals to customers to initiate control actions. For residential customers, these control actions include:

- Cycle air conditioners
- Cycle electric water heaters
- Cycle pool pumps

For commercial and industrial customers, these load control actions usually interact with systems which determine the precise actions to take, such as HVAC units and building energy management systems. More sophisticated load control capabilities include signaling load shifting requirements, so that facilities like hotels can pre-cool their plenums during the morning and cycle off their air conditioning at peak times.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-12	DRMS/LMS	AMI Headend	Load control signal List of HAN addresses	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low
HAN-29	AMI Headend	ESI/HAN Gateway	Load control signal	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low
HAN-27 (non-AMI alternative to HAN-12/ HAN-29)	DRMS/LMS	ESI/HAN Gateway	Load control signal	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low
HAN-31	ESI/HAN Gateway	Customer EMS	Load control signal (Level or percentage)	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low
HAN-33	ESI/HAN Gateway	Electric Vehicle	Load control signal (charging rate)	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low
HAN-34	ESI/HAN Gateway	Customer Appliances	Load control signal (start/stop cycling)	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low
HAN-35	Customer EMS	Customer Appliances	Load control signal (start/stop cycling)	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low
HAN-51	Customer EMS	Electric Vehicle	Load control signal (charging rate)	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low

2.2.2.2 Direct Load Shedding by Utilities

Direct load shedding can use the same technologies as direct load control but involves the use of a “scram” control command which shuts down all controllable devices, potentially including the meter's remote connect disconnect switch. It is used during emergency situations in which reducing load rapidly could avoid more serious power system problems.

Because of its more drastic actions, direct load shedding has more stringent security requirements than normal load control.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-12	DRMS/LMS	AMI Headend	Load control signal List of HAN addresses	Acknowledgment of receipt of load control signal	C – Low I – High A - High
HAN-29	AMI Headend	ESI/HAN Gateway	Load control signal	Acknowledgment of receipt of load control signal	C – Low I – High A - High
HAN-27 (non-AMI alternative to HAN-12/ HAN-29)	DRMS/LMS	ESI/HAN Gateway	Load control signal	Acknowledgment of receipt of load control signal	C – Low I – High A - High
HAN-31	ESI/HAN Gateway	Customer EMS	Load control signal (Scram)	Acknowledgment of receipt of load control signal	C – Low I – High A - High
HAN-33	ESI/HAN Gateway	Electric Vehicle	Load control signal (stop charging)	Acknowledgment of receipt of load control signal	C – Low I – High A - High
HAN-34	ESI/HAN Gateway	Customer Appliances	Load control signal (turn off)	Acknowledgment of receipt of load control signal	C – Low I – High A - High
HAN-35	Customer EMS	Customer Appliances	Load control signal (scram)	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low
HAN-51	Customer EMS	Electric Vehicle	Load control signal (stop charging)	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low

2.2.2.3 Direct Control of DER Generation Levels by Utilities

DER encompasses both generation and storage. Some generation, such as wind and photovoltaics, can be controlled only within very narrow limits, such as turning off a PV inverter if there is over-generation. Other generation, such as combined heat and power, fuel cells, diesel generators, and small hydro plants, have wider and more sophisticated capabilities to manage generation levels.

Energy storage is usually used as a source of later generation (the exception is the batteries of electric vehicles which are most likely to be used for the vehicle). Storage is particularly useful to shift load from on-peak to off-peak and to counterbalance the rapid fluctuations of renewable energy sources.

Some DER units at customer sites could be monitored in “near-real-time” and possibly directly controlled by the utility or a third party (e.g. an aggregator) via the AMI system, in an equivalent manner to load control, except to include both net export and import levels (combinations of generation and storage). Depending upon the DER controller capability (or the customer EMS capabilities), schedules for net export/import levels can be provided ahead of time so that the direct control is triggered within the customer site by these schedules.

Direct control of larger DER at larger commercial and industrial customer sites could have more stringent security requirements due to the larger impact on the power system, but the examples shown here are for smaller DER installations.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-12	DRMS/LMS	AMI Headend	DER control signal List of HAN addresses	Acknowledgment of receipt of DER control signal	C – Low I – Medium A - Low
HAN-29	AMI Headend	ESI/HAN Gateway	DER control signal	Acknowledgment of receipt of DER control signal	C – Low I – Medium A - Low
HAN-27 (non-AMI alternative to HAN-12/ HAN-29)	DRMS/LMS	ESI/HAN Gateway	DER control signal	Acknowledgment of receipt of DER control signal	C – Low I – Medium A - Low
HAN-31	ESI/HAN Gateway	Customer EMS	DER control signal (% generation, import/export level or %, urgency, etc.)	Acknowledgment of receipt of DER control signal	C – Low I – Medium A - Low
HAN-33	ESI/HAN Gateway	Electric Vehicle	DER control signal (rate of charging and/or discharging)	Acknowledgment of receipt of DER control signal	C – Low I – Medium A - Low

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-43	Customer EMS	DER	DER control signal (% generation, import/export level or %, urgency, etc.)	Acknowledgment of receipt of DER control signal	C – Low I – Medium A - Low
HAN-50	ESI/HAN Gateway	DER	DER control signal (% generation, import/export level or %, urgency, etc.)	Acknowledgment of receipt of DER control signal	C – Low I – Medium A - Low
HAN-51	Customer EMS	Electric Vehicle	DER control signal (rate of charging and/or discharging)	Acknowledgment of receipt of DER control signal	C – Low I – Medium A - Low

2.2.3 Outage Detection and Restoration

2.2.3.1 Outage Detection

Currently, most outage reporting is done by the customer via a phone call. In the future, the smart meter will be able to detect and report customer outages within a short time of their occurrence, including momentary outages.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-28	Meter	AMI Headend	Outage notification	Verification of outage (ping)	C – Low I – Medium A - Low
HAN-11	AMI Headend	OMS	Outage notification		C – Low I – Medium A - Low

2.2.3.2 Verification of DER Shut-Down or Islanding

Each time an outage occurs that affect the power grid with DER, the DER should either shut down or island itself from the rest of the grid, only feeding the “microgrid” that is directly attached to. In many cases the shut-down or islanding equipment in smaller installations is poorly installed or poorly maintained. This leads to leakage of the power into the rest of the grid and potential problems for the field crews.

Each time an outage occurs, meters that are designed to monitor net power can tell if the islanding occurred correctly, if they are installed at the right point in the system. This reporting can minimize crew safety and allow the utility to let the customer know that maintenance is required on their DER system. In most cases when the islanding fails, other problems also exist that reduce the efficiency of the DER system, costing the customer the power that they expected to get from the system.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-28	Meter	AMI Headend	DER Shut-down	Verification of outage (ping)	C – Low I – Medium A - Low
HAN-11	AMI Headend	OMS	DER Shut-down		C – Low I – Medium A - Low

2.2.3.3 Outage Restoration Verification

Smart meters can verify that power has been restored after an outage, including a timestamp for the restoration time. This function can either alert automatically or be requested of specific meters if they have not reported a restoration event when expected. For some utilities this function significantly improves their CAIDI/SAIDI indices, since often their crews may take several minutes to complete other actions before reporting the power back on. It can also be used to help isolate nested outages and help the field crews get to the root cause of those nested outages before they leave the scene.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-18	Field Crew Tool	OMS	Request for restoration status of selected meters	List of any meters not reporting restoration	C – Low I – Medium A - Low
HAN-11	OMS	AMI Headend	Request for restoration notification	Restoration notification	C – Low I – Medium A - Low
HAN-28	AMI Headend	Meter	Ping the status of the meter	Restoration notification	C – Low I – Medium A - Low

2.2.3.4 Scheduled Outage Notification

Notification of scheduled outages, usually required for power system construction or maintenance work, can be sent to affected customers via the AMI system or alternate method. If the customer has in-home displays, then the scheduled outage notification can be sent to those displays. If the customer is not at home or does not have any in-home displays, then notification could be sent by text message or email – also potentially used for notification of unplanned outages as well.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-11	OMS	AMI Headend	Scheduled outage notification	Acknowledgment	C – Low I – Medium A - Low
HAN-27	AMI Headend	ESI/ HAN Gateway	Outage notification		C – Low I – Medium A - Low

2.2.3.5 Planned Outage Restoration Verification

In completing work orders involving planned outages, it is important to verify that all of the customers affected by the work order have their power restored, and that there are no outstanding issues that need to be corrected prior to the crew leaving the area. The ability to “ping” every meter in the area that was affected by the work order and determine if there are any customers who are not communicating that they have power is useful to minimize return trips to the work area to restore single customers.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-18	Field Crew Tool	OMS	Request for restoration status of selected meters	List of any meters not reporting restoration	C – Low I – Medium A - Low
HAN-11	OMS	AMI Headend	Request for restoration notification	Restoration notification	C – Low I – Medium A - Low
HAN-28	AMI Headend	Meter	Ping the status of the meter	Restoration notification	C – Low I – Medium A - Low

2.2.3.6 Street Lighting Outage Detection

Street lighting can be critical to safety and crime-prevention, and yet monitoring which street lights are out is currently performed haphazardly by civil servants and concerned citizens. Neighborhood Area Networks (NANs) (as an extension to HAN networks) could be used to monitor these lights. This assumes that the street light has an intelligent controller that recognizes that the light is not functioning when it should be on.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-48	Street light	ESI/ HAN Gateway	Notification of street light failure	Verification	C – Low I – Medium A – Low
HAN-29	ESI/ HAN Gateway	AMI Headend	Notification of street light failure	Verification	C – Low I – Medium A – Low
HAN-11	AMI Headend	OMS	Notification of street light failure	Verification	C – Low I – Medium A - Low

2.2.4 Customer Energy Information

2.2.4.1 Customer Authorization of Energy Usage to ESP

Customers may want to authorize the transfer of their consumption, price, and billing related information from utilities to 3rd party vendors or energy service providers (ESP), so that these can manage the customer appliances and equipment to meet customer energy usage goals. The process would entail the customer requesting the utility to send their energy usage information to specific energy service providers periodically.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-30	Customer	CIS/MDMS	Request for their energy usage information to be sent to one or more energy service providers	Verification	C – Medium I – Low A – Low
HAN-52	MDMS	Aggregator/ Retail Energy Service Provider	Periodic energy usage information for authorized customers	Verification	C – High I – Medium A – Low

2.2.4.2 Customer Receiving Energy Usage from Utility

Energy usage information can be provided to the customer back from the utility after the metering data has been validated and priced. This can help the customer understand their energy usage patterns and assist them in improving that pattern.

Utilities can also provide a customer energy consumption advisory that allowed customers to indicate what they have for energy consuming devices and information about their home. In return, the utilities rank their consumption against similar homes and provide feedback on the equipment and appliances that were consuming significant energy.

This advisory can even suggest what should be replaced and the payback period on the replacement, based on energy usage. The comparison allows customers to see how they did against similar customers and where they ranked in energy consumption. This has been very useful in getting customers to pay more attention to their consumption.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-30	Customer	CIS/MDMS	Request for their energy usage information to be sent to the customer	Verification	C – Medium I – Low A – Low
HAN-10	MDMS	AMI Headend	Periodic energy usage and pricing information	Verification	C – High I – Medium A – Low
HAN-29	AMI Headend	ESI / HAN Gateway	Periodic energy usage and pricing information	Verification	C – High I – Medium A – Low
HAN-46	ESI / HAN Gateway	In-Home Display	Periodic energy usage and pricing information	Verification	C – High I – Medium A – Low

2.2.4.3 Customer Receiving Energy Usage Directly from Meter

Energy usage information can be provided to the customer directly from the meter as a estimate of the usage and pricing since the metering data has not been validated by the utility.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-32	Electric Metering	Customer EMS	Metering data	Verification	C – High I – Medium A – Low

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-45	Customer EMS	In-Home Display	Estimated energy usage and pricing information	Verification	C – High I – Medium A – Low

2.2.4.4 Customer Power Quality Notification

Customers can be notified if their meter is registering power quality issues, such as voltage sags and spikes, or unusual harmonics. This information can be used either to help the customer determine that devices within their site are causing problems, or to notify the customer that the utility has a power quality problem which they will fix.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-10	MDMS	AMI Headend	Power quality notification	Verification	C – High I – Medium A – Low
HAN-29	AMI Headend	ESI / HAN Gateway	Power quality notification	Verification	C – High I – Medium A – Low
HAN-46	ESI / HAN Gateway	In-Home Display	Power quality notification	Verification	C – High I – Medium A – Low

2.3 HAN Business Processes Involving Customer Energy Management

Management of customer energy demand and usage can involve both Load Management (LM) and management of Distributed Energy Resources (DER).

It is expected that most energy management will ultimately be handled through demand response "pricing" signals which may be an actual price of kWh or a fake "price" used to modify demand. However some energy management may be performed more directly through direct control.

Load management can involve both direct and indirect control of loads. Direct load control generally consists of a signal from the utility requesting either a partial load reduction or, in an emergency, a "scram" of all controllable loads. Indirect load control consists in a utility issuing a "pricing" signal.

DER will become an increasing part of Home Area Networks as customers install Photovoltaic (PV) systems, Plug-in Electric Vehicles (PEVs), backup power sources such as batteries and diesel generators, and energy storage to offset the variability of renewable energy. Although the economics of these DER devices are still changing rapidly as regulations change, technologies improve, and tax incentives reflect governmental decisions, it is clear that many DER devices will ultimately be installed at many customer sites.

Some of these DER systems will just operate independently. For instance, some PV systems will generate power when the sun shines, while some wind turbines will generate when the wind blows.

However, increasingly utilities need to be aware of aggregated smaller DER devices and may need some level of control over larger DER devices. In addition, demand response signals can be used to manage some DER for mutual benefit of customers, utilities, and possibly third parties.

For the purposes of this document, any stakeholders involved in monitoring and/or managing DER devices are called Energy Service Providers (ESPs). These ESPs could be a division of a utility, an affiliation of a utility, or a completely separate company. Different ESPs could have different focuses. Some may focus on managing aggregated DER to reflect aggregated pricing strategies. Some may manage individual DER devices through management and maintenance contracts. Still others may be concerned with power system reliability and efficiency that may involve local responses to power situations. And others may be more interested in carbon credits.

2.3.1 Demand Response in the HAN

Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff-based, while the prices may also be operationally-based or fixed or some combination. As noted below, real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.

(Note that the direct load control (DLC) functions performed by utilities are not considered as demand response functions, although there is a gray area in DLC functions on when and how the customer makes the decision to “respond to demand”.)

Subfunctions for demand response, some of which may not involve the AMI system directly, include:

- Enroll Customer
- Enroll in Program
- Enroll Device
- Update Firmware in HAN Device
- Send Pricing to device
- Initiate Load Shedding event
- Charge/Discharge PHEV – storage device

- Commission HAN device
- HAN Network attachment verification (e.g. which device belongs to which HAN)
- Third Party enroll customer in program (similar to, but not the same as the customer enrolling directly)
- Customer self-enrollment
- Manage in home DG (e.g. MicroCHP)
- Enroll building network (C&I – e.g. Modbus)
- Decommission device
- Update security keys
- Validate device
- Test operational status of device

It is assumed in these business process that the "Customer EMS" first receives the demand response "pricing" signal, although in some installations, this information will go directly to the customer appliances and devices without relying on any "Customer EMS".

2.3.1.1 Demand Response: Time of Use (TOU) Pricing

Time of use (TOU) pricing creates daily blocks of time for each type of day-of-the-week: for instance, on-peak is 12 noon to 6 pm M-F while off-peak is the rest of the time. Actual prices for on-peak and off-peak may vary by season. TOU metering has been used for many decades in many countries, and requires simpler meters than the smart meter. TOU is often used with net metering for photovoltaic system installations, since the PV system generates the most power during on-peak times, giving the customer even more benefit either by decreasing their load significantly during on-peak or by actually selling power back to the utility during this high price time.

Controllable devices on the HAN need to take the TOU rates into account. These updates will either be sent through the AMI system or through an external network such as GPRS.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-27	DRMS/LMS	ESI/HAN Gateway	TOU pricing updates	Acknowledgment that TOU update was received	C – Low I – Med A - Med
HAN-31	ESI/HAN Gateway	Customer EMS	TOU pricing updates	Acknowledgment that TOU update was received	C – Low I – Med A - Med
HAN-35	Customer EMS	Customer Appliances	TOU pricing updates	Acknowledgment that TOU update was received	C – Low I – Med A - Med

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-43	Customer EMS	Customer DER	TOU pricing updates	Acknowledgment that TOU update was received	C – Low I – Med A - Med
HAN-51	Customer EMS	Electric Vehicle	TOU pricing updates	Acknowledgment that TOU update was received	C – Low I – Med A - Med

2.3.1.2 Demand Response: Real Time Pricing (RTP)

Use of real time pricing (RTP) for electricity is common for very large customers, affording them an ability to determine when to use power and minimize the costs of energy for their business. The extension of real time pricing to smaller commercial customers and residential customers is possible with smart metering and on-premise customer EMS systems which can convert DR signals to explicit control commands to appliances and equipment. In addition, aggregators and/or energy service providers can be authorized by customers to respond to DR signals for them by issuing the control commands remotely.

Although RTP prices could be provided to customers by many different mechanisms, such as email or GPRS signals, the most likely method will be through the AMI system.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-12	DRMS/LMS	AMI Headend	RTP pricing updates	Acknowledgment that RTP update was received	C – Low I – Med A - Med
HAN-29	AMI Headend	ESI/HAN Gateway	RTP pricing updates	Acknowledgment that RTP update was received	C – Low I – Med A - Med
HAN-31	ESI/HAN Gateway	Customer EMS	RTP pricing updates	Acknowledgment that RTP update was received	C – Low I – Med A - Med
HAN-35	Customer EMS	Customer Appliances	RTP pricing updates	Acknowledgment that RTP update was received	C – Low I – Med A - Med
HAN-43	Customer EMS	Customer DER	RTP pricing updates	Acknowledgment that RTP update was received	C – Low I – Med A - Med

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-51	Customer EMS	Electric Vehicle	RTP pricing updates	Acknowledgment that RTP update was received	C – Low I – Med A - Med

2.3.1.3 Demand Response: Critical Peak Pricing (CPP)

Critical Peak Pricing (CPP) is used on the (typically) small number of days each year where the electric delivery system may be close to its limits due to emergency conditions and/or the price of energy is significantly higher than normal. The CPP signal is issued in a similar manner to RTP signals, but usually initiates a "scram" action to shut off or cycle off all indicated appliances and/or to generate more DER power.

As with RTP, these CPP signals could be in response to local conditions as well as more regional conditions.

The security requirements are deemed only medium availability for any single customer site since the requirement is for an aggregated response. However, as a aggregate, the need for most HANs to receive the CPP signal has a high availability requirement.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-12	LMS / DRMS	AMI Headend	Demand Response CPP price signal	Acknowledgment that DR signal was received	C – Low I – Med A - Med
HAN-29	AMI Headend	ESI/HAN Gateway	DR signal CPP price signal	Acknowledgment that DR signal was received	C – Low I – Med A – Med
HAN-31	ESI/HAN Gateway	Customer EMS	DR signal CPP price signal	Acknowledgment that DR signal was received	C – Low I – Med A – Med
HAN-35	Customer EMS	Customer Appliances	Control commands in response to CPP signal	Appliance status and response information	C – Low I – Low A – Low
HAN-43	Customer EMS	Customer DER	Control commands in response to CPP signal	DER status and response information	C – Low I – Low A – Low
HAN-51	Customer EMS	Electric Vehicle	Control commands in response to CPP signal	DER status and response information	C – Low I – Low A – Low

2.3.1.4 Demand Response: Ancillary Services (AS)

In addition to requests to lower demand, many other ancillary services could be requested of customers, particularly those that have DER devices on site, such as PV systems, wind turbines, fuel cells, combined heat and power, energy storage, and PEVs. These ancillary services could support the overall energy efficiency of the distribution systems, rather than just reflecting energy prices. Some of the ancillary services include:

- Go to default operating mode
- Control voltage within normal voltage band by sensing local voltage level and responding to it.
- Control vars to specified level (within normal var band), including providing maximum vars and/or minimum vars
- Damp oscillations on the power system both by random time responses to DR signals and by actively taking opposing actions (such as lowering voltage when a high voltage level is sensed)
- Respond to frequency deviations to minimize Area Control Error (ACE)

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-12	LMS / DRMS	AMI Headend	Demand Response AS price signal	Acknowledgment that DR signal was received	C – Low I – Med A - Med
HAN-29	AMI Headend	ESI/HAN Gateway	DR signal AS price signal	Acknowledgment that DR signal was received	C – Low I – Med A – Med
HAN-31	ESI/HAN Gateway	Customer EMS	DR signal AS price signal	Acknowledgment that DR signal was received	C – Low I – Med A – Med
HAN-35	Customer EMS	Customer Appliances	Control commands in response to AS signal	Appliance status and response information	C – Low I – Low A – Low
HAN-43	Customer EMS	Customer DER	Control commands in response to AS signal	DER status and response information	C – Low I – Low A – Low
HAN-51	Customer EMS	Electric Vehicle	Control commands in response to AS signal	DER status and response information	C – Low I – Low A – Low

2.3.2 DER Management by Energy Service Providers (ESPs)

Since most customers do not have the time or expertise to manage their own DER devices for scenarios any more sophisticated than “let them generate whenever possible”, ESPs can fulfill that role. To do that they must have appropriately authorized access to the DER devices.

2.3.2.1 Management of DER Generation and Storage by ESPs

Customers could decide to outsource the management of their DER generation and storage devices to the utility or a third party (e.g. an aggregator). DER devices would be monitored and controlled in “near-real-time” by via the AMI system or via external networks.

This monitored information can provide more detailed information on the actual generation output and available energy storage, so that expectations from demand response actions as well as direct load/generation control actions can be more precisely managed. This knowledge of DER capacity could, in fact, help set the prices for demand response, particularly for Locational Marginal Pricing (LMP), where the location of the DER devices is critical.

Other controls for DER could request ancillary services such as power factor / var shifting and frequency deviation damping. If a customer site includes both generation and storage devices, then some commands could request switching from exporting to the grid to charging up electric storage, vice versa, or a balance of both exporting and charging.

There is a large amount of diesel generation that is installed on customer sites to deal with outages on the grid. Some companies are now forming to manage these resources, not for outage, but for peak power production, bidding into the market a few megawatts at a time. While the use of these resources is a good thing, the penetration of private companies will never be as complete as if the utility were to work with their customers to equip most of this generation with controls and monitoring equipment.

Control of DER generation and storage provides utilities with more precise capability to manage power system reliability and efficiency than does demand response, which involves unknown acceptance constraints and limits by the customer. At the same time, direct control of DER can entail more serious security requirements, since even small amounts of generation that is deliberately or inadvertently handled inappropriately can lead to safety issues as well as have serious financial and legal impacts.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-21	Aggregator/ Retail Energy Services Provider	ESI/HAN Gateway	DER monitoring and control requests	DER monitored information and control acknowledgments	C – Low I – Medium A - Medium

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-31	ESI/HAN Gateway	Customer EMS	DER control signal (% generation, import/export level or %, urgency, etc.)	DER monitored information and control acknowledgments	C – Low I – Medium A - Medium
HAN-43	Customer EMS	Customer DER	DER control signal (% generation, import/export level or %, urgency, etc.)	DER monitored information and control acknowledgments	C – Low I – Medium A - Medium
HAN-50 (alternative to HAN-31 and HAN-43)	ESI/HAN Gateway	Customer DER	DER control signal (% generation, import/export level or %, urgency, etc.)	DER monitored information and control acknowledgments	C – Low I – Medium A - Medium

2.3.2.2 Plug-in Vehicle (PEV) Charging Management

Electric transportation, primarily Plug-in Electric Vehicles (PEVs) is a key area in the Smart Grid whose impact on the power system is still not clearly understood. Electric transportation could significantly reduce our dependency on foreign oil, increase the use of renewable sources of energy, and also dramatically reduce our carbon footprint. However, the current grid and market infrastructure cannot support mass deployments of PEVs. The introduction of millions of mobile electricity charging and discharging devices provides unique challenges to every domain on the Smart Grid, in particular the AMI system which will have the most direct connection with customer sites where PEVs will be charging (and potentially discharging as energy storage).

Two major scenarios are envisioned with the advent of plug-in electric vehicles (PEV), with one or the other or both actually playing out:

- PEV will not have any special tariffs or sub-meters, and therefore will add significantly to the load that the power system will have to serve, including increasing the cost of peak power.
- PEV will have special tariffs supported by sub-metering. Although still adding to the load, PEVs will be able to help balance on- and off-peak loads through shifting when and how fast they are charged and also eventually by providing storage and discharging capacity. Additional ancillary services, such as frequency deviation damping, could also improve energy efficiency and power quality. These shifting strategies will result from carefully tailored pricing and market incentives.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-21	Aggregator/ Retail Energy Services Provider	ESI/HAN Gateway	PEV monitoring and control requests	PEV monitored information and control acknowledgments	C – Low I – Medium A - Medium
HAN-31	ESI/HAN Gateway	Customer EMS	PEV control signal (% generation, import/export level or %, urgency, etc.)	PEV monitored information and control acknowledgments	C – Low I – Medium A - Medium
HAN-51	Customer EMS	Customer PEV	PEV control signal (% generation, import/export level or %, urgency, etc.)	PEV monitored information and control acknowledgments	C – Low I – Medium A - Medium
HAN-33 (alternative to HAN-31 and HAN-51)	ESI/HAN Gateway	Customer PEV	PEV control signal (% generation, import/export level or %, urgency, etc.)	PEV monitored information and control acknowledgments	C – Low I – Medium A - Medium

2.3.2.3 Combined DER and Energy Storage Management

Many vendors of renewable energy systems such as PV systems and wind turbines are looking at combining fluctuating renewable generation with energy storage to smooth the total output. This storage can be used to counter not only the variable generation but also variable loads to provide a more constant export or import of energy at the point of common coupling (the electrical interconnection point where the combined ES-DER system connects to the power grid).

These combined ES-DER systems can be managed as a whole (set an export/import level) or can be individually managed.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-21	Aggregator/ Retail Energy Services Provider	ESI/HAN Gateway	DER monitoring and control requests	DER monitored information and control acknowledgments	C – Low I – Medium A - Medium

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-31	ESI/HAN Gateway	Customer EMS	DER control signal (% generation, import/export level or %, urgency, etc.)	DER monitored information and control acknowledgments	C – Low I – Medium A - Medium
HAN-43	Customer EMS	Customer DER	DER control signal (% generation, import/export level or %, urgency, etc.)	DER monitored information and control acknowledgments	C – Low I – Medium A - Medium
HAN-50 (alternative to HAN-31 and HAN-43)	ESI/HAN Gateway	Customer DER	DER control signal (% generation, import/export level or %, urgency, etc.)	DER monitored information and control acknowledgments	C – Low I – Medium A - Medium

2.3.2.4 DER Maintenance Management by ESPs

ESPs can also undertake more interactive management of DER devices by performing remote maintenance monitoring, preventative maintenance assessments, diagnostics, and testing. Although any physical maintenance would need to be done on site, significant amounts can be performed remotely.

However, this more comprehensive interactions with DER devices requires higher levels of security to ensure only authorized access is permitted. This is reflected in the security requirement for high integrity.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-21	Aggregator/ Retail Energy Services Provider	ESI/HAN Gateway	DER maintenance monitoring and commands	Acknowledgments	C – Low I – High A - Medium
HAN-50	ESI/HAN Gateway	Customer DER	DER maintenance monitoring and commands	Acknowledgments	C – Low I – High A - Medium

2.4 HAN Business Processes Involving Third Party Remote Access

The term "third party" is used to denote an entity that is not directly involved with electricity management. Third parties can include:

- The customer when they are remote from their own site
- Gas and water utilities
- Vendors of products in the customer site
- Service providers, such as security monitoring and medical condition monitoring
- Regulatory or law enforcement agents

2.4.1 Remote Customer Access

2.4.1.1 Customer Access to HAN Functions from Remote Site

Customers will be able to access appliances and devices on their HAN from remote sites. For instance, they may want to change HVAC settings because they are coming home early or may want to have their TV record a show or may want to ascertain that their children are home (and are not watching TV).

Some of these access interactions may take place through a browser via the Internet or may be through cellphones via GPRS, or via other communication devices.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-42	Third party (customer at remote location)	ESI/HAN Gateway	Command sent to a customer appliance	Acknowledgments	C – Medium I – Medium A - Medium
HAN-34	ESI/HAN Gateway	Customer Appliances	Command sent to a customer appliance	Acknowledgments	C – Medium I – Medium A - Medium

2.4.1.2 HAN Function Notification to Remote Customer

Alternatively some appliances and devices could send notifications to customers. For instance, the "door access" device might notify the customer that her child has entered the house – or that they have not come home within the agreed-upon time! Or an appliance like the refrigerator may notify the customer that they require maintenance. Or a UPS or FedEx delivery person can notify the customer that a package has arrived.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-34	Customer Appliances	ESI/HAN Gateway	Notification of an event	Acknowledgments	C – Medium I – Medium A - Medium
HAN-42	ESI/HAN Gateway	Third party (customer at remote location)	Notification of an event	Acknowledgments	C – Medium I – Medium A - Medium

2.4.2 Gas and Water Functions

2.4.2.1 Gas and Water Metering through the HAN

Gas and water metering can be performed through the HAN as well as directly through the AMI system, depending upon cross-utility agreements on whether the electric utility will first collect the metering data or whether the gas/water utility will collect the metering data directly.

This business process assumes the former scenario: the gas and water utilities access their meters directly through the HAN.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-42	Third party (gas or water utility)	ESI/HAN Gateway	Request for meter reading	Meter readings Meter status Error messages from meters	C – Low I – Low A - Low
HAN-48	ESI/HAN Gateway	Water/Gas Meter	Request for meter reading	Meter readings Meter status Error messages from meters	C – Low I – Low A - Low
HAN-48	Water/Gas Meter	ESI/HAN Gateway	Meter readings	(Acknowledgment and/or errors)	C – Low I – Low A - Low
HAN-42	ESI/HAN Gateway	Third party (gas or water utility)	Meter readings	(Acknowledgment and/or errors)	C – Low I – Low A - Low

2.4.2.2 Leak Detection

For gas and water utilities, leaking water and gas are important to track down for both safety and conservation reasons. In the water industry, use of pressure transducers on smart meters has proven useful when doing minimum night flows to find unexpected pressure drops in the system. Normally the need is one pressure transducer meter per 500 to 1000 customers in an urban environment.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-48	Water/Gas Meter	ESI/HAN Gateway	Notification of a possible leak	Acknowledgments	C – Medium I – Medium A - Medium
HAN-42	ESI/HAN Gateway	Third party (gas or water utility)	Notification of a possible leak	Acknowledgments	C – Medium I – Medium A - Medium

2.4.2.3 Water Meter Flood Detection and Conservation Throttling

With the addition of some sensors, it is possible to detect if there is a sudden increase in water flow and a drop in pressure that is sustained and unusual, particularly during "water conservation" times. If a connect/disconnect switch is installed in a water meter, the water valve can be disconnected to prevent flooding, or can be throttled to prevent excess water usage.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-48	Water Meter	ESI/HAN Gateway	Notification of a possible leak	Acknowledgments	C – Medium I – Medium A - Medium
HAN-42	ESI/HAN Gateway	Third party (water utility)	Notification of a possible leak	Acknowledgments	C – Medium I – Medium A - Medium
HAN-42	Third party (water utility)	ESI/HAN Gateway	Request to shut or throttle water valve	Response to request	C – Low I – Low A - Low
HAN-48	ESI/HAN Gateway	Water Meter	Request to shut or throttle water valve	Response to request	C – Low I – Low A - Low

2.4.2.4 Gas Leak Isolation

Similar to flood prevention, additional sensors and sophisticated analysis is needed to detect gas leaks. These may be applied to aggregations of customer sites rather than individual sites, except for unique situations.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-48	Gas Meter	ESI/HAN Gateway	Notification of a possible leak	Acknowledgments	C – Medium I – Medium A - Medium
HAN-42	ESI/HAN Gateway	Third party (gas utility)	Notification of a possible leak	Acknowledgments	C – Medium I – Medium A - Medium
HAN-42	Third party (gas utility)	ESI/HAN Gateway	Request to shut or throttle gas valve	Response to request	C – Low I – Low A - Low
HAN-48	ESI/HAN Gateway	Gas Meter	Request to shut or throttle gas valve	Response to request	C – Low I – Low A - Low

2.4.3 Third Party Maintenance & Management of HAN Systems and Appliances

The following business processes all involve the same set of interactions between a third party and systems and/or appliances on a HAN. Therefore the following interactions apply to all of them.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
Internet, phone, etc.	Customer	Third party	Authorization for HAN systems and/or appliances to be monitored and maintained by the third party	Acknowledgments	C – Medium I – Low A – Low
HAN-42	Third party	ESI/HAN Gateway	Request or command sent to a HAN device	Acknowledgments	C – High I – High A - Medium

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
HAN-34	ESI/HAN Gateway	Customer Appliances	Request or command sent to a HAN device	Acknowledgments	C – High I – High A - Medium
HAN-34	Customer Appliances	ESI/HAN Gateway	Response to request or command	Acknowledgments	C – High I – High A - Medium
HAN-42	ESI/HAN Gateway	Third party	Response to request or command	Acknowledgments	C – High I – High A - Medium

2.4.3.1 Third Party Access for Outsourced Utility Functions

For some utilities, many of the business functions typically identified as using AMI systems may be provided by third parties rather than by the utility, and therefore would necessarily utilize public and/or private networks, such as the Internet or GPRS cellphone networks.

These business processes would be fundamentally the same as if provided by the utility, but the authorization process and the security requirements could be significantly different and probably requiring stronger authentication at each system handoff.

Some of the business functions provided by third parties could include:

- Prepaid metering
- Remote connect/disconnect
- Load management
- Emergency control
- Customer energy usage information
- HAN management

2.4.3.2 Third Party Security Management of HAN Applications

Customers will need access to HAN application accounts through a secure web portal where they can upload device and software security keys. Those keys will need to be sent through the AMI network to the meter to allow the HAN devices to provision and join with the meter.

Future functionality may include extraction of security keys out of the meter for storage in the utility's database. This will allow the keys to be downloaded back to a meter if it ever has to be replaced. This functionality will be required to eliminate the need to re-provision all the HAN devices in the house in the event of a meter replacement.

2.4.3.3 HAN System and Appliance Monitoring and Maintenance

Third parties, including appliance vendors could monitor and/or remotely maintain certain appliances. The customer would first have to authorize them to perform this monitoring and maintenance.

2.4.3.4 Home Security Monitoring

Today's security monitoring industry uses phone lines and other communications methods to monitor homes. The ability to hook security monitoring devices into a home area network and provide alerts and alarms through the HAN could lower the cost of home security monitoring making it more affordable to the people who live in areas most likely to need it.

2.4.3.5 Medical Equipment Monitoring

More and more medical equipment is being installed in homes as nursing homes and hospitals are getting too expensive to live in and more life support equipment is required for people who still can live at home unassisted most of the time. Today that equipment is only monitored by specialized companies and this seldom happens. It is a growing need especially for the elderly customers of the utility. While utilities may not wish to step into this role, the smart metering infrastructure can provide a way for authorized third parties to do so.