White Paper for NIST CSWG: Cyber Security Requirements of Business Processes Involving AMI Systems

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

Table of Contents

1. Introduction

1.1 Cyber Security: Balancing Costs versus Impacts

Cyber security must balance the cost of implementing security measures against the likelihood and impact of any security breaches. This balancing of cost vs. impact must take into account that excessive costs could impact customer rates, but that inadequate security measures could allow unnecessary power outages to those same customers. The cost/impact balancing also must recognize that no single security measure is 100% effective in preventing a security breach. Therefore, layered security measures must be applied, and methods must be developed for deterring, detecting, and coping with security attacks, along with audit trails for forensic analysis, possible legal actions, and training.

The first step in determining a good cost/impact balance is to develop security requirements for all "cyber assets", where these assets can be defined as physical systems/equipment, stored cyber software and information, and information flows between systems. *The latter assets, "the information flows between systems" can be considered the critical assets for determining the cyber security requirements and ultimately the cyber security solutions.*

1.2 Cyber Security: Implementation Driven

Cyber security solutions must ultimately be implementation-specific, driven by the requirements for security of all of the functions in the system. However, "typical" security requirements can be developed and used as checklists for actual implementations.

In corporate settings, security requirements address the confidentiality, integrity, and availability of data using "Information Technology (IT)" security solutions such as cryptography, certificates, and physical access control. However, in the Smart Grid, the complexity of stakeholders, systems, devices, networks, and environments precludes just IT security techniques or one-size-fits-all security solutions. Therefore, additional criteria must be used in selecting the cyber security measures. These additional criteria must take into account the constraints posed by device and network technologies, legacy systems, organizational structures, regulatory and legal policies, and cost criteria. They should also take advantage of the existence of sophisticated equipment and systems that are already being used in the power system industry.

1.3 Cyber Security: Utilization of Existing Power System Management Capabilities

Power system operations have been managing the reliability of the power grid for decades in which "Availability of Power" has been a major requirement, with the "Integrity of Information" as a secondary but increasingly critical, requirement. "Confidentiality of Customer Information" has also been vitally important in the normal revenue billing processes. Although focused on inadvertent security problems, such as equipment failures, careless employees, and natural disasters, many of the methods, technologies, and mindsets can be expanded to cover deliberate security attacks as well.

So, one of the most powerful security solutions is to utilize and expand existing power system management technologies to provide additional security measures. After all, these power system management technologies (e.g. SCADA systems, Energy Management Systems, Contingency Analysis applications, Fault Location, Isolation, and Restoration functions, as well as Revenue Protection capabilities) have been refined for years to cope with the ever-increasing reliability requirements and complexity of power system operations, and are designed to detect anomalous events, notify the appropriate personnel or systems, cope during a problem, take remedial actions, and log all events with very accurate timestamps.

In the past, there has been little need for distribution management except possibly some load shedding to avoid serious problems. In the future, with generation, storage, and load on the distribution grid, utilities will need to implement more sophisticated power-flow-based applications to "manage" the distribution grid. AMI systems can also be used to provide energy-related information and act as secondary sources of information These same capabilities could be designed to help manage security as well.

Metering has also addressed concerns about revenue protection and customer confidentiality for many years, although the advent of smart meters has expanded those concerns to a significant degree. However, many of the same concepts of revenue protection could also be used for the smart grid.

In fact, expanding existing power system management capabilities to cover specific security requirements, such as power system reliability, should be a major security requirement.

2. Business Processes Involving AMI Systems

2.1 Cyber Security for Business Processes

The following sections describe the key business processes involving AMI systems. These business processes may be implemented differently by different utilities 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 (updated) AMI System "FERC4+2" diagram developed by EPRI for the NIST Interim Roadmap. These interfaces indicate the types of information which flow across them as well as rough estimates of the basic security requirements (confidentiality, integrity, and availability). These can be viewed as "security-focused Use Cases" since they are focused only on the AMI system interfaces and only expanded enough to identify the security requirements.

Basic security requirements (confidentiality/privacy, integrity, and availability) are assessed as high, medium, or low for the logical interfaces between actors. 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.

Many of these AMI-related business processes were listed in the UCA International Users Group AMI-SEC Security Requirements v1 document. Now they are being expanded to directly indicate the logical interfaces and actors that will need specific security requirements.

2.2 Diagram of AMI System Derived from NIST Roadmap Diagrams

The AMI Systems Use Case diagram of Actors, Logical Interfaces, and Networks was derived from the FERC4+2 diagrams developed by the EPRI team for the NIST Phase 1 Interim Roadmap project (only minor corrections and a few enhancements were made). This AMI System diagram captures the key interfaces used by the business processes (Use Cases), although clearly the diagram is at a high level: drilling down into each of the systems would uncover additional interfaces. However, it is expected that the security requirements for these key interfaces are illustrative for all the similar interfaces.

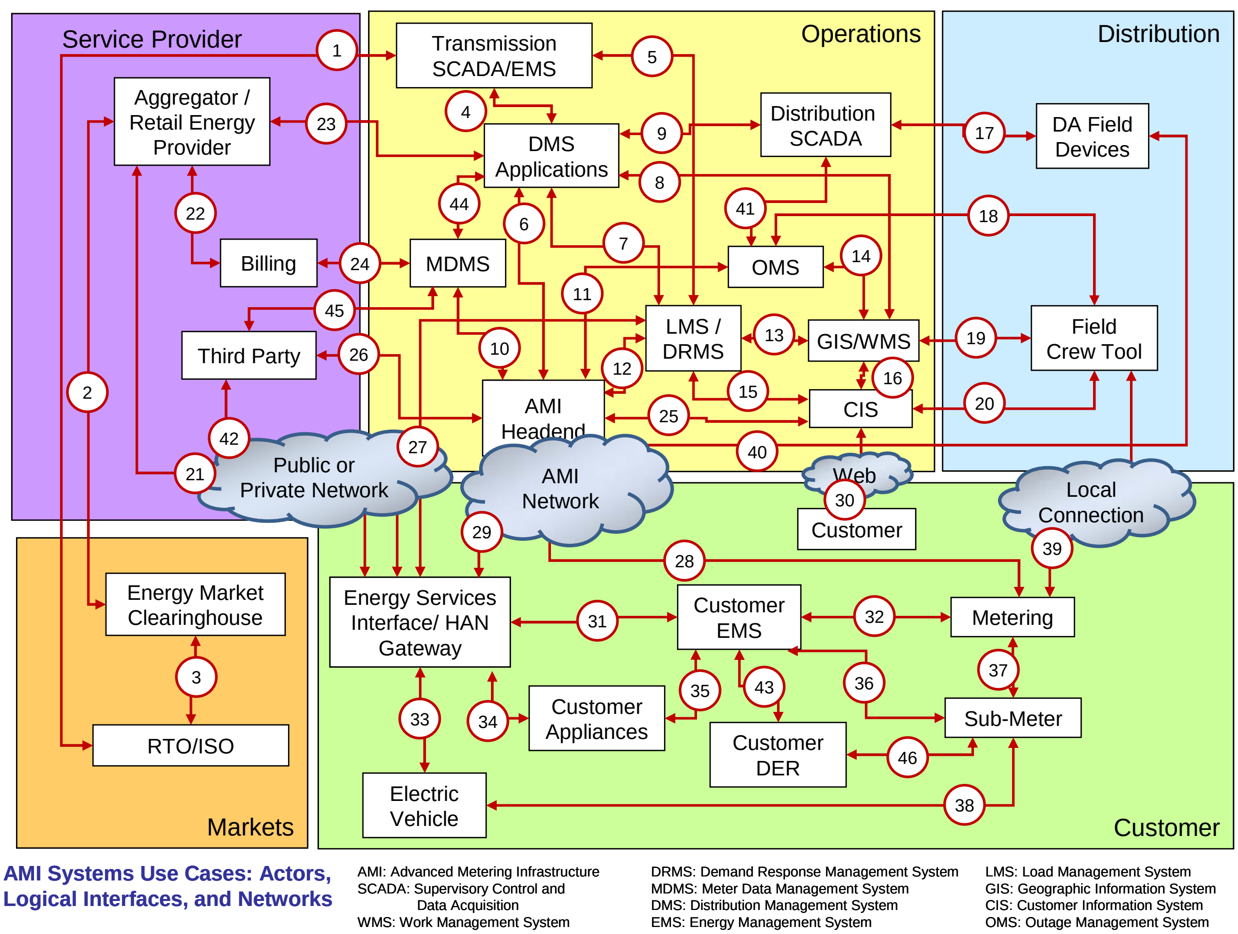

Figure 1: AMI System Actors, Logical Interfaces, and Networks

2.3 AMI System Actors and Logical Interfaces

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

- AMI-1: RTO/ISO – Utility EMS
- AMI-2: Energy Market Clearinghouse – Aggregator/Retail Energy Provider
- AMI-3: RTO/ISO – Energy Market Clearinghouse
- AMI-4: Utility EMS – DMS Applications
- AMI-5: Utility EMS – LMS/DRMS
- AMI-6: DMS Applications – AMI Headend
- AMI-7: DMS Applications – LMS/DRMS
- AMI-8: DMS Applications – GIS
- AMI-9: SCADA – DMS Applications
- AMI-10: MDMS – AMI Headend
- AMI-11: OMS – AMI Headend
- AMI-12: LMS/DRMS – AMI Headend
- AMI-13: LMS/DRMS – GIS
- AMI-14: OMS – GIS
- AMI-15: LMS/DRMS – CIS
- AMI-16: GIS – CIS
- AMI-17: SCADA – DA Field Devices
- AMI-18: OMS – Field Crew Tool
- AMI-19: GIS – Field Crew Tool
- AMI-20: CIS – Field Crew Tool
- AMI-21: Aggregator/Retail Energy Provider – ESI/HAN Gateway
- AMI-22: Aggregator/Retail Energy Provider – Billing
- AMI-23: Aggregator/Retail Energy Provider – DMS Applications
- AMI-24: Billing – MDMS
- AMI-25: CIS – AMI Headend
- AMI-26: Third Party – AMI Headend
- AMI-27: AMI Headend – ESI/HAN Gateway
- AMI-28: AMI Headend – Meter
- AMI-29: LMS/DRMS – ESI/ HAN Gateway
- AMI-30: Customer – CIS
- AMI-31: ESI/HAN Gateway – Customer EMS
- AMI-32: Customer EMS – Meter
- AMI-33: ESI/HAN Gateway – Electric Vehicle
- AMI-34: ESI/HAN Gateway – Customer Appliances
- AMI-35: Customer EMS – Customer Appliances
- AMI-36: Customer EMS – Sub-meter
- AMI-37: Meter – Sub-meter
- AMI-38: Electric Vehicle – Sub-meter
- AMI-39: Field Crew Tool – Meter
- AMI-40: DA Field Device – AMI Headend
- AMI-41: SCADA – OMS
- AMI-42: Third Party – ESI/HAN Gateway
- AMI-43: Customer EMS – Customer DER
- AMI-44: MDMS – DMS Applications
- AMI-45: MDMS – Third Party

3. AMI Metering Business Processes

3.1 Metering Services

Metering services provide the basic meter reading capabilities for generating customer bills. Different types of metering services are usually provided, depending upon the type of customer (residential, smaller commercial, larger commercial, smaller industrial, larger industrial) and upon the applicable customer tariff.

3.1.1 Periodic Meter Reading

Traditionally for residential customers and the smaller C&I customers, periodic meter reading services are performed monthly via a meter reader, possibly using handheld or mobile meter reading tools. It takes the current index reading from the meter and records it for billing and other purposes. For Time-of-Use (TOU) data from net metering or other TOU meters, intervals can be established such as "on-peak" and "off-peak", as defined in the utility's tariffs. In some utilities or under certain circumstances, actual meter reading is done less frequently, and bills rely on meter reading estimates which are "trued up" later.

In AMI systems, periodic meter reading will retrieve interval data (usually hourly data but possibly 15-minute or 5-minute data). The frequency of retrieving the data from the meter can vary from every 5 minutes, to hourly, to daily, and to monthly.

Among the benefits of AMI for periodic meter readings are the increased accuracy (fewer estimated reads, more exact reading dates/times), and the availability of the to-date meter readings during the billing cycle.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-10	MDMS	AMI Headend	(Periodically sent) List of meters to read	Meter readings Meter status Error messages from meters and AMI network	C – High I – High A - Low
AMI-28	AMI Headend	Meter	List of meters to read	Meter readings Meter status Error messages from meters and AMI network	C – High I – High A - Low
AMI 24	MDMS	Billing	Meter readings	(Acknowledgment and/or errors)	C – High I – High A - Low

3.1.2 On-Demand Meter Reading

Traditionally, on-demand meter reading is performed by sending a meter reader to the meter site around the time requested for the meter reading. Typically reasons for on-demand meter readings include:

- Move in / move out requests by customer
- Limited usage tariffs
- Billing questions by the customer
- Revenue protection concerns of utility
- Outage detection and restoration verification
- Sub-metering reading for DER, PEV, storage, or other separate metering to verify responses to direct load control commands

AMI systems will permit on-demand reads to take place almost immediately or more precisely at the scheduled date and time.

The customer can call to request an on-demand meter reading, or could use the customer web portal to request it. Various utility systems can also request an on-demand meter reading, including the Meter Data Management system, the Outage Management System, the Load Management system, and possibly DMS applications.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-30	Customer	CIS	Customer Move in/move out request	Acknowledgment Validated metering information	C – High I – Med A - Low
AMI-25	CIS	AMI Headend	Meter to read on-demand	Meter reading	C – High I – Med A - Low
AMI-11	OMS	AMI Headend	Ping request to determine if meter can respond	Ping response and/or meter reading	C – Low I – Low A - Low
AMI-12	LMS/DRMS	AMI Headend	Sub-meter to read to verify load control command	Sub-meter reading	C – High I – Med A - Low
AMI-06	DMS Applications	AMI Headend	Request voltage, var, frequency at meter	Electrical readings from meter	C – Low I – Low A - Low
AMI-10	MDMS	AMI Headend	List of meters to read	Meter readings	C – High I – Med A - Low

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-28	AMI Headend	Metering	On-demand request to read meter and other indicated information	Meter readings Error messages from meters	C – High I – High A - Low

3.1.3 Net Metering and/or Feed-in Tariffs for DER

When customers have the ability to generate or store power as well as consume power, net metering or feed-in tariffs can be applied to measure not only the flow of power in each direction, but also when the power flows occurred.

For net metering, Time of Use (TOU) tariffs are often employed, in which the price of power consumed is the same as the price for power generated, but that price is set according to the time period, usually higher in peak times. For feed-in tariffs, power generated can have a different price than power consumed during the same time period.

Today larger C&I customers and an increasing number of residential and smaller C&I customers have net metering or feed-in tariffs applied to their photovoltaic systems, wind turbines, combined heat and power (CHP), and other DER devices. As plug-in electric vehicles (PEVs) become available, these or special PEV tariffs will increasingly be implemented in homes and small businesses, even parking lots.

AMI systems can facilitate the management of net metering and special tariffs, and will become absolutely necessary if pricing becomes more dynamic and/or more fine-grained than currently used for TOU rates.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-10	MDMS	AMI Headend	(Periodically sent) List of meters to read	Meter readings Meter status Error messages from meters and AMI network	C – High I – High A - Low
AMI-28	AMI Headend	Meter	List of meters to read	Meter readings Meter status Error messages from meters and AMI network	C – High I – High A - Low
AMI 24	MDMS	Billing	Meter readings	(Acknowledgment and/or errors)	C – High I – High A - Low

3.1.4 Customer Selection of Billing Cycle Dates

Today, depending on the utility, electric bills are usually sent based on the meter reading schedules, not on a billing cycle selected by the customer. For certain customers, being able to select the billing cycle to match the date and frequency of their paycheck reduces the number of late or missing payments significantly, cutting collection costs and reducing the cost to all customers. Many multi-site commercial customers also prefer to have all the bills for each site to be coordinated to be sent at the same time or amalgamated into one bill so that they can be handled more efficiently.

AMI systems provide the flexibility to provide customers with bills when the customers prefer to receive them.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-10	MDMS	AMI Headend	(Sent when scheduled) List of meters to read	Meter readings Meter status Error messages from meters and AMI network	C – High I – High A - Low
AMI-28	AMI Headend	Meter	List of meters to read	Meter readings Meter status Error messages from meters and AMI network	C – High I – High A - Low
AMI 24	MDMS	Billing	Meter readings	(Acknowledgment and/or errors)	C – High I – High A - Low

3.2 Pre-Paid Metering

3.2.1 Prepayment of Energy

Customers who either want a lower rate or have a history of slow payment can benefit from prepaying for energy. Smart metering makes it easier to deploy new types of prepayment to customers and provide them with better visibility on the remaining hours of power, as well as extending time of use rates to prepayment customers.

AMI systems can also trigger notifications to customers when the pre-payment limits are close to being reached and/or have been exceeded. Customers can then add to their pre-payment amount over the web, or through the AMI system, or through conventional means.

When a prepayment limit has been reached with no payment, load demand can be limited, only critical loads can be serviced, total load can be completely disconnected, or other actions can be taken across the AMI system.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-32	Meter	Customer EMS	Pre-payment status	Notification of receipt of any alarms (close to limit, over limit)	C – High I – Medium A - Low
AMI-30	Customer	CIS	Customer pre-payment (debit card, credit card, Paypal, or other methods)	Acknowledgment Validated metering information	C – High I – High A - Low
AMI-25	CIS	AMI Headend	Amount of payment	Acknowledgment	C – High I – High A - Low
AMI-28	AMI Headend	Meter	Prepayment amount (either as monetary value or as equivalent metering data	Reset of prepayment amount	C – High I – High A - Low
AMI-10	MDMS	AMI Headend	(On non-payment) Disconnect of entire load, partial load, or load demand limiting	Meter readings Meter status Disconnect status	C – High I – High A - Low
AMI 24	MDMS	Billing	Meter readings and pre-payment amounts	(Acknowledgment and/or errors)	C – High I – High A - Low

3.2.2 Limited Energy Usage

Traditionally, customers who use pre-payment tariffs need to go through the utility customer representatives to learn about their current usage or to extend their energy limits. With AMI systems, customers can see their current usage and limits, and may be able to automatically extend their limits electronically (e.g. pay over the Internet or through the AMI system then updating their energy limits).

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-10	MDMS	AMI Headend	Set or reset limits for energy usage	Meter readings Meter status Limit status	C – High I – High A - Low
AMI-32	Meter	Customer EMS	Energy usage status	Notification of limit alarms (close to limit, over limit)	C – High I – Medium A - Low

3.2.3 Limited Demand

Customers can also have tariffs that limit demand at any time or for specific time periods (e.g. during on-peak times). Some C&I customers have rates that depended on the peak 15-minute demand. Some other customers actually have current limiting equipment to ensure limited demand.

AMI systems can set meters to establish these limits, provide customers with the information necessary to manage their demand limits more precisely and effectively, and issue notifications when limits are close to being exceeded or are being exceeded. In some cases, load demand limiters could be added to prevent demand limits from being exceeded.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-10	MDMS	AMI Headend	Set or reset limits for demand levels for different time periods	Meter readings Meter status Limit status Notifications of exceeded limits	C – High I – High A - Low
AMI-32	Meter	Customer EMS	Limit demand status	Notification of limit alarms (close to limit, over limit)	C – High I – Medium A - Low

3.3 Revenue Protection

3.3.1 Tamper Detection

Non-technical losses (or theft of power by another name) has long been an on-going battle between utilities and certain customers. In a traditional meter, when the meter reader arrives, they can look for visual signs of tampering, such as broken seals and meters plugged in upside down. During the analysis of the data, tampering that is not visually obvious may be detected, such as anomalous low usage.

With AMI systems, smart meters can immediately issue "tampering" alarms that are set off by a number of different sensors and routines in the meter. These tampering actions can include meter removal, meter tilt, and unauthorized access attempts (smart meters cannot be plugged in upside down).

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-28	Meter	AMI Headend	Tamper detection event codes Meter readings Meter status	Flag as "to be watched"	C – High I – Medium A - Low
AMI-10	AMI Headend	MDMS	Tamper detection event codes Meter readings Meter status	Flag as "to be watched	C – High I – Medium A - Low

3.3.2 Anomalous Readings

Some anomalous readings in the meter can trigger warning events which can be immediately investigated to determine if they are legitimate (people are on vacation or the factory has shut down an assembly line) or if they are due to tampering, such as wiring around the meter.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-25	MDMS	CIS	Anomalous meter readings – Flag to contact customer	Indication of "all OK" or "possible tampering"	C – High I – High A - Low

3.3.3 Periodic Meter Status to Detect Any Tampering

Some theft of power has occurred by the bypassing of the meter for a few days between scheduled readings by a meter reader. AMI systems will permit the status of meters to be verified at any time during the reading cycle.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-10	MDMS	AMI Headend	(Periodically sent) List of meters to check tampering status	Meter status	C – High I – High A - Low
AMI-28	AMI Headend	Meter	List of meters to check status	Meter status Any tampering indications	C – High I – High A - Low
AMI 25	MDMS	CIS	Possible tampering – Flag to contact customer	Indication of "all OK" or "possible tampering"	C – High I – High A - Low

3.3.4 Suspicious Meter

Some theft of power has occurred by the replacement of a certified meter with a "slow run" meter. AMI systems with smart meters will have each meter "registered" with an identity that cannot be tampered with without showing evidence of that tampering.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-28	AMI Headend	Meter	List of meters to read	Invalid meter registration ID or indication of tampering with registration ID	C – High I – High A - Low
AMI 10	AMI Headend	MDMS	Invalid meter registration ID	Flag meter as invalid	C – High I – High A - Low
AMI 25	MDMS	CIS	Possible tampering – Flag to contact customer	Indication of "all OK" or "possible tampering"	C – High I – High A - Low

3.4 Remote Connect / Disconnect

3.4.1 Remote Connect for Move-In

The customer initiates a request to move into a location that has electric service but is currently disconnected at the meter. The request could be for immediate action or for a specific date and time.

Traditionally, utilities send a metering service person to connect the meter. With an AMI system, the connection can be performed remotely by closing the remote connect/disconnect (RCD) switch, using the following steps:

- At the appropriate date and time, read the meter to get the latest reading and to verify that the meter is functional.
- Determine there is no backfeed current detected by the meter
- Issue the connect command to the RCD switch at the meter
- Verify that the meter is now connected

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI 25	CIS	MDMS	Date and time to issue meter connect command	Acknowledgment when action completed	C – High I – High A - Low
AMI-28	AMI Headend	Meter	(At appropriate date and time) Meter reading, Backfeed detection, RCD connect command, 2nd meter reading	Meter readings, RCD switch status	C – High I – High A - Low

3.4.2 Remote Connect for Reinstatement on Payment

Once a customer pays who was disconnected due to non-payment (or works out some mutually accepted agreements), the meter needs to be reconnected by closing the remote connect/disconnect (RCD) switch. The same process as for a move-in would be used.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI 25	CIS	MDMS	Date and time to issue meter connect command	Acknowledgment when action completed	C – High I – High A - Low
AMI-28	AMI Headend	Meter	(At appropriate date and time) Meter reading, Backfeed detection, RCD connect command, 2nd meter reading	Meter readings, RCD switch status	C – High I – High A - Low

3.4.3 Remote Disconnect for Move-Out

Traditionally, move-outs are handled by performing a special meter read ("soft" disconnect) around the time of the move-out. Since the power is not actually disconnected, this method can lead to illegal use of power after the move-out and before the next move-in.

With an AMI system, a move-out can have a "hard" disconnect that opens the RCD switch, typically using the following steps:

- Verify that the meter can be disconnected remotely
- Issue the disconnect command at the appropriate date and time
- Verify that the meter is disconnected
- Read the meter for the final billing.

In conjunction with the next meter reading during a subsequent move-in connection, any delta between the readings can be detected as a possible tampering or illegal usage of power.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI 25	CIS	AMI Headend	Date and time to issue meter disconnect command	Acknowledgment when action completed	C – High I – High A - Low
AMI-28	AMI Headend	Meter	(At appropriate date and time) Meter reading, RCD disconnect command, 2nd meter reading	Meter readings, RCD switch status	C – High I – High A - Low

3.4.4 Remote Disconnect for Non-Payment

The cost of collections for non-payment of electric bills is high, typically higher yet is the cost of disconnecting a customer – not only the lost revenue, but the cost of two special trips to the location, one to turn the power off and eventually another to turn it back on again. Remote disconnects offer a much lower cost for turning the power off, and once customers understand that a disconnect can be done immediately, collections costs may also decline.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI 25	CIS	AMI Headend	Date and time to issue meter disconnect command	Acknowledgment when action completed	C – High I – High A - Low
AMI-28	AMI Headend	Meter	(At appropriate date and time) Meter reading, RCD disconnect command, 2nd meter reading	Meter readings, RCD switch status	C – High I – High A - Low

3.4.5 Remote Disconnect for Emergency Load Control

Typically load shedding for emergency situations is performed by tripping an entire feeder, thus affecting all customers on that feeder. However, if some customers could get special rates for agreeing to the temporary suspension of electric service in support emergency load shed activities, then this would be an alternative to wide-scale rolling blackouts and/or circuit level interruptions. This type of selective load shedding provides the means for reducing power demands on a particular feeder, while selectively maintaining service to critical customers such as public infrastructure (i.e. traffic lights) and medical facilities.

AMI systems provide the ability to implement these emergency load shedding schemes.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI 25	CIS	AMI Headend	Date and time to issue meter disconnect command	Acknowledgment when action completed	C – High I – High A - Low
AMI-28	AMI Headend	Meter	(At appropriate date and time) Meter reading, RCD disconnect command, 2nd meter reading	Meter readings, RCD switch status	C – High I – High A - Low

3.4.6 Unsolicited Connect / Disconnect Event

Unsolicited connect/disconnect events can be caused by a number of activities, covered in the following Business Functions:

- Meter manually switched off by utility employee, including both valid and invalid switching
- Meter manually switched off by unknown party, including both valid and invalid switching
- Software/hardware failure switches meter off/on (also includes unauthorized command causing switch)
- Miscellaneous event causes meter to switch off/on
- Meter manually switched on by utility employee, including both valid and invalid switching
- Meter manually switched on by unknown party, including both valid and invalid switching

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-28	Meter	AMI Headend	Notification of unsolicited connect or disconnect of RCD switch	Meter readings, RCD switch status	C – High I – High A - Low
AMI 25	MDMS	CIS	Request to determine cause of connect or disconnect	Response to request	C – High I – High A - Low

3.5 Outage Detection and Restoration

3.5.1 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
AMI-28	Meter	AMI Headend	Outage notification	Verification of outage (ping)	C – Low I – Medium A - Low
AMI-11	AMI Headend	OMS	Outage notification		C – Low I – Medium A - Low

3.5.2 Shut-Down or Islanding Verification for DER

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
AMI-28	Meter	AMI Headend	DER outage notification	Verification of DER outage (ping)	C – Low I – Medium A - Low
AMI-11	AMI Headend	OMS	DER outage notification		C – Low I – Medium A - Low

3.5.3 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
AMI-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
AMI-11	OMS	AMI Headend	Request for restoration notification	Restoration notification	C – Low I – Medium A - Low
AMI-28	AMI Headend	Meter	Ping the status of the meter	Restoration notification	C – Low I – Medium A - Low

3.5.4 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
AMI-11	OMS	AMI Headend	Scheduled outage notification	Acknowledgment	C – Low I – Medium A - Low
AMI-27	AMI Headend	ESI/ HAN Gateway	Outage notification		C – Low I – Medium A - Low

3.5.5 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
AMI-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
AMI-11	OMS	AMI Headend	Request for restoration notification	Restoration notification	C – Low I – Medium A - Low
AMI-28	AMI Headend	Meter	Ping the status of the meter	Restoration notification	C – Low I – Medium A - Low

3.5.6 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. AMI systems could be used to monitor these lights.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-40	Street light	AMI Headend	Notification of street light failure	Verification	C – Low I – Medium A - Low
AMI-11	AMI Headend	OMS	Notification of street light failure	Verification	C – Low I – Medium A - Low

3.6 Meter Maintenance

3.6.1 Meter Connectivity Validation

Many utilities do not have accurate information on meter connectivity to the grid, including what phase it is connected to, and sometimes even what feeder it is connected to. As AMI systems are deployed, this type of validation can correct the circuit diagrams and power flow models to ensure they are accurate for engineering studies, real-time operational studies, and cyber security analysis of anomalous situations.

Metering connectivity information can also be used to help manage microgrids and other dynamic grid configuration changes.

Mobile meters, such as those that may be used for plug-in electric vehicles, are discussed elsewhere.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-28	Meter	AMI Headend	Meter grid connectivity status and possibly phase connection		C – Low I – Low A - Medium

3.6.2 Geo-Location

In asset databases today, many meters can be miles from their physical location. During the installation of the meters, GPS or other geo-location techniques can be used to provide accurate information on the meter's location. If the location of the meter accidentally is changed in the database it is possible to flag the problem. This is possible since the location of the circuit is known, helping to eliminate problems that creep in over the long life of electric (gas and water) networks.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-28	Meter	AMI Headend	Meter grid geographical location		C – Low I – Low A - Low

3.6.3 AMI Equipment Battery Management

Batteries will be used in many parts of AMI systems, including the AMI communication neighborhood nodes, gas meters, and water meters. Remote battery monitoring can help manage battery failure monitoring, battery replacement planning, and battery life extension.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-28	AMI Headend	Meter	Battery status		C – Low I – Low A - Low

4. Distribution Operations Business Processes Using AMI

4.1 Distribution Automation (DA) Using the AMI System

4.1.1 DA Equipment Monitoring and Control

When a utility implements distribution automation (DA), the Distribution SCADA systems typically monitors and controls DA field equipment via dedicated DA networks. However, some utilities are planning to use the AMI system for distribution automation. At a minimum, the AMI system could be used for direct monitoring of DA field equipment and could also allow more sophisticated control schemes of capacitor banks and voltage regulators on feeders, rather than relying on local actions triggered by time, current, or voltage levels. Other utilities also would like to monitor and control automated switches and fault indicators if the AMI network were able to stay alive during grid power outages, presumably via battery backup for critical nodes.

Some of the security-related issues of DA monitoring and control are:

- Media is usually narrowband, limiting the volume of traffic and impacting the types of security measures that are feasible.
- IEDs can be limited in compute power, impacting the types of security controls that can economically be implemented.
- IEDs are on poletops and other insecure locations.
- Wireless media is often less expensive than wired media, which mean that wireless vulnerabilities exists, and will require security controls appropriate for wireless.
- None of the communication protocols currently used (primarily DNP3 and sometimes IEC 61850) are typically implemented with security measures, although IEC 62351 (which are the security standards for these protocols) is now available.
- These functions have real-time operational requirements, with critical time latencies, which limits the choices for stopping or mitigating on-going attacks.
- Some of the equipment is legacy (particularly the RTUs) which limit the types of security controls that could be implemented without replacing or upgrading the equipment.
- Key management with thousands of devices is an issue that needs to be solved.

- Since confidentiality has not been perceived as important, and where the media and compute constraints apply, encryption may not necessarily be required for general messaging.

Assuming the use of the AMI System for DA monitoring and control, the following interfaces could be used.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-40	DA Field Equipment	AMI Headend	Power system information from DA equipment	Control commands to DA equipment	C – Low I – High A - Medium
AMI-6	AMI Headend	DMS Applications	Power system information from DA equipment	Control commands to DA equipment	C – Low I – High A - Medium

4.1.2 Smart Meters as One Source of Power System Operational Information

If more sensors were available in the distribution network, it would be possible to do distribution SCADA, with the deployment of smart meters and a near real-time communications network, it is possible to pick a sub-set of the smart meters and use them as strategically located sources of distribution grid information to provide a distribution SCADA-like capability. In addition some utilities are installing smart meters in place of RTUs for extending their current SCADA system further into the grid.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-28	Meter	AMI Headend	Power system information from meters		C – Low I – High A - Medium
AMI-6	AMI Headend	DMS Applications	Power system information from meters		C – Low I – High A - Medium

4.1.3 Smart Meters for Detecting Power System Cyber Attacks

Smart meters can be used to detect possible cyber security “attacks”, whether they are inadvertent mistakes or equipment failures or whether they reflect deliberate threats to the operation of the distribution grid.

Smart meters offer a way to detect anomalous behavior or activities across the entire distribution system. For instance, if voltage levels at a number of neighboring meters rapidly drop below the normal limit, it may indicate the failure of a voltage regulator or load tap changer. If a number of metering remote disconnect switches start turning off without being commanded by the utility, indicating a possible cyber attack via these switches, then the AMI system could take action such as issuing a broadcast command to all meters to ignore disconnect commands.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-28	Meter	AMI Headend	Power system information from meters, including alarms and events		C – Low I – High A - Medium
AMI-6	AMI Headend	DMS Applications	Power system information from meters	Commands to isolate or mitigate possible cyber security attacks	C – Low I – High A - Medium

4.1.4 Power System Equipment Protection

In the past, overloads on power system equipment for short periods of time were considered normal since they were designed (over-designed?) to operate at two or even three times their rated capacity for several hours on a peak day. Today these devices either have been engineered to run at loads much closer to their ratings or the power system is operating much closer to their limits for longer periods of time. Therefore, frequent overloads of multiple hours can cause serious degradation or failure of these devices. By being able to monitor the devices in real-time, preventative actions can be taken, such as shifting loads to other equipment or even initiating direct (or indirect) load control or well-focused load shedding.

Some power system information could come from the equipment itself, while other information could come from judiciously identified meters.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-40	DA Field Equipment	AMI Headend	Power system information from DA equipment	Control commands to DA equipment	C – Low I – High A - Medium
AMI-28	Meter	AMI Headend	Power system information from meters	Remote disconnect of specific meters	C – Low I – High A - Medium
AMI-29	LMS/DRMS	ESI/HAN Gateway	Load control command (direct or indirect)	Response to load control command	C – Low I – High A - Medium

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-6	AMI Headend	DMS Applications	Power system information from DA equipment	Control commands to DA equipment	C – Low I – High A - Medium

4.1.5 Personnel Safety via Site/Circuit Status

Tag out procedures are supposed to render a segment of the network dead and safe to work on. Unfortunately, with the addition of distributed generation to feeders and at customer sites, it is possible to have power system failure where the crew expects the circuit to be dead, to actually still be live. Using power flow models with accurate meter and DA equipment connectivity mapping, it would be possible to use these meters to determine if any power is still flowing through the presumably dead circuits. With the potential for the sales of plug-in hybrids to ramp up quickly in the next decade and the lack of DER-focused protection schemes, this may become an even larger issue.

This personnel safety function could prevent serious "security" impacts from inadvertent – or deliberate – security compromises.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-40	DA Field Equipment	AMI Headend	Power system live/dead status from DA equipment	Control commands to DA equipment to ensure dead circuits	C – Low I – High A - Medium
AMI-28	Meter	AMI Headend	Power system live/dead status from meters	Remote disconnect of customer DER equipment	C – Low I – High A - Medium
AMI-6	AMI Headend	DMS Applications	Power system information from DA equipment	Control commands to DA equipment	C – Low I – High A - Medium
AMI-11	AMI Headend	OMS	Power system outage information		C – Low I – High A - Medium
AMI-18	OMS	Field Crew Tool	Power system outage information		C – Low I – High A - Medium

4.1.6 Automation of Emergency Response

Today in a fire or other emergency situation involving customer facilities, the fire department normally handles the disconnection of the power and other utilities from the involved buildings, sometimes with a fire axe! With the availability of remote disconnects in meters, utilities can remotely and safely cut power to the buildings in danger, as well as shut off gas, water, and other utilities. This use of the remote disconnect capability can also make it easier to restore service after the emergency has been resolved.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI 25	CIS	AMI Headend	Immediate meter disconnect command	Acknowledgment when action completed	C – Low I – High A - High
AMI-28	AMI Headend	Meter	Immediate meter disconnect command	Meter readings, RCD switch status	C – Low I – High A - High

4.1.7 Dynamic Rating of Feeders

Operators can dynamically rate feeders based on the more accurate power system information retrieved via the AMI system from strategic locations. This permits the operators to decide when and for how long they can allow overloaded feeders beyond their normal ratings or when to perform multi-level feeder reconfigurations to balance the loads and avoid overloads.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-28	Meter	AMI Headend	Power system information from meters		C – Low I – High A - Low
AMI-6	AMI Headend	DMS Applications	Power system information from meters		C – Low I – High A - Low

4.2 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 more precise method of managing load and generation: as a callable and schedulable resource, it 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.

For all functions involving direct control actions, the commands must be validated either by the equipment being controlled or by the Energy Services Interface gateway into the customer site.

4.2.1 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
AMI-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
AMI-29	AMI Headend	ESI/HAN Gateway	Load control signal	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low
AMI-27 (non-AMI alternative to AMI-12/ AMI-29)	DRMS/LMS	ESI/HAN Gateway	Load control signal	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-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
AMI-33	ESI/HAN Gateway	Electric Vehicle	Load control signal (charging rate)	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low
AMI-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
AMI-35	Customer EMS	Customer Appliances	Load control signal (start/stop cycling)	Acknowledgment of receipt of load control signal	C – Low I – Medium A - Low

4.2.2 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
AMI-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
AMI-29	AMI Headend	ESI/HAN Gateway	Load control signal	Acknowledgment of receipt of load control signal	C – Low I – High A - High
AMI-27 (non-AMI alternative to AMI-12/ AMI-29)	DRMS/LMS	ESI/HAN Gateway	Load control signal	Acknowledgment of receipt of load control signal	C – Low I – High A - High

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

4.2.3 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
AMI-12	DRMS/LMS	AMI Headend	DER control signal List of HAN addresses	Acknowledgment of receipt of DER control signal	C – Low I – Medium A - Medium
AMI-29	AMI Headend	ESI/HAN Gateway	DER control signal	Acknowledgment of receipt of DER control signal	C – Low I – Medium A - Medium
AMI-27 (non-AMI alternative to AMI-12/ AMI-29)	DRMS/LMS	ESI/HAN Gateway	DER control signal	Acknowledgment of receipt of DER control signal	C – Low I – Medium A - Medium
AMI-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 - Medium
AMI-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 - Medium
AMI-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 - Medium

4.3 Distributed Energy Resource (DER) Management

The advent of decentralized electric power production is a reality in the majority of the power systems all over the world, driven by the need for new types of energy converters to replace the heavy reliance on oil, by the increased demand for electrical energy, by the development of new technologies of small power production, by the deregulation of the energy market, and by the increasing environmental constraints. These pressures have greatly increased the demand for Distributed Energy Resources (DER) systems which are interconnected with the distribution power systems.

Distribution power systems are and will continue to be the most impacted by DER, but transmission and the management of generation operations are also impacted. A number of studies on the wide-spread interconnection of DER systems have shown significant effects and impacts on operation of the entire electrical system.

As a result not only of DER systems, but also the need for greater efficiency and reliability of the power system, automation of the distribution systems is becoming a major requirement. This distribution automation implies new remote control functions, modified distribution configurations, increasingly intelligent protection systems, and the use of significantly more telecommunication and information technologies, including AMI systems to reach to DER systems at customer sites.

4.3.1 Outsourced Management of DER Generation and Storage

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 communications.

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.

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
AMI-23	Aggregator/ Retail Energy Services Provider	DMS Applications	DER monitoring and control requests	DER monitored information and control acknowledgments	C – Low I – Medium A - Medium
AMI-6	DMS Applications	AMI Headend	DER monitoring and control requests	DER monitored information and control acknowledgments	C – Low I – Medium A - Medium
AMI-29	AMI Headend	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
AMI-21 (non-AMI alternative to AMI-23/ AMI-6/ AMI-29)	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
AMI-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
AMI-43	Customer EMS	DER	DER control signal (% generation, import/export level or %, urgency, etc.)	DER monitored information and control acknowledgments	C – Low I – Medium A - Medium

4.3.2 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
AMI-23	Aggregator/ Retail Energy Services Provider	DMS Applications	PEV monitoring and control requests	PEV monitored information and control acknowledgments	C – Low I – Medium A - Medium
AMI-6	DMS Applications	AMI Headend	PEV monitoring and control requests	PEV monitored information and control acknowledgments	C – Low I – Medium A - Medium
AMI-29	AMI Headend	ESI/HAN Gateway	PEV monitoring and control requests	PEV monitored information and control acknowledgments	C – Low I – Medium A - Medium
AMI-21 (non-AMI alternative to AMI-23/ AMI-6/ AMI-29)	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
AMI-33	Customer EMS	PEV	PEV control signal (% generation, import/export level or %, urgency, etc.)	PEV monitored information and control acknowledgments	C – Low I – Medium A - Medium

4.4 Power Quality Management

4.4.1 Power Quality Monitoring via Smart Meters

Using smart meters, power quality can be monitored, including harmonics, wave form, phase angles, and other power quality indicators. The need continues to grow as large screen televisions and other consumer electronics devices are increasingly adding harmonics to the system. With the newest metering technology, some power quality monitoring is built into the meter and more is on the way. The AMI system can then be used to retrieve this power quality information either periodically or during major power quality events.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-28	Meter	AMI Headend	Power quality information		C – Medium I – Medium A - Low

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-6	AMI Headend	DMS Applications	Power quality information		C – Medium I – Medium A - Low

4.4.2 Asset Load Monitoring

With connectivity verification and geo-location information it is possible to group the devices in a tree structure that correctly shows connection points in the grid. With the ability to read intervals from the meters it is then possible to build a picture of the load that each asset (e.g. transformers, conductors, etc.) are subjected to. This allows an operator to monitor heavily loaded assets and look for ways to off load some of the demand from that asset. It also allows a maintenance planner to prioritize what maintenance should be done to maximize the reliability of the grid, as part of a reliability centered maintenance program.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-25	AMI Headend	CIS	Meter connectivity information		C – Low I – Low A - Low
AMI-16	CIS	GIS	Meter connectivity information		C – Low I – Low A - Low
AMI-8	GIS	DMS Applications	Potential overload information and locations		C – Low I – Low A - Low

4.4.3 Phase Balancing

One of the least talked about issues with losses in the distribution grid today is single phase load and the imbalance it can cause between the phases. These losses have seldom been measured in the grid and little study has been done of the amount of phase imbalance on the grid today. In early studies the chronic phase imbalance in several circuits that were monitored averaged over 10 percent. While correction is hard when the circuit is run as single phase laterals, in many cases there is enough load on the feeder portion of the circuit to allow rebalancing of the circuit to eliminate more than half of the chronic phase imbalance.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-25	AMI Headend	CIS	Meter phase connectivity		C – Low I – Low A - Low
AMI-16	CIS	GIS	Meter phase connectivity		C – Low I – Low A - Low
AMI-8	GIS	DMS Applications	Validated connectivity of loads per phase		C – Low I – Low A - Low

4.4.4 Load Balancing

When automated feeder reconfiguration and feeder segment reconnection can be used to move a portion of the load from one circuit to another, the instrumentation is not always available to make good choices or to be able to forecast the load in a way that makes the movement pro-active instead of reactive. The ability to use metering data to support the operation of these devices will allow the grid operator to perform load balancing after definitive studies rather than guesses.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-25	AMI Headend	CIS	Meter feeder segment location and load		C – Low I – Low A - Low
AMI-16	CIS	GIS	Meter feeder segment location and load		C – Low I – Low A - Low
AMI-8	GIS	DMS Applications	Validated meter feeder segment location and load		C – Low I – Low A - Low

4.5 Work Management

4.5.1 Work Scheduling Base on Predictive Maintenance Analysis

Maintenance can be more efficiently scheduled if it is based on predictive maintenance analysis, rather than on a fixed periodicity. Without such predictive analysis, some maintenance is performed that is not really required, while other devices fail because they did not receive timely maintenance. When smart metering information is available and used to do asset loading analysis and other data analysis, work can be more accurately dispatched to the crews in the field improving reliability in the system for the same number of jobs completed.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-14	OMS	GIS/WMS	Equipment outage information		C – Low I – Low A - Low
AMI-8	DMS Applications	GIS/WMS	Predicted maintenance results, with request to schedule maintenance		C – Low I – Low A - Low
AMI-19	GIS/WMS	Field Crew Tool	Schedule of maintenance activities for crew		C – Low I – Low A - Low

4.5.2 Field Crew Order Completion Automation

Some utilities have the field crew log the completion of their job prior to packing up; others want the crew ready to roll prior to completion of the order. Some want the crews to look around before leaving, some want the crew to leave and let the customers call if there is still an issue in the area. With smart metering, as restoration alerts come in, it is possible to automate the time the job was completed and some of the closing paperwork, allowing the crew to stay in the field longer each day and to do less paperwork overall.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-19	GIS/WMS	Field Crew Tool	Schedule of activities for crew	Completion information	C – Low I – Low A - Low

4.5.3 Field Worker Data Access

Access to information on field equipment location, status, ratings, and history can make field crews more efficient.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-19	GIS/WMS	Field Crew Tool	Request for information on equipment	Information on equipment	C – Low I – Low A - Low

4.6 Distribution Planning and Engineering

The following functions utilize information obtained from smart meters via the AMI system, but will not generally collect this information directly. Therefore, these functions do not have any security requirements in addition to those already needed while collecting the information.

4.6.1 Outage Prevention through Vegetation Management

Momentary outages normally increase as vegetation grows back in an area and starts to become potential issue for overhead lines. Smart metering allows the return of momentary outage information and allows the outage counts to be overlaid on a GIS system. This allows the planners to better target vegetation management people to the right locations. In the underground world, cable failures and splice failures can be found early, prior to a complete failure.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-14	OMS	GIS/WMS	Momentary outage information	Information on equipment	C – Low I – Low A - Low
AMI-8	GIS/WMS	DMS Applications	Outage counts	Schedule for vegetation management	C – Low I – Low A - Low

4.6.2 Regional and Local Load Forecasting

By aggregating metering data by feeder, substation, and/or region, it is possible to forecast regional and local loads and generation that can be used to prepare for and to set prices for both demand and supply.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-44	MDMS	DMS Applications	Aggregated metering data by location		C – Low I – Low A - Low
AMI-7	DMS Applications	LMS/DRMS	Pricing by location		C – Low I – Low A - Low

4.6.3 Simulations of Responses to Pricing and Direct Control Actions

As more detailed information is available through AMI systems on regional and local loads and generation, it will be possible to assess the responses of both customers and the power system to price-related actions as well as direct control actions. This ability to simulate the market a day or more in advance should allow for better planning and for the system to run with smaller amounts of rolling reserve and ancillary services.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-7	DMS Applications	LMS/DRMS	Pricing by location		C – Low I – Low A - Low
AMI-44	MDMS	DMS Applications	Responses by customers to pricing		C – Low I – Low A - Low

5. Customer Interaction Business Processes

5.1 Customer Services

5.1.1 Customer Energy Usage Information

Customers can request the utility to provide their energy usage to a 3rd party so that this 3rd party can provide certain services to the customers, such as recommending changes to their energy usage profiles.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-30	Customer	CIS	Request to let 3rd party have access to their energy usage	Acknowledgment	C – Low I – Low A - Low
AMI-45	MDMS	Third Party	Energy usage information from authorized customers	Acknowledgment	C – High I – High A - Low

5.1.2 Customer Power-Related Problem Assessment

When a customer calls today with a power-related problem, it is important to determine whether it is a customer-owned problem behind the meter or a utility-owned problem. Use of near real time information from smart meters can allow the customer service representative to collect more specific data, to determine if it is probably a utility problem, or, if it is a customer problem, to provide appropriate advice to the customer. This process reduces the dispatch of trucks for customer-owned problems and can reduce both call volume and call handling times.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-25	CIS	AMI Headend	Request for metering status	Metering status	C – Low I – Low A - Low
AMI-28	AMI Headend	Metering	Request for metering status	Metering status	C – Low I – Low A - Low

5.1.3 Customer Billing Dispute Management

The most frequent customer dispute is a high bill. Sometimes these bills are wrong due to meter reading errors or poor estimation of previous readings. The AMI system allows the customer representative to check the current meter reading directly from the meter while the customer is on the phone and re-calculate the bill if necessary. If the meter reading is correct, the customer representative can provide the customer with the details, including energy usage for every time period.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-25	CIS	AMI Headend	Request for metering data	Metering data	C – Low I – Low A - Low
AMI-28	AMI Headend	Metering	Request for metering data	Metering data	C – Low I – Low A - Low

5.1.4 Customer Energy Usage Display

As customers are put on TOU and/or Demand Response tariffs, they need to be able to see how much energy they are using at any given time, including in real-time and historically. They can then use this information to project the cost of energy for different usage patterns, and make decisions on how they are going to respond to these tariffs.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-32	Metering	Customer EMS (display)	Energy usage data		C – Low I – Low A - Low

5.2 Tariffs and Pricing Schemes

All of the tariff and pricing analysis is performed in the back office environment, epitomized by the interface between the CIS and the LMS/DRMS, by using aggregated customer information to determine tariffs (approved by regulators) and pricing schemes (reflecting the tariffs).

The following interface table is the same for all of these tariff and pricing schemes functions.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-15	CIS	LMS/DRMS	Aggregated customer information	Analyzed customer data reflecting possible tariffs and/or pricing schemes	C – Low I – Low A - Low

5.2.1 Tariff Design

Today a sample of the customers is used to determine what the customer profile should be and how that profile should be priced. In many cases the classification of the customers is very broad and does not really take into account the different ways that customers actually consume power.

For example, a young educated single male living in an apartment may have a lower usage than the young family across the hallway and they may both pay the same per kilowatt-hour of power. However, the young male many actually cost the utility more to serve, since the load factor for that single male may be much lower than the load factor for the young family. By being able to provide accurate data, better tariffs can be designed and better segmentation done to support a fair power price.

5.2.2 Rate Case Support

Today to get almost any change in what can be charged to the customers or what is placed in the rate base, it requires a rate case. In some rate cases the documents filed fill rooms and rooms in a building, mostly because the issues can be handled in a black and white manner. Experts are required to testify on many aspects of the rate case using data from other locations, since the complete data set to answer the question does not exist at the utility. While experts will not go away, and there will still be a lot of estimating, it is important to realize that smart meters provide a large data set to assist with the rate cases.

5.2.3 Tariff Assessments

Do critical peak tariffs create the response expected, does it do it for all segments of customers, and does it impact some customer segments more harshly than others. Use of smart meter data allows a better review of how the customers are responding to the tariffs and how to re-work them to better fit the needs of the society.

5.2.4 Cross Subsidization

An issue that is raised over and over again is cross subsidization of customers, one group of customers paying part of the cost of another group of customers. With our example in Tariff Design, more than likely the young family is subsidizing the young male. Regulators want to know what the cross subsidization is, they do not always want to eliminate it (e.g. the long distance rates for the telephone companies for decades financed the ability of everyone to have a phone). By having complete data on each and every customer, subsidization arguments no longer fall on "I think" arguments, but fall into the "I know" allowing the regulator to only have intended subsidies.

5.2.5 Customer Segmentation

Customer segmentation has traditionally been done by industry or by business segment or by customer type, not by the actual needs or profile of the customers. Regulators have never had enough data to make segmentation decisions that really classify customers together by the way they consume power and their needs for power quality or their creation of power quality issues that the utility needs to fix. Smart metering can provide the data to make meaningful segmentation decisions.

5.3 Demand Response

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

5.3.1 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.

Normal metering reading capabilities are all that are needed for the TOU function.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-10	MDMS	AMI Headend	(Periodically sent) List of meters to read	Meter readings Meter status Error messages from meters and AMI network	C – High I – High A - Low
AMI-28	AMI Headend	Meter	List of meters to read	Meter readings Meter status Error messages from meters and AMI network	C – High I – High A - Low
AMI 24	MDMS	Billing	Meter readings	(Acknowledgment and/or errors)	C – High I – High A - Low

5.3.2 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 broadcast radio signals, the most likely method will be through the AMI system.

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

5.3.3 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.

Interface	Actor #1	Actor #2	Information Sent	Information Returned	Security Req: CIA
AMI-12	LMS / DRMS	AMI Headend	Demand Response CPP price signal	Acknowledgment that DR signal was received	C – Low I – Med A - Med
AMI-29	AMI Headend	ESI/HAN Gateway	DR signal CPP price signal	Acknowledgment that DR signal was received	C – Low I – Med A – Med

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

5.3.4 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
AMI-12	LMS / DRMS	AMI Headend	Demand Response AS price signal	Acknowledgment that DR signal was received	C – Low I – Med A - Med
AMI-29	AMI Headend	ESI/HAN Gateway	DR signal AS price signal	Acknowledgment that DR signal was received	C – Low I – Med A – Med

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