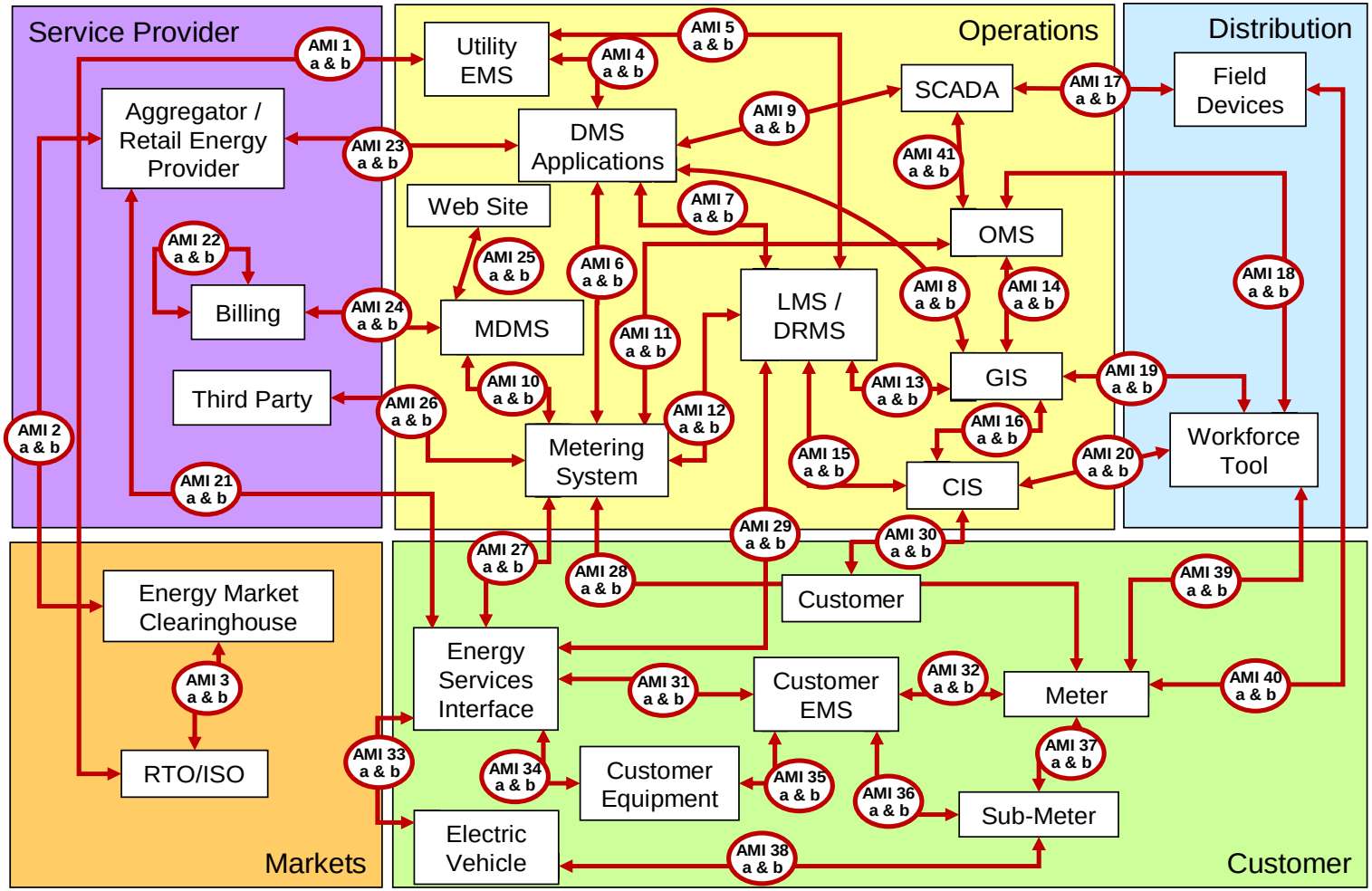
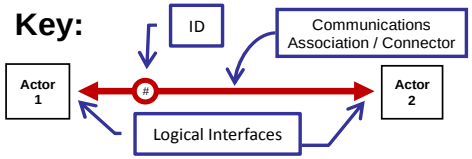
AMI Systems Use Cases: Actors and Logical Interfaces



MDMS: Meter Data Management System
DMS: Distribution Management System
EMS: Energy Management System

LMS: Load Management System
GIS: Geographic Information System
CIS: Customer Information System
OMS: Outage Management System

Key:

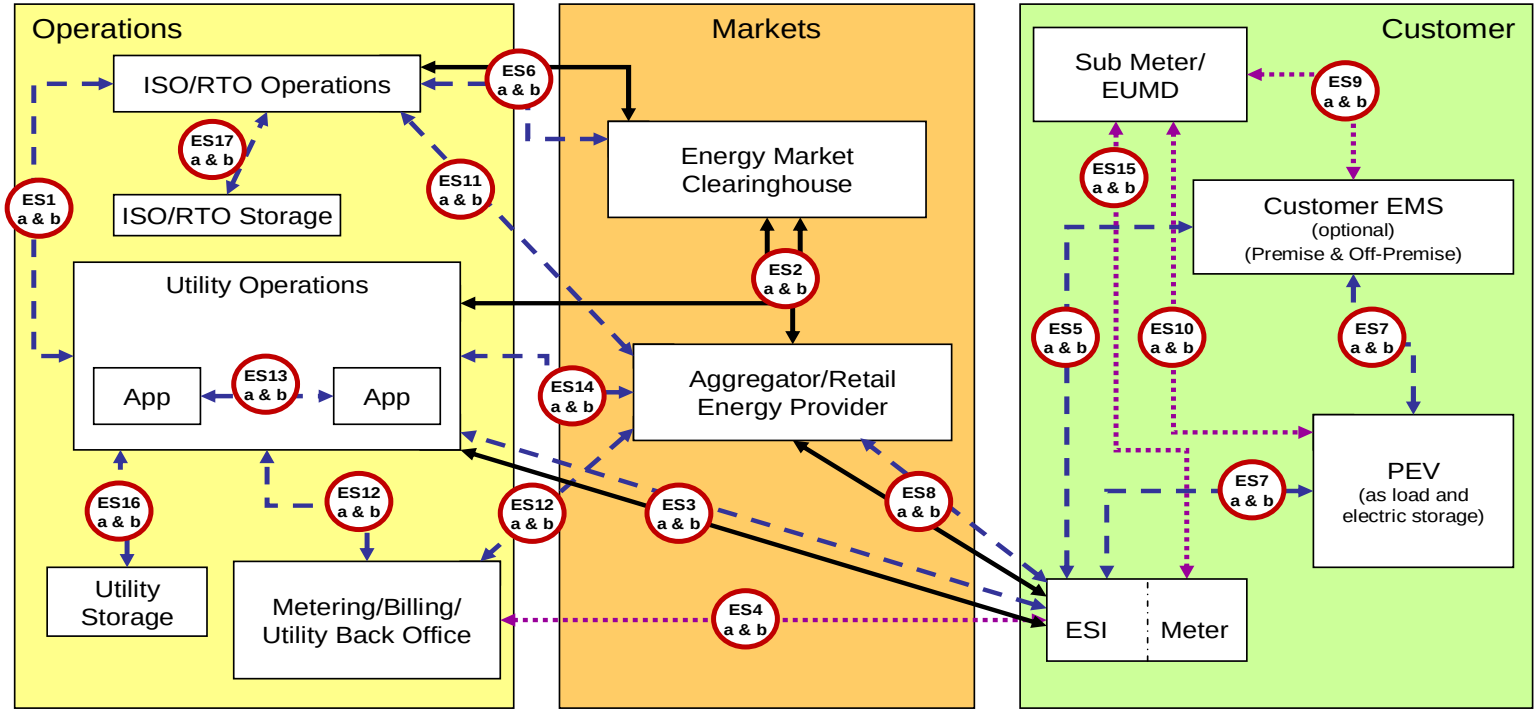


Interface #	Information Object	Interface Function
AMI 1	Request for aggregated load management (congestion management) in a particular wide area, price signals.	Between ISO/RTO and Transco, may be in a day ahead timeframe, in a hours in advances, or in a near real time via RTP signal
AMI 2a	Energy and Ancillary Service Prices	Between Energy Market Clearing House and Aggregator
AMI2b	Energy and Ancillary Service Bids approved by DISCO	Between the Aggregator and the Energy Market Clearing House
AMI 3	Energy and Ancillary Service bids, prices, schedules	Between ISO/RTO and Energy Market Clearing House
AMI 4a	Real Time Prices, Transmission Operating parameters	From Utility EMS to DMS, real-time data exchange
AMI 4b	Transmission bus load model updates	From DMS (DOMA) to Utility EMS, within a minute after each DOMA run
AMI 5	Aggregated load and/or demand response	Between utility EMS and LMS/DRMS
AMI 6	Distribution device data	Distribution device data and control (assuming using AMI network) between DMS and Metering system
AMI 7	Distribution level load and/or demand response	Between DMS and LMS/DRMS
AMI 8a	Load information updates associated with the distribution node	From GIS to DMS in minutes after significant changes. The challenge is the correctness and consistency of load and connectivity data.
AMI 8b	Connectivity and facility parameters data and load data associated with distribution nodes	From GIS to DMS, initial loading of data and incremental data updates as soon as significant changes occur. Each transmittal of data shall be checked on completeness and consistency of data. Large amount of data initially, smaller amounts for incremental changes. Data shall arrive in the DMS database within an hour after the changes was implemented in the field.
AMI 9a	Real-time measurements and statuses	From Field IEDs to Distribution SCADA. Information shall be delivered in 2-4 seconds. Each entry shall be time stamped. The information should be pre-processed for validity check, and then used for distribution state estimation.
AMI 9b	Real time data exchange for status and control	Between DMS and SCADA applications.
AMI 10	Meter reading and meter events	Between Metering system and MDMS
AMI 11	Outage events from meters	For outage detection and restoration conformation, between OMS and Metering systems.
AMI 12a	Voltages at the customer terminals and other points with AMI devices	From AMI devices to Load Management Systems, periodically together with kWh and kvar data.
AMI 12b	Higher harmonics data	This information can be accumulated in the AMI devices for predefined time intervals, with corresponding time stamps, dependent on the devise storage capacity and then be

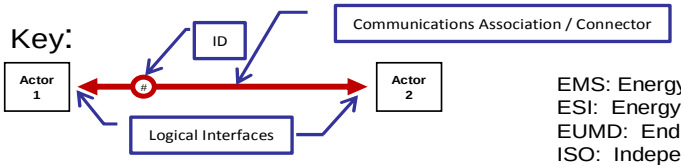
		transmitted to the Load Management Systems
AMI 12c	Load management control events	Between LMS/DRMS and Metering system using AMI Network
AMI 13	Distribution network model extended to include demand response resources, and DER	Between GIS and LMS/DRMS
AMI 14	Distribution network connectivity model	From GIS to OMS
AMI 15	Load model information associated with the distribution node at the customer premise	From Load Management Systems to CIS. Within minutes after the change of model information.
AMI 16	Service point to premise to meter	Between GIS and CIS (depends on what level of information GIS model maintains)
AMI 17	Commands to IEDs	From Distribution SCADA to Field IEDs. Information shall be delivered in 2-4 seconds.
AMI 18	Outage events and status.	Between OMS and Field Tool
AMI 19a	Maps, facility/asset data and as-built	Between GIS and Field Tool, for M&I/asset management
AMI 19b	Field design	Between GIS and Field Tool, for field graphical design
AMI 19c	Field as-built	Between GIS and Field Tool, for field as-built update
AMI 20	Custome premise and service order data	Between CIS and Field Tool
AMI 21	Customer info, authorization, DR program/event/singal, and communication.	Between DR Aggregator or REP and Customer EMS
AMI 22	?	
AMI 23	Aggregated load and/or demand response	Between DR Aggregator or REP and Utility DMS, when third party is resonsible for their side of load management?
AMI 24	Costomer usage data	Between Billing and MDMS
AMI 25	Meter reading and meter events	MDMS to Web Site (customer web presentment), also needs data from Billing/CIS
AMI 26	Custome usage data	Third party to utility (not directly from Metering system or MDMS, but a meter data warehouse or data mart. Called ADE interface.
AMI 27	Control events and signals	Control through AMI metering sytem and network
AMI 28	Meter reading, events, meter management	Between Metering system and Meter
AMI 29	Control events and signals	Between utility LMS/DRMS and Customer Energy Services Interface
AMI 30	?	not an interface
AMI 31	Customer info, authorization, DR program/event/singal, and communication.	Between DR Aggregator or REP and Customer EMS

AMI 32	Meter data and events	Between Meter and Customer EMS
AMI 33	Energy usage data, energy output	Between Energy Service Interface and EV
AMI 34	Control events and signals	Between Customer Energy Services Interface and equipment
AMI 35	Control events and signals	Between Cutomer EMS and load consumption equipment
AMI 36	Meter data, events	Between sub-meter and customer EMS
AMI 37	Meter to submeter relationship	Between meter and sub-meter
AMI 38	Meter data, events	Between EV and sub-meter
AMI 39	Meter maintenance, meter data upload/download	Between Meter and Field Tool
AMI 40	Meter data, command/control through meter	Assuming Field Device include AMI network devices
	Interfaces that are missing	
AMI **41**		Between CIS and MDMS
AMI **42**		Between CIS and Metering System
AMI **43**		Between Meter Asset Management System and MDMS
AMI **44**		Between Meter Asset Management System and Metering System
AMI **45**		Between DMS/OMS and MDMS
		Between GIS and MDMS

Electric Storage Use Cases: Actors and Logical Interfaces



Key:



EMS: Energy Management System
ESI: Energy Services Interface
EUMD: End Use Measurement Device
ISO: Independent System Operator
PEV: Plug-in Electric Vehicle
RTO: Regional Transmission Operator

Market and/or financial interfaces

Energy information interfaces

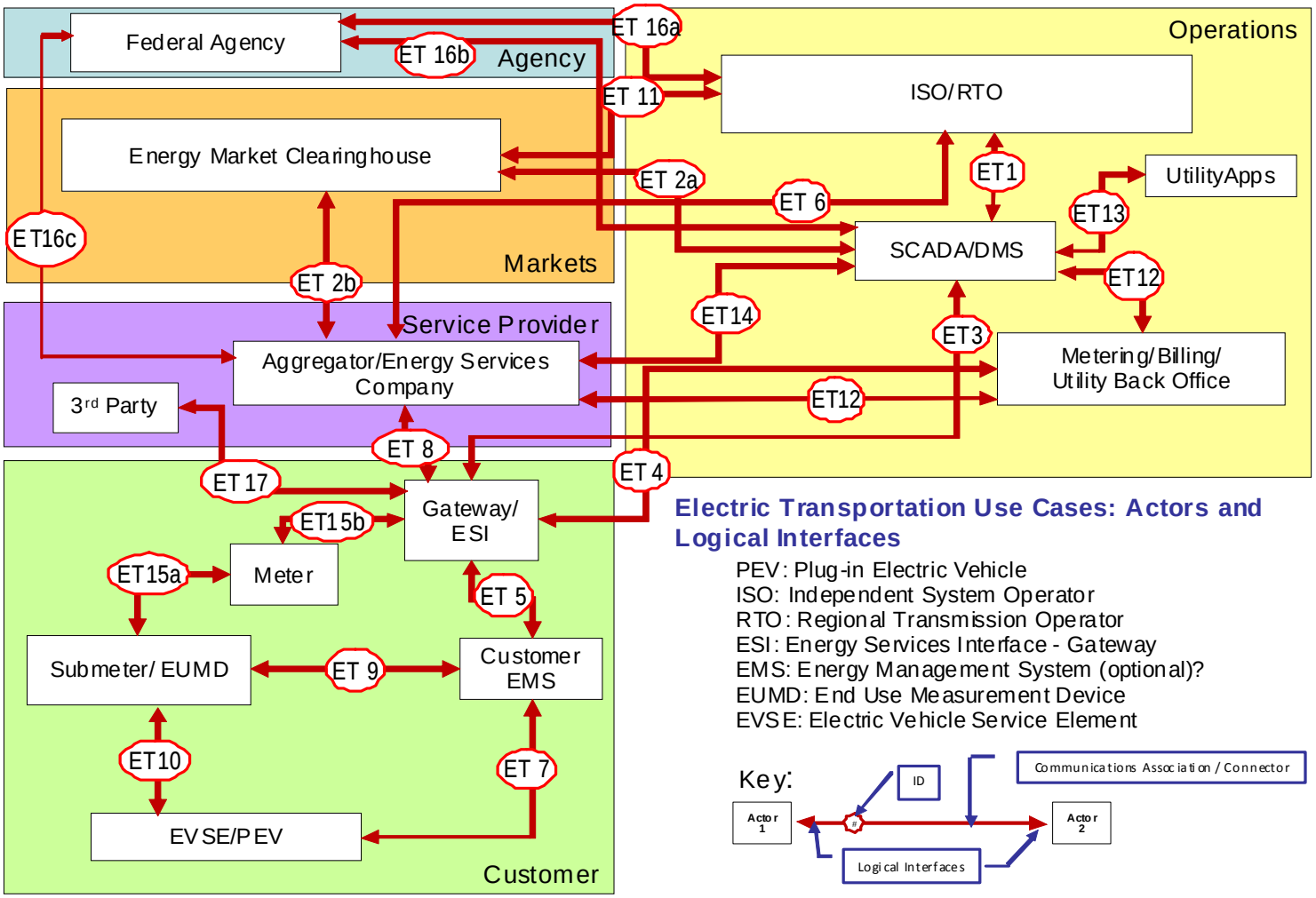
Metering information interfaces

Interface Reference	Information Object Name	Information Object Description
ES1a	Request for aggregated load management (congestion management) in a particular wide area, price signals.	From ISO/RTO to Utility Operations, may be in a day ahead timeframe, in a hours in advances, or in a near real time via RTP signal
ES1b	Utility operation data and available dispatchable load by means of DR, DER, PEV and ES	From Utility Operations to ISO/RTO, near real-time and forecasts for look-ahead studies.
ES2a	Energy and Ancillary Service Prices	From Energy Market Clearing House, to Aggregator and Utility Operations, may be in a day ahead timeframe, in a hours or minutes in advances
ES2b	Bids for ancillary services	From Aggregator and Utility Operations to Energy Market Clearing House
ES3a	Real Time Prices (market-based or reliability based), Direct triggers for enabling PEV storage use, charge interruptions, requests for near-real time measurements	From Utility Operations to Customer. VVWC and DOMA determine the voltage and loading critical sites and request near real-time measurement updates. VVWC under load reduction objective determines in which voltage-critical points load reduction would significantly increase the voltage and sends a triggering signal to this point for exercising discharge of PEV electric storage into grid. VVWC then lowers the voltage and adjusts capacitors to utilize the additional room created by the PEV discharge. The DCA and FLIR determine in which nodes the electric storage discharge would improve the restoration results and issue triggering signals to the corresponding sites. In case of an aggregated request for load reduction, the utility issues triggering commands to a large number of customers for demand response, electric storage discharge, and DER starts.
ES3b	Confirmations on	From selected customers with BMS to Utility Operations

Interface Reference	Information Object Name	Information Object Description
	execution of direct controls, requests, and reaction on RTP, transmission of requested real-time measurements; Real-time information	From ESI/Meter to Utility Operations. Real-time information about PEV as load and as electric storage.
ES4a	Load and consumption data, Start and End times for DR, ES, PEV connection and discharge. Other measurements; Object models	From customer to Metering Billing. Periodic data (every 1-5 min) by event data. From PEV interfaces and AMI to Utility Back Office. PEV and AMI analysis data
ES4b		From Metering Billing to customer
ES5a		
ES5b		
ES6a		
ES6b		
ES7a		
ES7b	Charging/discharging decisions	From ESI/Customer EMS to PEV
ES8a	Pricing information; Power system reliability information	From Aggregator/Retail Energy Provider to ESI. Actual and forecast pricing for particular time periods. From Aggregator/Retail Energy Provider to ESI. Information such as forecast overloads for utility equipment that is near the storage devices which could signal that these storage devices should not be charged during the forecast

Interface Reference	Information Object Name	Information Object Description
	Charging/discharging rates	times. From Aggregator/Retail Energy Provider to ESI
ES8b	Energy storage capacity	
ES9a		
ES9b		
ES10a		
ES10b		
ES11a	Pricing information; Power system reliability information	From Aggregator/Retail Energy Provider to ES owner. Actual and forecast pricing for particular time periods. Information such as forecast overloads for utility equipment that is near the storage devices which could signal that these storage devices should not be charged during the forecast times.
ES11b		
ES12a	Measurements and other data collected from customers; PEV analysis system output	From Metering/Billing to Utility Operations for processing in APPS From Utility Back Office to Aggregators
ES12b	Request for information updates	From Utility Operations to Metering/Billing
ES13a		
ES13b		
ES14a	Pricing information;	From Aggregator/Retail Energy Provider to ES owner. Actual and forecast

Interface Reference	Information Object Name	Information Object Description
		pricing for particular time periods.
	Power system reliability information	Information such as forecast overloads for utility equipment that is near the storage devices which could signal that these storage devices should not be charged during the forecast times.
ES14b		
ES15a		
ES15b		
ES16a	Charging/discharging decisions	From Utility operations to Utility storage. Market based energy schedule. Schedule and control the charging of electric storage devices.
ES16b	Charging/discharging information;	Utility storage to Utility operations. kW output at any point in time. kVAR output at any point in time.
	Available capacity;	Device capability at a point in time.
	Device health;	Condition of a storage device's internal system(s).
	Real power actual	Device power output at a point in time.
ES17a	Charging/discharging decisions	From ISO/RTO operations to ISO/RTO storage. Market based energy schedule. Schedule and control the charging of electric storage devices.
ES17b	Charging/discharging information;	From ISO/RTO storage to ISO/RTO operations. kW output at any point in time. kVAR output at any point in time.
	Available capacity;	Device capability at a point in time.
	Device health;	Condition of a storage device's internal system(s).
	Real power actual	Device power output at a point in time.



Electric Transportation Use Cases: Actors and Logical Interfaces

PEV: Plug-in Electric Vehicle
ISO: Independent System Operator
RTO: Regional Transmission Operator
ESI: Energy Services Interface - Gateway
EMS: Energy Management System (optional)?
EUMD: End Use Measurement Device
EVSE: Electric Vehicle Service Element

Key:

1.1ET Interface #1: Between SCADA/DMS and ISO/RTO

Brief Description: Since the ISO/RTO is responsible for coordinating generation and the grid to ensure a reliable power system, the SCADA/DMS must provide power system information to the ISO/RTO responsible for its region. This data may be sent from the SCADA/DMS system or may be retrieved directly from major substations. In return, the ISO/RTO can issue requests, commands, or potentially pricing signals to the SCADA/DMS in order to elicit some actions such as demand response, load management, or other ancillary service.

Comment [Annabelle1]: I am not sure I believe this is necessary. If it is, we should extract from existing documentation, not develop our own.

These interactions may be one-way deliberately to minimize security vulnerabilities of cross-organizational data exchanges. For instance, the ISO/RTO may collect data using their own RTUs in the substation, and may just issue emails or other notifications to computers not directly connected to the SCADA/DMS.

Item	Description
Diagram Identifier	ET1
Actor #1	ISO/RTO
Actor #2	SCADA/DMS
Description of network and/or media	•Two-way WAN with firewalls, or •One-way WAN for access of critical data from SCADA to ISO/RTO, and/or •One-way WAN for information from ISO/RTO to SCADA
Information exchanged	Power system data from the SCADA Operational information, commands, requests from the ISO/RTO
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	Vulnerabilities related to systems in different organizations exchanging data over a broadband wide area network. The one-way architectures minimize the vulnerabilities. Additional vulnerabilities if the public Internet is used.
Threats	Inadvertent: compromises of information due to mistakes, inadequate system design Deliberate: Industrial espionage Actual information being exchanged is not particularly attractive to deliberate attackers due to minimal effects of attack. Use of the WAN to access the SCADA or ISO/RTO systems is highly attractive.

Comment [Annabelle2]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

Item	Description
Impact	Incorrect distribution data leads to power system inefficiencies, higher generation costs, and potential distribution-level outages. Lost or incorrect commands or requests could also lead to these same types of impacts.
Constraints and/or issues	Different organizations can have different security policies, different enforcement level, and different security technologies, thus possibly leading to lack of interoperability, security gaps, and decreased availability. These interactions may be one-way deliberately to minimize security vulnerabilities of cross-organizational data exchanges. For instance, the ISO/RTO may collect data using their own RTUs in the substation, and may just issue emails or other notifications to computers not directly connected to the SCADA/DMS. Real-time data is being exchanged, with time latency requirements of 1 to a few seconds. No major constraints on types of security measures such as encryption, key management, etc.
Additional comments	

1.2**ET Interface #2: Between** Energy Market Clearinghouse and **SCADA/DMS** or Aggregator/Energy Services Company

Brief Description: This is the interface by which market information is received at the SCADA/DMS or the Aggregator/Energy Services Company, bids are sent by them, and the bid results received.

Item	Description
Diagram Identifier	ET2
Actor #1	Energy Market Clearinghouse
Actor #2	SCADA/DMS or Aggregator/Energy Services Company
Description of network and/or media	•
Information exchanged	Market requirements one way, market results (e.g., winning bids and market status/prices) the other way.
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests or accepted market deals
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	FERC 889
Additional comments	It is unclear what function the Energy Market Clearinghouse performs. It is described differently in two locations in the notes. It is either the market administration function commonly included within the ISO/RTO organization (as distinct from their operations function) or it is an entity that handles billing and payment functions when a PEV connects to a charging station not handled by its home utility back office. In the diagram it appears to relate more closely to the ISO/RTO market administration function (and is defined as such in the Roadmap document, and the other function is subsumed into the utility back office in the Roadmap document. The interface between the (local) utility back office and the overall billing and payment

Comment [Annabelle3]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

Item	Description
	clearinghouse may be missing, as well as the overall billing and payment clearinghouse on the diagram.

1.3ET Interface #3: Between SCADA/DMS and Customer Gateway/ESI

Brief Description: This is the interface through which the SCADA/DMS exchanges data with the PEV. The Customer Gateway/ESI is one of a number of passthrough interfaces on that path. At the beginning of a sequence of exchanges, some setup information must be exchanged to include:

- Identity and related authentication of the vehicle, individual (e.g., driver), and vehicle location.
- Enrollment information, such as identification of long-term account or plan for the vehicle and/or the individual, or temporary setup of an account/plan for the duration of the sequence (e.g., roaming). Some of this information must be shared between the SCADA/DMS and the Metering/billing/utility back office, and the exchange of this information with the PEV could be performed through either interface. This information could include that necessary for negotiation of a temporary arrangement and sending of a credit card number for billing purposes. Note that a null plan is still a plan.
- Capability information, such as the scope of commands, requests, and other information the vehicle can interchange with the SCADA/DMS. This information will necessarily be linked to both the account or plan, either long-term or temporarily set up, and the capabilities of the vehicle and/or its intermediaries and other customer site devices.

After completion of the setup, the information exchanged will mainly consist of requests and commands to the PEV and results from the PEV. Information from PEV could include state of charge, charging rate, charging constraints, metering either to pass through to metering/billing or as operational information. Information to PEV could include requests for information from PEV, passthrough of prices from clearinghouse or commands to change charging rate or feed power to grid.

Item	Description
Diagram Identifier	ET3
Actor #1	SCADA/DMS
Actor #2	Customer Gateway/ESI
Description of network and/or media	•
Information exchanged	Operational data between SCADA/DMS and Customer Gateway/ESI, who acts as interface for Customer. Would generally include requests and commands to PEV's.
Confidentiality, integrity and available cyber	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests

Item	Description
security requirements	
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	PEV related transaction data are likely to have the same privacy/confidentiality requirements as red-light-camera/speed-camera photographs and concepts for GPS-based highway mileage taxation.

Comment [Annabelle4]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.4ET Interface #4: Between Metering/billing/utility back office and Customer Gateway/ESI

Brief Description: This is the interface through which the Metering/Billing/Utility Back office exchanges data with the PEV and its associated metering and billing-related devices. The Customer Gateway/ESI is one of a number of passthrough interfaces on that path. At the beginning of a sequence of exchanges, some setup information must be exchanged either directly or via the SCADA/DMS to include:

- Identity and related authentication of the vehicle, individual (e.g., driver), and vehicle location.
- Enrollment information, such as identification of long-term account or plan for the vehicle and/or the individual, or temporary setup of an account/plan for the duration of the sequence (e.g., roaming). Some of this information must be shared between the SCADA/DMS and the Metering/billing/utility back office, and the exchange of this information with the PEV could be performed through either interface. This information could include that necessary for negotiation of a temporary arrangement and sending of a credit card number for billing purposes.
- Capability information, such as the scope of commands, requests, and other information the vehicle can interchange with the SCADA/DMS. This information will necessarily be linked to both the account or plan, either long-term or temporarily set up, and the capabilities of the vehicle and/or its intermediaries and other customer site devices.

After completion of the setup, the information exchanged will mainly consist of metering and billing information.

Item	Description
Diagram Identifier	ET4
Actor #1	Metering/Billing/Utility Back office
Actor #2	Customer Gateway/ESI
Description of network and/or media	•
Information exchanged	Metering and billing information requests to and responses from customer site meters and submeters via Customer Gateway/ESI
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	

Comment [Annabelle5]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

Item	Description
Threats	
Impact	
Constraints and/or issues	
Additional comments	PEV related transaction data are likely to have the same privacy/confidentiality requirements as red-light-camera/speed-camera photographs and concepts for GPS-based highway mileage taxation.

1.5ET Interface #5: Between Customer Gateway/ESI and Customer EMS

Brief Description: The Customer Gateway/ESI and Customer EMS are passthrough entities on the path between the various external actors (SCADA/EMS, Metering/billing/utility back office, Aggregator/Energy Services Company) and the PEV. These entities may be passthrough only or they may perform some functions, such as identification and authentication, that would otherwise need to be performed at the EVSE/PEV. Some of this distinction breaks down the metering and non-metering functions and the automated and human interactive functions.

Item	Description
Diagram Identifier	ET5
Actor #1	Customer Gateway/ESI
Actor #2	Customer EMS
Description of network and/or media	•
Information exchanged	Two way passthrough of data between actors external to the customer and the Customer EMS or metering and PEV connected to the Customer EMS. The Customer EMS is likely to also be a passthrough in some cases.
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	This interface is not between the communicating endpoints but is intermediate in the communications path. Must support security requirements between the communications endpoints.

Comment [Annabelle6]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.6ET Interface #6: Between Aggregator/Energy Services Company and ISO/RTO

Brief Description: The Aggregator/Energy Services Company serves as an interface for multiple customers and performs a variety of functions. To the extent some of those functions would otherwise be performed by the SCADA/DMS, this is the equivalent interface. Also, the Aggregator/Energy Services Company could be aggregating generation or storage providers in addition to PEVs and could be bundling a variety of generation and load-related services into a package within the jurisdiction of the ISO/RTO. This is the operational interface for all information exchange relevant to such activities.

Item	Description
Diagram Identifier	ET6
Actor #1	ISO/RTO
Actor #2	Aggregator/Energy Services Company
Description of network and/or media	•
Information exchanged	Operational data between ISO/RTO and Aggregator/Energy Services Company, who acts as interface for multiple customers. Would generally include requests and commands to PEV's.
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	

Comment [Annabelle7]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.7ET Interface #7: Between Customer EMS and EVSE/PEV

Brief Description: The Customer Gateway/ESI and Customer EMS are passthrough entities on the path between the various external actors (SCADA/EMS, Metering/billing/utility back office, Aggregator/Energy Services Company) and the PEV. These entities may be passthrough only or they may perform some functions, such as identification and authentication, that would otherwise need to be performed at the EVSE/PEV. Some of this distinction breaks down the metering and non-metering functions and the automated and human interactive functions.

Item	Description
Diagram Identifier	ET7
Actor #1	Customer EMS
Actor #2	EVSE/PEV
Description of network and/or media	•
Information exchanged	Passthrough of information from external actors via Customer Gateway/ESI and Customer EMS to EVSE/PEV
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	

Comment [Annabelle8]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.8ET Interface #8: Between Aggregator/Energy Services Company and Gateway/ESI

Brief Description: The Aggregator/Energy Services Company serves as an interface for multiple customers and performs a variety of functions. The Customer Gateway/ESI and Customer EMS are passthrough entities on the path between the various external actors (SCADA/EMS, Metering/billing/utility back office, Aggregator/Energy Services Company) and the PEV. These entities may be passthrough only or they may perform some functions, such as identification and authentication, that would otherwise need to be performed at the EVSE/PEV. Some of this distinction breaks down the metering and non-metering functions and the automated and human interactive functions.

Item	Description
Diagram Identifier	ET8
Actor #1	Aggregator/Energy Services Company
Actor #2	Gateway/ESI
Description of network and/or media	•
Information exchanged	Passthrough of disaggregated/allocated information between other actors (ISO/RTO, SCADA/DMS, Energy Market Clearinghouse, or Metering/Billing/Utility back office) and the PEV.
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	

Comment [Annabelle9]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.9ET Interface #9: Between Customer EMS and Submeter/EUMD

Brief Description: The Customer Gateway/ESI and Customer EMS are passthrough entities on the path between the various external actors (SCADA/EMS, Metering/billing/utility back office, Aggregator/Energy Services Company) and the PEV. These entities may be passthrough only or they may perform some functions, such as identification and authentication, that would otherwise need to be performed at the EVSE/PEV. Some of this distinction breaks down the metering and non-metering functions and the automated and human interactive functions.

The Submeter/EUMD is a device that meters two way flow of energy between the PEV and the grid. If the PEV is the only load, the Submeter/EUMD might not be distinct from the meter.. Otherwise, either the data is forwarded for inclusion in the metering data or forwarded via the Customer EMS. This particular interface is the one by which the data is forwarded via the customer EMS.

Item	Description
Diagram Identifier	ET9
Actor #1	Customer EMS
Actor #2	Submeter/EUMD
Description of network and/or media	•
Information exchanged	
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	

Comment [Annabelle10]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.10ET Interface #10: Between Submeter/EUMD and EVSE/PEV

Brief Description: The Submeter/EUMD is a device that meters two way flow of energy between the PEV and the grid. If the PEV is the only load, the Submeter/EUMD might not be distinct from the meter. This is the interface between the PEV and the Submeter/EUMD. The information over the interface is likely the status of the PEV relative to the metering function, if any is needed by the Submeter/EUMD. Such information could include the status of SCADA/DMS commands being executed by the PEV (if not transferred from the Customer EMS). The information is subject to allocation of functions among the Submeter/EUMD, EVSE/PEV, Customer EMS, Gateway/ESI, and other actors within the customer premises,

Item	Description
Diagram Identifier	ET10
Actor #1	Submeter/EUMD
Actor #2	EVSE/PEV
Description of network and/or media	•
Information exchanged	
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	

Comment [Annabelle11]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.11ET Interface #11: Between Energy Market Clearinghouse and Aggregator/Energy Services Company

Brief Description: This duplicates Interface 2.

Item	Description
Diagram Identifier	ET11
Actor #1	Energy Market Clearinghouse
Actor #2	Aggregator/Energy Services Company
Description of network and/or media	•
Information exchanged	
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	Appears to be duplicate interface

Comment [Annabelle12]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.12ET Interface #12: Between Metering/Billing/Utility Back Office and Aggregator/Energy Services Company

Brief Description: The Aggregator/Energy Services Company serves as an interface for multiple customers and performs a variety of functions. The particular information transferred over this interface depends on the business relationships and allocation of functions among the Aggregator/Energy Services Company and the other actors external to the customer site (ISO/RTO, SCADA/EMS, Metering/billing/utility back office, and Energy Market Clearinghouse). Information over this interface will generally involve metering and billing, but could also include the setup functions described under Interface 3. The information could be aggregated or disaggregated, depending on allocation of functions.

Item	Description
Diagram Identifier	ET12
Actor #1	Metering/Billing/Utility Back Office
Actor #2	Aggregator/Energy Services Company
Description of network and/or media	•
Information exchanged	
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	

Comment [Annabelle13]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.13ET Interface #13: Between SCADA/DMS and Utility Apps

Brief Description: This is the interface between the SCADA/DMS and applications used by the SCADA/DMS.

Item	Description
Diagram Identifier	ET13
Actor #1	SCADA/DMS
Actor #2	Utility Apps
Description of network and/or media	•
Information exchanged	Data to Utility Apps, results to SCADA/DMS
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	This interface may be internal to the SCADA/DMS, depending on how the Utility Apps are implemented

Comment [Annabelle14]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.14ET Interface #14: Between SCADA/DMS and Aggregator/Energy Services Company

Brief Description: The Aggregator/Energy Services Company serves as an interface for multiple customers and performs a variety of functions. The particular information transferred over this interface depends on the business relationships and allocation of functions among the Aggregator/Energy Services Company and the other actors external to the customer site (ISO/RTO, SCADA/EMS, Metering/billing/utility back office, and Energy Market Clearinghouse). In general, data from the SCADA/DMS will be aggregated commands and data to the SCADA/DMS will be aggregated results.

Item	Description
Diagram Identifier	ET14
Actor #1	SCADA/DMS
Actor #2	Aggregator/Energy Services Company
Description of network and/or media	•
Information exchanged	Operational data between SCADA/DMS and Aggregator, who acts as agent for multiple customers. Could include requests and commands to PEV's, metering and billing data, or other.
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	

Comment [Annabelle15]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.15ET Interface #15: Between Meter and either Customer Gateway/ESI or Submeter/EUMD

Brief Description: These interfaces provide the flow of metering requests and metering data. The Submeter/EUMD is a device that meters two way flow of energy between the PEV and the grid. If the PEV is the only load, the Submeter/EUMD might not be distinct from the meter. Otherwise, either the data is forwarded for inclusion in the metering data or forwarded via the Customer EMS. This particular interface is the one by which the data is forwarded via the meter and the Gateway/ESI.

Item	Description
Diagram Identifier	ET15
Actor #1	Meter
Actor #2	Customer Gateway/ESI or Submeter/EUMD
Description of network and/or media	•
Information exchanged	
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	

Comment [Annabelle16]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.16ET Interface #16: Between Federal agency and or SCADA/DMS or Aggregator/Energy Services Company

Brief Description: This is an interface of unclear purpose with an indeterminate Federal agency (or possibly a state or local agency). Given that individual customer transaction data is likely to have privacy protection similar to banking transactions and is likely to require a court order to make it available to law enforcement, this is most likely a tariff filing interface in which operational systems do not participate.

Item	Description
Diagram Identifier	ET16
Actor #1	Federal agency
Actor #2	ISO/RTO or SCADA/DMS or Aggregator/Energy Services Company
Description of network and/or media	•
Information exchanged	Defined in the Roadmap document as a Federal Agency that requires information on interactions involving electric transportation. It is unclear what agency that might be and under what legal authority they might be acting. Could be intended to cover the use case in Section 4.6.2.2 of the Roadmap document. This involves the exchanges necessary to file a tariff and apply for and receive approval. The exchange is part of a legal proceeding and is just as likely to come from a law firm engaged by the market participant as from the market participant itself. The SCADA/DMS is unlikely to be involved in the exchange.
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	"Federal Agency" is more likely "Federal Agency or State PUC"

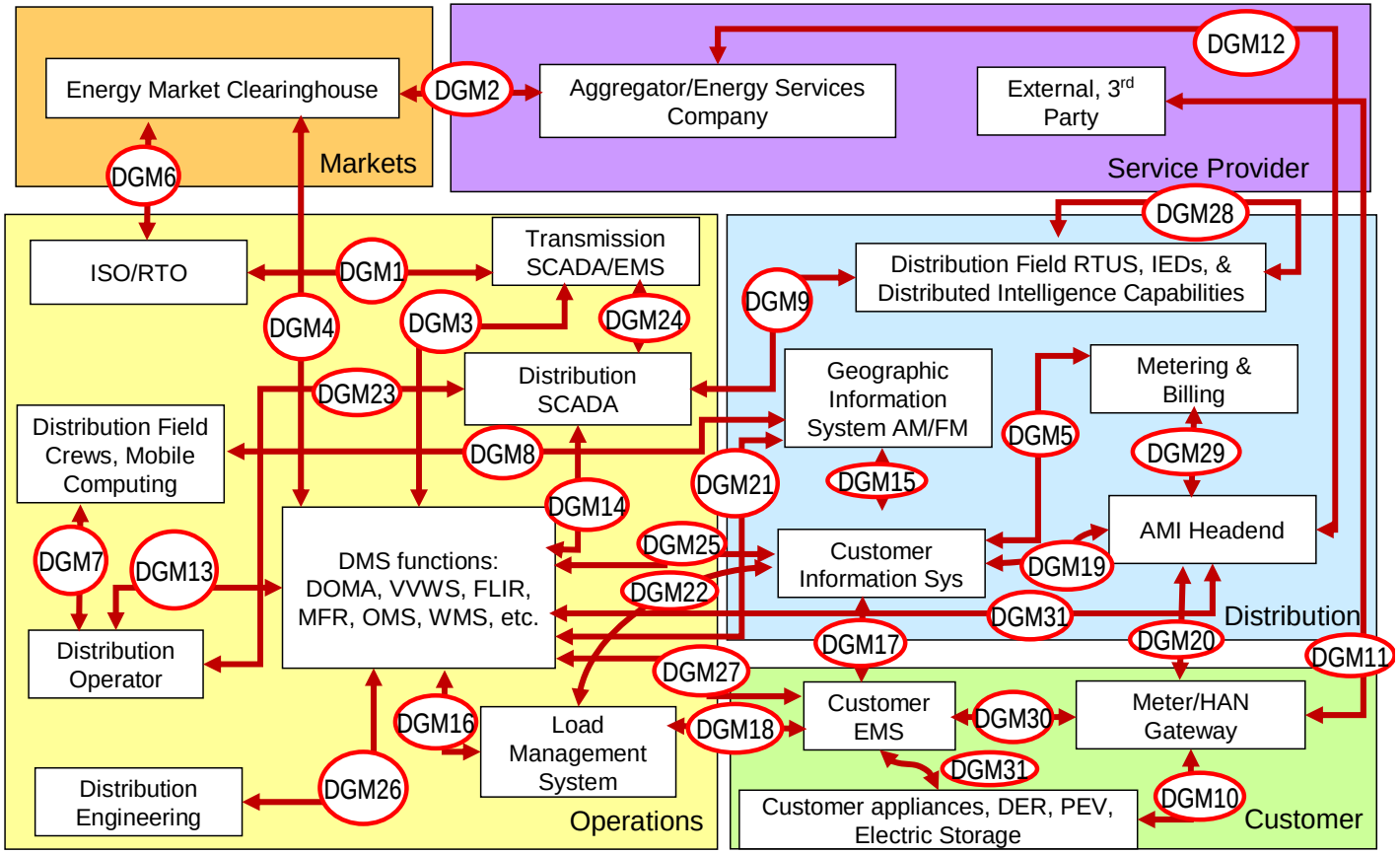
Comment [Annabelle17]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???

1.17ET Interface #17: Between Customer Gateway/ESI and Third party

Brief Description: This is an interface of unknown purpose with a third party who is authorized to interface to the Customer Gateway/ESI. The information exchanged depends on the purpose of the interface.

Item	Description
Diagram Identifier	ET17
Actor #1	Customer Gateway/ESI
Actor #2	Third party
Description of network and/or media	•
Information exchanged	Unknown.
Confidentiality, integrity and available cyber security requirements	Integrity of data, availability within the performance constraints, confidentiality, authentication of information exchanges, non-repudiation of commands or requests
Vulnerability classes	
Threats	
Impact	
Constraints and/or issues	
Additional comments	It is unclear who the third party might be and what function they might be performing.

Comment [Annabelle18]: I am not sure we should separate vulnerabilities and threats – I think they really overlap. Also, I would not necessarily include threat agents as a separate category. What do you think???



Distribution Grid Management Use Cases: Actors and Logical Interfaces

DOMA: Distribution Operations Model & Analysis
VVWS: Volt-Var-Watt
FLIR: Fault Location, Isolation, Restoration

MFR: Multi-Feeder Reconnection
OMS: Outage Management System
WMS: Work Management System

Key:

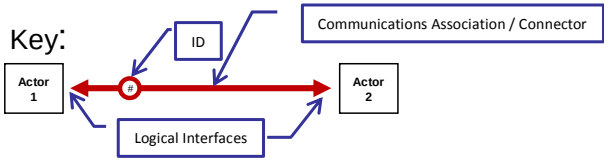


Table of Contents

1. INTRODUCTION 35

1.1 Purpose 35

1.2 Security Assessment Based on Use Case Interfaces and Associated Assets . 35

2. SECURITY ELEMENTS 37

2.1 Types of Vulnerabilities 37

2.1.1 People, Policy, and Procedure 37

2.1.2 Platform 38

2.1.3 Network 40

2.2 Types of Threats 41

2.3 Types of Impacts 42

2.4 Types of Constraints and Issues Affecting Security 43

3. DISTRIBUTION GRID MANAGEMENT INTERFACES**ERROR! BOOKMARK NOT DEFINED.**

3.1 DGM Interface #1: Between ISO/RTO and Transmission SCADA/EMS..... 45

3.2 DGM Interface #2: Between Energy Market Clearinghouse and Aggregator/Energy Services Provider 47

3.3 DGM Interface #3: Between Transmission SCADA/EMS and DMS Functions. 49

3.4 DGM Interface #4: Between Energy Market Clearinghouse and DMS Functions50

3.5 DGM Interface #5: Between Customer Information System and Metering & Billing System 52

3.6 DGM Interface #6: Between Energy Market Clearinghouse and ISO/RTO 53

3.7 DGM Interface #7: Between Distribution Operator and Distribution Field Crews54

3.8 DGM Interface #8: Between Distribution Field Crews and Geographic Information Systems 56

3.9 DGM Interface #9: Between Distribution SCADA and Distribution Field IEDs.. 57

3.10 DGM Interface #10: Between Meter/HAN Gateway and Customer DER, ES, PEV, & Appliances 58

3.11 DGM Interface #11: Between External 3rd Party and Meter/HAN Gateway 59

3.12 DGM Interface #12: Between Aggregator/Energy Services Provider and AMI Headend 61

3.13 DGM Interface #13: Between Distribution Operator and DMS Functions 62
3.14 DGM Interface #14: Between Distribution SCADA System and DMS Functions63
3.15 DGM Interface #15: Between Geographic Information Systems and Customer Information System 65
3.16 DGM Interface #16: Between DMS Functions and Load Management System (LMS) 66
3.17 DGM Interface #17: Between Customer Information System (CIS) and Customer EMS 67
3.18 DGM Interface #18: Between Load Management System (LMS) and Customer EMS 68
3.19 DGM Interface #19: Between Customer Information System (CIS) and AMI Headend 69
3.20 DGM Interface #20: Between AMI Headend and Meter/HAN Gateway 71
3.21 DGM Interface #21: Between DMS Functions and Geographical Information System (GIS) 73
3.22 DGM Interface #22: Between Customer Information System (CIS) and Load Management System (LMS) 74
3.23 DGM Interface #23: Between Distribution Operator and Distribution SCADA System 75
3.24 DGM Interface #24: Between Distribution SCADA System and Transmission SCADA/EMS 76
3.25 DGM Interface #25: Between DMS Functions and Customer Information System (CIS) 78
3.26 DGM Interface #26: Between DMS Functions and Distribution Engineering 79
3.27 DGM Interface #27: Between DMS Functions and Customer EMS 80
3.28 DGM Interface #28: Between Distributed Field IEDs and Other Distributed Field IEDs 82
3.29 DGM Interface #29: Between AMI Headend and Metering/Billing System 83
3.30 DGM Interface #30: Between Meter/HAN Gateway and Customer EMS..... 84
3.31 DGM Interface #31: Between DMS Functions and AMI Headend 85

Introduction

1.18Purpose

Cyber security solutions must ultimately be implementation-specific, driven by the requirements for security of all of the functions in the system. Typically, security requirements address the integrity, confidentiality, and availability of data. In the Smart Grid, the complexity of stakeholders, systems, devices, networks, and environments precludes simple or one-size-fits-all security solutions. Therefore, additional criteria must be used in selecting the cyber security measures. These additional criteria will take into account the constraints posed by device and network technologies, legacy systems, regulatory and legal policies, and cost criteria.

NIST is developing a security framework to provide appropriate guidance to implementers of Smart Grid systems. The first step in this process has been to identify key Use Cases which have requirements and constraints that impact security solutions. In parallel, the CSCTG Vulnerabilities subgroup has identified and categorized vulnerabilities, the Bottom Up CSCTG subgroup has identified key known security issues, and several existing cyber security-related standards have been listed and mapped.

The next step needs to assess all of this input and develop cyber security information that is both specific enough to be applicable to specific environments, while general enough to permit the implementation of different cyber security solutions that meet the cyber security requirements or embrace new security technologies as they are developed. This cyber security information can then be used in subsequent steps to select cyber security controls for the Smart Grid.

1.19Security Assessment Based on Use Case Interfaces and Associated Assets

The Use Cases developed for the NIST Interim Roadmap, including the Security-Significant Use Cases and the FERC4+2 Use Cases provide snapshots of key functions of the Smart Grid. Many of these Smart Grid Use Cases also demonstrate architectures that can introduce unique security vulnerabilities, provide environments for unique types of threats, result in different types of negative impacts, and constrain the potential security solutions. Therefore it is vital to assess each of the interfaces and their associated assets (e.g., hardware, devices, systems, firmware, software applications, and information exchanges) which were identified in these Use Cases to determine their unique security-related characteristics.

Although these Use Cases do not cover all functions of the entire Smart Grid, they do cover many of the key areas where special considerations will impact the cyber security controls ultimately applied during implementation. Therefore, for a top-level generic approach, assessing the cyber security-related issues at these Use Case interfaces assist in understanding the cyber security requirements, will provide the input for developing a more complete security architecture, and will provide critical security information to users and vendors of Smart Grid systems.

For each interface identified in a Use Case, the cyber security assessment will need to cover:

- **Vulnerability Classes.** *A vulnerability is a flaw or oversight in an existing control that may possibly allow a threat agent to exploit it to gain unauthorized access to assets.* The Vulnerabilities Task Force of the CSCTG identified a very large number of

vulnerabilities. The security assessment needs to identify specific factors that could make certain vulnerabilities more likely or more of a concern for specific interfaces and the assets connected to those interfaces.

- **Threats stemming from key Threat Agents**. *A threat is an event with an undesired impact, such as the loss, disclosure, or damage of an asset. A threat agent is the entity that may cause a threat to happen.* The Common Criteria has a long list of potential threats. The security assessment needs to identify those that may pose particular problems in the physical and cyber environment where the asset is located, the attractiveness of the assets to threat agents, and the potential for inadvertent compromises of those assets.
- **Types of impacts**. *An impact is a negative consequence resulting in a financial, legal, regulatory, and/or societal cost.* The types of impacts from security breaches can vary significantly, from minor embarrassments to major blackouts. Because the actual effect of a security breach in financial, legal, regulatory, or societal terms must be case-by-case specific, this general security assessment can only identify the types of impacts, not their actual values.
- **Constraints for implementing certain security measures**. Some environments, devices, systems, and interfaces have certain constraints on what types of security measures could be implemented. These constraints include limited computer processing capabilities, restricted bandwidth for exchanging data, rigorous time latency requirements, and cross-organizational legal agreements. The cyber security assessment needs to identify these constraints for each interface and the associated assets.

Cyber security must address both specific interfaces (e.g., encryption for confidentiality over a wireless network) as well as end-to-end (e.g., an operator action must be authenticated between his HMI action across all networks and systems to the device he is controlling in the field). Cyber security also must be layered not only to prevent security breaches but to deter, detect, and audit these breaches.

In addition to each interface in a Use Case, the actors in these Use Cases can also be targets of security threats. Usually these "actors" are multiple systems and devices, not a single asset, so that security assessment of these actors may entail additional layered assessments of increasingly detailed assets. However, as a start at this top level security assessment, these actors can be viewed as a "single entity" within a single security environment, so that the assets that make up the actors can be likewise viewed as belonging within a single security environment. After the top level assessment is completed, additional security assessments can drill down within security environments as needed.

Therefore a security assessment of the interfaces identified in the NIST Roadmap Use Cases should be undertaken using the following methodology and tables:

1. Use the FERC4+2 diagrams to identify each interface. Each interface has an associated number (identifier). This will be used to uniquely identify each interface.
2. Identify the actors – these are listed in the diagrams
3. Describe the semantic layer, the syntactic layer, the network layer, and/or the physical media layer, if known or relevant. Include standards and other protocols typically used or planned to be used (e.g. in the "Low Hanging Fruit" list)
4. Briefly describe the types of information that are exchanged. Include any security-related common practices or issues

5. Fill out a table for the interface. The white items are general information; the grey items are security related. The purpose is to identify the key security requirements, vulnerabilities, threats, types of impacts, and constraints associated with the interface.
6. This table, reflecting ***examples*** of interface security issues, can then act as guidelines to the selection of cyber security requirements needed by the Smart Grid.

Security Elements

1.20Types of Vulnerabilities

People, Policy, and Procedure

People

- Insufficient trained personnel
- Insufficient identity validation / background checks

Policy

- Inadequate security policy (800-82 3-3)
- Inadequate information assurance program
- Inadequate security training and awareness program (800-82 3-3)
- Inadequate privacy policy
- Inadequate periodic security audits (800-82 3-3)
- Inadequate security oversight by management
- Unnecessary system access
- Inadequate continuity of operations or disaster recovery plan (800-82 3-3)
- Inadequate documentation of installed assets (800-82 3-5)
- Inadequate review and/or retention of logs (800-82 3-6)
- Inadequate change and configuration management policy
- Inadequate information/data handling/retention/storage/destruction policy
- Inadequate electronic communications policy (acceptable use for all types of devices and information used)

Procedure

- Inadequate risk assessment process
- Inadequate risk management process
- Inadequate incident response process
- Inadequate identity protection; data privacy
- Inadequate monitoring of security-related events
- Inadequate patch management process
- Inadequate backup processes (OS, Application, database)
- Inadequate segregation of duties/roles/access control

Platform

Platform Configuration Vulnerabilities

- Inadequate security architecture and design (800-82 3-3)
- Installed security capabilities not enabled by default (800-82 3-6)
- Absent or deficient equipment implementation guidelines (800-82 3-3)
- Lack of prompt security patches from software vendors (800-82 3-4)
- Default configurations are used (800-82 3-4)
- Unneeded services running (800-82 3-6)

Platform Hardware Vulnerabilities

- Inadequate monitoring and alerting
- Physical Environmental Conditions
- Inadequate testing of security changes (800-82 3-5)
- Inadequate physical protection for critical systems (800-82 3-5)
- Inadequate Physical Access Control (800-82 3-5)
- Inadequate Network/Logical Access Control (800-82 3-5)
- Lack of backup power (800-82 3-5)
- Loss of environmental control (800-82 3-5)
- Single point of failure for critical components (800-82 3-5)

Platform Software/Firmware Vulnerabilities

- API Abuse (OWASP)
- Authentication Vulnerability (OWASP)
- Authorization Vulnerability (OWASP)
- Code Permission Vulnerability (OWASP)
- Availability Vulnerability (OWASP)
- Code Permission Vulnerability (OWASP)
- Code Quality Vulnerability (OWASP)
- Concurrency Vulnerability (OWASP)
- Configuration Vulnerability (OWASP)
- Cryptographic Vulnerability (OWASP)
- Encoding Vulnerability (OWASP)
- Environmental Vulnerability (OWASP)
- Error Handling Vulnerability (OWASP)
- General Logic Error Vulnerability (OWASP)
- Input Validation Vulnerability (OWASP)
- Logging and Auditing Vulnerability (OWASP)
- Password Management Vulnerability (OWASP)
- Path Vulnerability (OWASP)
- Range and Type Error Vulnerability (OWASP)
- Sensitive Data Protection Vulnerability (OWASP)
- Session Management Vulnerability (OWASP)
- Synchronization and Timing Vulnerability (OWASP)
- Unsafe Mobile Code (OWASP)
- Use of Dangerous API (OWASP)
- Unauthorized firmware modification (OWASP)
- Insufficient firmware validation (OWASP)
- Denial of Service (OWASP)
- Remote access vulnerabilities (OWASP)
- Buffer overflow (800-82 3-6)
- Mishandling of undefined, poorly defined, or “illegal” conditions (800-82 3-6)
- Use of insecure industry-wide protocols (800-82 3-6)
- Use of clear text (800-82 3-6)

- Inadequate malware protection (800-82 3-7)

Network

Network Configuration Vulnerabilities

- Inadequate network security architecture (800-82 3-8)
- Poorly configured security equipment (800-82 3-8)
- Inappropriate Lifespan for Authentication Credentials/Keys (800-82 3-8)
- Inadequate access controls applied (800-82 3-8)

Network Hardware Vulnerabilities

- Inadequate physical protection of network equipment (800-82 3-9)
- Unsecured physical ports (800-82 3-9)
- Loss of environmental control (800-82 3-9)
- Non-critical personnel have access to equipment and network connections (800-82 3-9)
- Lack of redundancy for critical networks (800-82 3-9)

Network Perimeter Vulnerabilities

- Firewalls nonexistent or improperly configured (800-82 3-10)
- Control networks used for non-control traffic (800-82 3-10)
- Control network services not within the control network (800-82 3-10)

Network Monitoring and Logging Vulnerabilities

- Inadequate firewall and router logs (800-82 3-11)
- No security monitoring on the network (800-82 3-11)

Communication Vulnerabilities

- Critical monitoring and control paths are not identified (800-82 3-12)
- Standard, well-documented communication protocols are used in plain text (800-82 3-12)
- Authentication of users, data or devices is substandard or nonexistent (800-82 3-12)
- Lack of integrity checking for communications (800-82 3-12)

Wireless Connection Vulnerabilities

- Inadequate authentication between clients and access points (800-82 3-13)
- Inadequate data protection between clients and access points (800-82 3-13)

1.21Types of Threats

Broad categories of threats are:

- **Loss of Confidentiality** – Unauthorized access to information
- **Loss of Integrity** – Unauthorized modification or theft of information, including acceptance of false data
- **Loss of Availability / Denial of Service** – Interruption or prevention of authorized access to information within the required timeframe
- **Authentication Violation** – Inability to determine or establish authenticity or authorization
- **Lack of Accountability** / **Repudiation**– Denial of action that took place or claim of action that did not take place

Specific types of threats under these broad categories include:

- Loss of confidentiality
  - Eavesdropping
  - Traffic analysis
  - EM/RF interception
  - Indiscretions by personnel
  - Media scavenging
- Loss of integrity
  - Alter
  - Destroy
- Loss of availability / Denial of service
  - Resource exhaustion
  - Integrity violation

  - Theft
  - Destruction
- Authentication violation
  - Masquerade
  - Bypassing control
  - Authorization violation
  - Physical intrusion
  - Man-in-the-middle
  - Replay
  - Virus/worms
  - Trojan horse
  - Trapdoor
  - Service spoofing
- Loss of accountability / Repudiation
  - Altered logs
  - Erasing of logs
- General threats affecting many threat categories
  - Errors and omissions
  - Fraud and theft
  - Sabotage
  - Loss of infrastructure support, such as power
  - Espionage
  - Malicious code
  - Disclosure

1.22Types of Impacts

Broad types of impacts are:

- Customer impacts
- Utility impacts
- Third party impacts
- Societal impacts

Each of the categories include 5 different types of impacts:

- **Direct financial impacts**, including loss of revenue, higher costs, additional unnecessary costs, unstable/unknown future costs, legal costs, etc. Although most impacts could ultimately be translated into financial impacts, this may not always be the most important measure.
- **Power reliability and power quality impacts**, including increased number and length of outages, increased number of momentary outages, poorer power quality, and unreliable operation of distributed generation, etc.
- **Safety impacts**, including decreased visibility into unsafe or insecure situations, decreased physical plant security, decreased privacy protection, and increased energy dependence on unreliable or unfriendly sources.
- **Energy efficiency impacts**, including increased energy usage, increased demand during peak times, increased energy losses, etc.
- **Energy environmental and conservation impacts**, including increased greenhouse gases (GHG) and other pollutants, increased generation from inefficient energy sources, and decreased ability to use renewable sources of energy.
- **Privacy impacts**, including failure to safeguard confidential information
- **Regulatory impacts**, including failure to meet regulatory requirements.
- **Legal impacts**, including financial and criminal impacts.
- **"Good name" impacts**, including negative press reports, decreased customer confidence, and decreased effectiveness of marketing products

1.23Types of Constraints and Issues Affecting Security

Types of constraints (usually as a result of the balancing of cost versus security) that limit the types, thoroughness, and/or effectiveness of security measures, include:

- **Low bandwidth of communications channels**, which limits the types of security measures which could be employed per channel.
- **Microprocessor constraints on memory and compute capabilities**, which limits the types of security measures which could be employed.
- **Wireless media**, which can pose certain types of additional security challenges.
- **Immature or proprietary protocols**, which may not be adequately tested either against inadvertent compromises or deliberate attacks.
- **Cross-organizational interactions**, which limit trust and compatibility of security policies and measures.
- **Real-time operational requirements**, which entail short acceptable time latencies, and limit the choices for stopping or mitigating on-going attacks.
- **Legacy end-devices and systems**, which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- **Legacy communication protocols**, which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- **Insecure locations**, which cannot be made more secure due to their physical environment or ownership.
- **Key management for large numbers of devices**, which can limit the methods for deploying and revoking keys.
- **Patch management for sensitive devices**, which limits the frequency of updating security patches.
- **Unknown or rapidly changing types of interactions**, which complicate the decisions on the types and severity of security threats and impacts.
- **Environmental concerns**, which limit the types of security measures.
- **Legal constraints**, which limit the types of security measures which could be employed, such as wiretapping of suspected hackers or blocking all 3rd party access.
- **Personnel constraints**, which limit the number of properly trained personnel to manage and secure resources. This includes the lack of any security training of most customers.
- **Negative public image or fears**, which can limit what functions are deployed and the types of security measures mandated or regulated.
- **Security budgetary constraints**, which limit the purchased tools and services to properly monitor, test, and protect the resources.

1.24 DGM Interface #1: Between ISO/RTO and Transmission SCADA/EMS

Brief Description and/or Purpose of Interface:

The purpose of ISOs and RTOs is exemplified by the CAISO mission statement, *"For the benefit of our customers, we:*

- *Operate the grid reliably and efficiently*
- *Provide fair and open transmission access*
- *Promote environmental stewardship*
- *Facilitate effective markets and promote infrastructure development*
- *All through the provision of timely and accurate information.*[1]

The Transmission SCADA/EMS system monitors, analyzes, and controls the transmission system. The SCADA system collects real-time information while the EMS uses power flow-based applications and other tools to analyze the current and near-term state of the transmission grid.

Some of the timely and accurate information mentioned is exchanged with those transmission utilities that are in the ISO/RTO territory. The transmission utility SCADA/EMS provide real-time data on their transmission grid, and the ISO/RTO provides current operating conditions information, including curtailments and emergency alarms.

Item	Description
Diagram Identifier	DGM #1
Actor #1	ISO/RTO SCADA/EMS at regional operations center
Actor #2	Multiple transmission SCADA/EMS at utility operations centers
Description of interface: media, network and/or protocol	Broadband WAN with firewalls, VPNs, etc., sometimes privately owned or sometimes dedicated, telecom-owned network IEC 60870-6 (ICCP) protocol predominantly used

[1] California Independent System Operator (CAISO) Mission Statement, http://www.caiso.com/docs/2005/09/28/200509281333048821.html

Item	Description
Information exchanged	1. Transmission system real-time operational data from the transmission SCADA/EMS 2. Operational information, commands, requests from the ISO/RTO SCADA/EMS
Confidentiality, integrity and available cyber security requirements	• Integrity of data • Availability within the performance constraints • Authentication of information exchanges • Non-repudiation of commands or requests • Confidentiality (less critical)
Vulnerability classes	Vulnerabilities related to systems in different organizations exchanging data over a broadband wide area networks.
Threats	• *Inadvertent*: Mistakes, inadequate system design, by-passing controls, resource exhaustion • *Deliberate*: Masquerade, man-in-the-middle, physical intrusion, resource exhaustion, spoofing, repudiation
Impact	• Incorrect or missing transmission data can cause reliability problems with the power system, ranging from trivial to serious, including wide-spread blackouts. • Additional impacts are inefficient operations, incorrect response to market prices for transmission paths and/or generation. • Lost or incorrect commands or requests could also lead to these same types of impacts.

Item	Description
Constraints and/or issues	• ICCP has authentication and encryption security through IEC 62351, but this security is not always implemented. • Different organizations can have different security policies, different enforcement level, and different security technologies, thus possibly leading to lack of interoperability, security gaps, and decreased availability. • These interactions may be one-way deliberately to minimize security vulnerabilities of cross-organizational data exchanges. For instance, the ISO/RTO may collect data using their own RTUs in the substation, and may just issue emails or other notifications to computers not directly connected to the SCADA/EMS. • Real-time data is being exchanged, with time latency requirements of 1 to a few seconds. • No major constraints on types of security measures such as encryption, key management, etc.
Additional comments	

1.25DGM Interface #2: Between Energy Market Clearinghouse and Aggregator/Energy Services Provider

Brief Description and/or Purpose of Interface:

The Energy Market Clearinghouse manages the energy market, including both wholesale and retail energy markets.

The Aggregator/Energy Services Provider (ESP) manages the DER and load of groups of customers who have signed up with the ESP, according to various tariffs provided by the utility, as agreed to by the State Regulators. The ESP can use the Energy Market Clearinghouse to trade in energy and many different types of ancillary services, depending on local regulations and utility tariffs. Examples include:

- Demand pricing for energy
- Critical Peak Pricing
- Emergency pricing
- Load following

- Spinning reserve
- Operational reserve
- Voltage support
- Volt/var support
- Microgrid management

The ESP bids into the market for the different energy services, which are matched to offers and either accepted or rejected. The results of accepted bids are monitored by appropriate methods, including general smart metering, DER metering, status, and measurements, Energy Storage metering, status, and measurements, and PEV metering, status, and measurements. This information is used to validate the accepted bids during settlements and billing/invoicing of the ESP through the Energy Market Clearinghouse.

Item	Description
Diagram Identifier	DGM #2
Actor #1	Energy Market Clearinghouse
Actor #2	Aggregator/Energy Services Provider
Description of interface: media, network and/or protocol	Broadband public WAN with firewalls, VPNs, etc. No specific standards for retail trading, although most likely XML-based, such as web services
Information exchanged	Energy bids, offers, pricing, bid acceptance
Confidentiality, integrity and available cyber security requirements	• Confidentiality of pricing and bids is critical • Non-repudiation is critical • Integrity is critical
Vulnerability classes	Vulnerabilities related to systems in different organizations exchanging data over a broadband wide area networks.
Threats	•
Impact	•

Item	Description
Constraints and/or issues	• Different organizations can have different security policies, different enforcement level, and different security technologies, thus possibly leading to loss of confidentiality, lack of interoperability, security gaps, and decreased availability. • No major constraints on types of security measures such as encryption, key management, etc.
Additional comments	

1.26DGM Interface #3: Between Transmission SCADA/EMS and DMS Functions

Brief Description and/or Purpose of Interface:

The Transmission SCADA/EMS system monitors, analyzes, and controls the transmission system. The SCADA system collects real-time information while the EMS uses power flow-based applications and other tools to analyze the current and near-term state of the transmission grid.

The DMS functions, many of which use models of the electrical connectivity and power flows to simulate the actual power system, can analyze real-time conditions, and estimate/forecast near-term power system conditions. From this analysis, other DMS functions can determine what actions could or should be taken to improve these conditions, whether for managing outages and emergencies, or improving reliability, efficiency, or environmental conditions. These DMS functions will need to handle increasingly complex conditions, as more DER and PEVs are implemented at customer premises, and demand response alters customer behavior. Some additional functions include Outage Management and Work Management.

For the most effective power system management, the EMS and DMS need to exchange power system information in real-time and near-real-time, since the state of one can affect the other, including improving or decreasing reliability and efficiency.

Item	Description
Diagram Identifier	DGM #3
Actor #1	Transmission SCADA/EMS
Actor #2	DMS Functions

Item	Description
Description of interface: media, network and/or protocol	Broadband privately owned or privately leased WAN and/or LAN, even if the transmission and distribution utilities are different companies. IEC 60870-6 (ICCP) protocol can be used for exchanging real-time power system data. Alternately, EMS and DMS applications can access databases of key data updated in gateway systems by the other applications
Information exchanged	Real-time transmission and distribution data Power flow results, including reliability and efficiency information
Confidentiality, integrity and available cyber security requirements	• Integrity is the key requirement • Availability is increasingly important as these systems rely on each other more
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Different organizations can have different security policies, different enforcement level, and different security technologies, thus possibly leading to loss of confidentiality, lack of interoperability, security gaps, and decreased availability. • No major constraints on types of security measures such as encryption, key management, etc.
Additional comments	

1.27DGM Interface #4: Between Energy Market Clearinghouse and DMS Functions

Brief Description and/or Purpose of Interface:

The Energy Market Clearinghouse manages the energy market, including both wholesale and retail energy markets. When interfacing with the DMS functions, it is usually acting for the retail energy market. In particular for the retail market, it can provide a market for:

- Local marginal pricing (LMP) for energy

- Critical Peak Pricing (CPP)
- Emergency pricing
- Load following
- Spinning reserve either from available DER generation or load shedding
- Operational reserve either from available DER generation or load shedding
- Voltage support
- Volt/var support
- Microgrid management

The DMS functions, many of which use models of the electrical connectivity and power flows to simulate the actual power system, can analyze real-time conditions, and estimate/forecast near-term power system conditions. From this analysis, other DMS functions can determine what actions could or should be taken to improve these conditions, whether for managing outages and emergencies, or improving reliability, efficiency, or environmental conditions. These DMS functions will need to handle increasingly complex conditions, as more DER and PEVs are implemented at customer premises, and demand response alters customer behavior. Some additional functions include Outage Management and Work Management.

Item	**Description**
Diagram Identifier	DGM #4
Actor #1	Energy Market Clearinghouse
Actor #2	DMS Functions
Description of interface: media, network and/or protocol	Broadband public WAN with firewalls, VPNs, etc. No specific standards for retail trading, although most likely XML-based, such as web services
Information exchanged	Offers and acceptance of bids, plus other market-related information
Confidentiality, integrity and available cyber security requirements	• Confidentiality is critical
Vulnerability classes	
Threats	•

Item	Description
Impact	•
Constraints and/or issues	• Different organizations can have different security policies, different enforcement level, and different security technologies, thus possibly leading to loss of confidentiality, lack of interoperability, security gaps, and decreased availability. • No major constraints on types of security measures such as encryption, key management, etc.
Additional comments	

1.28DGM Interface #5: Between Customer Information System and Metering & Billing System

Brief Description and/or Purpose of Interface:

The Customer Information System (CIS) contains utility customer information, such name, address, tariff, payment records, etc.

The Metering & Billing System collects the customer metering data, performs VEE (validation, estimation, and editing) of this data, applies the appropriate tariff, and issues bills to the customer. Metering and billing are typically provided by the utility, but in the future these services may be outsourced to energy service providers by some utilities

Item	Description
Diagram Identifier	DGM #5
Actor #1	Customer Information System
Actor #2	Metering & Billing System
Description of interface: media, network and/or protocol	LAN within the utility "Back Office", or, if metering and billing is performed by an energy service provider, then a broadband public or private WAN MultiSpeak is used in small utilities. Proprietary protocols (such as those from SAP) are used in most other utilities

Item	Description
Information exchanged	Metering data Customer information, including tariffs
Confidentiality, integrity and available cyber security requirements	• Confidentiality is critical • Integrity is critical
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Privacy can be a major issue related to sensitive customer information • Given the direct financial impacts to customers on their bills, accuracy is crucial including inadvertent errors or incorrectly handled data • On both WAN and LAN configurations, no major constraints on types of security measures such as encryption, key management, authentication, etc.
Additional comments	

1.29DGM Interface #6: Between Energy Market Clearinghouse and ISO/RTO

Brief Description and/or Purpose of Interface:

The Energy Market Clearinghouse manages the energy market, including both wholesale and retail energy markets.

The purpose of ISOs and RTOs is to operate the grid reliably and efficiently, and to provide fair and open transmission access via long-term contracts and a wholesale energy spot market for both energy and ancillary services.

The interactions are between them are bids, offers, and resulting agreements.

Item	Description
Diagram Identifier	DGM #6
Actor #1	Energy Market Clearinghouse
Actor #2	ISO/RTO
Description of interface: media, network and/or protocol	Broadband public WAN with firewalls, VPNs, etc. NAESB OASIS standard for wholesale trading
Information exchanged	Bids, offers, resulting agreements, and other market-related information
Confidentiality, integrity and available cyber security requirements	• Confidentiality is critical • Integrity is critical • Availability within market time windows is critical
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Different organizations can have different security policies, different enforcement level, and different security technologies, thus possibly leading to loss of confidentiality, lack of interoperability, security gaps, and decreased availability. • No major constraints on types of security measures such as encryption, key management, etc. • Security has long been recognized as very important in these interactions, and is generally implemented through standard security measures
Additional comments	

1.30DGM Interface #7: Between Distribution Operator and Distribution Field Crews

Brief Description and/or Purpose of Interface:

The Distribution Operator instructs and authorizes the distribution field crews to perform work on the distribution system. This work can include switching feeder segments, repairing circuits, replacing equipment, checking circuits, and other often dangerous work around high voltage equipment. The Distribution Operator must ensure the safety of the crews.

In addition to voice communications, the Distribution Operators can send data to mobile laptop computers in the field crew trucks, and crews can request information, fill out forms, and send job completion information.

Item	Description
Diagram Identifier	DGM #7
Actor #1	Distribution Operator
Actor #2	Distribution Field Crews
Description of interface: media, network and/or protocol	Wireless communications via a trunked mobile radio system or other wireless WAN systems. Proprietary protocols are used
Information exchanged	Switching instructions, digital maps, equipment descriptions, authorization forms, responses to authorizations.
Confidentiality, integrity and available cyber security requirements	• Integrity is critical for safety reasons •
Vulnerability classes	
Threats	• Theft of laptops or other mobile computing devices
Impact	• Physical safety
Constraints and/or issues	• If narrowband wireless systems (e.g. trunked mobile radio systems) are used, they can limit the types of security that can be implemented, and can pose additional types of security vulnerabilities
Additional comments	

1.31DGM Interface #8: Between Distribution Field Crews and Geographic Information Systems

Brief Description and/or Purpose of Interface:

The Geographic Information System (GIS), also called an Automated Mapping and Facilities Management (AM /FM) system, contains digital maps of the distribution power system, usually overlaid on the land maps of streets and houses. It also contains the detailed information about the equipment on the distribution system, such as voltage regulators, capacitor banks, and feeder switches.

Distribution field crews rely heavily on maps of the power grid topography and equipment descriptions stored in Geographic Information Systems (GIS). The basic maps are usually pre-loaded on their mobile laptops, but updates and specific equipment information may be accessed over a wireless system. Alternatively, "as built" updates to the maps can be uploaded to the GIS (or often to a database which can be used to update the GIS).

Item	Description
Diagram Identifier	DGM #8
Actor #1	Distribution Field Crews
Actor #2	Geographic Information Systems
Description of interface: media, network and/or protocol	Wireless communications via a trunked mobile radio system or other wireless WAN systems. Proprietary protocols are used
Information exchanged	Maps, equipment information, "as-built" updates
Confidentiality, integrity and available cyber security requirements	• Integrity is important
Vulnerability classes	
Threats	• Theft of laptops or other mobile computing devices
Impact	•
Constraints and/or issues	• If narrowband wireless systems (e.g. trunked mobile radio systems) are used, they can limit the types of security that can be implemented, and can pose additional types of security vulnerabilities
Additional comments	

1.32DGM Interface #9: Between Distribution SCADA and Distribution Field IEDs

Brief Description and/or Purpose of Interface:

The Distribution SCADA system monitors and controls distribution equipment in substations and on feeders if distribution automation has been implemented. It is the main method that distribution operators have to know the real-time status of the "primary" middle voltage distribution system, but it does not cover the "secondary" low voltage distribution system, leaving distribution operations essentially "blind" to the secondary system.

Distribution field equipment can range from the "legacy" Remote Terminal Units (RTUs) in substations to Intelligent Electronic Devices (IEDs). Some IEDs can communicate only with the SCADA system, but some have "distributed intelligence" in which they communicate with each other in the field to do automated switching if they detect a power system fault (see DGM Interface #28).

The distribution SCADA system receives real-time information (alarms, status, measurements) from the field equipment and issues control commands to that equipment. In addition, various settings can be downloaded. Time synchronization data is also frequently sent to ensure accurate time stamping of real-time data and logs.

Item	Description
Diagram Identifier	DGM #9
Actor #1	Distribution SCADA
Actor #2	Distribution Field IEDs
Description of interface: media, network and/or protocol	900 MHz Multiple Address Radio (MAS) is a common media, configured at 9600 bps point-to-multipoint. AMI systems may be used in the future, if they can provide the performance, reliability, and availability required. DNP3 is the most common protocol IEC 61850 is viewed as the protocol to be used in the future.
Information exchanged	Real-time information (alarms, status, measurements) from the field equipment. Control commands to that equipment. Settings and time synchronization.
Confidentiality, integrity and available cyber security requirements	• Integrity is critical • Availability is critical on the order of a few seconds latency

Item	Description
Vulnerability classes	
Threats	•
Impact	• Physical safety
Constraints and/or issues	• 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, but that is becoming less of an issue. • IEDs are on poletops and other insecure locations
Additional comments	

1.33DGM Interface #10: Between Meter/HAN Gateway and Customer DER, ES, PEV, & Appliances

Brief Description and/or Purpose of Interface:

The gateway between the AMI system and the Home Area Network (HAN) provides a security block/firewall as well as containing applications to allow specific types of information to flow between the AMI and the HAN.

The customer equipment on the HAN includes:

- Distributed Energy Resources (DER) such as photovoltaic systems, wind turbines, diesel generators, and combined heat and power (CHP)
- Electric Storage (ES) such as batteries and flywheels
- Plug-in Electric Vehicles (PEV) which can be both load (charging) and generation (discharging)
- Appliances, such as air conditioners, electric water heaters, pool pumps, and the increasing plethora of smart appliances

For distribution grid management, the most important information exchanged is the near-real-time power system information, such as load, generation, available generation, voltage, vars, etc.

Item	Description
Diagram Identifier	DGM #10

Item	Description
Actor #1	Meter/HAN Gateway
Actor #2	Customer DER, ES, PEV, & Appliances
Description of interface: media, network and/or protocol	LAN within a customer premise, typically ZigBee, HomePlug, or similar wireless or wired communications media. Smart Energy Profile (SEP) is becoming the protocol of choice, but most implementations still use proprietary protocols
Information exchanged	For distribution grid management, the most important information exchanged is the near-real-time power system information, such as load, generation, available generation, voltage, vars, etc.
Confidentiality, integrity and available cyber security requirements	• Integrity is important • Confidentiality can be very important if multiple stakeholders are involved
Vulnerability classes	•
Threats	• Inadvertent and deliberate security compromises due to very insecure environment
Impact	• Could have financial impact if information is compromised
Constraints and/or issues	• HAN is under customer control, and customers often do not understand or apply security measures
Additional comments	

1.34DGM Interface #11: Between External 3rd Party and Meter/HAN Gateway

Brief Description and/or Purpose of Interface:

External 3rd Parties are any entity that has been authorized to exchange information with some other entity in the customer premises. The types of purposes and types of data exchanged are extensive, and, for the most part, unknown at this time. Examples of such 3rd parties could include home security monitoring, medical monitoring, vendors monitoring their appliance performance, or even the customer turning on his air conditioner and his microwave to cool the house and heat his dinner shortly before he gets home.

The gateway between the AMI system and the Home Area Network (HAN) provides a security block as well as containing applications to allow specific types of information to flow between the AMI and the HAN.

Item	Description
Diagram Identifier	DGM #11
Actor #1	External 3rd Party
Actor #2	Meter/HAN Gateway
Description of interface: media, network and/or protocol	Both wired and wireless media are possible, most likely broadband in order to meet the potentially large amount of traffic The most likely network is the public Internet, but others are possible, particularly for commercial and/or industrial customers who can implement private networks, at least up to a central site The protocols are most likely to be the Internet protocols
Information exchanged	A wide range of types of information, mostly unknown at this time, since these types of interfaces have not been implemented in many places
Confidentiality, integrity and available cyber security requirements	• Security requirements will vary tremendously, depending upon the applications. Authentication will be primary consideration
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• This interface is probably the one of most concern from a privacy and general security point of view, since it will be “open” to many entities, with potential threats from many different sources to impact the power grid
Additional comments	

1.35DGM Interface #12: Between Aggregator/Energy Services Provider and AMI Headend

Brief Description and/or Purpose of Interface:

The Aggregator/Energy Services Provider (ESP) manages the DER and load of groups of customers who have signed up with the ESP, according to various tariffs provided by the utility, as agreed to by the State Regulators. The ESP can use the Energy Market Clearinghouse to trade in energy and many different types of ancillary services, depending on local regulations and utility tariffs.

The AMI system headend is the manager/controller of the AMI network, and handles all interactions between external applications and the meter. It can also manage separate information exchanges between external applications and the gateway to the HAN. These AMI systems are very proprietary and quite new, so they are all being updated fairly continuously.

With this interface to the AMI headend, the Aggregator/Energy Services Provider (ESP) could possibly be providing out-sourced metering and billing services to the utility, as well as using the AMI system to manage customer DER and loads.

Item	Description
Diagram Identifier	DGM #12
Actor #1	Aggregator/Energy Services Provider
Actor #2	AMI Headend
Description of interface: media, network and/or protocol	Most likely a private WAN (owned or leased), although potentially the public Internet could be used for some data. The network is most likely to be internet-based Protocols are proprietary, although conceptually either CIM or MultiSpeak could be used
Information exchanged	Outsourced metering and billing, DER and load management monitoring and control information, ultimately to be exchanged across the AMI network through the HAN gateway to the DER units and loads in the customer premises
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•

Item	Description
Impact	•
Constraints and/or issues	• Different organizations can have different security policies, different enforcement level, and different security technologies, thus possibly leading to lack of interoperability, security gaps, and decreased availability. • The AMI headend is a particularly sensitive system since problems (inadvertent or security attacks) with its management of the AMI network and with its interfaces with meters can impact so many customers.
Additional comments	

1.36DGM Interface #13: Between Distribution Operator and DMS Functions

Brief Description and/or Purpose of Interface:

The Distribution Operator uses the DMS functions to analyze the state of the distribution grid and make decisions on actions to take to respond to outages, improve efficiency, improve reliability, and other distribution functions. This interaction can include functions where the operator makes all decisions and initiates all actions (the most common today), but in the future will consist of more advisory and eventually autonomous actions by the DMS functions, such as responding within seconds to outages and overload situations, with just reporting back to the operator on what took place. These autonomous actions will become increasingly necessary as more DER is installed in customer premises and utility substations, as tariffs make demand response more attractive to customers, and as microgrids and other power system configurations make managing the distribution grid more complex.

The DMS functions, many of which use models of the electrical connectivity and power flows to simulate the actual power system, can analyze real-time conditions, and estimate/forecast near-term power system conditions. From this analysis, other DMS functions can determine what actions could or should be taken to improve these conditions, whether for managing outages and emergencies, or improving reliability, efficiency, or environmental conditions. These DMS functions will need to handle increasingly complex conditions, as more DER and PEVs are implemented at customer premises, and demand response alters customer behavior. Some additional functions include Outage Management and Work Management.

The actual interface between the Distribution Operator and the DMS functions is the Human-Machine Interface (HMI).

Item	Description
Diagram Identifier	DGM #13
Actor #1	Distribution Operator
Actor #2	DMS Functions
Description of interface: media, network and/or protocol	HMI over LAN – usually in the same building, but alternately over private WAN
Information exchanged	Settings and visual monitoring of information
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• No standards exist for HMIs, although there are many best practices for presenting information clearly
Additional comments	

1.37DGM Interface #14: Between Distribution SCADA System and DMS Functions

Brief Description and/or Purpose of Interface:

The Distribution SCADA system monitors field data and issues control commands to field equipment, based on distribution operator commands or automated commands from the DMS functions. The Distribution SCADA systems today primarily monitor and controls only distribution equipment in substations, although some utilities are implementing distribution automation of feeder equipment, which allows this feeder equipment to be monitored and controlled as well. It is expected that the amount of distribution equipment that will be monitored and controlled by the distribution SCADA system will increase rapidly as additional power system data can be retrieved from selected smart meters.

The DMS functions, many of which use models of the electrical connectivity and power flows to simulate the actual power system, can analyze real-time conditions, and estimate/forecast near-term power system conditions. From this analysis, other DMS functions can determine what actions could or should be taken to improve these conditions, whether for managing outages and emergencies, or improving reliability, efficiency, or environmental conditions. These DMS functions will need to handle increasingly complex conditions, as more DER and PEVs are implemented at customer premises, and demand response alters customer behavior. Some additional functions include Outage Management and Work Management.

Item	Description
Diagram Identifier	DGM #14
Actor #1	Distribution SCADA System
Actor #2	DMS Functions
Description of interface: media, network and/or protocol	Typically a LAN within the same room or building Vendor-specific protocols or the ICCP protocol can be used. CIM and/or MultiSpeak may be used in the future
Information exchanged	Real-time data, automated control commands
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Not many security issues at this interface, unless the systems are organized into different security domains
Additional comments	

1.38DGM Interface #15: Between Geographic Information Systems and Customer Information System

Brief Description and/or Purpose of Interface:

The Geographic Information System (GIS), also called an Automated Mapping and Facilities Management (AM /FM) system, contains digital maps of the distribution power system, usually overlaid on the land maps of streets and houses. It also contains the detailed information about the equipment on the distribution system, such as voltage regulators, capacitor banks, and feeder switches.

The Customer Information System (CIS) contains utility customer information, such name, address, tariff, payment records, historical energy usage, meter ID, etc.

The interface between the GIS and CIS permits the customer information to be linked to their physical location on the digital maps.

Item	Description
Diagram Identifier	DGM #15
Actor #1	Geographic Information Systems
Actor #2	Customer Information System
Description of interface: media, network and/or protocol	Usually a LAN, often in the same building. If the CIS is outsourced to another organization, then a private WAN is used. Proprietary protocols are the most common although there are efforts to develop standards
Information exchanged	Customer information and facilities information
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Privacy of the customer information may become an issue if sensitive data is provided to the GIS
Additional comments	

1.39DGM Interface #16: Between DMS Functions and Load Management System (LMS)

Brief Description and/or Purpose of Interface:

The DMS functions, many of which use models of the electrical connectivity and power flows to simulate the actual power system, can analyze real-time conditions, and estimate/forecast near-term power system conditions. From this analysis, other DMS functions can determine what actions could or should be taken to improve these conditions, whether for managing outages and emergencies, or improving reliability, efficiency, or environmental conditions. These DMS functions will need to handle increasingly complex conditions, as more DER and PEVs are implemented at customer premises, and demand response alters customer behavior. Some additional functions include Outage Management and Work Management.

The Load Management System (LMS) takes the results of the DMS analysis of distribution requirements to determine how best to implement them via customer actions, working either through direct load control or indirectly through pricing signals.

Configurations and scenarios can differ significantly, but in one scenario, the load management system would actually determine the pricing signals based on distribution requirements, identifying each type of customer, each type of ancillary service, and each type of DER, storage, PEV, appliance. Alternatively these pricing signals could be set by energy service providers based on market clearinghouse prices submitted by the DMS functions (see DGM Interface #4).

Item	Description
Diagram Identifier	DGM #16
Actor #1	DMS Functions
Actor #2	Load Management System
Description of interface: media, network and/or protocol	LAN, usually in the same building, or private WAN if in separate locations Usually proprietary protocols, with CIM and/or MultiSpeak as future object models
Information exchanged	Requirements from the DMS functions for load management Responses from load management on actions taken
Confidentiality, integrity and available cyber security requirements	•

Item	Description
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Not many security issues at this interface, unless the systems are organized into different security domains
Additional comments	

1.40DGM Interface #17: Between Customer Information System (CIS) and Customer EMS

Brief Description and/or Purpose of Interface:

The Customer Energy Management System (EMS) is responsible for managing the customer's energy usage, based on customer preferences, tariffs, pricing signals, available DER, PEVs, and "smart" appliance capabilities.

The Customer Information System (CIS) contains utility customer information, such name, address, tariff, payment records, historical energy usage, meter ID, etc.

This interface is a "logical" interface, in that any information exchanges would either be verbal from customer telephone conversations with a utility customer representative, or entered manually by the customer into their EMS from information provided on Internet web pages, or routed through the HAN gateway via the AMI network (see DGM #30).

Item	Description
Diagram Identifier	DGM #17
Actor #1	Customer Information System (CIS)
Actor #2	Customer EMS
Description of interface: media, network and/or protocol	"Logical" interface No standards for any types of information exchanges

Item	Description
Information exchanged	To Customer EMS: Customer tariff information, payment options such as pre-payment, DER tariff information From Customer EMS: PEV registration, tariff agreements
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Privacy is a very important aspect of these interactions between customer EMS and CIS
Additional comments	

1.41DGM Interface #18: Between Load Management System (LMS) and Customer EMS

Brief Description and/or Purpose of Interface:

The Load Management System takes the results of the DMS analysis of distribution requirements to determine how best to implement them via customer actions, working either through direct load control or indirectly through pricing signals.

Configurations and scenarios can differ significantly, but in one scenario, the load management system would actually determine the pricing signals based on distribution requirements, identifying each type of customer, each type of ancillary service, and each type of DER, storage, PEV, appliance. Alternatively these pricing signals could be set by energy service providers based on market clearinghouse prices offered by the DMS functions for different energy and ancillary services (see DGM Interface #4).

The Customer Energy Management System (EMS) is responsible for managing the customer's energy usage, based on customer preferences, tariffs, pricing signals, available DER, PEVs, and "smart" appliance capabilities.

The interface between the Load Management System (LMS) and the Customer EMS may be direct in which load shed commands are issued directly to customer appliances using paging systems or other direct multicast communications media, or it may be indirect through pricing or command signals via the AMI system.

Item	Description
Diagram Identifier	DGM #18
Actor #1	Load Management System
Actor #2	Customer EMS
Description of interface: media, network and/or protocol	Paging or one-way radio system (legacy) Via the AMI system
Information exchanged	Load management signals to change load and/or generation, either as commands or pricing signals Response to load management signals, indicating degree of compliance or non-compliance
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Load management signals whether direct load control or indirect pricing or energy request signals, can have profound effects on customer reactions. If these signals are compromised, serious power system consequences could result, as well as serious customer reactions to the Smart Grid.
Additional comments	

1.42DGM Interface #19: Between Customer Information System (CIS) and AMI Headend

Brief Description and/or Purpose of Interface:

The Customer Information System (CIS) contains utility customer information, such name, address, tariff, payment records, historical energy usage, meter ID, etc.

The AMI system headend is the manager/controller of the AMI network, and handles all interactions between external applications and the meter. It can also manage separate information exchanges between external applications and the gateway to the HAN. These AMI systems are very proprietary and quite new, so they are all being updated fairly continuously.

The CIS is typically used by utility "customer service representatives" who answer calls from customers on billing issues, move-ins/move-outs, changing tariffs, and other utility-customer interactions. The CIS can then be used to request "on-demand" meter reads or scheduled "move-outs", and other interactions with the customer meter. The CIS may also be used in the future to exchange information with the customer, such as new services, current rate plans, registering PEVs, etc.

Item	Description
Diagram Identifier	DGM #19
Actor #1	Customer Information System (CIS)
Actor #2	AMI Headend
Description of interface: media, network and/or protocol	LAN or private WAN Proprietary protocols are currently used, but CIM and/or MultiSpeak are planned to be used in the future.
Information exchanged	Requests from CIS to AMI headend for on-demand meter reads, scheduled remote connect/disconnects, non-payment disconnects, sub-meter reads Response to CIS requests, as well as requests from customers through the AMI system for PEV registration, rate information, energy services, etc.
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Privacy of customer information within the CIS as well as collected through the AMI headend will be critical
Additional comments	

1.43DGM Interface #20: Between AMI Headend and Meter/HAN Gateway

Brief Description and/or Purpose of Interface:

The AMI system headend is the manager/controller of the AMI network, and handles all interactions between external applications and the meter. It can also manage separate information exchanges between external applications and the gateway to the HAN. These AMI systems are very proprietary and quite new, so they are all being updated fairly continuously.

The gateway between the AMI system and the Home Area Network (HAN) provides a security block/firewall as well as containing applications to allow specific types of information to flow between the AMI and the HAN.

The customer equipment on the HAN includes:

- Distributed Energy Resources (DER) such as photovoltaic systems, wind turbines, diesel generators, and combined heat and power (CHP)
- Electric Storage (ES) such as batteries and flywheels
- Plug-in Electric Vehicles (PEV) which can be both load (charging) and generation (discharging)
- Appliances, such as air conditioners, electric water heaters, pool pumps, and the increasing plethora of smart appliances

The interface between the AMI headend and the Meter and/or HAN gateway is the AMI network. The AMI network typically consists of a high bandwidth backbone WAN from the AMI headend to strategic locations where data concentrators are located, and then narrowband communication channels from the data concentrators to the customer meter (and/or HAN gateway). The latter narrowband communications is often radio-based, but can also be power line carrier or GPRS (cellphone data). The radio-based systems are often meshed for improved coverage and availability.

Item	Description
Diagram Identifier	DGM #20
Actor #1	AMI Headend
Actor #2	Meter/HAN Gateway

Item	Description
Description of interface: media, network and/or protocol	Proprietary AMI network, using broadband WAN and narrower band, often meshed, radio systems to the meter and HAN gateway. ANSI C12.22 is the most commonly used protocol – it has recently been updated with security but needs assessment on the new functionalities. ANSI C12.19 is the object model for the meter No specific object models have been developed for interactions with devices and systems across the HAN gateway. Object models exist for some DER, but none yet for PEV
Information exchanged	Metering data Requests for metering data Interactions with HAN devices (these could vary from none to very many of differing types and security requirements)
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	In the AMI space, there is increasing likelihood that mesh routing protocols will be used on wireless links. Wireless suffers from several well-known and often easily exploitable attacks partly due to the lack of control to the physical medium (the radio waves). Modern mechanisms like 802.11i have worked to close some of these holes for standard wireless deployments. However, wireless mesh technology potentially opens the door to some new attacks in the form of route injection, node impersonation, L2/L3/L4 traffic injection, and traffic modification. Most current on-demand and link-state routing mechanisms do not specify a scheme to protect the data or the routes the data takes, primarily because of the distributed nature of the system itself. They also generally lack schemes for authorizing and providing integrity protection for adjacencies in the routing system. Imposing a central authority to control those mechanisms provides a single point of failure and is against the core design principle. These issues need to be explored and addressed by experts in that area and applicable technology utilized in the AMI space.

Item	Description
Additional comments	

1.44DGM Interface #21: Between DMS Functions and Geographical Information System (GIS)

Brief Description and/or Purpose of Interface:

The DMS functions, many of which use models of the electrical connectivity and power flows to simulate the actual power system, can analyze real-time conditions, and estimate/forecast near-term power system conditions. From this analysis, other DMS functions can determine what actions could or should be taken to improve these conditions, whether for managing outages and emergencies, or improving reliability, efficiency, or environmental conditions. These DMS functions will need to handle increasingly complex conditions, as more DER and PEVs are implemented at customer premises, and demand response alters customer behavior.

The Geographic Information System (GIS), also called an Automated Mapping and Facilities Management (AM /FM) system, contains digital maps of the distribution power system, usually overlaid on the land maps of streets and houses. It also contains the detailed information about the equipment on the distribution system, such as voltage regulators, capacitor banks, and feeder switches.

The DMS functions need the GIS data to create the physical and normal electrical connectivity of the distribution power flow topological model. The GIS can also provide locations and nameplate information of distribution equipment in the substations and on the feeders.

Item	Description
Diagram Identifier	DGM #21
Actor #1	DMS Functions
Actor #2	Geographical Information System (GIS)
Description of interface: media, network and/or protocol	Usually a LAN with a firewall, often in the same building. If the GIS is in another location, then a private WAN is used. Proprietary protocols are the most common although there are efforts to develop standards for geographical information. Eventually CIM and/or MultiSpeak may be used to retrieve the equipment data
Information exchanged	Topological data and equipment nameplate data from the GIS to the DMS Typically no information flow from DMS to GIS (except requests to clean up bad data)

Item	Description
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Not many security issues at this interface, unless the systems are organized into different security domains
Additional comments	

1.45DGM Interface #22: Between Customer Information System (CIS) and Load Management System (LMS)

Brief Description and/or Purpose of Interface:

The Customer Information System (CIS) contains utility customer information, such name, address, tariff, payment records, historical energy usage, meter ID, etc.

The Load Management System (LMS) takes the results of the DMS analysis of distribution requirements to determine how best to implement them via customer actions, working either through direct load control or indirectly through pricing signals.

The CIS provides the LMS with all the necessary customer information that the LMS needs to issue load control commands or pricing signals to specific customers. In return the LMS provides the CIS with the commands issued to the customers or the types of signals requesting customer actions. This information will be used by the CIS as input to the metering and billing system.

Item	Description
Diagram Identifier	DGM #22
Actor #1	Customer Information System (CIS)
Actor #2	Load Management System (LMS)

Item	Description
Description of interface: media, network and/or protocol	LAN with firewall, usually in the same building, or private WAN if in separate locations Usually proprietary protocols, with CIM and/or MultiSpeak as future object models
Information exchanged	Customer information to LMS to issue load control commands and/or signals Update customer information in CIS to reflect the load control commands or signals issued to the customers, including what was requested, when requested for, amount requested, etc.
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• These systems are usually organized into different security domains, so a firewall is necessary
Additional comments	

1.46DGM Interface #23: Between Distribution Operator and Distribution SCADA System

Brief Description and/or Purpose of Interface:

The Distribution Operator uses the Distribution SCADA to view the real-time data from the distribution system and to issue control commands to field equipment.

The actual interface between the Distribution Operator and the DMS functions is the Human-Machine Interface (HMI).

Item	Description
Diagram Identifier	DGM #23

Item	Description
Actor #1	Distribution Operator
Actor #2	Distribution SCADA System
Description of interface: media, network and/or protocol	HMI over LAN – usually in the same building, but alternately over private WAN
Information exchanged	Visual displays of real-time information and data entry for changes and commands to field equipment
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• No standards exist for HMIs, although there are many best practices for presenting information clearly
Additional comments	

1.47DGM Interface #24: Between Distribution SCADA System and Transmission SCADA/EMS

Brief Description and/or Purpose of Interface:

The Distribution SCADA system monitors and controls distribution equipment in substations and on feeders if distribution automation has been implemented. It is the main method that distribution operators have to know the real-time status of the "primary" middle voltage distribution system, but it does not cover the "secondary" low voltage distribution system, leaving distribution operations essentially "blind" to the secondary system.

The Transmission SCADA/EMS system monitors, analyzes, and controls the transmission system. The SCADA system collects real-time information while the EMS uses power flow-based applications and other tools to analyze the current and near-term state of the transmission grid.

These two systems exchange mostly real-time data to augment the equipment directly monitored by each: the transmission SCADA provides key transmission information, while the Distribution SCADA provides selected distribution information that could affect the transmission system operations. In addition, results from analyses are exchanged if these results could affect operations.

Item	Description
Diagram Identifier	DGM #24
Actor #1	Distribution SCADA System
Actor #2	Transmission SCADA/EMS
Description of interface: media, network and/or protocol	LAN or private WAN if physically separate or belonging to different organizations ICCP is often used if these systems come from different vendors. Alternately, proprietary protocols are used.
Information exchanged	Real-time data, settings, and results for relevant analyses
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Different organizations can have different security policies, different enforcement level, and different security technologies, thus possibly leading to loss of confidentiality, lack of interoperability, security gaps, and decreased availability. • No major constraints on types of security measures such as encryption, key management, etc.
Additional comments	

1.48DGM Interface #25: Between DMS Functions and Customer Information System (CIS)

Brief Description and/or Purpose of Interface:

The DMS functions, many of which use models of the electrical connectivity and power flows to simulate the actual power system, can analyze real-time conditions, and estimate/forecast near-term power system conditions. From this analysis, other DMS functions can determine what actions could or should be taken to improve these conditions, whether for managing outages and emergencies, or improving reliability, efficiency, or environmental conditions. These DMS functions will need to handle increasingly complex conditions, as more DER and PEVs are implemented at customer premises, and demand response alters customer behavior. Some additional functions include Outage Management and Work Management.

The Customer Information System (CIS) contains utility customer information, such name, address, tariff, payment records, historical energy usage, meter ID, etc.

This interface provides the DMS functions with aggregated customer load data, including typical load shapes. (The CIS may not directly provide this data – there may an engineering application which collects the data from the CIS and Metering systems and performs the aggregations and analyses of this load information).

Item	Description
Diagram Identifier	DGM #25
Actor #1	DMS Functions
Actor #2	Customer Information System (CIS)
Description of interface: media, network and/or protocol	LAN with firewall, or private WAN Usually proprietary protocols, with CIM and/or MultiSpeak as future object models
Information exchanged	Aggregated load information from CIS to DMS functions Not expected to have significant data from DMS to CIS
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•

Item	Description
Constraints and/or issues	• These systems are usually organized into different security domains, so a firewall is necessary
Additional comments	

1.49DGM Interface #26: Between DMS Functions and Distribution Engineering

Brief Description and/or Purpose of Interface:

The DMS functions, many of which use models of the electrical connectivity and power flows to simulate the actual power system, can analyze real-time conditions, and estimate/forecast near-term power system conditions. From this analysis, other DMS functions can determine what actions could or should be taken to improve these conditions, whether for managing outages and emergencies, or improving reliability, efficiency, or environmental conditions. These DMS functions will need to handle increasingly complex conditions, as more DER and PEVs are implemented at customer premises, and demand response alters customer behavior. Some additional functions include Outage Management and Work Management.

Distribution engineering typically includes short-term studies to assess distribution concerns or changes, including distribution equipment setting changes, equipment replacements, maintenance efforts, and operational changes for improved efficiency and reliability. Distribution engineering also develops longer term planning for new construction and re-construction.

The information from short-term DMS functions is used by Distribution Engineering for their improvements, maintenance activities, and longer range planning. The Distribution Engineering information can be used by the DMS functions to study “what if” scenarios, plan for scheduled work, and develop contingency plans for scheduled outages.

Item	Description
Diagram Identifier	DGM #26
Actor #1	DMS Functions
Actor #2	Distribution Engineering
Description of interface: media, network and/or protocol	LAN with firewall, or private WAN Usually proprietary protocols, with CIM and/or MultiSpeak as future object models

Item	Description
Information exchanged	The DMS functions can provide power system models, real-time data, calculated/estimated data The Distribution Engineering provides schedule work plans including scheduled outages
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• These systems are usually organized into different security domains, so a firewall is necessary
Additional comments	

1.50DGM Interface #27: Between DMS Functions and Customer EMS

Brief Description and/or Purpose of Interface:

The DMS functions, many of which use models of the electrical connectivity and power flows to simulate the actual power system, can analyze real-time conditions, and estimate/forecast near-term power system conditions. From this analysis, other DMS functions can determine what actions could or should be taken to improve these conditions, whether for managing outages and emergencies, or improving reliability, efficiency, or environmental conditions. These DMS functions will need to handle increasingly complex conditions, as more DER and PEVs are implemented at customer premises, and demand response alters customer behavior. Some additional functions include Outage Management and Work Management.

The Customer Energy Management System (EMS) is responsible for managing the customer's energy usage, based on customer preferences, tariffs, pricing signals, available DER, PEVs, and "smart" appliance capabilities.

This interface is a "logical" interface, in that any information exchanges either could be routed through the AMI network (see DGM #31) or through the Internet to the HAN gateway.

The information exchanged could include customer outage restoration time (assuming the Customer EMS still has power), planned work that could cause momentary or more permanent outages in the future, scheduled distribution maintenance efforts which could affect the reliability or power quality

for the customer, and other utility-customer energy services. The Customer EMS could update the DMS functions on availability of DER or other power-related issues.

Item	Description
Diagram Identifier	DGM #27
Actor #1	DMS Functions
Actor #2	Customer EMS
Description of interface: media, network and/or protocol	Either the AMI network or the public Internet No object models have been develop yet, although CIM and/or MultiSpeak could eventually be used
Information exchanged	The DMS provides energy services information The Customer EMS provides customer power-related status and information
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Both the AMI network and the public Internet pose privacy and other security issues. The AMI network may have limited bandwidth for some types of exchanges.
Additional comments	

1.51DGM Interface #28: Between Distributed Field IEDs and Other Distributed Field IEDs

Brief Description and/or Purpose of Interface:

Some distributed Intelligent Electronic Devices (IEDs) can communicate with each other in the field to do automated reclosing and switching if they detect a power system fault in order to isolate the fault to only the affected feeder segment rather than the entire feeder, and restore power to the other feeder segments.

The "information" exchanged is both via sensors that detect faults and open circuit breakers, as well as digital exchanges of data to determine which IEDs should perform which actions.

Item	Description
Diagram Identifier	DGM #28
Actor #1	Distributed Field IEDs
Actor #2	Other Distributed Field IEDs
Description of interface: media, network and/or protocol	Wireless media between IEDs DNP3 is the most common protocol
Information exchanged	Data to inform IEDs which reclosers should open or close and which switches should be in which states
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• Limited range of the wireless communications • Field equipment cannot be physically protected • Most do not yet incorporate cyber security measures
Additional comments	

1.52DGM Interface #29: Between AMI Headend and Metering/Billing System

Brief Description and/or Purpose of Interface:

The AMI system headend is the manager/controller of the AMI network, and handles all interactions between external applications and the meter. It can also manage separate information exchanges between external applications and the gateway to the HAN. These AMI systems are very proprietary and quite new, so they are all being updated fairly continuously.

The Metering & Billing System collects the customer metering data, performs VEE (validation, estimation, and editing) of this data, applies the appropriate tariff, and issues bills to the customer. Metering and billing are typically provided by the utility, but in the future these services may be outsourced to energy service providers by some utilities.

The information from the AMI headend to the Metering & Billing system is almost entirely metering data. Information to the AMI system can include remote connect/disconnect commands to meters, as well as settings, firmware uploads, and error handling interactions.

Item	Description
Diagram Identifier	DGM #29
Actor #1	AMI Headend
Actor #2	Metering/Billing System
Description of interface: media, network and/or protocol	LAN with firewall or private WAN if separated CIM and MultiSpeak have standards for this interface, although CIM does not have many implementations as yet
Information exchanged	Metering information from the AMI headend to the Metering/Billing system Settings and commands such as remote connect/disconnect from the Metering/Billing system
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•

Item	Description
Constraints and/or issues	• Security for some commands such as remote connect/disconnect is of very high priority since the potential impact of disconnecting large numbers of meters is seen as not only a financial impact, but also a political and social impact
Additional comments	

1.53DGM Interface #30: Between Meter/HAN Gateway and Customer EMS

Brief Description and/or Purpose of Interface:

The gateway between the AMI system and the Home Area Network (HAN) provides a security block/firewall as well as containing applications to allow specific types of information to flow between the AMI and the HAN.

The Customer Energy Management System (EMS) is responsible for managing the customer's energy usage, based on customer preferences, tariffs, pricing signals, available DER, PEVs, and "smart" appliance capabilities.

This interface must be able to handle pricing signals, direct energy management signals, information from and to the utility, information from and to third parties, and many still unknown interactions.

Item	Description
Diagram Identifier	DGM #30
Actor #1	Meter/HAN Gateway
Actor #2	Customer EMS
Description of interface: media, network and/or protocol	ZigBee meshed radio and HomePlug powerline carrier are the primary media used for HANs The Smart Energy Profile is expected to become the protocol for the HAN, with mappings to CIM and IEC 61850, but proprietary solutions are still prevalent
Information exchanged	Pricing signals, direct energy management signals, information from and to the utility, information from and to third parties, and many still unknown interactions

Item	Description
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• The functions of the Customer EMS and the capabilities of the HAN are still wide open, since very few have yet been precisely determined or implemented.
Additional comments	

1.54DGM Interface #31: Between DMS Functions and AMI Headend

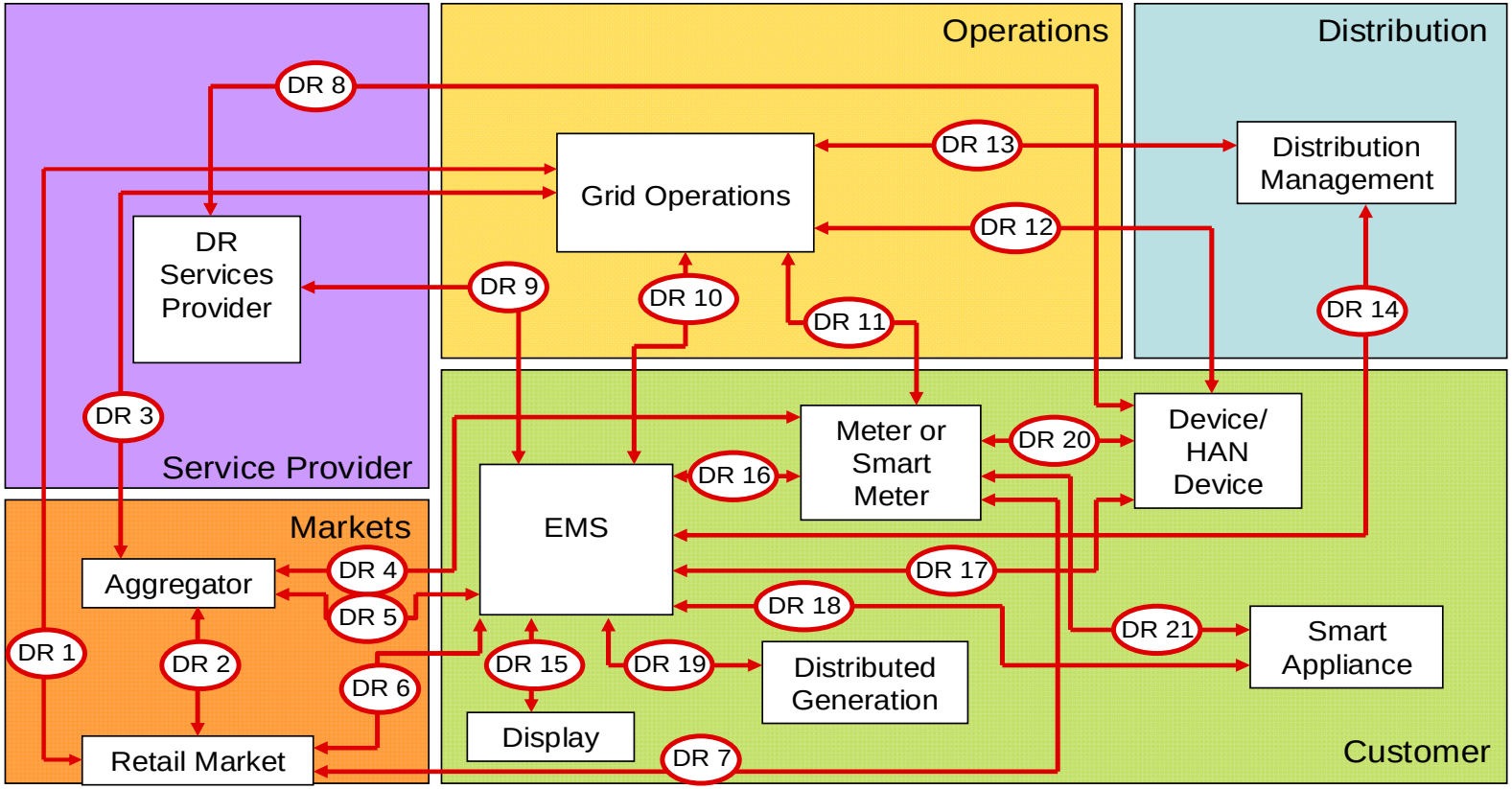
Brief Description and/or Purpose of Interface:

The DMS functions, many of which use models of the electrical connectivity and power flows to simulate the actual power system, can analyze real-time conditions, and estimate/forecast near-term power system conditions. From this analysis, other DMS functions can determine what actions could or should be taken to improve these conditions, whether for managing outages and emergencies, or improving reliability, efficiency, or environmental conditions. These DMS functions will need to handle increasingly complex conditions, as more DER and PEVs are implemented at customer premises, and demand response alters customer behavior. Some additional functions include Outage Management and Work Management.

The AMI system headend is the manager/controller of the AMI network, and handles all interactions between external applications and the meter. It can also manage separate information exchanges between external applications and the gateway to the HAN. These AMI systems are very proprietary and quite new, so they are all being updated fairly continuously.

The Outage Management System (OMS) receives meter outage information through the AMI headend, and is expected to be one of the main benefits of Smart Metering. Other DMS function information may include pricing and energy request signals, particularly those reflecting local conditions, such as feeder overloads, PV system voltage ancillary services, PEV charging and discharging signals, etc.

Item	Description
Diagram Identifier	DGM #31
Actor #1	DMS Functions
Actor #2	AMI Headend
Description of interface: media, network and/or protocol	LAN with firewall, or private WAN CIM and MultiSpeak are the standard information models for outage information between OMS and the AMI headend. Other DMS functions do not yet have specific standard information models.
Information exchanged	Outage information, pricing and energy signals, unknown additional information
Confidentiality, integrity and available cyber security requirements	•
Vulnerability classes	
Threats	•
Impact	•
Constraints and/or issues	• The information exchange requirements between the DMS and the AMI headend, except for outage information, are not known. Local pricing or energy requests may come directly from the utility-owned DMS or may be routed through aggregators and other 3rd parties. Most likely there will be variations across utilities and regulatory environments as to how these interactions become configured.
Additional comments	

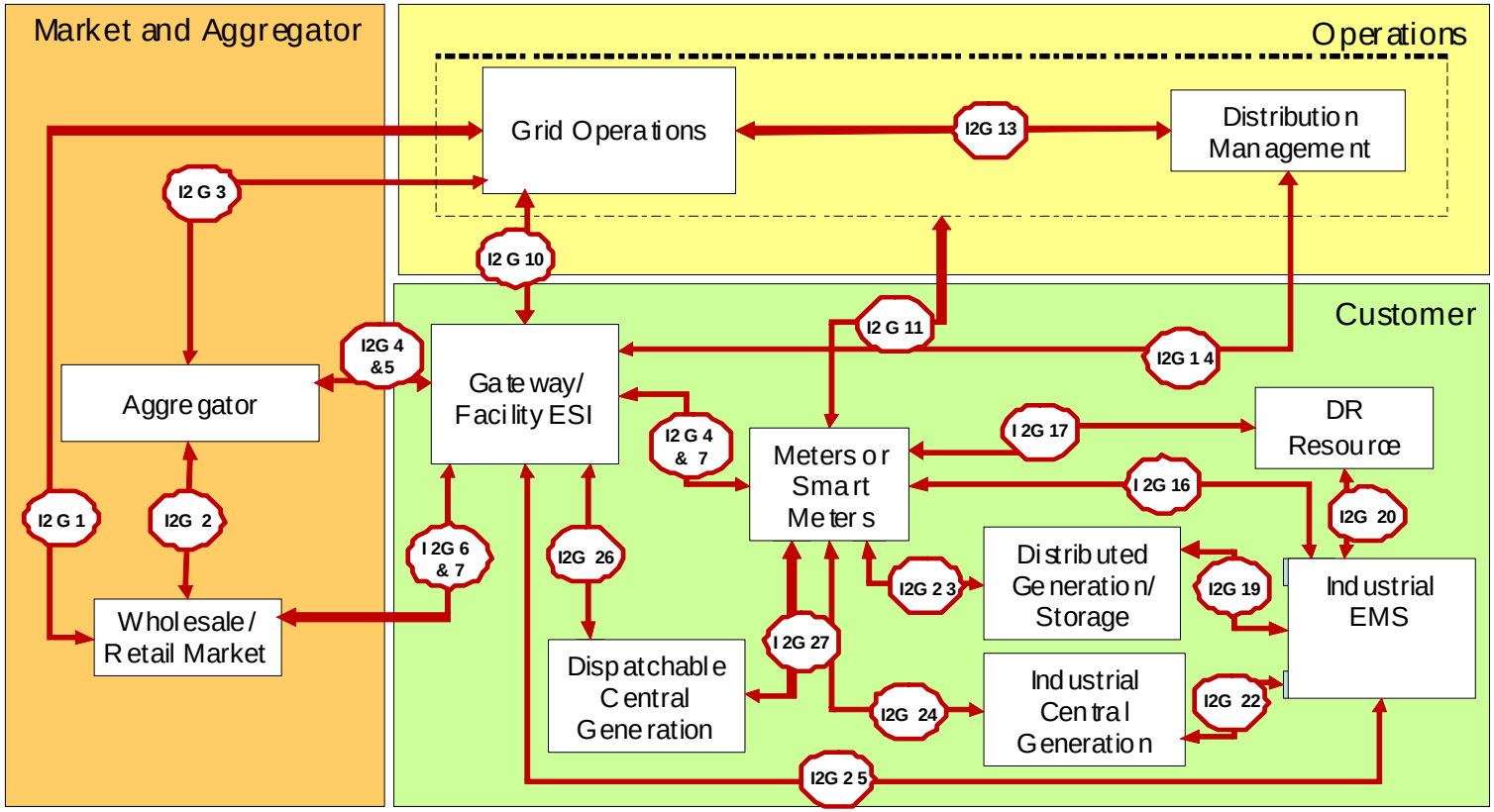


Demand Response Use Cases: Actors and Logical Interfaces

HAN: Home Area Network
EMS: Energy Management System
DR: Demand Response

Interface #	Information Object Name	Information Object Description
DR 1	Retail Market – to – Grid Operations	Retail Market – to – Grid Operations
DR 2	Retail Market – to – Aggregator	Retail Market – to – Aggregator Retail Market exchanges pricing information and demand with Aggregator
DR 3	Aggregator – to – Grid Operations	Aggregator – to – Grid Operations
DR 4	Aggregator – to – Meter or Smart Meter	Aggregator – to – Meter or Smart Meter Aggregator interfaces with Meter or Smart Meter for pricing information and usage monitoring and control.
DR 5	Aggregator – to – EMS	Aggregator – to – EMS
DR 6	Retail Market – to – Meter or Smart Meter	Retail Market – to – Meter or Smart Meter
DR 7	DR Service Provider – to – Device/HAN Device	DR Service Provider – to – Device/HAN Device
DR 8	DR Service Provider – to EMS	DR Service Provider – to EMS Load information to and from EMS.
DR 9	EMS – to – Grid Operations	EMS – to – Grid Operations Demand change based on price.
DR 10	EMS – to – Grid Operations	EMS – to – Grid Operations Real-time load information from all points
DR 11	Grid Operations – to – Meter or Smart Meter	Grid Operations – to – Meter or Smart Meter Grid Operations receiving I/O of demand and controlling Meter or Smart Meter.
DR 12	Grid Operations – to – Device/HAN Device	Grid Operations – to – Device/HAN Device Grid Operations receiving I/O of demand and controlling Device/HAN Device.

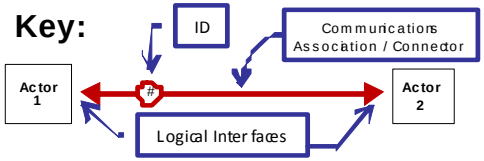
Interface #	Information Object Name	Information Object Description
DR 13	Grid Operations – to – Distribution Management	Grid Operations – to – Distribution Management Grid Operations monitors and controls system supply and demand and interfaces with Distribution Management
DR 14	Appears to be an error.	Appears to be an error.
DR 15	EMS – to – Display	EMS – to – Display Customer interface to EMS for monitoring and control.
DR 16	EMS – to – Meter or Smart Meter	EMS – to – Meter or Smart Meter EMS I/O with Meter or Smart Meter for demand information and control of Smart Devices.
DR 17	EMS – to – Device/HAN Device	EMS – to – Device/HAN Device EMS controls Smart Devices through Device/HAN Device
DR 18	EMS – to – Smart Appliance	EMS – to – Smart Appliance The customer's EMS controls Smart Appliances based on input.
DR 19	EMS – to – Distributed Generation	EMS – to – Distributed Generation The customer’s EMS received and controls the use of Distributed Generation
DR 20	Meter or Smart Meter – to – Device/HAN Device	Meter or Smart Meter – to – Device/HAN Device The meter displays the event type, scheduled event date/time (start and end) and hourly event pricing for customer viewing. I/O with Smart Meter and Device/HAN device interface with EMS for overall command and control.
DR 21	Meter or Smart meter – to – Smart Appliance	Meter or Smart meter – to – Smart Appliance Meter controls demand/use of smart appliance.
DR 22	Distribution Management – to – EMS	Distribution Management – to – EMS I/O about demand and control of EMS.



I2G Demand Response Use Cases: Actors and Logical Interfaces

ESI: Energy Services Interface
EMS: Energy Management System
DR: Demand Response

Key:



Priority I2G Interfaces:

- Interdomain between “Operations and Customer” and “Markets and Customer” – These are the interfaces numbered 10, 14, 11, 4&5 and 6&7 in the I2G DR Use Case Diagram. NOTE: Some of these interfaces will have overlapping semantics and need to be designed together.

- Intradomain between Gateway/Meter and EMS. These are the interfaces numbered 4&7 (may be physically in the same box as the Gateway), 16 and 25.

Some Interface Requirements :

a. The Gateway receives standardized inbound messages and sends standardized outbound messages.
b. All messages will be sent with sufficient and complete metadata.
c. All messages must support the addition of information without affecting the EMS
d. All messages must be signed and encrypted.
e. The source of all messages must be validated and trusted.

Some Inbound message types to Gateway

a. Pricing Message - with Realtime Pricing Values and Future Pricing Vector
b. Reliability Event Message – for curtailment event notification
c. Time Sync Message - for validation of time synchronization
d. Status Request Message - To validate system state including the readiness to respond to DR events
e. Current Meter Request Message
f. Historical Meter Request Message

Some Outbound message types from Gateway

a. Current Meter Data Message
b. Historical Meter Data Message
c. Status Message - with Gateway state data such as errors, warnings, ability to accept and respond to events and other relevant information

I2G use cases and actors

1.55Introduction

Industrial electric power consumers range the gamut from small concerns operating in industrial zoned locations with distribution level power voltages to large facilities on dedicated campuses receiving power at transmission level voltages. They may also have dedicated power sources for generation or combined heat and power.

Manufacturers will have specific concerns as power customers. Production processes are typically carefully planned/scheduled and highly optimized. In addition to revenue loss, shutting down power unexpectedly can endanger equipment, material in process, and even personnel. When shut down, equipment may need to be recalibrated and brought up to working temperatures before operation can resume. Even the ambient temperature around production equipment can affect its performance and resulting product quality. For these reasons, industrial consumers will be very concerned with the availability of power and its quality during production. They will not cede direct control of loads or local energy resources for production to a utility or third party. However, power use is a considerable cost of production and industrial consumers may treat it as another input resource cost to be managed. They may be able to schedule shutdowns, reschedule production, or activate local power resources in response to power event or price signals. The types and rate of response will vary with the customer, but generally predictive pricing (such as day ahead) or demand signals will be needed for demand response from this customer class. Industrial facilities may also be willing to partner with a utility company to automate a demand reduction or shift, but only on the basis of a pre-arranged agreement with clearly stated terms. Despite these challenges, the industrial consumer provides perhaps the greatest opportunity to exploit the Smart Grid due to its large energy use, technical sophistication using automation and resource management systems, and significant onsite generation resources.

1.56Demand Response use cases

4.4.2.2 Customer Management System Manages Demand in Response to Pricing Signals

The utility DR solution shall provide the ability to manage pricing signal programs designed to reduce load. It accomplishes this by managing the transmission of price signal information to DR-aware customer systems or devices. This solution shall also provide interactions with customers to convey price signal information; communications is shown via the meter or the Gateway/ Facility ESI.

4.4.2.3 Customer Reduces their Usage in Response to Pricing or Voluntary Load Reduction Events

The grid can share responsibility for peak load management with customers by sharing economic incentives to reduce load. These incentives may be shared in advance by day-ahead pricing or in real time during a critical event. Energy customers will develop a variety of strategies to respond once

economic incentives are in place. Industrial customers will require interfaces that support negotiation of possible load reductions occurring hours or days after the first incentive signal from the grid.

To enable customers to meet this need, the smart grid must provide them with timely price, event, and usage information. For competitive markets in software and equipment to assist customers, there must be national system market based upon information standards.

From a power customer point of view, 4.4.2.2 is a sub-case of this use case (4.4.2.3). The difference seems to be that, in 4.4.2.2, a particular utility/grid system is driving the production of signals to the customer (but the customer has no reason to be aware of this).

4.4.2.6 Utility procures energy and settles wholesale transactions

Operations for the Retail Market receives and prepares bids and offers into the wholesale energy market and evaluates the incoming bids from the wholesale market against the needs and the cost of operation. To facilitate this process, the Retail Market needs to know what resources, such as distributed generation, industrial central generation or demand response, are available and for how long. Some time after a wholesale transaction has been completed, the Retail Market settles the transaction using actual usage data gathered by the metering system during the period specified in the transaction. The data is used to prepare bills and invoices to multiple parties involved in the transaction based on contracts and tariffs.

4.4.2.7 Dynamic Pricing—Energy and Ancillary Services Aggregation

An Aggregator collects energy and ancillary services bids and offers from Dynamic Pricing and other DER subscribing customers. The Service Provider combines those bids into an aggregate bid into the market operations bid/offer system. When accepted, the Service Provider notifies the end customer of the status and requests scheduling of the services.

For the Industrial consumer DR use cases diagram we changed Demand Response Service Provider to Aggregator. However, it's not clear that this use case was ever DR service specific.

4.4.2.9 VVWC with DR, DER, PEV, and ES

The application calculates the optimal settings of voltage controller of LTCs, voltage regulators, DER, power electronic devices, capacitor statuses, and may enable Demand Response to amplify the effect of load-reducing volt/var control.

Not sure what is meant by "may enable Demand Response". Assume that this means "may use Demand Response" which would mean that the application would require information regarding industrial consumer Demand Response resources and be able to send signals to Gateway/Facility

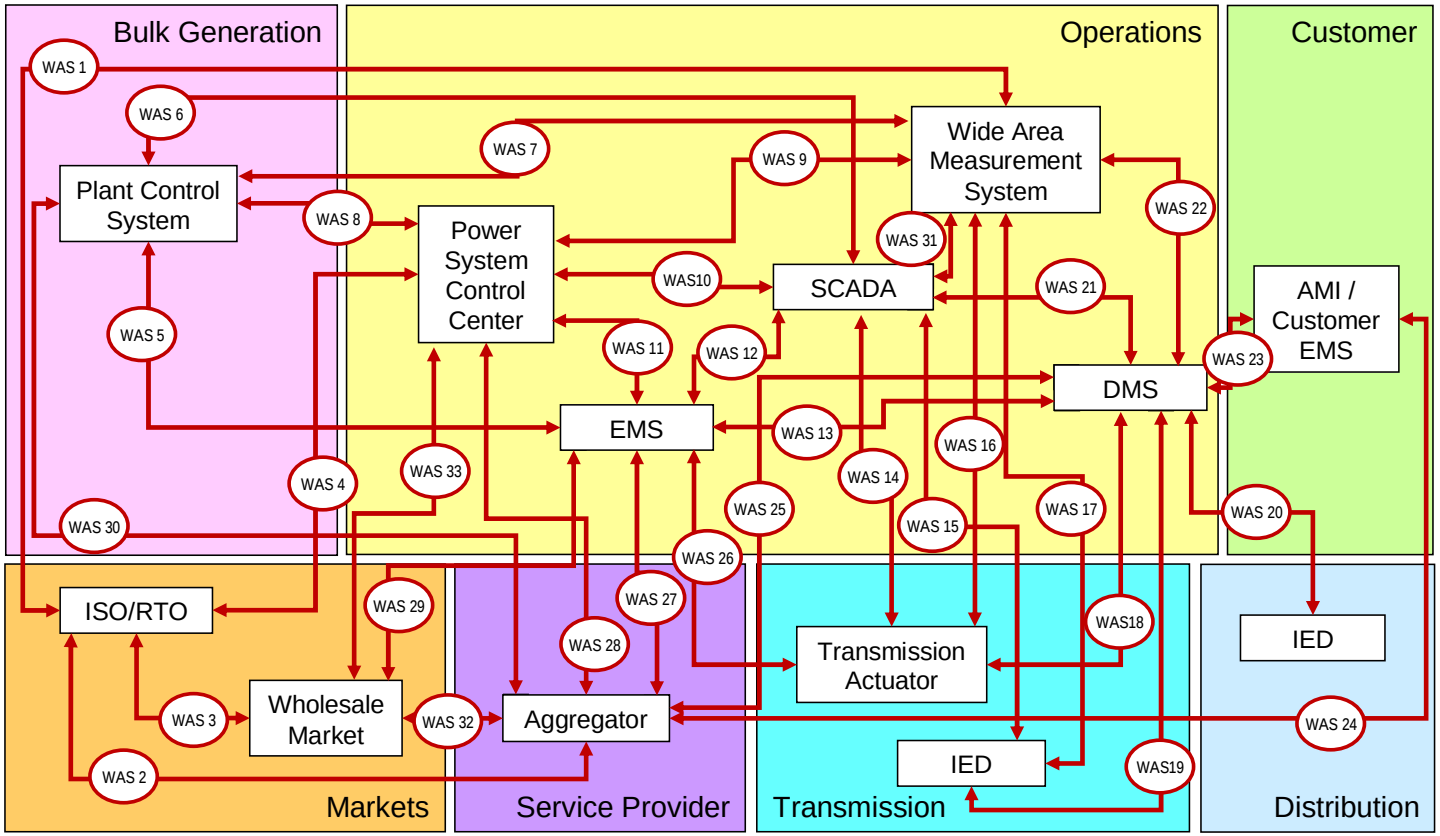
ESI to control their use (with the constraints that go along with this for industrial Demand Response resources). This should be made clearer or the use case should be removed from the DR section.
How is this use case different from 4.8.2.3 which has the same title in the Distribution Grid Management section of the interim roadmap document?

4.4.2.10 Consumer Curtails Power Consumption Due to Use of Substitute Energy Sources

A Customer with local generation resources, such as Industrial Central Generation, may monitor changing costs (direct costs and/or environmental costs) of electricity and fuels available to power local generators, and activate these alternative resources to curtail use of electricity from the grid when conditions are favorable. This would make use of dynamic/or time period specific price and associated pollution characteristics for the electric power provided from the grid and would require similar information for the fuels powering local sources. Grid operations/distribution may wish notification when large reductions in load such as this occur.

Actor	Domains	Description
Wholesale/Retail Market	Markets	A market in which electricity and other energy services are sold. For purposes of this diagram the key information is price, which is set by tariff, markets, and/or intermediaries.
Aggregator	Markets	An Aggregator combines the curtailment or demand or DER of two or more customers into a single purchasing unit to negotiate the purchase or sale of electricity in the retail market. Aggregators act in retail and wholesale markets.
Grid Operations	Operations	Grid operations manage services for the distribution of electricity (and gas and water) to and from customers and may serve customers who do not choose direct access.
Distribution Management	Operations	Controls distribution of energy. May alternatively be considered part of Grid Operations in the Operations domain.
Gateway/ Facility ESI	Customer	The Facility Energy Services Interface acts as the communication gateway between the ISO/RTO/utility and the industrial facility. Provides cyber security and, often, coordination functions that enable secure interactions between relevant industrial customer devices and systems and the Utility.
Dispatchable Central Generation	Customer	Dedicated central generation is dispatchable by the ISO/RTO/utility on short-notice. Real-time control interfaces permit both direct and indirect control of central station generation as well as control-center to control-center communications.

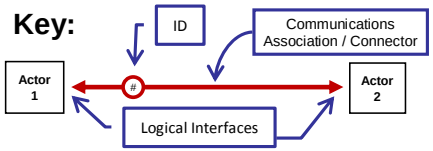
Meters or Smart Meters	Customer	Unless otherwise qualified, a device used in measuring watts, vars, var-hours, volt-amperes, or volt-ampere-hours. Called a Smart Meter when part of an advanced metering infrastructure (AMI). Today typically located at the customer facility and owned by the distributor or retail provider, but may be owned by the customer.
Distributed Generation	Customer	A “virtual” generation station located on industrial facility powered by wind, solar, bio-diesel or process by-products. It may: 1) be integrated into industrial automation systems and controlled by industrial plant operations or 2) integrated directly into grid operations.
Industrial Central Generation	Customer	A generation station often co-located with industrial facilities. The primary function of these stations is to provide power to the industrial facility, but they can also export excess power to the grid under favorable economic conditions or in an emergency. These are generally considered base-load resources but may be dispatchable with sufficient notice and planning.
DR Resource	Customer	Real or aggregate Demand Response resource controlled by the customer in response to pricing or other curtailment signals from the utility. Industrial DR is enabled subject to production needs and according to terms negotiated between customer and utility.
Industrial EMS	Customer	A function performed by customer systems and personnel that plans and manages energy use and industrial energy resources in response to production plans, pricing signals from the utility and other energy suppliers, curtailment signals, and other conditions. This actor is separated from the Gateway to isolate utility interfacing concerns from those in the industrial domain where different domain specific system classes, models, and protocols are in use. This is an abstraction. These functions may well be performed by a single system in an implementation.



Wide-Area Situational Awareness (WASA) Use Cases: Actors and Logical Interfaces

IED: Intelligent Electronic Device
DMS: Distribution Management System
EMS: Energy Management System
SCADA: Supervisory Control and Data Acquisition
AMI: Advanced Metering Infrastructure

Key:



Interface #	*Information Object Name*	*Information Object Description*
WAS 1	Request for aggregated load management (congestion management) in a particular wide area, price signals.	Between ISO/RTO and Transco, may be in a day ahead timeframe, in a hours in advances, or in a near real time via RTP signal
WAS 2	Energy and Ancillary Service Prices	Between Energy Market Clearing House and Aggregator
WAS 2	Energy and Ancillary Service Bids approved by DISCO	Between the Aggregator and the Energy Market Clearing House
WAS 3	Real Time Prices, Transmission Operating parameters, Requests from EMS applications for load management objective of VVWC function.; Results of SE and Network Sensitivity Analysis	From Utility EMS to DMS, real-time data exchange
WAS 3	Transmission bus load model updates	From DMS (DOMA) to Utility EMS, within a minute after each DOMA run
WAS 4	Energy, Ancillary Service Bids, Schedules	From the Aggregator to Disco
WAS 4	Authorization of submitted Schedules for Energy and Ancillary Services	From Disco to the Aggregator
WAS 5	Load model information associated with the distribution node	From Load Management Systems to CIS. Within minutes after the change of model information.
WAS 6	Energy and Ancillary Service bids, prices, schedules	Between ISO/RTO and Energy Market Clearing House
WAS 7	Work orders	From Distribution Operator to Field crews
WAS 7	Work-order related information, reports	From Field crews to the Distribution Operator
WAS 8	Updates on circuit connectivity and facility parameters	From Field Crews to GIS (DB administrator), within an minutes after the change in the field is completed.
WAS 8	Request for updates on a particular circuit connectivity and facility parameters	From GIS (DB administrator) to Field Crews or Work Management System, hours-days ahead notice.
WAS 9	Real-time measurements and statuses	From Field IEDs to Distribution SCADA. Information shall be delivered in 2-4 seconds. Each entry shall be time stamped. The information should be pre-processed for validity check, and then used for distribution state estimation.
WAS 9	Commands to IEDs	From Distribution SCADA to Field IEDs. Information shall be delivered in 2-4 seconds.
WAS 10	Weather forecast and other major event data	From external systems to Load management systems, within minutes after new relevant data is generated

Interface #	*Information Object Name*	*Information Object Description*
WAS 10	Request for particular Weather and other major event data	From Load management systems to external systems, within minutes after the need in additional data occurs.
WAS 11	Energy and Ancillary Service agreements, other relevant data	From the Aggregator and the Customer EMS, within minutes after the agreement is finalized
WAS 11	Energy and Ancillary Service bids, agreement requests, other relevant information	From the Customer EMS to the Aggregator, within minutes after the needs occurs
WAS 12	Energy and Ancillary Service agreements, other relevant data	From the Aggregator to the Customer Smart meter (or AMI system), within minutes after the agreement is finalized
WAS 12	Energy and Ancillary Service bids, agreement requests, other relevant information	From the Customer Smart meter (or AMI system) to the Aggregator, within minutes after the needs occurs
WAS 13	Setup of the DMS functions (objectives, additional or changed limits, other options)	From the Distribution Operator to the DMS functions, within seconds after the need occurs. This interface can be replaced by interfaces 14 and 22 in series.
WAS 13	Statuses and Summary results of the DMS application, alarms, messages	From the DMS functions to the Distribution Operator, to within 1-2 seconds after the results are generated by the DMS application. This interface can be replaced by interfaces 14 and 22 in series.
WAS 14	Real-time measurements and statuses from field IEDs	From Distribution SCADA to DMS, within 1-2 seconds after the SCADA database is updated with new data. Each entry should have a timestamp of retrieving form the IED.
WAS 14	Commands, selected calculation results, dynamic limits, etc.	From DMS to Distribution SCADA, within 1-2 seconds after the results are generated by DMS.
WAS 15	Load information associated with the distribution node	From CIS to GIS within minutes after load data updates.
WAS 15	Connectivity data needed for association of loads with the point of connection	From GIS to CIS within minutes after connectivity data updates
WAS 16	Real-time load information from critical points	From load Management system to DMS, within an hour after significant change, including the load management capabilities
WAS 16	List of operation-critical points	From DMS (DOMA) to Load Management Systems
WAS 16	Rapid voltage changes (Momentary outages, Sags, Swells, Flicker)	This information can be accumulated in the AMI and Customer EMS devices with corresponding time stamps, dependent on the devise storage capacity and then be transmitted to the Load Management Systems
WAS 17	Voltages at the customer terminals and other points with AMI devices	From Customer EMS devices to CIS, periodically together with kWh and kvar data.
WAS 17	Information relevant to individual customer generated by CIS	From CIS to Customer EMS devices, periodically and by event, based on billing cycles and other contractual agreements.

Interface #	*Information Object Name*	*Information Object Description*
WAS 18	Real-time load information from all points	From Customer EMS to Load Management Systems, near real-time. 5 minutes
WAS 19	Voltages at the customer terminals and other points with AMI devices	From AMI devices to CIS, periodically together with kWh and kvar data.
WAS 19	Voltages at the customer terminals and other points with AMI devices	From Customer EMS devices to Load Management Systems, periodically together with kWh and kvar data.
WAS 19	Higher harmonics data	This information can be accumulated in the Customer EMS devices for predefined time intervals, with corresponding time stamps, dependent on the devise storage capacity and then be transmitted to the Load Management Systems
WAS 18, 20, 16	Outage detection from all affected AMI and Customer EMS devices	From AMI and From Customer EMS to DMS, near real time, within 3 minutes after sustained loss of power. May be a large amount of data that should not block transmission of data.
WAS 20	Real-time load information from all points	From AMI to Load Management Systems, near real-time. 5 minutes
WAS 20	Voltages at the customer terminals and other points with AMI devices	From AMI devices to Load Management Systems, periodically together with kWh and kvar data.
WAS 20	Higher harmonics data	This information can be accumulated in the AMI devices for predefined time intervals, with corresponding time stamps, dependent on the devise storage capacity and then be transmitted to the Load Management Systems
WAS 21	Load information updates associated with the distribution node	From GIS to DMS in minutes after significant changes. The challenge is the correctness and consistency of load and connectivity data.
WAS 21	Connectivity and facility parameters data and load data associated with distribution nodes	From GIS to DMS, initial loading of data and incremental data updates as soon as significant changes occur. Each transmittal of data shall be checked on completeness and consistency of data. Large amount of data initially, smaller amounts for incremental changes. Data shall arrive in the DMS database within an hour after the changes was implemented in the field.
WAS 22	SCADA data (measurements, statuses, alarms, tags, etc.)	From Distribution SCADA to the Distribution Operator, within 1-2 sec after received from the field IEDs
WAS 22	Supervisory Control, Data Request, Demand of execution of a DMS function	From the Distribution Operator to Distribution SCADA, within 1-2 sec after entering the commands