PNNL-26413

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

Connected Equipment Maturity Model

Version 1.0

May 2017

JB Butzbaugh
ET Mayhorn
GP Sullivan
SA Whalen

U.S. DEPARTMENT OF
ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, **makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

**Available to DOE and DOE contractors from
the Office of Scientific and Technical
Information,
P.O. Box 62, Oak Ridge, TN 37831-0062**
www.osti.gov
**ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov**

**Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov**

PNNL-26413

Connected Equipment Maturity Model

Version 1.0

JB Butzbaugh
ET Mayhorn
GP Sullivan[1]
SA Whalen

May 2017

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

[1] Principal, Efficiency Solutions, LLC, Richland, Washington.

Summary

The U.S. Department of Energy's (DOE) Office of Energy Efficiency and Renewable Energy (EERE) envisions a future in which the intelligent functionality and features of connected equipment unlock new energy-related services for consumers, building owners, and electricity providers. In particular, DOE is focused on engaging in activities that advance four categories of energy-related services—end-user, grid, energy market, and societal services.

The Connected Equipment Maturity Model (CEMM) evaluates the high-level functionality and characteristics that enable equipment to provide the four categories of energy-related services through communication with other entities (e.g., equipment, third parties, utilities, and users). The CEMM will help DOE, industry, energy efficiency organizations and research institutions benchmark the current state of connected equipment and identify capabilities that may be attained to reach a more advanced, future state.

The CEMM is defined by five high-level domains that capture critical functionality in the evaluation of connected equipment maturity: (1) End-User Services, (2) End-User Experience, (3) Grid, Energy Market and Societal Services, (4) Communication and Networking, and (5) Cybersecurity. Collectively, these domains express capabilities that enable the four categories of energy-related services.

The CEMM's five domains consist of 17 categories. These categories represent logical groupings of the core functions, features, and characteristics within their parent domain. Each category contains a set of maturity questions, which provide a means for evaluating the current state of key characteristics and capabilities of connected equipment. As maturity questions increase from maturity indicator level (MIL) 1 to MIL 3, they encourage more innovative functionality and scalable solutions for connected equipment. By applying the CEMM, organizations can use the results to devise strategies to advance the maturity of connected equipment functionality.

Acknowledgments

The authors acknowledge the dedication and technical expertise of all the organizations and individuals who participated in the development of the Connected Equipment Maturity Model (CEMM), especially the Technical Working Group:

- Chris Granda (Appliance Standards Awareness Project)
- Curt Kirkeby (Avista Utilities)
- Daniel Johnson (California Energy Commission)
- Ken Rider (California Energy Commission)
- Richard Lord (Carrier Corporation)
- John Taylor (Consortium for Energy Efficiency)
- Brian Seal (Electric Power Research Institute)
- Michael Beyerle (GE Appliances)
- Shane Dewing (Intel Corporation)
- Jedidiah Bentz (Johnson Controls)
- Jon Douglas (Lennox Corporation)
- Chris Tracy (Lennox Corporation)
- Keith Dennis (National Rural Electric Cooperative Association)
- Pierre Delforge (Natural Resources Defense Council)
- Noah Horowitz (Natural Resources Defense Council)
- Robin Roy (Natural Resources Defense Council)
- Mary Anderson (Pacific Gas and Electric)
- Albert Chiu (Pacific Gas and Electric)
- Pat Eilert (Pacific Gas and Electric)
- Ed Elliott (Pacific Gas and Electric)
- Don Brundage (Southern Company)
- Justin Hill (Southern Company)
- Alison Gotkin (United Technologies Research Center)
- Hayden Reeve (United Technologies Research Center)

The authors are very appreciative of the guidance and support from Joe Hagerman, Senior Policy Advisor, Building Technologies Office, Office of Energy Efficiency and Renewable Energy, U.S. Department of Energy. The authors would also like to recognize the management support of Andrew Nicholls and Dennis Stiles of Pacific Northwest National Laboratory.

Terms and Definitions

Adequately Performed: Actions or functions completed to fulfill basic or expected requirements.

Ad Hoc Testing: An informal or improvised approach to assessing the viability or performance of a component, device or system.

Administrative User: A person with access and capability to perform technical functions to or on a software network.

Aftermarket: A non-factory/original equipment manufacturer (OEM) part, accessory, or upgrade available for an existing component, device, or system.

Auto-Configure: An approach whereby a server or other system assigns unique addresses in a dynamic real time setting.

Auto-Discovery: A function performed by a set of tools designed to collect data and record any changes made to a networked software system.

Automated: The ability to react to a single variable, or limited set of variables, without self-governance.

Automated Scheduling: Algorithms designed to assign single or multiple actions based on inputs, actions, or predetermined constraints.

Autonomous: The ability to react to an indefinite number of variables, learn from past events, self-govern and proactively pursue objectives.

Appropriate Credentials: Identification or system recognition that is used for verification of identity for authentication.

Backward Compatible: The ability to successfully interface and function with prior versions of a hardware or software system.

Behind-the-Meter: Terminology identifying equipment, appliances, and services which occur or are located on the customer side of the junction box where utilities and services make the local connection to the building or facility.

Cascade: A series of steps which occur in sequence.

CEMM Answer Scale: Four-tiered scale (incomplete, partial, most, complete) used to identify the degree to which of the functions or characteristics are implemented in the product development process.

CEMM Categories: Connected Equipment Maturity Model organizational structure used to characterize logical groupings of related equipment capabilities.

CEMM Domains: Connected Equipment Maturity Model organizational structure used to characterize high-level logical groupings of categories.

Connected Equipment: Equipment, appliances, and electronics capable of communicating with other devices, communication networks, or management systems for the purpose of making decisions and responding accordingly with physical action or informational content. These actions or content may enable activities including, but not limited to: energy management, emergency operation, maintenance needs, projection of future states, measurement and verification (M&V), or forms of transactive controls.

Customize Operations: Modifications of standard conditions to meet individual user or other non-standard requirements.

End-user Consent: Permission provided by the user of a system to afford access for interventions such as monitoring, data collection, or condition assessment.

End-user Services: Energy and energy-related products, services, and rights that end users purchase to balance and co-optimize their overall energy costs, comfort, and convenience.

Energy Market Services: Energy and energy-related products, services, and rights that the electric power grid offers to reflect the costs of production and delivery of power and energy to customers in everyday operations.

Expansion Module: Device or component that enables extra facilities to be added or upgraded at a future date.

External Control Signal: Information or a direct command received from outside the actionable device.

External Entity: Any non-local group which may access the network or service in which the connected equipment operates.

Faults: A non-standard condition or defect in a component, device, or system which may lead to unintended operation and/or failure.

Feedback: Data resulting from local measurements which is used in the control of the connected system.

Grid-connected Equipment: A subset of Connected Equipment which includes equipment and appliances capable of communicating with other connected equipment, communication networks, or management systems for the purpose of with physical action to operate more effectively or efficiently from a utility (macro) perspective. These actions or content may enable activities including, but not limited to: utility load shedding, utility load balancing, grid maintenance needs, emergency grid operation, or forms of transactive controls.

Grid Services: Energy and energy-related products, services, and rights that the electric power grid purchases or incentivizes because they are required for its reliable operation.

Harmful Operating Conditions: Operations of a component, device, or system in a manner that potentially impairs the hardware, software, or user beyond expected operational characteristics.

Historical Performance Data: Chronological functional information collected and stored either resident to the system or at an external location.

Information Model: The vocabularies, concepts, definitions and relationships provided in an organized framework to be delivered and used in a variety of innovative ways.

Internet of Things: The set of internet protocol (IP) addressable devices that interact with the physical environment.

Interoperability: The ability of different information technology systems and applications to communicate, exchange data, and perform functions while making use of the use the exchanged information.

Intended/Normal Operation: Actions or functions that were included as part of the original design intent.

Machine Learning: Ability of the connected equipment to use data to improve the operating algorithms which serve to control operation of the equipment.

Maintenance: The process of upkeep for the purposes of preservation of a component, device, or system.

Maturity: State of advancement or development.

Maturity Indicator Level (MIL): Levels that gauge the lowest to highest levels of advancement (i.e., measurable scale) for a particular discipline.

Misuse by External Parties: The unauthorized operation of a component, device, or system in a manner not consistent with owner’s intent, or activity that potentially impairs the hardware and/or software beyond expected operational characteristics.

Open Platform Communications Unified Architecture: An industrial machine-to-machine communication protocol for interoperability developed by the OPC Foundation

Open Standard: Standards developed and maintained by nationally recognized standards body or stakeholder alliance through a collaborative or consensus process and available to the general public.

Operating Conditions: The ambient setting typically specified by the manufacturer and required for the proper function of a component, device, or system.

Opt-in: Permission granted to a third party to allow for future communication or correspondence.

Optimization: The ability to combine preferences into the most advantageous combination to achieve a benefit.

Performance Degradation: A progression of reduced functionality of a component or system.

Plug-and-Play: A feature of a system that allows for detection, configuration, and full function once it is connected.

Preference: The optional ability to select an operating condition with respect to an established range of operation.

Pre-Programmed: Commands or other functionality which are resident to a component or system prior to its installation.

Proprietary Standard: Standards developed and controlled by one company or vendor.

Quality-of-Service: A defined measure of performance centered on the concept that certain metrics (e.g., transmission rates, error rates, or other network characteristics) can be measured, improved, and potentially guaranteed in advance.

Real Time: Actions or activities which update at the same rate as the information is received.

Remote Access: The ability to access the control system of a connected component, device, or system from a different physical location.

Remote Interface: User portal (e.g., a mobile device) enabling control of preferences and operating conditions of connected equipment.

Remote Means: To send a communication digitally through email, text, application, or similar means, from a component, device, or system to a user.

Remote Notification: A digital communication sent/received through email, text, application, or similar means, from a component, device, or system to a user.

Safe Mode: Operating mode in which functions, actions, and operations are active, but limited, so the system can be assessed for functional issues.

Sensed Operating Environment: Conditions used to establish, describe, or define the ambient setting relevant to a given component, device, or system.

Service Code: Unique identifying code used to specify a specific maintenance activity.

Service Provider: A qualified and licensed organization which provides maintenance, or repair operations for a component, device or system.

Societal Services: Energy and energy-related products, services, and rights that have a value agreed upon and acknowledged by society, monetized by a governing entity, with benefits provided to all involved or affected parties.

Updatable: To bring a component, device or system to current state by adding new information or making corrections.

Upgradable: To bring a component, device or system to a new state by the replacement of an existing arrangement or structure.

Acronyms and Abbreviations

AHAM	Association of Home Appliance Manufacturers
AHRI	Air-Conditioning, Heating and Refrigeration Institute
ASCII	American National Standard Code for Information Interchange
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
BCF	Buildings Cybersecurity Framework
BTO	U.S. Department of Energy, Building Technologies Office
C2M2	Cybersecurity Capability Maturity Model
CEE	Consortium for Energy Efficiency
CEMM	Connected Equipment Maturity Model
CIM	Common Information Model
DOE	U.S. Department of Energy
EBCDIC	Extended Binary Coded Decimal Interchange Code
EERE	U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy
GWAC	GridWise Architecture Council
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
NERC	North American Electric Reliability Corporation
OCF	Open Connectivity Foundation
OPC UA	Open Platform Communications Unified Architecture
OSI	Open Systems Interconnection
PNNL	Pacific Northwest National Laboratory
R&D	Research & Development
RDF	Resource Description Framework
RFI	Request for Information
SOAP	Simple Object Access Protocol
SG IMM	Smart Grid Interoperability Maturity Model
SGMM	Smart Grid Maturity Model
UDDI	Universal Description, Discovery and Integration
USNAP	Universal Smart Network Access Port Alliance
XML	Extensible Markup Language
XSD	XML Schema Definition

Contents

Figures

Tables

1.0 Introduction

The Connected Equipment Maturity Model (CEMM) evaluates the high-level functionality and characteristics that enable equipment to provide energy-related services through communication with other entities (e.g., equipment, third parties, utilities, and users). The CEMM was designed to help DOE, industry, energy efficiency organizations and research institutions benchmark the current state of connected equipment and identify capabilities that may be attained to reach a more advanced, future state.

1.1 Intended Audience

The intended audience is any organization interested in benchmarking or tracking the evolution of connected equipment capabilities over time. This includes DOE, manufacturers, industry associations, utilities, regional energy efficiency program sponsors, energy efficiency advocates, state energy agencies, public utility commissions, universities, and research institutions.

1.2 Structure of Document

There are eight sections and an appendix in the model.

1. **Introduction**
   States the purpose and objectives of the model.
2. **Background and Importance**
   Provides background on DOE's interest in the progression of connected equipment as well as the development approach for the model.
3. **About Connected Equipment**
   Defines connected equipment, as established in previous efforts.
4. **Maturity Model Concept**
   Describes the maturity model concept, including its typical design and use.
5. **DOE Maturity Models**
   Provides background on DOE maturity models.
6. **Model Architecture**
   Depicts the framework of the CEMM, including its layers.
7. **Use of Model**
   Characterizes recommendations for how to implement the CEMM, including how to answer maturity questions and summarize assessment results.
8. **Domains, Categories and Maturity Questions**
   Describes each of the domains and categories defined for the CEMM, including a list of maturity questions ordered by maturity indicator level.
9. **Appendix: GridWise Architecture Council Interoperability Layers**
   Describes the interoperability layers of the GridWise Architecture Council stack.

2.0 Background and Importance

The DOE's Office of Energy Efficiency and Renewable Energy (EERE) envisions a future in which the intelligent functionality and features of connected equipment unlock new energy-related services for consumers, building owners, and electricity providers.[1] In particular, DOE is focused on engaging in activities that advance four categories of energy-related services—end-user, grid, energy market, and societal services.[2]

Residential and commercial equipment markets are evolving as more product lines are introduced with connected features. However, these connected features often disregard or understate functionality that can provide energy-related benefits. Consequently, a tool is needed to articulate, encourage, and evaluate the maturity of connected equipment functionality and features in support of DOE's vision.

Based on discussions at a 2015 technical meeting,[3] the Building Technologies Office (BTO) and industry stakeholders concluded that a method should be developed for benchmarking and tracking the evolution of connected equipment functionality and features in the marketplace. Of particular interest to industry is the ability to track progress internally and/or compare equipment maturity and associated manufacturer competencies with peers. The CEMM offers a tool for revealing trends, identifying technology gaps, informing roadmap development, and prioritizing investments for connected equipment. DOE can use the model to gain a national level assessment to track the progress of connected equipment technology and services, as well as offer insights for strategic planning.

On behalf of DOE, the Pacific Northwest National Laboratory (PNNL) developed the initial framework and content for version 1.0 of the CEMM in consultation with the Technical Working Group. This group was formed voluntarily and included representation from manufacturers, industry associations, utilities, state energy agencies, energy efficiency advocates, and research institutions. The Technical Working Group provided feedback on the CEMM structure and maturity questions for the capture of connected equipment functions deemed most important for tracking over time.

[1] DOE EERE. March 2014. Buildings-to-Grid Technical Opportunities: Introduction and Vision. Accessed August 10, 2016: http://energy.gov/sites/prod/files/2014/03/f14/B2G_Tech_Opps--Intro_and_Vision.pdf

[2] Somasundaram S, et. al. December 2014. Transaction-Based Building Controls Framework, Volume 1: Reference Guide. PNNL -23302, Pacific Northwest National Laboratory, Richlan Accessed September 14, 2016: http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23302.pdf (Last updated September 2016)

[3] DOE. 2015. "Technical Meeting: Physical Characterization of Connected Buildings Equipment." Accessed August 10, 2016: http://energy.gov/eere/buildings/downloads/technical-meeting-physical-characterization-connected-buildings-equipment

3.0 About Connected Equipment

DOE has convened public meetings[1,2] with representatives from industry, academia, advocacy groups, and government organizations to discuss issues related to grid-connected equipment. These discussions focused on the physical characterization of commercial and residential end-use appliances and equipment, metrics for measurement, identification of grid services, and benefits of grid connectivity. These meetings, as well as subsequent public comments in the Federal Register, resulted in the development of *A Framework for Characterizing Connected Buildings Equipment*, which included definitions of key terms.[3] DOE is basing its definitions of connected equipment in the CEMM on how this framework defines them.

Equipment: *Building nodes and systems that consume, store, or generate electricity while providing services and amenities within buildings or on a building site. Examples of equipment include: water heaters, refrigerators, computers, lighting, HVAC, heat pumps, room air conditioners, electric vehicle chargers, PV inverters, or energy storage to name a few.*

Connected: *The capability of equipment to receive and transmit digital signals (e.g., to/from equipment, buildings, utilities, end users, and/or third-party providers), make decisions, and respond accordingly with physical action or informational content. Connected equipment also includes features that enable, for example, the projection of future states, measurement and verification (M&V), or maintenance needs. This definition of connected goes beyond merely the ability to communicate and includes the notion of intelligent functionality whether co-located within the equipment or uncoupled from the equipment. It also reflects the standardization of sending and receiving signals to enable interoperability.*

[1] 79 Fed. Reg. 19322 (April 8, 2014).

[2] 79 Fed. Reg. 32542 (June 5, 2014).

[3] DOE. 2015. A Framework for Characterizing Connected Buildings Equipment. Accessed September 14, 2016: https://www.regulations.gov/document?D=EERE-2014-BT-NOA-0016-0047

4.0 Maturity Model Concept

A maturity model is a structured tool for evaluating and benchmarking the progression of characteristics, attributes, practices, or processes for a particular discipline over time. Maturity models also identify attributes required to achieve more advanced future states for the subject under evaluation.

An organization or industry can use a maturity model to have its practices, processes, and methods evaluated against a set of attributes that establish a benchmark.[1] Typically, these attributes are based on the best practices in the discipline, and are drawn from standards, codes, or consensus agreements that are considered important to the discipline undergoing evaluation. Once an organization has established its benchmark, it can determine strategic pathways for performance improvement, such as targeted investment.

As organizations benchmark their capabilities using a maturity model, they can compare strengths and weaknesses of individual organizations as well as across the industry. This can reveal opportunities to catalyze advancement of a discipline by optimizing efficiencies within the industry, such as developing partnerships and other collaborative efforts, to take advantage of organizational competencies.

Maturity models are structurally designed using maturity indicator levels that gauge the lowest to highest levels of advancement in a particular discipline. The various attributes within a maturity indicator level provide a measurable scale for an organization to determine its current status as well as the capabilities needed to reach a more advanced state.

The CEMM is a progression model, providing the scale and advancement pathway for connected equipment attributes. The objective of the CEMM is to provide a vision for connected equipment progression or improvement, which is represented by the development of new and improved versions of attributes over time.

[1] Caralli, R., Knight M., and Montgomery, A. November 2012. Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability. Carnegie Mellon University and Software Engineering Institute.

5.0 DOE Maturity Models

DOE has developed maturity models in similar technical areas to the CEMM, including Cybersecurity[1], Smart Grid[2], and Interoperability[3]. These models differ from the CEMM as they focus predominantly on developing specifications and evaluating organizational practices, processes, strategy, and plans.

- The Cybersecurity Capability Maturity Model (C2M2) is designed to evaluate and improve cybersecurity strategies and practices implemented by organizations in all sectors (e.g., buildings, electricity).
- The Smart Grid Maturity Model (SGMM) assesses electric utility plans and initiatives for grid modernization by identifying opportunities for strategy and program improvement.
- The Smart Grid Interoperability Maturity Model (SG IMM) evaluates critical aspects of interface agreements between interacting parties engaging in smart grid initiatives at the organizational, informational, and technical levels. It is intended for use by stakeholder alliances or standards bodies to facilitate establishment of specifications with consideration for important aspects of interoperability.

In addition to its usefulness as an evaluation tool, the CEMM is designed to encourage the development of functionality and features that enable integrated smart grid solutions for end-use equipment. The CEMM overlaps with the SG IMM as both consider and encourage the use of interoperability standards and specifications. However, the CEMM is solely focused on whether the functionality facilitating interoperability resides in the connected equipment under evaluation. The SG IMM assesses interoperability from a broader, holistic approach. It articulates the methods, processes and tools that measure, facilitate and improve interoperable integration at a granular scale. It also proposes best practices for how organizations can partner to develop interoperable solutions. While the results of a CEMM evaluation can reveal opportunities or gaps for improving interoperability, the SG IMM identifies the processes an organization can implement to improve upon or resolve these interoperability gaps.

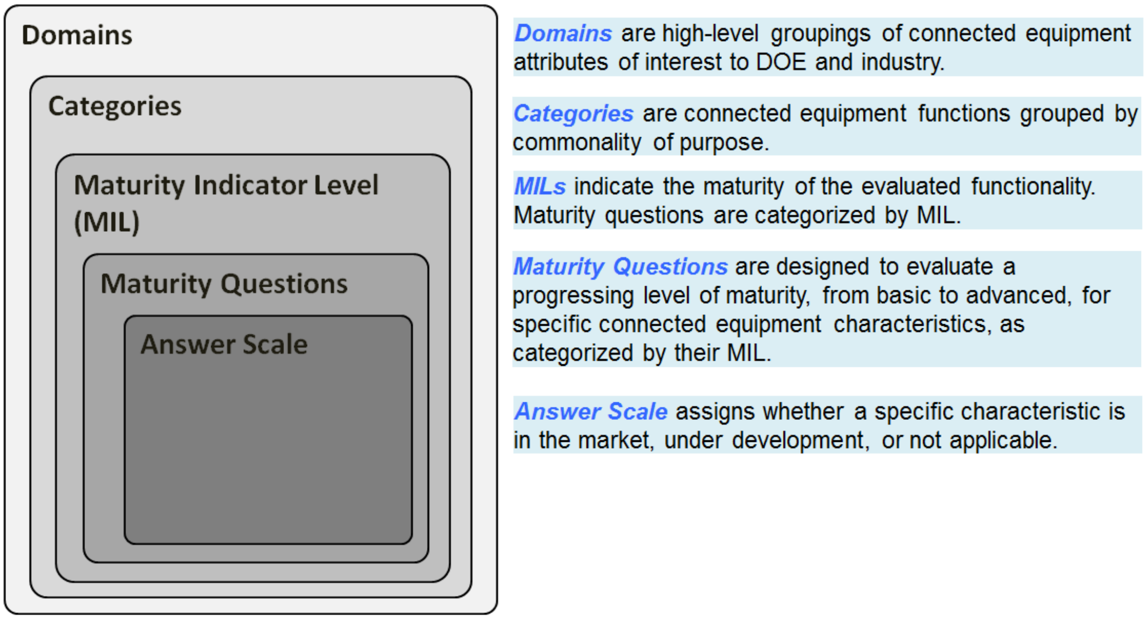
[1] DOE. Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) web page. Accessed December 20, 2015: http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity

[2] Solving Energy Institute. Smart Grid Maturity Model (SGMM) web page. Accessed December 20, 2015: http://www.sei.cmu.edu/smartgrid/

[3] The GridWise Architecture Council. Smart Grid Interoperability Maturity Model Beta Version. Accessed December 20, 2015: http://www.gridwiseac.org/pdfs/imm/sg_imm_beta_final_12_01_2011.pdf

6.0 Model Architecture

The CEMM framework consists of a three-layer hierarchy, as illustrated in Figure 1. The bottom-most layer is a set of “maturity questions” that address the functions defining connected equipment at each maturity level. Maturity questions provide a means for evaluating the current state of key characteristics and capabilities of connected equipment. The questions are grouped into “categories,” which form the second layer of the model. Categories organize maturity questions into logical groupings of related functionality. The top layer of the model is a set of “domains,” each composed from a set of related categories and chosen based on their high-level interest to DOE, industry, research institutions, and efficiency organizations.



Domains are high-level groupings of connected equipment attributes of interest to DOE and industry.

Categories are connected equipment functions grouped by commonality of purpose.

MILs indicate the maturity of the evaluated functionality. Maturity questions are categorized by MIL.

Maturity Questions are designed to evaluate a progressing level of maturity, from basic to advanced, for specific connected equipment characteristics, as categorized by their MIL.

Answer Scale assigns whether a specific characteristic is in the market, under development, or not applicable.

Figure 1. CEMM Architecture

As shown in Table 1, the CEMM has four maturity indicator levels (MILs), ranging from least advanced (0) to most advanced (3). Each category’s set of maturity questions is organized by MIL. Maturity questions designated as MIL 3 target industry leading, forward-looking functionality on the cutting edge of current technological innovation. MIL 2 maturity questions target intermediate functionality with moderate sophistication. MIL 1 maturity questions target essential functionality. MIL 0 indicates that MIL 1 was not achieved for the connected equipment functionality under evaluation.

Table 1. CEMM Maturity Indicator Levels

MIL	State	Description
3	Advanced	Industry leading, forward looking, cutting edge
2	Intermediate	Achievable today, moderate sophistication
1	Basic	Essential functionality
0	None	MIL1 is not achieved

Maturity questions are answered according to a four-tier answer scale, depicted in Table 2, depending on the degree to which functions or characteristics are implemented in the product development process. The answer scale was designed to reveal opportunities to organizations interested in accelerating the development and market adoption of connected equipment functionality.

A maturity question is answered “Incomplete” when the functionality is either not in demonstration or not applicable. Typically, functionality at this stage is still in the applied research and development (R&D) phase of technological innovation. The “Partial” answer is given when the functionality is currently in demonstration. Functionality at this stage is in need of validation to justify production and/or procurement. The “Most” answer is given when a function is demonstrated in a prototype and going to the market in 12 months. Functionality at this stage is in the process of market deployment and may need go-to-market assistance. The “Complete” answer is given when a function is fully implemented in a product in the market. Functionality at this stage is in the process of gaining market share and may need market adoption support to cross the chasm from the early adopter market to the early majority market.

The Technical Working Group provided critical feedback on answer scale layout and composition. Both the “Partial” and “Most” answers were endorsed by the Technical Working Group as gateways in the product development and deployment process. The Technical Working Group suggested that functionality in demonstration and functionality prepared to go to market are two distinct milestones that deserve explicit answers in the model.

Table 2. CEMM Answer Scale

Answers/Responses	Description
Incomplete	Function is not in demonstration or is not applicable
Partial	Function is in demonstration
Most	Function is demonstrated in a prototype and going to market in 12 months
Complete	Function is fully implemented in a product in the market

After answering the maturity questions, results can be aggregated across categories, domains, and MILs to gain unique perspectives of connected equipment maturity. Figure 2 illustrates a simple aggregation of a single category’s answers across the three MILs of maturity questions. In this example, all nine of the category’s MIL 1 maturity questions, and thus functionalities, are considered Complete. The seven MIL 2 maturity questions and associated functionalities are in progress, as depicted with a mix of Complete, Most, Partial, and Incomplete answers. MIL 3 functionalities are also in progress, but without a Complete answer to any of the category’s four MIL 3 maturity questions. While CEMM answers can be aggregated in any number of ways, the Technical Working Group appreciated the visual representation of answer aggregation at the category level according to MIL and suggested the inclusion of Figure 2 in the Model Architecture section (section 6.0).

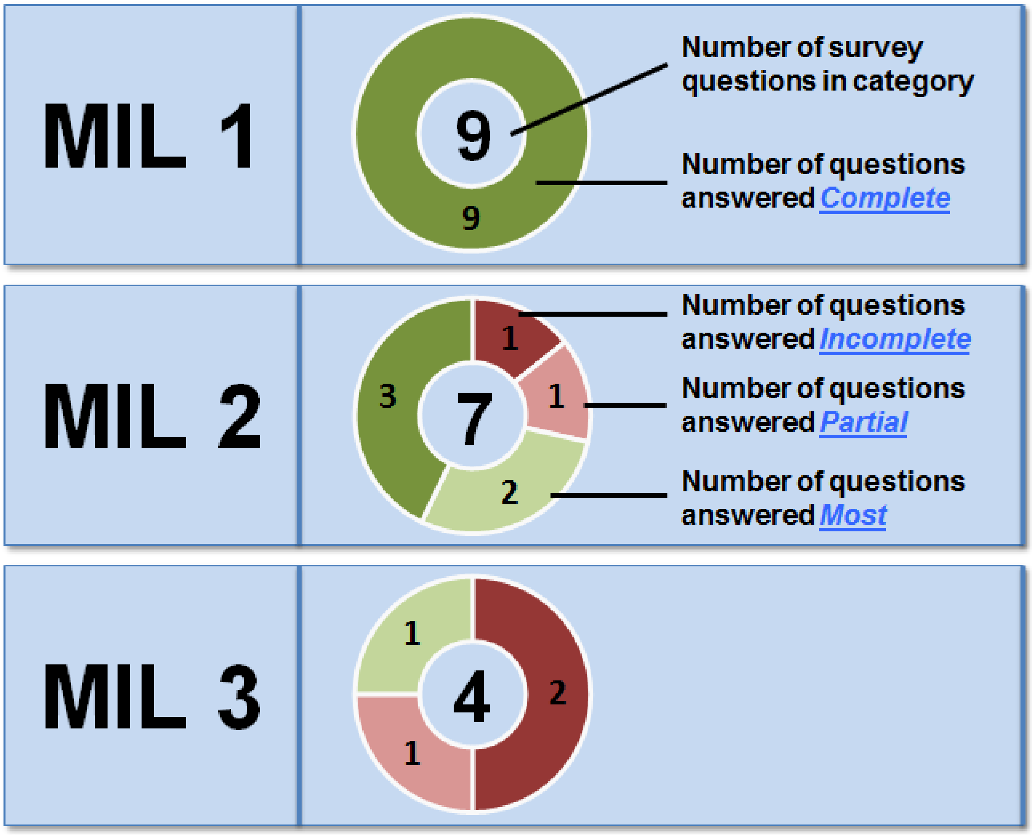


Figure 2. Example of CEMM Answer Aggregation

7.0 Use of Model

The CEMM is intended for use by organizations interested in understanding the state of connected equipment maturity in providing energy-related services. By applying the model to a specific type or line of connected equipment, organizations can use the results to devise strategies to advance the maturity of connected equipment functionality.

It is recommended that organizations assemble a team to conduct a CEMM evaluation. Ideally, this team includes personnel with a range of specialties, such as information technology, engineering, operations, marketing, and management. As a unit, the team should have strong familiarity with the organization’s role in the development of connected equipment. If the team can identify or assign a facilitator, this can improve the evaluation process, but is not required.

After a team completes a CEMM evaluation, an organization can use the results to identify gaps in functionality and determine the extent to which these gaps are meaningful to address. Specifically, an organization can prioritize resolving performance gaps that best enable it to meet its objectives. Once gaps are prioritized, an organization can begin devising strategies and associated tactics to improve functionality. This may include applying the CEMM to connected equipment of other industries to gain a better understanding of the competencies of potential partners.

An organization may repeat the CEMM process periodically to assess whether its strategies and tactics are effective at achieving progress. In particular, when major changes in the organization, market, or technology occur, reevaluation may be necessary to realign strategies and tactics to achieve the intended results.

7.1 DOE

DOE may conduct CEMM evaluations in collaboration with manufacturers and industry associations. Manufacturers may have the opportunity to provide information or input for DOE-developed evaluations. Any information or data provided by manufacturers would not be made publicly available. The results of manufacturer-specific and industry-wide CEMM evaluations may be used to inform DOE decision making for its R&D, commercialization, technology demonstration, and market transformation efforts. This may include the development of industry progress reports, technology road maps, grants, and programs to advance connected equipment maturity. Over the long term, the CEMM has the potential to enable a variety of partnership opportunities between DOE and industry.

7.2 Manufacturers and Industry Associations

Manufacturers may conduct CEMM evaluations of their own product lines as well as the product lines of other manufacturers in the market. They can use the results of these evaluations to compare their products across the industry, which can guide strategic planning such as decisions for R&D, commercialization, product marketing, partnerships/alliances, and mergers and acquisitions. CEMM evaluations of an entire industry can identify market segments that are either undeveloped or underdeveloped as prospects for potential growth. Industry associations, such as the Air-Conditioning, Heating and Refrigeration Institute (AHRI) or Association of Home Appliance Manufacturers (AHAM), may conduct CEMM evaluations of their manufacturer members or collect member evaluations in the development of an industry-wide evaluation. These associations can use CEMM results to pinpoint opportunities for collaboration among manufacturers and bring together appropriate candidates for partnership initiatives.

7.3 Utilities, Regional Energy Efficiency Programs, and National Energy Efficiency Consortiums

Utilities, regional energy efficiency programs, and national energy efficiency consortiums may use the CEMM to design technology development and/or market transformation initiatives. These organizations may conduct CEMM evaluations by investigating products available in the market, showcased at tradeshows and offered exclusively by their manufacturer partners. They can use the results of industry-wide CEMM evaluations to identify appropriate technologies to fulfill programmatic goals. This can lead to coordinating R&D incentives, including the "Golden Carrot" approach,[1] with manufacturers to spur the development of technological specifications in certain appliances and equipment. Utilities, regional energy efficiency program sponsors, and national energy efficiency consortiums can also use CEMM results to identify technologies in need of demonstration and deployment initiatives for proof-of-concept. Furthermore, they can use results to gain insight for designing market transformation programs, such as the development of demand-side management initiatives, rebates, low-interest loans, and consumer education campaigns.

7.4 Energy Efficiency Advocates

Energy efficiency advocates may conduct CEMM evaluations by collaborating with manufacturers, along with researching products in the market and displayed at tradeshows. The results of these evaluations can guide organizational goals and initiatives. This can include providing grants for R&D and technology demonstration. Results can also add insight for developing market transformation initiatives, such as consumer outreach or voluntary standards. Furthermore, these CEMM-influenced activities can lead to co-funding or partnerships with utilities, manufacturers, and other interested parties.

7.5 State Energy Agencies

State energy agencies may conduct CEMM evaluations by researching products in the market. They can use the results of these evaluations to identify potential technologies for demonstration and deployment activities, which can fulfill proof-of-concept or serve as a bridge between the proof-of-concept and full commercialization steps in the development process. State energy agencies can also use CEMM evaluation results to design market transformation efforts, such as tax credits, low-interest loans, voluntary specifications, or mandatory standards that can increase the market adoption of certain connected functionalities.

7.6 Universities and Research Institutions

Universities and research institutions may conduct CEMM evaluations based on investigating products in the market or displayed at tradeshows. The results of evaluations can guide their R&D and commercialization strategies. For instance, evaluation results can identify technologies for focused joint research partnerships with manufacturers, which can lead to the sharing of R&D cost and intellectual property. Universities and research institutions can also use results to identify potential manufacturer partners for licensing agreements, catalyzing technology transfer to established manufacturers and/or emerging start-up companies.

[1] JW Feist et al. 1994. Super-Efficient Refrigerators: The Golden Carrot from Concept to Reality. ACEEE Buildings Summer Study Proceedings. Accessed September 12, 2016: http://aceee.org/files/proceedings/1994/data/papers/SS94_Panel3_Paper08.pdf

8.0 Domains, Categories and Maturity Questions

The CEMM is defined by five high-level domains that capture critical functionality in the evaluation of connected equipment maturity:

1. End-User Services
2. End-User Experience
3. Grid, Energy Market and Societal Services
4. Communication and Networking
5. Cybersecurity

Collectively, these domains express capabilities that enable the grid, energy market, end-user, and societal services described in the *Transaction-Based Building Controls Framework, Volume 1: Reference Guide*.[1] This framework was commissioned by DOE to augment the energy savings potential of buildings. The CEMM domain structure complements this framework by offering flexibility to organizations using the model. Organizations have the option of choosing a specific domain or group of domains to target in their evaluations, depending on their needs. For this reason, the Technical Working Group supported the CEMM structure as responsive to user objectives.

The CEMM's five domains consist of 17 categories. These categories represent logical groupings of the core functions, features, and characteristics within their parent domain. The Technical Working Group provided valuable insight as to which domains and categories warranted inclusion in the CEMM. For instance, the Cybersecurity domain was added to the model at the suggestion of the Technical Working Group. The organization of domains and their respective categories is summarized in Table 3.

Table 3. CEMM Domains and Categories

Domain	Categories
End-User Services	Maintenance and Repair Optimization Equipment Protection
End-User Experience	Ease of Installation and Use Awareness and Education
Grid, Energy Market and Societal Services	Status Load Control Intelligence Measurement and Verification
Communication and Networking	Interface Agreement Compatibility Reliability Interoperability

[1] Somasundaram S, RG Pratt, BA Akyol, N Fernandez, NAF Foster, S Katipamula, ET Mayhorn, A Somani, AC Steckley, and ZT Taylor. 2014. Transaction-Based Building Controls Framework, Volume 1: Reference Guide. PNNL-23302, Pacific Northwest National Laboratory, Richland, WA.

Domain	Categories
Cybersecurity	Identification Protection Detection Response Recovery

The CEMM's maturity questions encourage innovative functionality and scalable solutions as they proceed from MIL 1 to MIL 3. As connected equipment advances, it becomes more interoperable within its network of connected entities (e.g., associated equipment, utilities, third parties, users), and thus better coordinated using the commands and information these entities provide. This coordination involves a level of decision making or control, beginning with end-user activated functions and operations (i.e., operations requiring end-user intervention).

Automation is the next step in the progression of connected equipment decision making. Connected equipment with automated control responds to a single or limited set of variables, following a script in which all possible courses of action have already been made.[2] This method of decision making is limited by design, and therefore unable to respond to unplanned situations without intervention.

Autonomous intelligence provides an advanced level of decision making that's capable of unlocking a myriad of functional opportunities for energy-related services. Connected equipment with autonomous control can react to an indefinite number of variables, learn from each scenario it encounters, self-govern, and proactively pursue objectives. It accomplishes these objectives by utilizing sophisticated learning algorithms and leveraging vast sets of data (real time and historic) to identify trends, analyze patterns, and anticipate responses.[3] As connected equipment becomes more autonomous, it increases its ability to act on the information it receives through the interoperable entities in its network.

8.1 End-User Services

The End-User Services domain addresses functionality in which the primary motivation is to enable end users to increase efficiency and improve operation of equipment. The value of these services is considered "behind the meter," which is to say that they are delivered on the customer's premises. To facilitate end-user services, connected equipment should possess capabilities that improve the integrity and convenience of maintenance and repair, optimization, and equipment protection.

8.1.1 Maintenance and Repair

The Maintenance and Repair category assesses capabilities that assist equipment end users, owners, or service technicians in maintaining properly-functioning equipment through notifications of maintenance events, such as scheduled replacement, or through advanced automated detection. Automated detection can include ongoing active monitoring of equipment subsystems for performance degradation. By identifying degradation proactively, equipment owners can conduct timely, low-cost repairs rather than catastrophic equipment replacement. It also ensures reliable, efficient operation of equipment.

[2] Frost, Chad. "Challenges and Opportunities for Autonomous Systems in Space." U.S. Frontiers of Engineering Symposium. September 22, 2010.
[3] U.S. Department of Defense, Defense Science Board. "Summer Study on Autonomy." June 2016. Washington, DC.

Table 4. Maintenance and Repair Questions

MIL1	1. If authorized by the end user, can remote notifications be sent (e.g., via email, text, mobile application) to indicate *regularly scheduled maintenance* is needed for equipment?
	2. Can an interval for regularly scheduled maintenance notifications be programmed (e.g., reset or modified to occur sooner than prescribed) by the end user?
MIL2	1. If authorized by the end user, can an approved service provider access the equipment remotely to assess repair or maintenance needs?
	2. Are performance degradation and faults detected through automated prompts?
	3. If authorized by the end user, can remote notifications be sent to indicate the need for *performance-related maintenance or repair* (e.g., identified maintenance or repair is not predetermined and scheduled)?
	4. If authorized by the end user, can remote notifications be sent when maintenance or repair is detected as underway and complete?
	5. If authorized by the end user, can instructions to carry out maintenance and repair be received remotely?
	6. Can the status and need for replacing consumable components and items (e.g., air filters, anode rods, etc.) be evaluated?
	7. Is the equipment's maintenance history stored over its lifetime for access by end users or entities authorized by end users?
	8. If authorized by the end user, can information regarding the implications of delaying maintenance or repair (e.g., impacts on energy consumption, equipment degradation, end-user costs, etc.) be received?
	9. Is the fault detection or diagnostic approach based on specifications maintained by a nationally or internationally recognized standards body[4] or stakeholder alliance?[5]
MIL3	1. If authorized by the end user, can service providers be selected and scheduled automatically for performing maintenance or repair?
	2. Are performance degradation and faults detected through autonomous diagnosis?
	3. Can maintenance and repair work be determined autonomously based on the detected performance degradation and faults?
	4. Is the adequacy and effectiveness of maintenance or repair detected autonomously (e.g., detects whether equipment's status has been restored as intended)?
	5. If authorized by the end user, can the equipment's consumable components and items (e.g., air filters, anode rods) be ordered automatically once they are detected as needing replacement?
	6. Can multiple maintenance needs, or equipment faults, be detected concurrently for repair?
	7. Has the fault detection or diagnostics approach been tested and verified for compliance with a standard specification maintained by a nationally or internationally recognized standards body (e.g., ANSI, ASHRAE, IEC, IEEE, ISO) or stakeholder alliance (e.g., OCF, CEE, USNAP)?

[4] Examples of nationally or internationally recognized standards bodies include: American National Standards Institute (ANSI), American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE), and International Organization for Standardization (ISO).

[5] Examples of nationally or internationally recognized stakeholder alliances include: Open Connectivity Foundation (OCF), Consortium for Energy Efficiency (CEE), and Universal Smart Network Access Port Alliance (USNAP).

8.1.2 Optimization

Connected equipment may utilize programs, schedules, and algorithms to co-optimize parameters such as energy efficiency, desired comfort levels, convenience, and other end-user preferences. The Optimization category addresses the level of sophistication of these capabilities, which can range from a simple automation program using rule-based algorithms to autonomous, multi-objective optimization leveraging extensive sets of data and engaging in machine learning with every scenario it encounters.

Table 5. Optimization Questions

MIL1	1. Is the end user able to create a program or schedule that determines equipment operation in the future? 2. Are default, pre-programmed or pre-scheduled options offered for equipment operation? 3. Are operating algorithms devised to minimize energy use? 4. Does optimization consider end-user preferences in equipment performance (e.g., optimization adheres to user-specified temperature limitations, schedules, or bill savings goals)?
MIL2	1. Is advice provided to the end user for scheduling equipment operation? 2. Can the equipment accommodate authorized third-party programming or scheduling? 3. Does optimization utilize historical equipment performance data in optimizing future equipment operation? 4. Is optimization information stored throughout the equipment's lifetime for future access by the equipment owner or a third party designated by the equipment owner? 5. Is the optimization approach based on specifications maintained by a nationally or internationally recognized standards body (e.g., ANSI, ASHRAE, IEC, IEEE, ISO) or stakeholder alliance (e.g., OCF, CEE, USNAP)?
MIL3	1. Does optimization autonomously account for historical patterns and future projections of relevant environmental data (e.g., temperature, humidity, weather, air quality)? 2. Is performance data from other equipment leveraged in determining equipment optimization? 3. Has optimization performance been tested and verified as compliant with specifications maintained by a nationally or internationally recognized standards body (e.g., ANSI, ASHRAE, IEC, IEEE, ISO) or stakeholder alliance (e.g., OCF, CEE, USNAP)?

8.1.3 Equipment Protection

The Equipment Protection category assesses whether the equipment's embedded controls prevent damage and misuse by end users and third parties. Manufacturers set operating parameters and modes to protect equipment from incurring damage and keep end users safe. As equipment connectivity and intelligence advances, new considerations and opportunities emerge for protecting equipment.

Table 6. Equipment Protection Questions

MIL1	1.	Does the equipment have controls or operating parameters in place to prevent damage from misuse (i.e., operation in a manner that is inconsistent with manufacturer's intent) by end users or authorized third parties?
MIL2	1.	Does the equipment generate and store data related to the circumstances causing harmful operating conditions (i.e., operation that potentially impairs hardware or software beyond expected degradation levels)?
	2.	Does the equipment automatically return to normal operating conditions after harmful operating conditions are no longer detected?
	3.	Can the equipment enter a "safe mode" (i.e., operating mode in which functions and operations are active, but limited, so the system can be assessed for functional issues) when harmful operating conditions are detected (e.g., operation posing risk to equipment or end users)?
	4.	If authorized by the end user, can remote notifications be sent when the equipment has entered "safe mode" operation?
MIL3	1.	Are equipment operations adjusted autonomously to prevent circumstances that can lead to harmful operating conditions?

8.2 End-User Experience

The End-User Experience domain assesses connected equipment functionality that improves an end user's interactions with the equipment through enhanced physical and informational exchanges. The end user's experience is improved as equipment installation and usage requires less effort. End users can maximize the value of their equipment when they have data and analysis revealing the settings and conditions that suit their performance priorities.

8.2.1 Ease of Installation and Use

While connected equipment possesses greater operational functionality and sophistication than unconnected equipment, consumers expect a similar or lower level of effort in its installation, configuration, and use. The Ease of Installation and Use category addresses functionality and characteristics that make the equipment more convenient to install and easier to use through automation and remote access (i.e., access via smartphones, tablets, laptops, etc.). As connected equipment advances, end-user intervention should become less cumbersome, more intuitive, and less frequent. In addition, technical support should be widely available and easy to understand for end users in need of troubleshooting instructions due to installation, connectivity, application, and equipment issues.

Table 7. Ease of Installation and Use Questions

MIL1	1.	Can software and hardware be installed and uninstalled by the end user?
	2.	Can the equipment be installed without the need for additional hardware or software?
	3.	Can authorized users modify equipment operation settings or control equipment directly through remote means (e.g., smartphone, tablet, laptop, etc.)?
	4.	During the equipment configuration process, are end users provided guidance on how to select or specify appropriate user inputs?
	5.	Is technical support contact information provided to end users for troubleshooting installation, connectivity, application, or equipment issues?

MIL2	1.	If authorized by the end user, can software automatically be updated or patched as new versions become available?
	2.	If authorized by the end user, can new software be upgraded automatically (e.g., software enabling functionality of other connected equipment)?
	3.	Can authorized users modify equipment operation settings or control equipment directly through predefined voice or motion commands?
	4.	Is the user interface considered user friendly for *one class* of end users (e.g., novice or sensory impaired) based on analysis of user preference data, such as interviews, focus groups, surveys or other studies?
MIL3	1.	If authorized by the end user, can new software upgrades be evaluated autonomously to determine whether they are suitable for the equipment, and installed if deemed appropriate?
	2.	Are equipment settings adjusted autonomously based on sensed changes in end user status and activity (e.g., presence/location, body temperature)?
	3.	Is the user interface considered user friendly for *multiple classes* of end users based on analysis of user preference data, such as interviews, focus groups, surveys or other studies?
	4.	Is one-stop technical support (e.g., hotline, interactive online chat) available to end users for troubleshooting installation, connectivity, application, and equipment issues?
	5.	Are end users offered opt-in opportunities autonomously to add or access supplementary features and functionality for equipment operation?

8.2.2 Awareness and Education

Connected equipment can capture, store, analyze, and transmit data for the purposes of end user awareness and education. The analysis of equipment performance and use data across various settings and conditions can reveal opportunities. Given information and analysis about historical equipment performance, end users can modify settings, programs, or usage patterns to improve equipment efficiency, lower operating costs, and increase equipment longevity. The Awareness and Education category addresses the richness of information provided to the end user as well as the sophistication of data analytics in offering recommendations to improve equipment performance.

Table 8. Awareness and Education Questions

MIL1	1.	Is equipment operation, performance and use data captured and accessible to the end user?
	2.	Can end users access equipment performance data (e.g., energy use) in real time?
MIL2	1.	Does the end user have access to the equipment's historic performance and use data across end user settings, environmental conditions, and other relevant circumstances impacting equipment operation?
	2.	Is the end user provided with analytical graphs, tables, or displays of the equipment's historical performance and use across relevant circumstances impacting equipment operation?
MIL3	1.	Is the equipment's historical performance and use data analyzed autonomously to identify opportunities for performance improvement?
	2.	Are end users offered suggestions for improving equipment performance and use based on the equipment's autonomous analysis of historical performance and use data?

8.3 Grid, Energy Market and Societal Services

Service providers are in the process of creating new and innovative products and services to accommodate the evolving Smart Grid. The high priority challenges of this effort include simplification of market rules, expanding aggregator capabilities, information communication, and managing growth.[6] Load management enables the grid flexibility to accommodate the integration of renewable energy generation. Given the appropriate program designs, information exchange, intelligence, and control automation, end users can be empowered to act in their best interests while also making decisions that are good for overall system operational efficiency. The Grid, Energy Market and Societal Services domain defines functionality that enables equipment to provide physical and informational responses that improve electric power grid reliability and resilience. These capabilities allow entities to manage electric demand, such as shaving peak load or providing ancillary services that assist with grid operation.

8.3.1 Status

The Status category assesses the ability of equipment to report or communicate real-time status information in increasing levels of detail. The equipment status system may report operating status to inform an authorized requesting entity of the equipment's availability to participate in load control requests. Status may be needed to confirm actual participation in load control. In addition, status information can be used by the requesting entity to assist in estimating the impact of load response in real time.

Table 9. Status Questions

MIL1	1. Is the equipment's ON/OFF status communicated to the authorized requesting entity?
MIL2	1. Is the equipment's operating status, such as mode or variable load standing, communicated to the authorized requesting entity? 2. Can the equipment indicate whether it is available to respond to the external control signal? 3. Can the equipment provide informational responses to external control signals based on specifications maintained by a nationally or internationally recognized standards body (e.g., ANSI, ASHRAE, IEC, IEEE, ISO) or stakeholder alliance (e.g., OCF, CEE, USNAP)?
MIL3	1. Does the equipment confirm it is responding to the external control signal as intended? 2. Are the informational responses tested for compliance with a standard specification maintained by a nationally or internationally recognized standards body (e.g., ANSI, ASHRAE, IEC, IEEE, ISO) or stakeholder alliance (e.g., OCF, CEE, USNAP)?

8.3.2 Load Control Intelligence

The Load Control Intelligence category assesses the ability of connected equipment to respond to an external signal or entity (e.g., utility) and whether load can be curtailed or adjusted up and down to

[6] National Institute of Standards and Technology. January 2010. Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. U.S. Department of Commerce. Washington, DC. Accessed July 29, 2016: https://www.nist.gov/document-16676

provide greater energy demand flexibility. This functionality may consider circumstances such as forecasts of future equipment loads or grid conditions in load control determinations.

Load control intelligence progresses from simple, direct load control mechanisms in which end users have minimal control over their equipment to negotiation-based mechanisms in which the equipment's intelligence and requesting entities resolve load control solicitations through market-based transactions. These negotiation-based mechanisms rely on information exchange, historical data, end-user preferences, rules, and/or routines to determine equipment operation. The highest level of maturity is expected to empower end users to make informed energy use decisions based on their opportunity cost, thereby enabling a large-scale, market-based solution for reliable grid operations.

Table 10. Load Control Intelligence Questions

MIL1	1.	Can the equipment turn ON/OFF automatically in response to an external control signal?
	2.	Can the end user override the external control signal through the equipment's onboard control (e.g., manual interface)?
	3.	Is forecasted equipment load control based on single-variable logic (e.g., historic operating data)?
MIL2	1.	Can the equipment load be decreased discretely (e.g., through mode, cycle, speed) in response to an external control signal?
	2.	Are end user-defined operating limits (e.g., program, schedule, rate threshold) used to determine the equipment's automatic response to an external control signal?
	3.	Is forecasted equipment load control based on automation of a single variable or input (e.g., historic operating data, weather data, end-user settings)?
	4.	Can the equipment provide physical responses to external control signals based on specifications maintained by a nationally or internationally recognized standards body (e.g., ANSI, ASHRAE, IEC, IEEE, ISO) or stakeholder alliance (e.g., OCF, CEE, USNAP)?
MIL3	1.	Can the equipment load be *both* increased and decreased discretely in response to an external control signal?
	2.	Does the equipment's response to an external control signal account for end user defined operating limits and ambient/environmental conditions?
	3.	Does the equipment enable autonomous load variation through a negotiation-based mechanism (e.g., transactive-based controls), which can automatically establish agreements for energy-related services to be received or offered by equipment?
	4.	Is the equipment's intelligence capable of sensing grid operating conditions (e.g., frequency or voltage) and adjusting operation autonomously to assist with grid stability?
	5.	Is forecasted equipment load control based on autonomous analysis of multiple variables or inputs such as historic operating data, weather data, end-user settings, and future energy prices or incentives?
	6.	Are the physical responses tested and verified for compliance with a standard specification maintained by a nationally or internationally recognized standards body (e.g., ANSI, ASHRAE, IEC, IEEE, ISO) or stakeholder alliance (e.g., OCF, CEE, USNAP)?

8.3.3 Measurement and Verification

The Measurement and Verification category addresses functionality that supports end user, utility, and authorized third-party auditing activities. The purpose of this functionality is to support accurate billing or validation of responses to grid-requested services, which may be contractually binding. Measurement and Verification maturity questions focus on the equipment's ability to capture, process, and report energy information with a focus on relevant metrics needed for auditable program impact evaluations.

Table 11. Measurement and Verification Questions

MIL1	1.	Is the equipment's power and energy use information provided?
	2.	Does the power and energy use information result from estimated values?
MIL2	1.	Does the power and energy use information result from measured data with resolution *greater than one hour*?
	2.	Are price or incentive signals along with the resulting control response logged?
	3.	Are the reasons for not responding to external signals (e.g., end user override, schedule override, equipment malfunction) logged?
MIL3	1.	Does the power and energy use information result from measured data with resolution of *one hour or less*?
	2.	Are conditions (e.g., internal temperature, occupancy, and external temperature) relevant to load response logged?
	3.	Are the latest recognized measurement and verification protocols (e.g., International Performance Measurement and Verification Protocol – 2012 IPMVP) used in the analysis and reporting of results?
	4.	Are the results of load control intervention logged and communicated to the utility or authorized entity for evaluation purposes (e.g., power reduction, energy savings)?

8.4 Communication and Networking

Communication and networking functionality allows connected equipment to transmit and receive signals and information to and from other connected entities. This domain consists of four categories that focus on assessing functionality and characteristics that enable connected equipment to communicate in a multi-vendor environment, adapt to the changes in communications standards and technologies, exchange messages reliably, and operate in an interoperable or plug-and-play fashion.

8.4.1 Interface Agreement

An interface is the point of connection with interacting entities or equipment. To exchange meaningful information between two or more interacting systems or equipment, an interface agreement is established to define the informational exchange, how this exchange will take place, and how the information achieves a shared outcome. The agreement can be expressed in standardized specifications, which can be implemented by multiple entities interested in interacting for common purposes.

Open standards, agreed upon by stakeholder alliances and recognized bodies, have greater potential to accelerate the interoperability, and thus market penetration, of the various types of connected equipment.

The Interface Agreement category assesses the maturity of the communication protocols implemented in the evaluated connected equipment. The progression advances from the use of closed or proprietary protocols to open protocols to protocols that have been tested for compliance.

The GridWise Architecture Council (GWAC), formed by DOE to promote and enable interoperability among the many entities that interact with nation's electric power system, has identified eight interoperability layers, referred to as the GWAC Stack, that represent important aspects to consider for reaching interface agreements at the organizational, informational, and technical levels (summarized in Appendix A). The upper four layers are relevant to how the exchange of information is utilized for specific services and pragmatic aspects of interoperability. The business procedure layer is implicitly considered in other CEMM categories, such as Load Control Intelligence, Optimization, and Maintenance and Repair. The Interface Agreement category focuses on the lower four layers of the GWAC stack (Basic Connectivity, Network Interoperability, Syntactic Interoperability, and Semantic Understanding), which are related to the communication protocols for exchanging and understanding information.

Table 12. Interface Agreement Questions

MIL1	1. Are closed/proprietary communication protocols incorporated for the basic connectivity layers? 2. Are closed/proprietary communication protocols incorporated for the network interoperability layer? 3. Are closed/proprietary communication protocols incorporated for the syntactic interoperability layer? 4. Is a closed/proprietary information model implemented to provide semantic understanding of exchanged data and messages?
MIL2	1. Are the open protocols implemented for the basic connectivity layer maintained by a nationally or internationally recognized standards body (e.g., ANSI, ASHRAE, IEC, IEEE, ISO) or stakeholder alliance (e.g., OCF, CEE, USNAP)? 2. Are the open protocols implemented for the network interoperability layer maintained by a nationally or internationally recognized standards body (e.g., ANSI, ASHRAE, IEC, IEEE, ISO) or stakeholder alliance (e.g., OCF, CEE, USNAP)? 3. Are the open protocols implemented for the syntactic interoperability layer maintained by a nationally or internationally recognized standards body (e.g., ANSI, ASHRAE, IEC, IEEE, ISO) or stakeholder alliance (e.g., OCF, CEE, USNAP)? 4. Is the information model implemented for the semantic understanding layer maintained by a nationally or internationally recognized standards body (e.g., ANSI, ASHRAE, IEC, IEEE, ISO) or stakeholder alliance (e.g., OCF, CEE, USNAP)?

MIL3	1. Have the communication protocols implemented for the basic connectivity layer been tested and verified for compliance using procedures defined by a nationally or internationally recognized standards body or stakeholder alliance? 2. Have the communication protocols implemented for the network interoperability layer been tested and verified for compliance using procedures defined by a nationally or internationally recognized standards body or stakeholder alliance? 3. Have the communication protocols implemented for the syntactic interoperability layer been tested and verified for compliance using procedures defined by a nationally or internationally recognized standards body or stakeholder alliance? 4. Has the information model implemented for the semantic understanding layer been tested and verified for compliance using procedures defined by a nationally or internationally recognized standards body or stakeholder alliance?

8.4.2 Compatibility

Communications technologies typically have shorter lifespans than residential and commercial equipment, and thus have the potential to become obsolete before the equipment has reached the end of its useful life. To prevent connected equipment from becoming prematurely stranded, communication protocols should be backward and forward compatible. In addition, connected equipment should be able to undergo updates and upgrades to its communications software and hardware. This will allow connected equipment to remain interoperable and capable of communicating with third parties. Maturity in the Compatibility category is based on the ability of the information model to provide context for existing and planned end-user and/or grid services, sophistication of firmware upgrades to communication mechanisms, and the ability to communicate with multiple devices and entities.

Table 13. Compatibility Questions

MIL1	1. Does the implemented information model provide semantic understanding of data and messages exchanged for *existing* energy-related end-user and/or grid services (e.g., building energy management and/or demand response for peak load reduction)? 2. Do updates to communication protocols or information models require disabling equipment communications? 3. Do upgrades of communication protocols or information models require disabling equipment communications? 4. Does the interface support communication with a third-party hub/network device *OR* communication with at least one third-party service provider (e.g., utilities, implementers)?
MIL2	1. Can updates to communication protocols or information models be performed without disabling communications? 2. Can upgrades of communication protocols or information models be performed without disabling communications? 3. Does the interface support communication with *both* a third-party hub/network device as well as at least two third-party service providers (e.g., utilities, implementers)? 4. If authorized by the user, can updates/upgrades to communication protocols or information models be evaluated and installed autonomously for compatibility purposes? 5. Can an interface expansion module be installed to enable the equipment to communicate using different communication protocols for basic connectivity than initially supported?

MIL3	1. Does the information model provide semantic understanding of data and messages exchanged for *existing and planned* energy-related end-user and/or grid services (e.g. control of equipment to meet building operating objectives and provide grid frequency regulation services)?

8.4.3 Reliability

The Reliability category assesses the ability of the equipment to manage and recover from losses, delays, or interference in communications. Reliable equipment possesses the capability to detect and auto-recover from communications errors. This capability is dependent on the logic addressing the loss-of-communications as well as the quality-of-service logic that enables message prioritization.

Table 14. Reliability Questions

MIL1	1. Can communication errors caused by significant channel noise or other signal impairments be detected? 2. Are error messages stored or alerts generated after a loss or degradation of communication? 3. Is specific default logic implemented to preserve core functionality of equipment in the event of communication degradation or loss (e.g., air conditioner switches to default temperature setting after several minutes of communication failure)?
MIL2	1. Can communication errors or degradation caused by channel noise or other signal impairments be resolved automatically? 2. Can a network connection be re-established automatically after a disconnection without human intervention? 3. In the event of communication degradation or loss, are equipment operations adjusted automatically to preserve the equipment's core functionality and provide intended services?
MIL3	1. Does the equipment support predefined and customizable Quality-of-Service features (i.e., delivery is prioritized for alerts with high severity over alerts with low severity)?

8.4.4 Interoperability

DOE defines interoperability as the ability to exchange actionable information between two or more systems within a home or building, or across and within organizational boundaries. Interoperability relies on the shared meaning of the exchanged information, including agreed-upon expectations and consequences, for the response to the information exchange. Fundamentally, seamless interoperability requires reliable, hi-fidelity, and secure exchange of information.[7]

Interoperability facilitates "plug-and-play" operation of connected equipment systems, allowing disparate types of connected equipment to communicate and operate in unison. For end users, this reduces manual configuration and prevents the sidelining of certain connected equipment from connecting and

[7] DOE EERE. February 2016. "The National Opportunity for Interoperability and its Benefits for a Reliable, Robust, and Future Grid Realized Through Buildings." Page ii. Accessed September 14, 2016: http://energy.gov/sites/prod/files/2016/03/f30/Interoperability%20and%20National%20Benefits%20Through%20Buildings-031616.pdf

functioning with others. More broadly, interoperability leads to scalable deployment of connected equipment and enables consumer choice. The Interoperability category assesses the sophistication of functionality and features that promote "plug-and-play" capabilities, including the addressability, discovery, and configuration of equipment communications, as well as support of multiple communication paths to enable consumer choice.

Table 15. Interoperability Questions

MIL1	1. Is the equipment uniquely identifiable and addressable *locally* within a network? 2. Are multiple communication protocols supported that utilize the same or different types of data transmission media (e.g., Ethernet (IP) and ZigBee (non-IP) or Ethernet (IP) and Wi-Fi (IP)) to enable consumer choice?
MIL2	1. Is the equipment uniquely identifiable and addressable *universally* within a network? 2. Are different communication protocols supported that utilize at least two different types of data transmission media (e.g., Ethernet (IP) and ZigBee (non-IP)) in the event that one communication path is interrupted? 3. Can the equipment automatically announce its presence or identity to other connected entities for auto-discovery? 4. Can equipment specifications (e.g., rated power, capacity, etc.) and capabilities (e.g., communication protocols supported) be provided to an authorized, requesting entity through an online registry? 5. Can the equipment's intelligence query other connected equipment on the network to discover their equipment specifications (e.g., rated power, capacity, etc.) and capabilities (e.g., communication protocols supported) through an online registry?
MIL3	1. Can equipment specifications (e.g., rated power, capacity, etc.) and capabilities (e.g., communication protocols supported) be communicated directly to an authorized, requesting entity? 2. Can the equipment's intelligence query other connected equipment on the network to receive their equipment specifications (e.g., rated power, capacity, etc.) and capabilities (e.g., communication protocols supported) through direct communication? 3. Are communication settings autonomously configured for the end user based on the auto-discovery of the network, sensors, and authorized users and connected equipment?

8.5 Cybersecurity

Cybersecurity is the protection of information systems from theft or damage to the hardware, software, and information within them, as well as from the disruption or misdirection of the services they provide. A cybersecurity event is an action or attempted action to gain unauthorized access to, disrupt, or misuse an end user's connected equipment or information stored on connected equipment systems. These events occur when cybersecurity threats are carried out. A cybersecurity threat is any circumstance or event with the potential to adversely impact equipment operations through data transmitted from hardware or software (e.g., unauthorized access, destruction, disclosure, modification of information, and/or denial of service). Threats exploit cybersecurity vulnerabilities, which are weaknesses or flaws in hardware, software, data, or data flows.

The cybersecurity domain assesses the connected equipment intelligence and functionality that identifies, protects, detects, responds to, and recovers from cybersecurity events. A robust cybersecurity system should identify all hardware, software, and data flows exchanged with the connected equipment to determine points of access. Access to equipment should be limited to authorized entities engaging in permitted activity to safeguard equipment. Equipment operation and data traffic should be monitored to detect cybersecurity events. Once detected, responses will be engaged to confine and eradicate the cybersecurity event. After the event is eradicated, operation should be restored, vulnerabilities patched, and authorities alerted. [8, 9]

The cybersecurity systems for connected equipment are evolving from automated to autonomous defense software. Traditional automated measures, such as antivirus software, are important for preventing and addressing cybersecurity threats. However, as cybersecurity events have become more sophisticated, a need has risen for cybersecurity software with autonomous intelligence, capable of discovering and neutralizing threats instantly, and learning from previous cybersecurity events.

8.5.1 Identification

The Identification category addresses functionality that recognizes and manages the assets (i.e., hardware and software) with which data is transmitted. As assets and flows of data are recognized, inventoried, and mapped, cybersecurity risks are identified for the equipment, as well as its associated systems, data, and capabilities. These cybersecurity risks are prioritized according to their vulnerabilities and potential threats. Managing and analyzing requested additions or changes to assets, data flows, and end users helps prevent the introduction of new and unacceptable vulnerabilities in the operating environment. Inventory change management accounts for the full life cycle of all hardware and software in the equipment's network, including acquisition, deployment, operation, and retirement.[10]

Table 16. Identification Questions

MIL1	1. Does an authorized end user have the ability to manually conduct an electronic inventory of all end users and assets (i.e., physical equipment and software) with which the equipment exchanges data? 2. Does an authorized end user have the ability to manually map data flows for all inventoried assets? 3. Does an authorized end user have the ability to manually identify and prioritize cybersecurity vulnerabilities for the equipment based on assets with which it exchanges data?
MIL2	1. Does the equipment's intelligence automatically develop an inventory of all end users and assets with which the equipment exchanges data? 2. Does the equipment's intelligence automatically map all data flows for all inventoried assets? 3. Does the equipment's intelligence automatically identify and prioritize cybersecurity vulnerabilities based on assets with which it changes data?

[8] National Institute of Standards and Technology. 2014. "Framework for Improving Critical Infrastructure Cybersecurity." Version 1.0. U.S. Department of Commerce. Washington, DC. Accessed September 1, 2016: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[9] DOE's Buildings Technology Office is also developing a national Buildings Cybersecurity Framework (BCF) to systematically help identify, protect, detect, respond, recover and mitigate cyber threats to buildings and facilities. This Framework will provide further guidance on enhancing cybersecurity in buildings.

[10] Pacific Northwest National Laboratory. 2016. Buildings Cybersecurity Capability Maturity Model Evaluation Toolkit. Accessed September 14, 2016: https://bc2m2.pnnl.gov/

MIL3	1.	Are cybersecurity vulnerabilities identified and prioritized autonomously for the equipment as well as for all assets with which the equipment exchanges data?
	2.	Are additions, subtractions or changes to inventoried assets evaluated autonomously for vulnerabilities before authorization for data exchange?
	3.	Are cybersecurity threats identified, profiled and prioritized autonomously for the equipment and all assets with which it exchanges data?

8.5.2 Protection

The Protection category addresses functionality that safeguards equipment and systems to ensure the secure exchange of data. Protecting connected equipment involves limiting access to the equipment in the delivery of functions. Access is granted to hardware, software, and end users based on specific requirements and revoked when access is no longer necessary. These requirements are based on the hardware, software, and end users that should have access, circumstances calling for this access, limits of allowable access, and authentication parameters. Improper access can lead to unauthorized use, disclosure, destruction, or modification, as well as unnecessary exposure to cybersecurity risks.

Table 17. Protection Questions

MIL1	1.	Can connected access be limited manually through credentials or other means to end users, processes or devices authorized by the equipment owner or administrative user?
	2.	Can rights to connected functionality and operation be limited manually to activities and transactions which are authorized by the equipment owner or administrative user?
MIL2	1.	Is connected access restricted automatically, without intervention from an end user, to authorized processes or assets through a recognition mechanism?
	2.	Are connected operations restricted automatically to authorized activities and transactions without intervention by an end user?
MIL3	1.	Is connected access limited automatically to authorized users based on biometric credentials (e.g., fingerprint, facial recognition)?
	2.	Is data protected autonomously at rest and during transmission to prevent cybersecurity events (e.g., through the use of power resets, data obfuscation, sequence manipulation, signature cloaking)?

8.5.3 Detection

The Detection category addresses functionality that discovers the occurrence of a cybersecurity event. Detecting cybersecurity events involves monitoring data traffic continuously between connected equipment and its associated hardware and software. It also entails monitoring equipment access and operation for anomalous activity and patterns. Detection algorithms determine when a cybersecurity event is occurring as well as verify the effectiveness of protective measures.

Table 18. Detection Questions

MIL1	1. Is data automatically scanned in real time as it is exchanged with other assets?
MIL2	1. Is malicious or unauthorized code (e.g., malware) detected automatically in the data exchanged with other assets? 2. Are anomalous access attempts detected autonomously as indicators of cybersecurity events? 3. Are operational environments monitored autonomously for unusual behavior that may indicate a cybersecurity event?
MIL3	1. Are machine learning algorithms utilized to improve autonomous detection of cybersecurity events? 2. In instances of false positives (i.e., mistaken detection of a cybersecurity event) and false negatives (i.e., undetected cybersecurity event that was eventually discovered), is detection intelligence improved autonomously to address the source of the issue without compromising future detection?

8.5.4 Response

The Response category addresses functionality that takes action to address a detected cybersecurity event. This involves limiting impact and potential damage. Equipment operation is restrained to prevent harm to itself and end users. Equipment communication is confined to prevent the cybersecurity event from spreading to other hardware and software. Sensitive end-user and equipment data is destroyed. Most importantly, the cybersecurity event is eradicated.

Table 19. Response Questions

MIL1	1. Does the equipment transition to an operationally benign mode to prevent harm to the equipment and its end user(s) once a cybersecurity event is detected? 2. Do responses eradicate a cybersecurity event without the need for replacement of the equipment or its components?
MIL2	1. Does the response automatically alert other assets that a cybersecurity event is taking place? 2. Are cybersecurity events automatically contained from spreading to and harming other assets with which data is exchanged?
MIL3	1. If authorized by the end user, can the response involve automatically destroying sensitive end-user data (e.g., credit/debit card information) and equipment usage data (e.g., time of use)?

8.5.5 Recovery

The Recovery category addresses functionality that maintains equipment resilience and restores capabilities impaired due to a cybersecurity event. Following a cybersecurity event, the equipment's inventory of assets should be evaluated for vulnerabilities and updated accordingly. Operating configurations and settings should either be reset to their initial state or restored to their state prior to the event. Cybersecurity protection, detection, and response intelligence should analyze cybersecurity event data autonomously and update algorithms to defend against future cybersecurity events.

Table 20. Recovery Questions

MIL1	1. Is relevant cybersecurity event data captured for purposes of digital forensics?
	2. If the equipment has not endured physical damage from the cybersecurity event, can operating configurations, settings and inputs reset to the state that existed upon purchase?
MIL2	1. After a cybersecurity event, are operating configurations and inputs recovered and restored to their state prior to the event?
	2. Can cybersecurity event data be transmitted securely for digital forensics by the appropriate entities (e.g., manufacturer, vendor, law enforcement)?
MIL3	1. Is cybersecurity protection, detection and response intelligence improved autonomously (e.g., via large-scale machine learning, reinforcement learning) using historical cybersecurity event data?

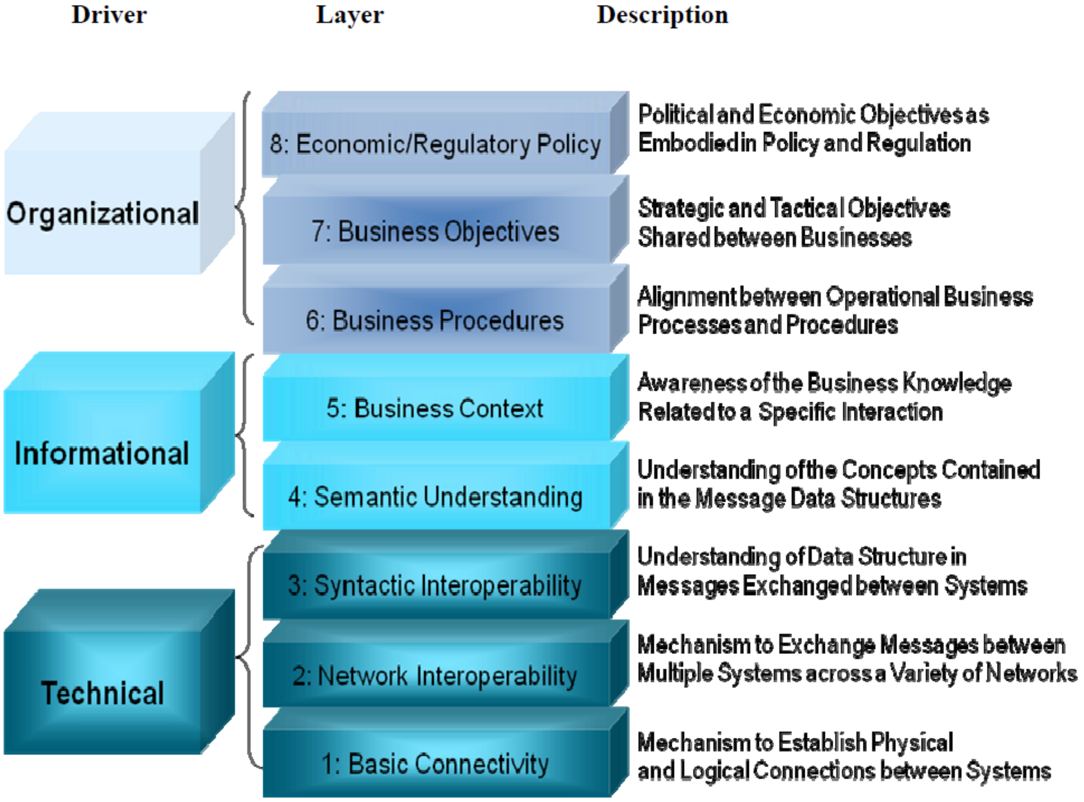
Appendix A

GridWise Architecture Council Interoperability Layers

Appendix A

GridWise Architecture Council Interoperability Layers

The GridWise Architecture Council (GWAC) has identified eight interoperability layers (as shown in Figure 3) that enable system integration with the Smart Grid. The upper layers represent how exchanged information is used for providing specific services and pragmatic aspects of interoperability.



Driver
Layer
Description
Organizational
Informational
Technical
8: Economic/Regulatory Policy
7: Business Objectives
6: Business Procedures
5: Business Context
4: Semantic Understanding
3: Syntactic Interoperability
2: Network Interoperability
1: Basic Connectivity
Political and Economic Objectives as Embodied in Policy and Regulation
Strategic and Tactical Objectives Shared between Businesses
Alignment between Operational Business Processes and Procedures
Awareness of the Business Knowledge Related to a Specific Interaction
Understanding of the Concepts Contained in the Message Data Structures
Understanding of Data Structure in Messages Exchanged between Systems
Mechanism to Exchange Messages between Multiple Systems across a Variety of Networks
Mechanism to Establish Physical and Logical Connections between Systems

Figure 3. GWAC Interoperability Layers[1]

Basic Connectivity protocols describe the data transmission medium, the associated low-level data encoding, and the transmission rules for accessing the medium. These protocols are established to enable the digital exchange of data between interacting parties as well as to form reliable communications paths. This interoperability layer can be mapped to the physical and data link layers of the Open Systems Interconnection (OSI) seven-layer model, which provide the following functions:

- Hardware media access and electrical connectivity
- Character encoding, transmission, reception, and decoding
- Low-level data contention and flow control

[1] National Institute of Standards and Technology. September 2014. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. Page 38. Last accessed September 14, 2016 at: https://www.nist.gov/sites/default/files/documents/smartgrid/NIST-SP-1108r3.pdf

- Media connection establishment and termination
- Transference of data between network nodes
- Correction of errors that occur during transmission

Network Interoperability protocols focus on addressing issues that arise from transporting information between interacting parties across multiple communication networks. This interoperability layer maps to the network, transport, session, and application layers of the OSI model, which provides the following functions:

- Translation of logical addresses and names into physical addresses.
- Transparent and reliable transfer of data between systems, which includes:
  - Transference of data between the source and destination through network intermediaries, such as switches and routers
  - Management of network congestion
  - Management of message delivery order.

Syntactic Interoperability protocols consist of the rules governing the format and structure for encoding information exchanged between interacting parties. This layer maps to the application and presentation layers of the OSI model, which provide the following functions:

- Translation of character data from one format to another, such as Extended Binary Coded Decimal Interchange Code to American National Standard Code for Information Interchange (EBCDIC to ASCII)
- Message content structure, such as Simple Object Access Protocol (SOAP) encoding
- Message exchange patterns, such as Synchronous Request/Response or Asynchronous Publish/Subscribe.

Semantic Interoperability protocols (or information models) are usually domain-specific (i.e., pertains to one area of expertise, such as a car, a building, or a power system) and are typically expressed in an object-oriented form in terms of classes, properties, and relationships. These models consist of rules governing the definition of data structure content, concepts, and their relationship to each other, as well as constraints on the information concepts (i.e. include expressions for resolving situations where two differently named classes in different models mean the same thing or when a class is a subset or superset of another class). Examples of standard information models include the following:

- Common Information Model (CIM) power model—(International Electrotechnical Commission [IEC] 61970 CIM—based on Resource Description Framework [RDF])
- Models based on universal description, discovery, and integration (UDDI)
- Object models based on XML (Extensible Markup Language) schema definition (XSD)
- Object models based on Open Platform Communications Unified Architecture (OPC UA)
- Object models based on the IEC 61850 substation automation standard.

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

Proudly Operated by **Battelle** *Since 1965*

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov