Communication Protocols and Standards for Residential Demand Response

DR18.12

Prepared by:
A. Vaddiraj / W. Johnson

Electric Power Research Institute (EPRI)

September 2021

SOUTHERN CALIFORNIA EDISON®
An EDISON INTERNATIONAL® Company

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Communication Protocols and Standards for Residential Demand Response

Current Status and Future Opportunities

DR 18.12

EPRI Project Manager:
A. Amarnath

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI), prepared this report:

Principal Investigators

A. Vaddiraj
W. Johnson

This report describes research sponsored by EPRI.

EPRI would also like to acknowledge Southern California Edison for the direction and strategic guidance on this project:

Mark S. Martinez
Senior Portfolio Manager, Emerging Markets and Technology Program
Southern California Edison

This publication is a corporate document that should be cited in the literature in the following manner:

Communication Protocols and Standards for Residential Demand Response: Current Status and Future Opportunities. EPRI, Palo Alto, CA: 2021. InsertSAPNumberHere.

ABSTRACT

This report describes the communication protocols and networking technologies in use or emerging for control of residential Demand Response (DR) resources. It describes three important application-layer (functional) protocols that are the subject of emerging grid codes and standards: OpenADR, IEEE 2030.5, and CTA-2045. It also provides a general overview of four important messaging services that may be used by DR protocols: eXtensible Messaging and Presence Protocol (XMPP), Message Queuing and Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), and Data Distribution Service (DDS). New and emerging telecommunications services available for use by DR protocols, such as 5G cellular, low-earth-orbit satellites, and cloud-based proprietary systems, are also included.

Descriptions and comparisons of the protocols are provided, based on the Open Systems Interconnection and Internet models. Cyber security of the protocols is described, and a bibliography focused primarily on relevant EPRI research publications is included.

Keywords

Demand Response
Distributed Energy Resources (DERs)
Energy management system (EMS)
Communication protocols
Open standards
Cyber security

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

EXECUTIVE SUMMARY

Deliverable Number: InsertSAPNumberHere

Product Type: Technical Update

Product Title: Communication Protocols and Standards for Residential Demand Response: Current Status and Future Opportunities

---

PRIMARY AUDIENCE: Electric Utilities - Demand Response Program Developers and Implementors, Energy Service Providers, Aggregators, Distribution System Operators (DSOs), Independent System Operators (ISOs)

SECONDARY AUDIENCE: Communication Technology Product Manufacturers

KEY RESEARCH QUESTION

What are the developing automation and control protocols that can be used to communicate with end-user premises for demand response and load control programs for residential end-users?

RESEARCH OVERVIEW

This report provides an objective status update of Demand Response (DR) automation and control protocols for the residential sector. Information in the report will give readers knowledge of the essential features of key automation and control protocols, their applications, innovative non-DR systems and technologies that are on the horizon and that could be adapted for DR applications, and the currently observable technology gaps that need to be overcome to have effective mass market communications for evolving residential DR programs. The report also provides an overview of emerging standards and technologies in the automation and control protocol market for other related applications.

KEY FINDINGS

- Application protocols for residential DR programs that have currently been adopted by the energy service providers in California, such as utilities, municipal agencies, community choice aggregators, and third-party providers, are designed and implemented using a layered architecture that allows them to operate over many different telecommunication protocols and media.

- Most DR protocols in use today do not contain unique cyber security features but instead rely on the underlying standardized communication protocols that include secure architecture applications and securitized transport networks to provide security (such as encryption to insure privacy and integrity of communications).

- Different protocols are being specified by various entities in varying jurisdictions for controlling both residential DR devices and inverter attached DER (such as batteries and PV). Multiple protocols are used depending on specific use cases and application and service requirements.

- New underlying telecommunication options are emerging, such as 5G cellular, low-earth-orbit satellites, and the next generation of Wi-Fi, that DR providers will have to understand and accommodate for developing new communication pathways for the mass market.

- Existing cloud-based proprietary solutions for device control, including consumer goods smart home automation, will have to be accommodated by utilities (or their aggregators) to successfully incorporate residential DR programs that will include those new appliances and devices as reliable operational resources.

WHY THIS MATTERS

The current ecosystem of advanced communications systems is rapidly evolving to serve the growing markets of personal mobility and consumer convenience, business and industry, education, transportation, entertainment, science, and health services. Many electric utilities are evaluating these platforms for their automation and control protocols to determine which to use to communicate with end-user premises for residential DR programs. This assessment requires an objective study of the commercially available automation and control protocols to determine which are appropriate for their enterprise.

To answer these and many other questions, this report provides an objective review of these platforms and the leading automation and control protocols for the residential sector. The automation and control protocols in use in the residential sector today rely on supporting networking services to deliver their messages. In some cases, the application-layer protocols can make use of different supporting messaging services, increasing the number of deployment decisions to be made when deploying such systems. New and emerging telecommunications options will also change the landscape for secure residential communications for future models of demand response.

HOW TO APPLY RESULTS

This report can be used by utilities, energy service providers, product manufacturers, and automation and control protocol alliances to work towards greater product interoperability for offering effective demand response programs in a carbon-constrained economy. The report can be used as a reference guide to gain a basic understanding of the technologies discussed and to make an informed assessment of where the emerging trends are to be found. A bibliography highlighting EPRI research reports is also provided.

LEARNING AND ENGAGEMENT OPPORTUNITIES

- The project results were transferred to different stakeholders from Emerging Markets and Technology (EM&T) Program to DR Programs, Codes and Standards and other groups within SCE and other utilities.
- The results can also be used by CAISO, CPUC and other IOUs for better engaging customer participation in DR and, in turn, reduce the demand on the grid.

EPRI CONTACTS: Ammi Amarnath, Senior Technical Executive, Electrification & Customer Solutions Research Area, aamarnath@epri.com

PROGRAM: P170 Customer Technologies

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

Background of Communication Technologies for Demand Response

Demand response, in one form or another, has been around for decades and has been an important tool for electric utilities to manage customer demand when supply side resources in times of extreme situations were unable to provide the desired reliability of service. Often the utility would develop a remote-controlled system to allow customers to enroll in a program and receive compensation in exchange for the utility directly managing their usage, usually the air conditioner or electric water heater. The early automation and control protocols that were developed to communicate with controllable residential loads were quite primitive until the 1970s because of the absence of sophisticated microprocessors capable of handling complex automation and control instructions.

Since then, there has been rapid development of automation and control technologies as microprocessors controlling automation and control functions have become more powerful and the underlying electronic circuitry has become compact enough to fit into the smallest devices. These automation and control technologies are based on a set of messages that are sent from a central management system. The messages are sent via electronic signals that follow a specific format. The combination of the physical transport mechanism, the format of the messages, and the meaning of the messages collectively form the "application protocol" for automation and control. Examples of early automation and control communication protocols include X-10 and Z-Wave.

The Evolution of Demand Response

Over the decades, the sophistication of these messages and the protocols that implement them have evolved. Figure 1-1 summarizes these changes, grouping them into three generations. As can be seen, DR has evolved in a rather short time from the early days of the 1970s to more sophisticated applications, as shown in "Demand Response 3.0."

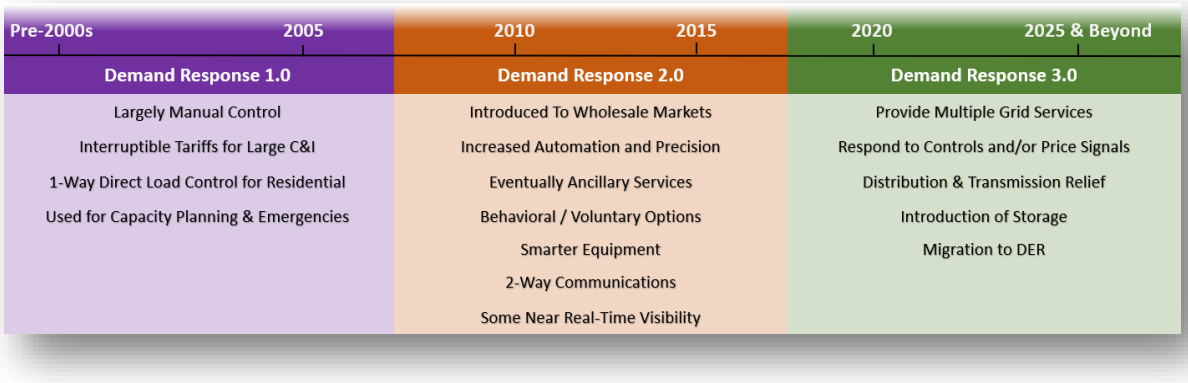


Figure 1-1:

Evolution of Demand Response[1]

Direct Load Control

In a traditional DR 1.0 Direct Load Control (DLC) program, a utility would send a one-way electronic signal directly to high-consumption electrical appliances at residential sites to turn them off during times of peak demand. When the peak demand period was over, a second signal was sent from the utility to the appliances to turn them back on again. These were the early (but very important) methods that utilities had to manage grid reliability. By directly managing end use devices such as air conditioners and pool pumps, the utility could often achieve many MWs of demand reduction (depending on how many devices they had installed) and thereby avoid rotating outages and forced "black outs." While viewed as primitive by today's standards, the systems used at the time were reliable since advanced communications were extremely limited. However, the drawback of the one-way method was that individual performance tracking of the program's effectiveness was non-existent, as there was no "return loop" of communications from the customer site.

Two-Way Communication

DR 2.0's Two-Way Communication for DR was a necessary advance over DLC programs to ensure that the systems were operating effectively. With 2-Way DR, utilities send electronic signals to residences over a two-way communication network, either to local Energy Management Systems ("gateways") or directly to smart devices. These messages result in adjustment of the consumption of certain electrical appliances upward or downward (subject to being overridden by the end-user). When the DR event period is over, a signal restores the appliances to their initial settings. The end-user's devices or energy management system may periodically upload consumption data to the utility using the same communication link; this information can be used by the utility when forecasting end-use demand profiles for electricity pricing.

Both DLC and 2-Way DR require: 1) a communication link between the utility and the end user or device; and 2) a mutually understood automation and control protocol that controls energy consumption levels at the end-user site during event periods. One major difference between the two is that DLC programs send signals to turn customer premises equipment off during peak demand periods (only), whereas 2-Way DR typically provide the end user with signals relating to a wide range of grid conditions (including emergencies).

"Prices-to-Devices"

A further refinement of the 2-Way DR mechanism, introduced in DR 3.0, has a model that uses prices to signal or motivate desired changes in demand. These are usually combined with a more sophisticated gateway or smart grid device that allows automated decision-making by the controller or appliance when it receives an indication of a new or future price. Such a mechanism can also be used to communicate preexisting price schedules to automate response to a time-of-use residential tariff.

---

[1] "Demand Response Fundamentals and Evolution," slide 20, *Demand Response Evolution*, PLMA 2018 (https://www.peakload.org/demand-response-training).

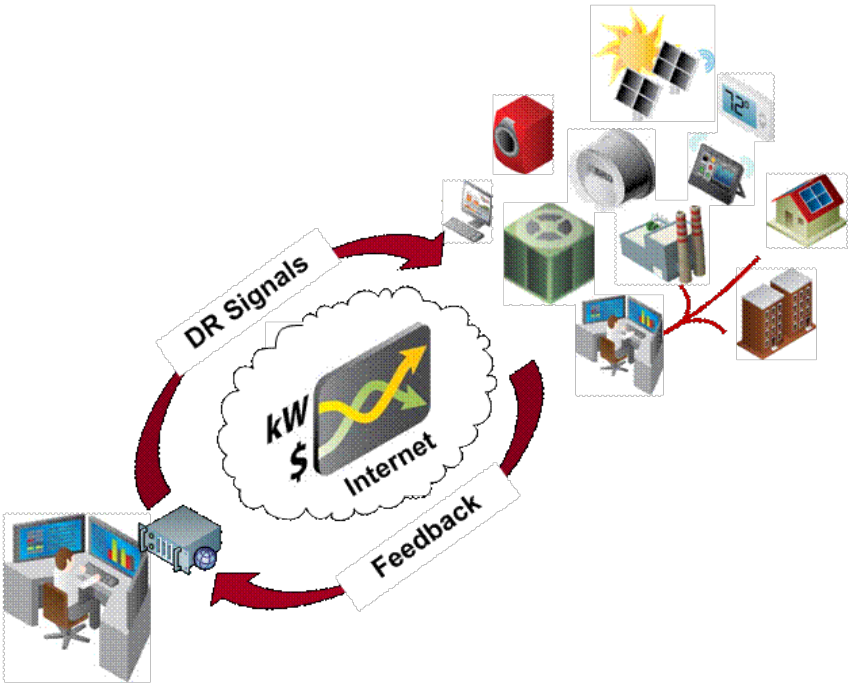


Figure 1-2
The General Structure of DR Communications

As summarized in Figure 1-2, DR 3.0 communications would occur between a system operator (shown at the lower left) and one or more DR or DER assets (in the upper right). Messages flow in both directions. The DR signals themselves may consist of general information (such as grid status), motivational messages (prices or tariffs), or dispatch instructions (either schedules or immediate reliability actions).[2]

The Need for Two-way Automation and Control Protocols for DR Programs

When a utility communicates with a customer participating in a DR program today, it is frequently a requirement that the utility receive end-user energy consumption data in return. This might be used to price electricity for the next day or to confirm that the end user's consumption was modified as requested. This two-way flow of data between the utility and the customer's premises requires a two-way application protocol running over a suitable communication infrastructure, absent which a utility would lack access to critical energy consumption information.

Fortunately for the utilities and for future demand response program designers, today's new communications protocols that have replaced many of the older systems can provide this level of information, leading to more effective DR programs and a wider range of applications for multiple residential devices. The following illustrations show how current DR programs can reach both traditional appliances and a wider range of future end uses that include "distributed energy resources" (DERs) such a solar panels, backup systems, and even electric vehicles, that

---

[2] *Common Demand Response Functions for Heating, Ventilating, and Air Conditioning (HVAC): A Summary of Demand Response Functionality Discussed in the Industry to Date.* EPRI, Palo Alto, CA: 2017. 3002011045.

can be part of the future DR program design for residential markets as envisioned by policymakers and researchers in today's modern environment.

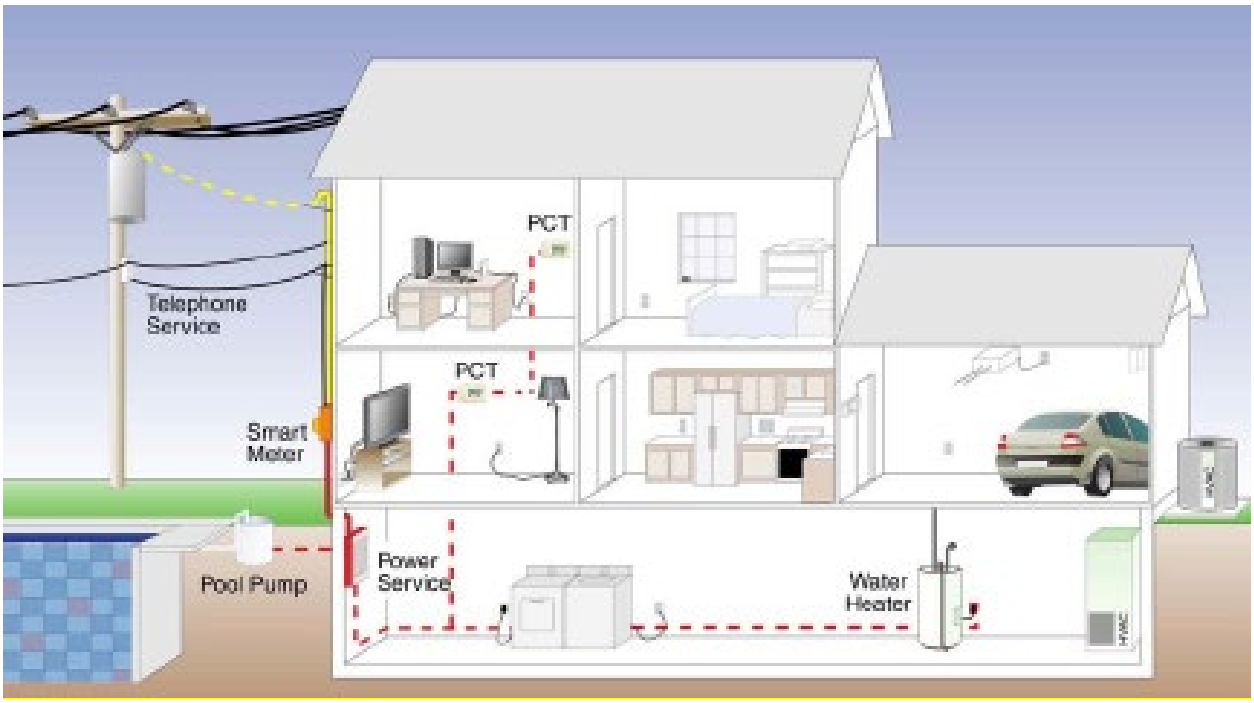


Figure 1-3
Common End Use Devices That Are Being Controlled by Utilities in Residential DR Programs

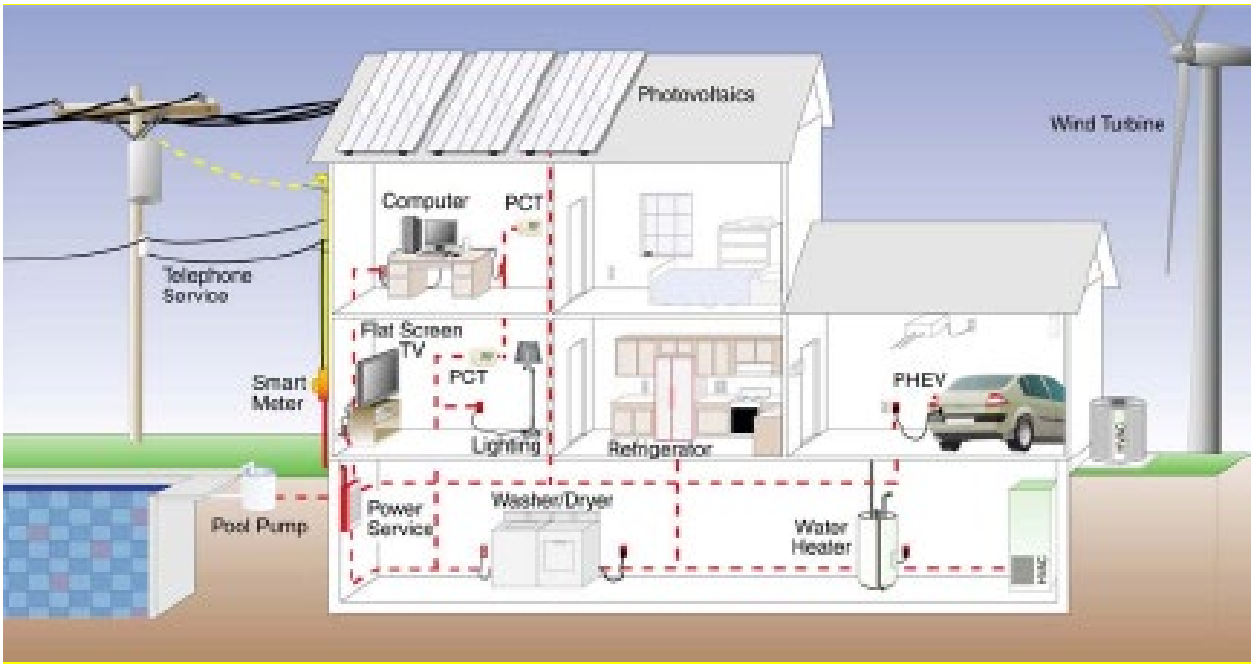


Figure 1-4
A Future Home with Renewable Energy Sources, Energy Storage Systems, and Plug Loads Communicating with the Utility Grid for DR and DER Programs

2
AUTOMATION AND CONTROL PROTOCOL ARCHITECTURES

Automation and control protocols are sets of definitions and procedures that controllers and end-use devices follow to communicate with each other. The protocols contain defined messages that can be sent from the controller to an end-use device to motivate or direct a change in certain attributes (settings) of the device (e.g., on/off, reduce, standby, etc.).

An automation and control protocol stack defines the following minimum layers:

1. The interface to the physical transport medium that will ultimately carry the messages (wires, radio, etc.)
2. The logical link between the two communicating devices (software to check that messages moving between nodes of the network are error-free)
3. A network layer (an addressing system that allows messages to be routed to their intended recipients by using unique network addresses)
4. An application layer, which defines messages based on "objects" that represent the different attributes of the end-use devices that are to be controlled and "services" that manipulate the objects to change the operational status of an end-use device (for example, turn on/turn off, dim, raise temperature, etc.)

The Open Systems Interconnection Model

Protocols and communication technologies are often defined with reference to the Open Systems Interconnection (OSI) Basic Reference Model, developed by the International Organization for Standardization (ISO). The OSI model provides a seven-layer abstract representation of the communication protocols used between any two systems. In the model, each layer provides services to the layer above it and makes use of services provided by the layer below it. This layered model was created to provide a reference structure with which developers could easily decompose and group services into separate layers (rather than view the entire protocol definition as a single complex structure).

The Seven Layers of the OSI Model

The seven layers of the OSI Model (from top to bottom) are:

Layer 7 – Application: This layer provides services to application processes and issues commands to the Presentation Layer. This is the layer in which the DR-specific messages flow. This layer also contains certain "helper" messaging systems (called "middleware") that facilitate the exchange of the application-specific messages. The DR application layer protocols included in this report are OpenADR, IEEE 2030.5, and CTA-2045. Several middleware systems are also discussed in this report; a familiar example of such a system is Hypertext Transfer Protocol (HTTP), which forms the basis of the World Wide Web.

Layer 6 – Presentation: This layer manages the format and meaning of the application data so that it can be interpreted correctly. This layer provides flexibility in the types of systems that can exchange data. Two systems with different notations can display the same data in their own format by using the Presentation Layer. Examples of Presentation Layer protocols include American Standard Code for Information Interchange (ASCII), Musical Instrument Digital Interface (MIDI), and The Moving Picture Experts Group (MPEG) protocols.

Layer 5 – Session: This layer establishes, maintains, and severs communication sessions between two systems in the network. It synchronizes applications running on two different systems so they can communicate reliably and accurately with each other without interference from other sessions running on those systems or other systems on the network. In the usual Internet protocol stack, the Transmission Control Protocol (TCP) performs functions of the Session Layer.

Layer 4 – Transport: This layer may provide end-to-end acknowledgement of data sent between a sender and a receiver to establish a reliable stream (called a "connection-oriented" service). Some Transport Layer protocols can adjust the number of data segments that may be sent from the sender to the receiver at one time. This feature is used to provide flow control in the network during periods of congestion. Examples of Transport Layer protocols include the connection-oriented Transmission Control Protocol (TCP) and the connectionless User Datagram Protocol (UDP).

Layer 3 – Network: This layer provides an addressing system that is independent of the underlying transport technology. It is a connectionless ("send-and-forget") service (since the sender at this layer does not know if the recipient got the data or not). Network layer addressing is used to direct data packets from the sender to the receiver across multiple interconnected networks using a routing protocol. Examples of Network Layer protocols include Internet Protocol (IP) and Address Resolution Protocol (ARP).

Layer 2 – Data Link: This layer, also known as the Logical Layer, provides flow control and error checking to ensure that a reliable stream of data flows between adjacent nodes in the network. It provides the digital frames in which data are carried over a single network hop. The Data Link Layer also defines a physical address that allows the digital frame to go from the sender to one or more receivers of the data on the same network. Some Data Link Layer protocols have the option of creating broadcasts from a sender to all the other possible recipients on the network. Examples of Data Link Layer protocols include Fiber Distributed Data Interface (FDDI), Synchronous Data Link Control (SDLC), High-level Data Link Control (HDLC), Asynchronous Transfer Mode (ATM), and Token Ring. Ethernet (802.11) and Wi-Fi (802.11) are combinations of Physical and Data Link Layers.

Layer 1 – Physical: This layer defines the mechanical and electrical properties of the interface between the system and the physical media that will carry the electronic signal. It also defines how the electrical signal is interpreted into data. Examples of physical layer protocols include RS-232, RJ-45, etc.

The Importance of the OSI Model for Open Standards and Interoperability

The seven-layer stack of the OSI Basic Reference Model provides a universally accepted means of comparing different protocol stacks. Each protocol defines its behavior at one or more layers

of the OSI stack. Some protocols combine adjacent layers of the OSI stack into a single communication layer.

Two vendors' products may interoperate if they use a common protocol to communicate (i.e., have the same specifications for the various layers of this open standard). Some DR protocols predefine what standard is used at which layer, others provide options. Two systems must use the same standards at each layer to interoperate. If they do not use the same standards at every layer, adapters/translators may be necessary. The complexity and cost of adapters/translators depends on the standards and number of devices in need of adapters/translators. As a result, the seven-layer OSI Basic Reference Model can be used to develop open standards-based communication protocols for establishing interoperability between products.

Using the OSI Model to Compare Automation and Control Protocols

Each automation and control protocol can be mapped to one or more layers the seven-layer OSI stack. Comparing one automation and control protocol with another simply uses a visual depiction of each protocol stack and the seven-layer OSI stack

Figure 2-1 shows an example of how the seven-layer OSI stack can be used to compare two DER protocols – OpenADR and IEEE 2030.5. In this example, the two protocols share similar lower layer standards, the key differences being in the Application Domain.

			IEEE 2030.5	Open ADR 2.0
Application Domain	Layer 7	DER/DR Data Model	IEC 61850-7-420, IEC 61968-5	OpenADR v2.0 Profiles
		Application	HTTP	HTTP, XMPP
	Layer 6	Presentation	TLS	TLS 1.2
Network/ Transport Domain	Layer 5	Session	Any (Ex: TCP Session Management)	Any (Ex: SSL)
	Layer 4	Transport	TCP	TCP
Physical Domain	Layer 3	Network	IP	IP
	Layer 2	Data Link	Any (Ex: IEEE 802.2)	Any (Ex: IEEE 802.2)
	Layer 1	Physical	Any (Ex: IEEE 802.1x)	Any (Ex: IEEE 802.1x)

Figure 2-1
Example Comparison of Internet Protocols with the Seven-layer OSI Basic Reference Model[3]

[3] *DER Protocol Reference Guidebook– 4th Edition: Understanding the Characteristics of Communications with Distributed Energy Resource (DER) and Demand Response Technologies.* EPRI, Palo Alto, CA: 2020. 3002018544.

Comparing the various communication protocol standards to the OSI seven-layer Reference Model makes it easier to see how they relate to each other and what interfaces and adapters are needed for them to interoperate.

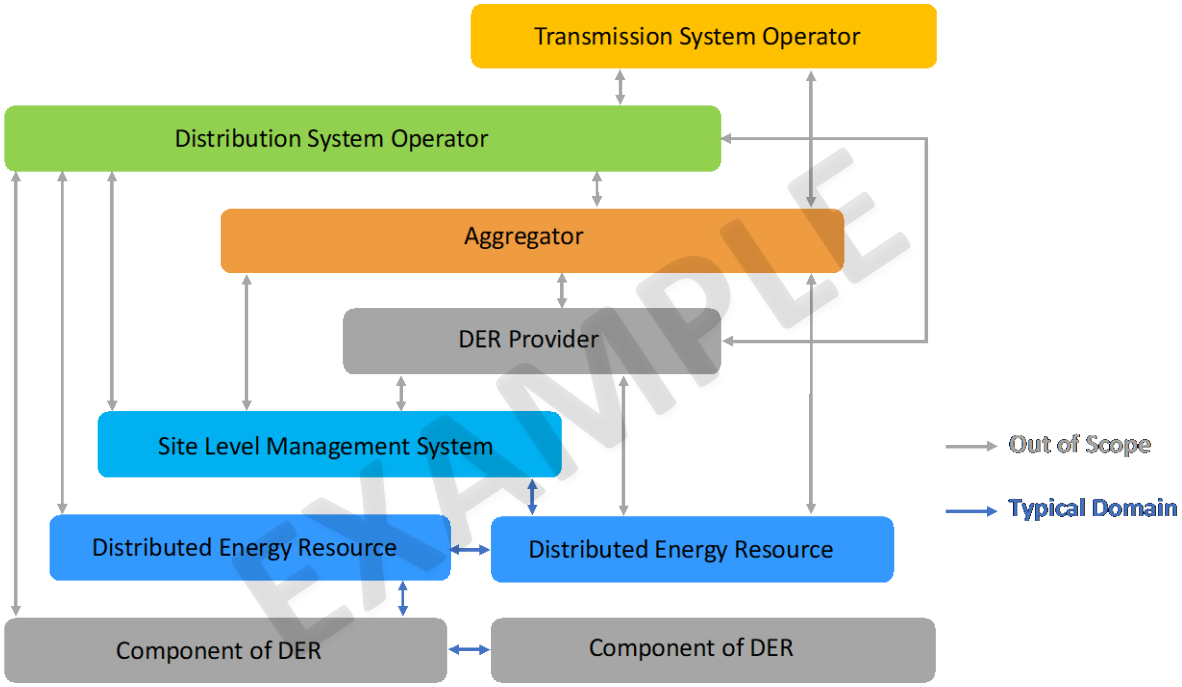
Deployment Architectures for DR Protocols

The three DR protocols described in this report all operate at the Application Layer of the OSI model. However, their general scope and utilization varies. This section contains descriptions of the architectural environments appropriate to each protocol.

Understanding the Architecture Diagrams

Besides their internal structures (as described by the OSI Reference Model), it is important to remember that a protocol may be one of many used across the overall control architecture. The architecture overviews contained later in this report provide textual and visual descriptions of how each protocol fits into such a broader architecture. Protocols can be deployed at any level in the control hierarchy; however, different characteristics make some protocols more suitable to some areas than others. These characteristics may include functionality, common usage, grid code requirements, and others. For example, the contents of a protocol's information model may limit its applicability outside of a particular domain. Consider Open ADR. OpenADR contains information needed to communicate with an individual DR resource and implement the DR paradigms described in Background of Communication Technologies for Demand Response. It does not contain the information model for smart inverters. Smart inverters require a different set of functionalities set by local grid codes including automatic control of output based on local voltage, settings to cease generation if grid voltage exceeds tolerances, or changing power factor and reactive power out. In this example, OpenADR is suitable for communications between a distribution utility and a behind-the-meter (BTM) technology, but more focused on demand response than BTM smart inverter control.

In the architecture diagrams like the one shown in Figure 2-2, all information exchanges where protocols generally might operate are indicated by arrows. When illustrating the application domain of a specific protocol, the areas in which it typically operates are indicated by black arrows, while the areas in which it is not typically used are grayed out.



* Example only

Figure 2-2
Example of an Architecture Overview (SunSpec Modbus Protocol)

The architecture shown in Figure 2-2 is representative of those typically found in the industry for monitoring and control of DER (including DR). It is possible that other architectural elements exist, however this overview is intended to cover most situations. The entities included are:

- **Transmission System Operator (TSO):** The entity that controls the transmission of energy at a regional level. Transmission systems typically operate from 69kV up to 765kV.
- **Distribution System Operator (DSO):** The entity that controls the distribution of electricity in local markets. Distribution systems typically operate from 4kV to 46kV. DSO-managed distribution systems are electrically connected to TSO-managed transmission systems.
- **Aggregator:** Intermediaries between TSOs or DSOs and consumers, aggregators allow multiple resources to act as a single entity when participating in an energy market. Aggregators may control fleets of distributed energy resources, including solar, storage, or demand response technologies. Aggregators provide an energy resource to the utility in the form of a large group of managed resources.
- **DER Provider:** A DER provider is the operator of a distributed energy resource (including DR resources).

- **Site-Level Management System:** Some DERs have a site controller that controls multiple, connected DER. Facility management systems, building management systems, and microgrids are some common examples of Site-Level Management Systems.
- **Distributed Energy Resource:** The distributed energy resource is the equipment providing or consuming energy (supply or controllable load). Examples of DER include solar PV systems, energy storage systems, and DR technologies. It is important to note that a DER is defined by its point of control: if a single controller manages a collection of other technologies, then the site is the DER and the individual technologies are components of the DER. An example of this is solar and storage on a site with a site controller. This is likely considered a single DER.
- **Component of DER:** DER can consist of multiple components. In the example of a large pad-mount energy storage system, there may be a battery management system, meters, inverters, and other supporting equipment. Each component may communicate with other components, as well as with a central site controller

3
APPLICATION PROTOCOLS

This section contains descriptions of three standardized application protocols that are often used to communicate with residential DR and/or DER resources. Each protocol is described in terms of nine key criteria selected to present a comprehensive overview of the protocol in a way that makes it easy to compare one protocol to another. The following criteria are used:

Technical Overview: A high-level description of the protocol with a brief history, it includes an illustration showing communication paths in a typical deployment architecture and may contain an example of an implementation of the protocol to help the reader understand its context and application.

Adoption: A summary of how widely the protocol is used (including any insights about why this is the case), this also provides information about the products on the market today. It includes use in products ranging from individual devices to control systems.

Devices and Technologies: An overview of the types of devices supported by the protocol and the type of functions it supports (for example, direct control instructions or "inform and motivate" messages).

Implementation: A high-level description of how the protocol works and an assessment of the complexity of the system and general requirements for implementation, this section also highlights any notable dependencies that are associated with using this protocol.

Test Tools and Certification: A discussion of currently available test tools and certification processes.

Cyber Security Features: An overview of how security is addressed in the protocol (if it addresses security features at all). This includes information about whether these security requirements are included in conformance testing.

Regulatory Framework: A summary of whether the protocol is required or suggested as part of grid codes or other regulations.

Governance and Maintenance: This section identifies the entity that manages the protocol standard and reviews potential changes, the process used to update the standard, and information about past, present, or future revisions.

Relevant Reports: A list of significant EPRI and third-party reports related to this protocol, this may include case studies, lab tests, government work, or other research.

OpenADR

Focused on communications with DR resources (including residential resources), OpenADR (Open Automated Demand Response) provides both information and control settings for scheduled DR events. It is a profile of the OASIS (Organization for the Advancement of

Structured Information Standards) Energy Interoperation V1.0 standard, which also defines services for use with two other profiles: TeMIX (for transactive energy) and Price Distribution.

Industry adoption of OpenADR is firmly established in some jurisdictions and is expanding in others. The protocol is supported by many products and OpenADR adapters allow the protocol to be used with additional smart grid devices. Many products that only support proprietary device-level protocols can use a cloud-based ecosystem to translate OpenADR to and from these proprietary messages for interoperation. The growing inclusion of OpenADR in building codes and equipment standards is expected to encourage growth in this area.

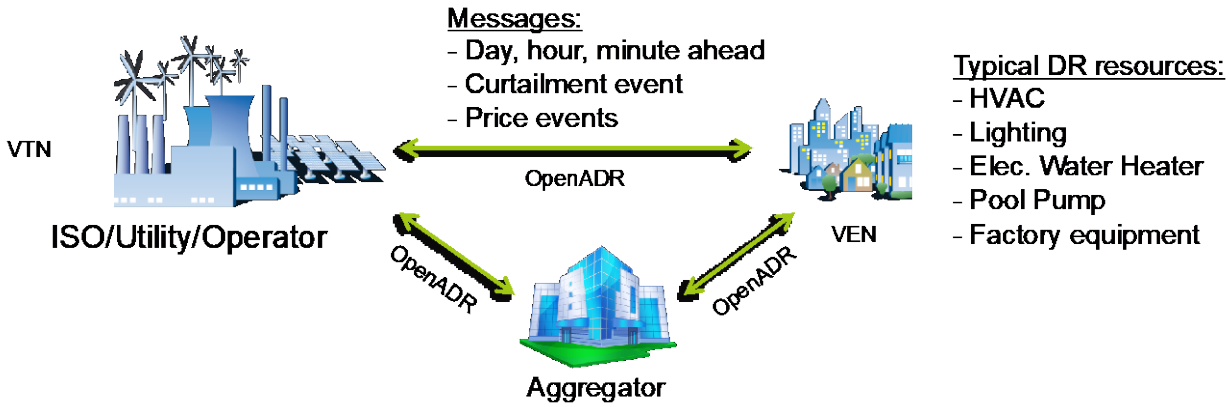


Figure 3-1
Overview of OpenADR Deployments

Technical Overview

OpenADR is a bidirectional application-layer protocol for managing distributed resources. Originally designed for use with Critical Peak Period (CPP) DR tariffs, the current version can support a wide range of programs. The standard defines signals that may direct or motivate desired behaviors, expressing the requests either in grid operations terms (such as absolute or relative power levels) or as descriptions of the state of the grid (using qualitative levels or energy prices, for example). Both telemetry and history reports can be created and exchanged.

The central concept in OpenADR is an "event," which is described by a signal (value), a start time, and a duration. Events can be divided into "intervals" and any number of intervals may be included in a single event (the sum of the durations of the intervals being equal to the duration of the overall event). It is generally assumed that an event will be communicated well in advance of its start time, to give a resource time to prepare (such as by precooling a home or by suitably adjusting appliance run times). After an event is created, it can be subsequently modified or canceled, and event recipients can communicate their decision to opt out of participation in the event (if that is allowed by the DR program in which they are enrolled). OpenADR is typically used to control multiple resources (aggregations or abstractions of devices) rather than directly control the individual devices themselves. This means that the usual recipient of an OpenADR event message is often a residential gateway (Home Energy Management System) or similar controller.

OpenADR communications always occur between pairs of directly connected interfaces, but because these roles can be implemented recursively, OpenADR can implement a hierarchical

tree, with intermediate nodes containing both a server interface connected a client below it in the tree while simultaneously connecting to a client interface on the node immediately above it. For this reason, OpenADR interfaces are called either Virtual Top Nodes or Virtual End Nodes, as shown in Figure 3-1.

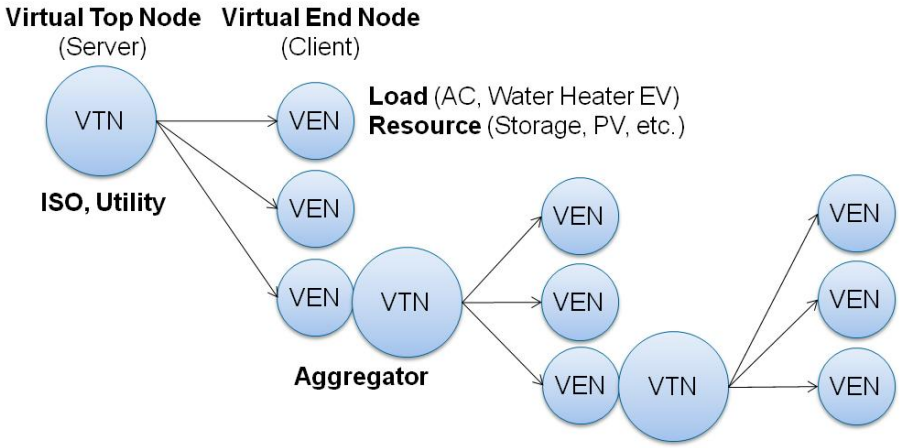


Figure 3-2
Sample OpenADR Hierarchical Architecture

Due to the richness (and consequent complexity) of the full standard (known as "Profile B"), a simplified version (called "Profile A") is also available for use by devices with limited computing power or network capacity. In Profile A, all events use a simple four-level qualitative signal, the meaning of which is defined by the DR program.

Since DR and DER are becoming more common, OpenADR is now being explored to control both loads and inverters. Because OpenADR primarily addresses generalized or aggregated resources (rather than devices), it does not contain information models with detailed device-specific characteristics (settings, load information, power levels, etc.), Rather, it focuses on higher-level grid controls that allow a local management system, owner, or utility to manage their resources via abstract signals, such as grid status and prices.

OpenADR is intended for use in open Internet-based environments and therefore includes specific requirements to ensure the security of the network. Messages exchanged with connected controllers are expressed as encrypted XML (eXtensible Markup Language) and are sent via HTTP (HyperText Transport Protocol) or XMPP (eXtensible Messaging and Presence Protocol). An option for even higher security (XML signatures) is also specified.

OpenADR is commonly used to control loads. Because OpenADR addresses resources, it does not contain information models with detailed device characteristics (load information, power levels, etc.), Rather, it focuses on higher-level grid controls to allow a site management system, owner, or utility to manage the system via high-level signals, such as grid status or prices.

OpenADR is intended for use in open Internet-based environments and therefore includes specific requirements to ensure the security of the network. Messages exchanged with the connected controllers are expressed in encrypted XML and are sent via HTTP or XMPP.

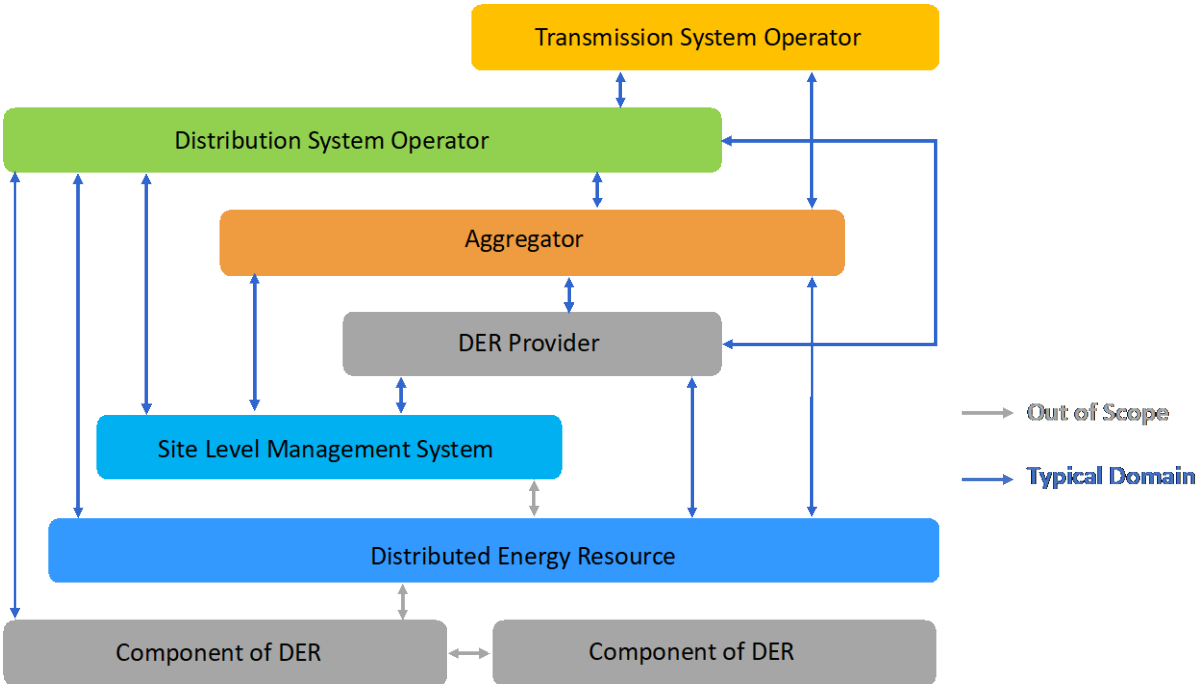


Figure 3-3:
OpenADR Architecture Overview

Example Application: Forecasting a period of stress on the grid, a utility or system operator issues a DR event for the following day, indicating a need for reduced demand during the late afternoon hours. This could be signaled qualitatively (such as by invoking a CPP tariff peak period) or quantitatively (by requesting that a residence reduce its consumption during those hours by a specific amount relative to its usual baseline consumption). The OpenADR signal is received by the resource's energy management system and an appropriate response strategy is invoked. For example, the system may lower the cooling temperature setpoint below its normal setting for the early afternoon (to pre-cool the home), then raise it to an above-normal value during the event period. The device-specific actions performed when responding to the event are usually not explicitly stated in the OpenADR message (though they may be for common devices like thermostats).

Adoption

OpenADR is a profile (subset) of the OASIS Energy Interoperation standard and has been approved as an IEC standard (IEC 62746-10-1) in 2019. It has seen broad adoption in California (where it was created) and in Japan. It is also used when a generic, open standard is desired for integrating a heterogeneous mix of devices, such as in many "bring your own thermostat" programs. Furthermore, OpenADR is being required as part of other standards, such as AHRI's forthcoming 1380P standard for variable-speed HVAC equipment, "Methods for Coordinated Energy Management in Residential Applications," and in California's Title 24 building code related to nonresidential HVAC Controls, Lighting Controls, and Electronic Messaging Center Controls. Recently, the British Standards Institution (the national standards body of the UK) mandated the use of OpenADR in its latest Publicly Available Specification for Energy Smart Appliances (BSI PAS 1878:2021).

Devices and Technologies

The targets for OpenADR are often aggregated DR resources, not individual devices. Hence, many of the certified products are gateways, controllers, and other types of energy management systems. Devices that implement OpenADR, either internally or via an external control unit (such as a CTA-2045 UCM) can also be certified. OpenADR can also be used to communicate with vendor clouds to manage DR functionality for proprietary devices such as connected thermostats.

Many OpenADR-capable products are available in the market. The OpenADR Alliance lists more than 240 certified products on its website (https://products.openadr.org).

Implementation

OpenADR services are expressed as XML messages and are usually transported over HTTP running on a TCP/IP network stack (very similar to how the worldwide web operates). An alternative, lighter weight method that uses XMPP networking is also included in the specification. A guide containing information for utilities on how to implement OpenADR for various DR and DER scenarios can be obtained from the OpenADR Alliance (www.openadr.org/dr-program-guide).

Test Tools and Certification

The OpenADR Alliance runs the official certification program for OpenADR products; information on the program is available from the Alliance (www.openadr.org/certification-process). To assist companies in the development of OpenADR 2.0-compliant products, the Alliance has engaged a test tool partner, QualityLogic (www.qualitylogic.com). Useful during development and required for certification testing, more information on the QualityLogic tool is available from the Alliance (www.openadr.org/openadr-test-tool).

Cyber Security

To be certified, an OpenADR product must implement Transport-Layer Security (TLS, also called "Secure HTTP"). OpenADR clients and servers (called "VENs" and "VTNs," respectively) use PKI certificates for authentication. However, the security requirements for any specific deployment may be established by agreement among the participants. For example, the BSI PAS requires the use of OpenADR's "high security" option that uses XML signatures to secure all or part of the XML message payloads. It also specifies the use of Transport Layer Security version 1.3, which was defined in August 2018 (after the most recent OpenADR specification had been published).

Regulatory Framework

OpenADR has been required by California's CPUC for several years, and the current revision of California's building codes mandates its use starting in 2020. Japan has used OpenADR since 2013 in utility-to-aggregator communications for both DR and DER (PV curtailment). In March 2021 BSI issued its PAS 1878, which describes the requirements for energy smart appliances in the UK, along with a companion document describing the practices for DR with which it is intended to be used. The BSI specifications are part of a national initiative to advance the secure, interoperable, and functional use of smart appliances, including smart electric vehicle charge points, for the active control of electricity demand on the UK grid.

Governance and Maintenance

OpenADR is a profile (subset) of the OASIS Energy Interoperation standard and has been approved as an ANSI standard (IEC 62746-10-1). Although OpenADR's "parent" standard (Energy Interoperation) is maintained by OASIS, the OpenADR Alliance, an industry consortium, maintains the OpenADR specification itself. The OpenADR Alliance coordinates working groups to review and update the specification as needed.

The most recent OpenADR specifications were released in 2013 (Profile A, V1.0) and 2015 (Profile B, V1.1). Although the Alliance is currently considering extensions to improve how the protocol might address DER management, any changes are expected to take the form of an addendum, leaving the base protocol definitions unchanged. Copies of the OpenADR specifications are available at no cost from the OpenADR Alliance (www.openadr.org/specification) or, for a fee, from the IEC (https://webstore.iec.ch/home).

Relevant EPRI Reports

- *Communication Protocol Mapping Guide 1.0, OpenADR 2.0 to ANSI/CTA-2045-A: Requirements for Exchanging Information Between OpenADR 2.0 Clients and ANSI/CTA-2045 Technologies*. EPRI, Palo Alto, CA: 2019. 3002008854.
- *OpenADR 2.0 Open Source Virtual Top Node (VTN) User's Manual.* EPRI, Palo Alto, CA: 2017. 3002011483.
- *Residential Battery Energy Storage: Demand Response Opportunities with OpenADR 2.0b—Field Deployments and Performance Analysis*. EPRI, Palo Alto, CA: 2020. 3002017985.
- *Embedded System Security Assessment: Kyrio OpenADR Evaluation Kit—Information and Communications Technology and Security Architecture for Distributed Energy Resources Integration.* EPRI, Palo Alto, CA: 2018. 3002014145.
- EPRI's Distributed Energy Resources Testbed and Toolkit: An Overview of EPRI Test Tools for DER Integration. EPRI, Palo Alto, CA: 2019. 3002016138.

IEEE 2030.5

The original form of Zigbee (1.0) was a suite of high-level protocols for low-power mesh networks based on IEEE 802-15.4 intended for home automation and similar local applications. The enhanced version of Zigbee, Smart Energy Profile (SEP 2.0) was standardized as IEEE 2030.5. It operates over TCP/IP and adopts many of the device models from IEC 61850 to provide a wide-area protocol for DER communications. While most attention currently relates to its selection as the default protocol for California's Rule 21, 2030.5 also includes "function sets" for price communications and DR (among others).

The history of IEEE 2030.5 has been a subject of some confusion. The protocol started out as "Zigbee Smart Energy 1.x," a widely deployed Home-Area Network (HAN) for the smart grid. As a local HAN protocol (only) it was limited by its use of a single underlying network technology (IEEE 802.15.4 wireless technology at 2.4 GHz running the Zigbee PRO stack). It was subsequently revised to be transport layer-agnostic and ported to run on the TCP/IP stack, emerging as "Zigbee Smart Energy Profile 2" in 2008. The IEEE subsequently adopted this as its standard 2030.5 in 2013. The 2018 version of the standard incorporates both California Rule 21 and IEEE 1547-2018 functionality.

IEEE 2030.5 is an application layer specification formerly referred to as SEP 2.0. It was developed as a secure communication protocol to integrate consumer's smart devices into the smart grid, including smart loads, electric vehicles, and distributed energy resources (DERs). The protocol reduces communications architectural challenges by using the familiar Internet Protocol (IP) and supporting a variety of protocols at the physical layer (including Ethernet, Wi-Fi, powerline communications, and low-power radio technologies).

IEEE 2030.5 includes "function sets" for price communication and for DR/DLC. Its information model is derived from IEC 61850-7-420 and the *Common Functions for Smart Inverters* (EPRI 3002008217, 2017).

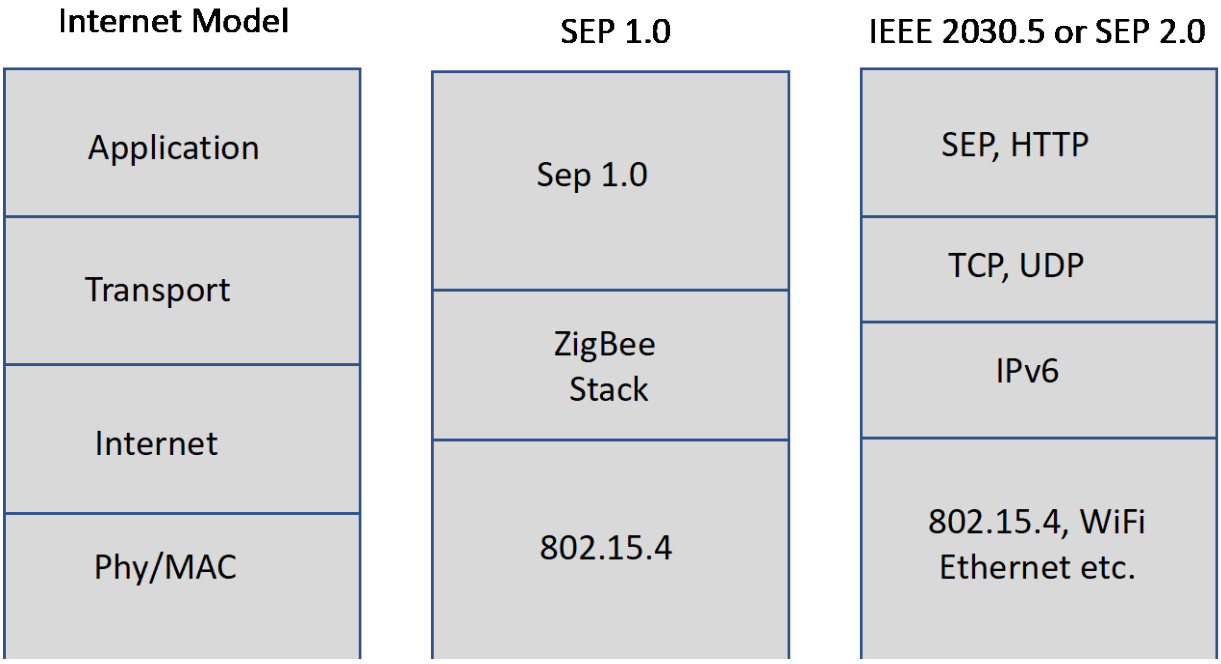


Figure 3-4
The structure of SEP 1.0 and IEEE 2030.5 (SEP 2.0) compared to the Internet Model (TCP/IP)

IEEE 2030.5 is one of the standard device-level communication protocols listed in the most recent version of IEEE 1547. Presently, no DR vendors support IEEE 2030.5 natively. Therefore, network gateway devices must be used at the DER to adapt from 2030.5 to local DR resources. In California, IEEE 2030.5 has been selected as the default application-level protocol for communications between a utility and an aggregation for controlling inverters. This is captured in the California grid code, Rule 21. The California IOUs, through the California Smart Inverter Profile (CSIP), envisions three different scenarios for using IEEE 2030.5 to communicate with DER: 1) direct-to-inverter communications; 2) inverter communications mediated by an energy management system controlling the DER; and 3) inverter communications mediated by a DER operator/aggregator. In the architectural diagram below, IEEE 2030.5 is not listed as a protocol between utilities and aggregators because the protocol does not currently support management of DER groups (aggregated control of DER), only pass-through messaging. Pass-through messaging is the model applied in California. If aggregation is used, IEC 61968-5 Distributed Energy Operation is a better fit architecturally because it is purpose-built to support aggregation

(DER groups) for internal system-to-system communication including DERMS-to-DMS or utility-to-third party aggregation.

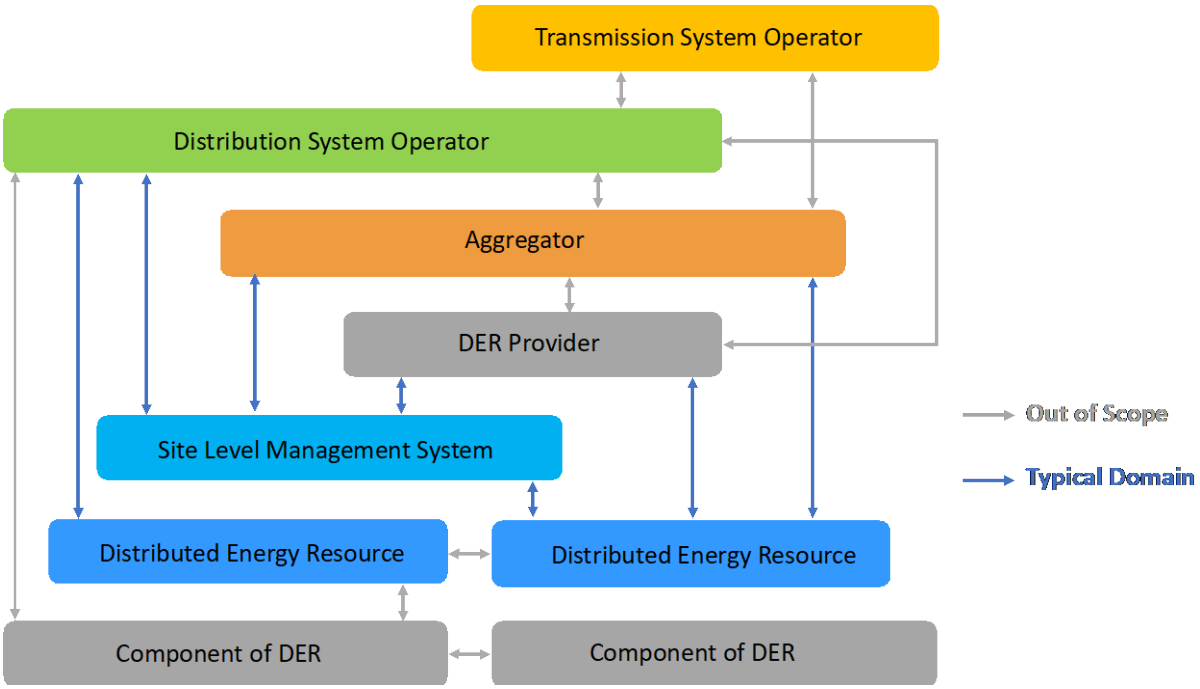


Figure 3-5
IEEE 2030.5 Architecture Overview

Adoption

IEEE 2030.5 has attracted much attention due to being one of the DER device-level communication protocols listed in the most recent draft of IEEE 1547. However, it has yet to see significant use for DR. It is premature to discuss adoption of this protocol because 2030.5's application (even for DER) is relatively new. Several California utilities have conducted laboratory testing using IEEE 2030.5 to evaluate its smart inverter functions. One of the IOUs is conducting a pilot project to demonstrate its application to DER. No demonstrations of its use for DR or DLC have been identified thus far.

Devices and Technologies

IEEE 2030.5 supports a variety of consumer devices, including energy storage, load control devices (like thermostats), electric vehicles, pool pumps, water heaters, energy management systems such as HEMS (Home Energy Management Systems), aggregators, and cloud servers.

Implementation

IEEE 2030.5 uses a client-server network architecture. The server hosts the necessary device information, which is accessed using "polling" or "subscription/notification" patterns. The most common (and simpler) of these is polling. IEEE 2030.5 clients use REpresentational State Transfer or "RESTful" web services (HTTP) or Message Queuing and Telemetry Transport (MQTT) to access the information on the server.

IEEE 2030.5 uses XML for encoding its commands and data. Schemas specify how to format and label data in the XML files so it can be recognized by participating systems. In XML, the content is made human readable because both the measurement values and their metadata (labels) are included in the messages.

IEEE 2030.5 uses the Internet Protocol (IP) and supports a variety of protocols at the physical layer (including Ethernet, Wi-Fi, powerline communications, and a variety of low-power radio technologies). This may reduce the architectural challenges for utilities when designing systems to communicate with consumer devices.

Test Tools and Certification

QualityLogic (www.qualitylogic.com) is the primary provider of industry test software and capabilities for IEEE 2030.5. QualityLogic's IEEE 2030.5 Test System consists of four test suites: Ad Hoc Testers for IEEE 2030.5 clients and servers and Functional Test Suites (FTS) for IEEE 2030.5 clients and servers.

Functional Test Suite V2.0 implements 101 server and client tests defined by the Consortium for SEP 2 Interoperability, Test Specification V1.0. The Ad Hoc Testers are designed to support interoperability testing. They are reference implementations of the IEEE 2030.5 client and server functions defined by the IEEE specification. These include functions such as direct load control, price communication, messages to energy control systems and their owners, availability and settings, etc.

Cyber Security

A complete implementation of the IEEE 2030.5 communication stack also includes all the mandated cybersecurity features specified in the standard. This ensures that all transactions between clients and servers are secured using HTTP over TLS (also called HTTPS). All IEEE 2030.5 devices use digital certificates to authenticate their identity. Once authenticated by a server, devices can access different resources in the server based on their identity and the permissions associated with that identity. All data transactions between the server and device are encrypted at the transport layer using a secure cipher suite.

Regulatory Framework

IEEE 2030.5 is one of the approved protocols in IEEE 1547. Also, IEEE 2030.5 has been designated as the default application-level protocol in California's grid code for DER, Rule 21. Both of these focus on distributed resources used for generation. This is creating broad industry support for the standard, including improved software development capabilities, greater industry experience using the protocol, and its implementation in utility control systems. This may indirectly lower barriers to the adoption of the protocol for demand response.

Governance and Maintenance

The IEEE 2030.5 standard is owned and managed by the IEEE. The IEEE 2030.5 Working Group ensures proper governance, providing a fair and open opportunity to all interested stakeholders to participate in the process of maintaining and evolving the specification. As with other IEEE standards, the update processes used are rigorous, transparent, and well planned. An update is initiated by the IEEE and the process is carried out through the dedicated working group.

The Connectivity Standards Alliance is the recently rebranded Zigbee Alliance founded in 2002. It focuses on SEP 1.0, which remains wedded to IEEE 802.14.5 mesh networking. Therefore, the Zigbee Alliance's work would not be relevant outside the HAN environment.

Relevant EPRI Reports

- *PG&E Case Study – Attack Models and Security Gaps in Distributed Energy Resource Interoperability Standards: IEEE 2030.5 and 1547 Security Gaps, Impact Scenarios, and Mitigations.* EPRI, Palo Alto, CA: 2019. 3002016040.
- *Cyber Security Assessment IEEE 2030.5 Protocol for Distributed Energy Resource Integration.* EPRI, Palo Alto, CA: 2020. 3002019255.
- *IEC 61968-5 Distributed Energy Optimization to Open Field Message Bus (OpenFMB) Mapping.* EPRI, Palo Alto, CA: 2019. 3002016145.
- *EPRI's Distributed Energy Resources Testbed and Toolkit: An Overview of EPRI Test Tools for DER Integration.* EPRI, Palo Alto, CA: 2019. 3002016138.
- *EPRI's Distributed Energy Resources Integration Toolkit: An Overview of EPRI Tools for Testing and Implementing Open Protocols.* EPRI, Palo Alto, CA: 2018. 3002013623.

ANSI/CTA-2045 ("EcoPort")

Technical Overview

As shown in Figure 3-6, ANSI/CTA-2045 is a "modular communications port" standard that defines interface requirements for (1) a smart energy device (called a "Smart Grid Device" by the standard, typically a load) and (2) a communication module that plugs into and communicates with the device over the CTA-2045 physical port. Compared to other protocols designed to transport and exchange data between machines connected to a shared network, ANSI/CTA-2045 focuses on information exchange between the module and the smart energy device to which it is connected. The intent of the standard is to provide a means by which device manufacturers may reduce their risk of embedding a network technology into their products that may change over the life of the product.

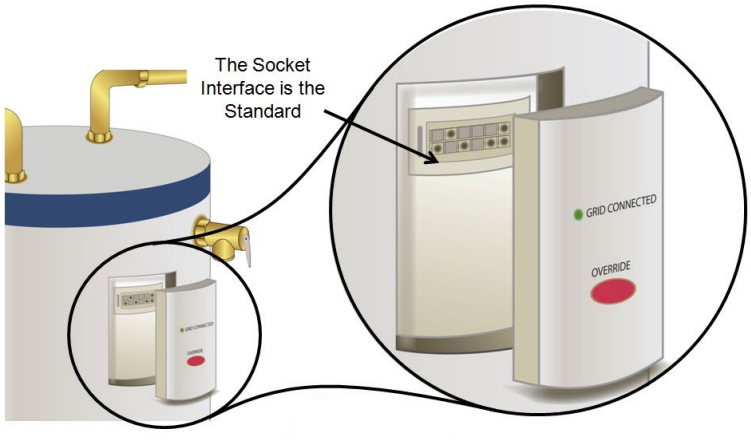


Figure 3-6
The Modular Approach of CTA-2045

The CTA-2045 module, referred to as a "Universal Communication Module" or UCM, provides the means for networks to be connected to the resource. It's important to note that the CTA-2045 standard does not specify or presume anything about this network. In practice, communication modules have been built to bridge CTA-2045-connected resources to networks such as Wi-Fi, cellular, and AMI, using application-layer protocols including OpenADR or proprietary protocols.

Officially called the "Modular Communications Interface for Energy Management," the CTA-2045 standard was first released in February 2013 by the Consumer Electronics Association (which has since become the "Consumer Technology Association"). It was created by a consortium of stakeholders to provide a single, standardized interface for smart grid-enabled devices. Since connectivity for shared networks is implemented in the UCM, device manufacturers need only design, manufacture, and distribute equipment with one standard communications capability (CTA-2045), regardless of the network to which the device will eventually be connected. This is intended to protect buyers (and manufacturers) from obsolescence as new networks and protocols emerge and allows equipment to be switched between different programs and geographies merely by replacing the UCM.

CTA-2045 defines two form factors to accommodate a large variety of devices. The AC form factor can support power line carrier and higher power communication technologies, while a more compact DC-based socket and plug combination is used for lower-power RF networks.

CTA-2045's physical connection to a DER allows it to the be a mechanism for entities upstream of a DER to communicate with the DER. The information models include detailed device information (load information, power levels, etc.) but also include higher-level grid controls to allow a site management system, owner, or utility to manage the system via abstract signals, such as grid status or prices. The information models apply to the connection between the CTA-2045 UCM and the smart energy device. Other protocols can be used between the UCM and the upstream entity.

CTA-2045 is not a networking protocol like IP, it is a machine interface protocol. CTA-2045 only defines requirements for the form factors and for communications between a module and the DER to which it is physically connected. The diagram below shows CTA-2045 as used between upstream entities (aggregator, DER provider, or distribution system operator) and the DER, but it is important to note that this scenario relies on other communications standards to fully implement the connection between the upstream entity (such as an aggregator) and the DER.

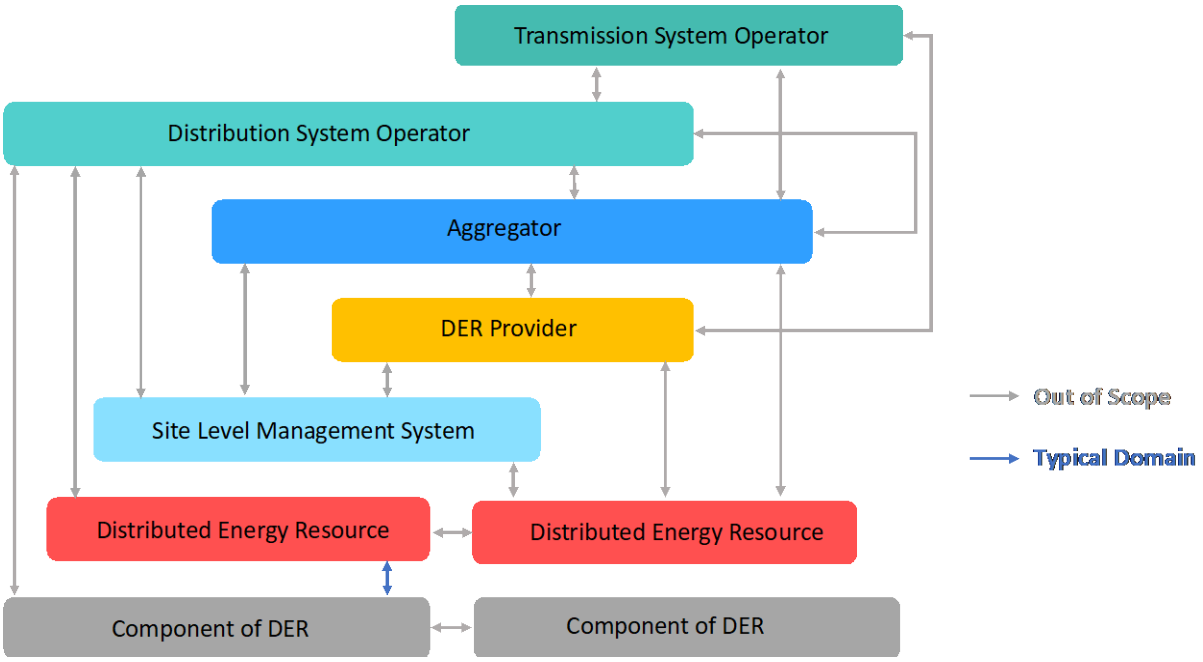


Figure 3-7
ANSI/CTA-2045-B Architecture Overview

Adoption

Starting in 2019, adoption of the CTA-2045 standard has seen exponential growth across the industry. The following table includes links to state laws, standards, and specifications that depend on this standard.

Table 3-1
CTA-2045 State Laws, Standards, and Specifications

Entity/Source	Title
Northwest Energy Efficiency Alliance	Advanced Water Heater Specification
Consortium of Energy Efficiency	CEE Residential Water Heating Specification
Air-Conditioning, Heating, & Refrigeration Institute	AHRI 1380 (I-P) Demand Response through Variable Capacity HVAC Systems in Residential and Small Commercial Applications
Environmental Protection Agency's ENERGY STAR® Program	ENERGY STAR® Program Requirements Product Specification for Residential Water Heaters Eligibility Criteria Version 3.3 Draft 2
Washington State	House Bill 1444 APPLIANCE EFFICIENCY STANDARDS
California Energy Commission	Appendix JA13 – Qualification Requirements for Heat Pump Water Heater Demand Management Systems

With the growing adoption of CTA-2045, there has come new interest in increasing the visibility of the standard and developing a testing certification program. The OpenADR Alliance has recently announced that it will be taking the lead for these activities for CTA-2045. The

Consumer Technology Association will continue to the standards organization that owns the standard. As part of this new initiative, there will be an introduction of a new name for CTA-2045-enabled devices: in the future, the connector will be known as *EcoPort*.

Devices and Technologies

The target for CTA-2045 is residential and light-commercial smart-grid resources. It supports a mixture of generic and device type-specific commands. Smart inverters are also supported by the standard through pass-through of the SunSpec Modbus protocol.

The modular approach of CTA-2045 requires two components for the system to work: a UCM and the DER. These two may be supplied from the same vendor/manufacturer or supplied separately.

Smart-Grid Devices: CTA-2045 products started to become available in 2016. Some CTA-2045-equipped products are available in the market through big box stores. Others are available on request directly from manufacturers. UL-certified products, including pool pumps, thermostats, electric vehicle supply equipment (EVSE), packaged terminal air conditioners (PTACs), water heaters (HPWH and resistive), and load switches, available today. Six manufacturers—some with significant market share in their industry—support CTA-2045 in at least one of their models.

UCMs: Communications modules available today are supplied by three manufacturers. The communications technologies supported are Wi-Fi and FM Radio Data System (RDS). Some vendors are looking to support cellular. Since the communication technologies are dependent on program requirements, it is expected that more modules will become available in the market as more utility programs adopt CTA-2045.

Implementation

The standard defines the application-layer, link-layer, physical layers (RS-485 or Serial Peripheral Interface, SPI), electro-mechanical specifications of the connectors, and the dimensions of the UCM and socket for the two different types of communication modules. A CTA-2045 implementation includes the physical/media access layers (the AC or DC form-factor interfaces); a data link layer that provides link handling, ACK/NAK, error codes, negotiation (of speed, message length, and power), bit-error detection and retries, and basic DR messages at the network and application layers. It also can pass unmodified messages from other network protocols (such as IEEE 2030.5, OpenADR, or proprietary) through to the device.

Test Tools and Certification

Starting in 2021, the first independent ANSI/CTA-2045 certification service will be available to the industry through the OpenADR Alliance. EPRI has produced a general CTA-2045 software simulator, a water heater simulator, test cables, open-source implementations containing schematics and source code, and tools to aid in the development and testing of ANSI/CTA-2045 products.

Cyber Security

CTA-2045 is not a networking protocol; rather, it is a device interface protocol. It only defines requirements for the form factor and communications between a module and device that are

physically connected to each other. Hence, it is claimed that there is no need for cyber security (though this is disputed by cybersecurity specialists).

Regulatory Framework

CTA-2045 is referenced in AHRI-1380 (variable capacity heat pumps), NEEA specifications (heat pump water heaters), CEE initiatives (water heaters and pool pumps), Washington HB 1444 - 2019-20 (water heaters) and Energy Star (water heaters). The state of Oregon has filed administrative order 330-092-0020(17) which requires that electric storage water heaters have a communication port compliant with the CTA-2045 standard. This order will go into effect in September 2021.

Governance and Maintenance

The standard is governed by the Communications Technology Association (CTA), an ANSI-accredited standards development organization and the sponsors of the annual Consumer Electronics Show in Las Vegas. The standard is under the jurisdiction of the "Consumer Electronics Networking Committee for Energy Management Working Group 1 - Modular Communication Interface."

The most recent release of the core standard, ANSI/CTA-2045-B, was published in February 2021. Related standards include ANSI/CTA-2045.2 ("Modular Communications Interface for Firmware Transfer Message Set") and ANSI/CTA-2045.3 ("Modular Communications Interface for Thermostat Message Set"). An emerging ANSI/CTA-2045.4 is expected define how compliant modules will be able to communicate with the outside world via TCP/IP, either locally through a HEMS or through a third-party cloud. All the standards are available from CTA (www.cta.tech).

Relevant EPRI Reports

- *ANSI/CTA-2045-A Water Heater Test Procedures: Information Exchange and Demand Response.* EPRI, Palo Alto, CA: 2019. 3002016940.
- *Communication Protocol Mapping Guide 1.0, OpenADR 2.0 to ANSI/CTA-2045-A: Requirements for Exchanging Information Between OpenADR 2.0 Clients and ANSI/CTA-2045 Technologies.* EPRI, Palo Alto, CA: 2019. 3002008854.
- *Performance Test Results: CTA-2045 HVAC Thermostat: Testing Conducted at the National Renewable Energy Laboratory.* EPRI, Palo Alto, CA: 2017. 3002011747.
- *Performance Test Results: CTA-2045 Water Heater: Testing Conducted at the National Renewable Energy Laboratory.* EPRI, Palo Alto, CA: 2017. 3002011760.
- *Performance Test Results: CTA-2045 Electric Vehicle Supply Equipment—Testing Conducted at the National Renewable Energy Laboratory.* EPRI, Palo Alto, CA: 2017. 3002011757.

4
MESSAGING SERVICES ("MIDDLEWARE")

Many application protocols make use of additional application-layer software to facilitate communications. These "helper" technologies are often called "middleware" because they mediate between the functional applications and the lower layers of the network. They may provide services like message addressing and routing, error handling, or resource discovery. Such "helper" technologies will be referred to as messaging services in this report.

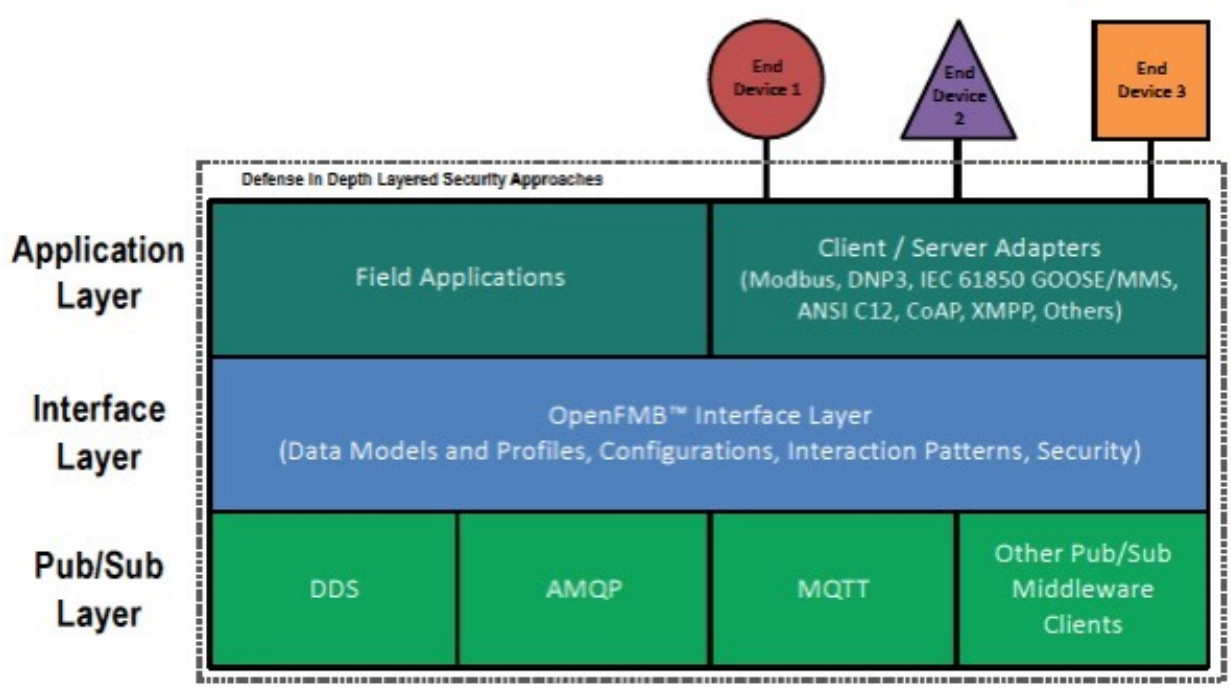
One common example of such a messaging service, HTTP (HyperText Transport Protocol), is widely used with client-server network architectures. With HTTP, a client system (such as a Web browser) sends a request to a server (such as a Web site), which responds with both the appropriate functional information as well as various status (completion or error) codes.[4] The use of HTTP allows functional protocols to use simple commands to send and receive information, without being concerned with the details of establishing connections between systems and processing communication errors. HTTP is one of the most important protocols on the Internet today (it is the basis of the World Wide Web) and it is also widely used by other applications.

The choice of messaging software can have a significant impact on the processing and communications burdens placed on edge devices. HTTP is a stateless protocol, meaning that the server does not retain information about clients between requests. However, HTTP messages are usually sent over TCP, and TCP always creates sessions between systems when exchanging messages. Therefore, the TCP layer must create a new session for every HTTP message exchange, which is expensive in terms of power and bandwidth and introduces communication delays.

Open Field Message Bus (OpenFMB), shown in Figure 4-1, is a logical bus that may use various middleware protocols Rather than client-server, the OpenFMB logical bus emphasizes the use of publish/subscribe integration patterns so that devices, such as those located in a residence, can "talk" directly to each other. OpenFMB facilitates such distributed intelligence by moving decision-making closer to the point of application.

OpenFMB includes several existing standard middleware technologies in its design. Four of these with potential relevance for residential DR are discussed in the following section: CoAP, XMPP, DDS, and MQTT.

[4] The mode of interaction in which the client system initiates the information exchange by sending a request to the server is called "pull" mode. If the client system is willing to expose its public IP address, then the server can initiate data exchanges (this is called "push" mode). Due to security concerns, HTTP is mostly used in "pull" mode.



Source: NAESB RMQ.26 Open Field Message Bus (OpenFMB) Model Business Practices

Figure 4-1
Open Field Message Bus (OpenFMB™) Architecture, Containing Several Middleware Components

Definition of a Messaging Service

A messaging service is one of several sets of rules and procedures that a controller and an end-use device both follow when communicating with each other. Messaging services provide mechanisms for addressing and routing messages that contain the application protocol commands and information being sent between a controller to an end-use device.

The overall automation and control protocol stack defines the following minimum layers:

1. The physical transport layer (i.e., wired, wireless, PLC, etc.)
2. The logical link layer between the two communicating devices (this layer checks that the digital signal that reaches either endpoint is error-free)
3. A network layer (this defines an addressing system that allows a controller to communicate with multiple end-use devices by using their unique network addresses)
4. An application layer, which defines "objects" to represent the different attributes of the end-use devices that are to be controlled and "services" to manipulate the objects to change the operational status of an end-use device (e.g., turn on/turn off, dim, raise temperature, etc.)

Like the automation and control protocol itself (the functional commands), messaging services also occupy the application layer, where they make use of the underlying network layers to direct the protocol messages to the proper recipients.

As in Section 3 above, each service description in this section contains information on up to nine key criteria. These were selected to present a comprehensive overview of the service in a way that makes it easy to compare one service to another. The following criteria are used:

- **Technical Overview:** A high-level description and a brief history of the service, this may contain an example of an implementation of the service to help the reader understand its context and application.
- **Adoption:** A summary of how widely the service is used (including any insights about why this is the case), this also provides information about the number of products on the market today. It includes use in products ranging from individual devices to control systems.
- **Devices and Technologies:** An overview of the types of devices supported by the service and the type of functions it supports (direct control or "inform and motivate").
- **Implementation:** A high-level description of how the service works and an assessment of the complexity of the system and general requirements for implementation, this section also highlights any notable dependencies that are associated with using this service.
- **Test Tools and Certification:** A description of currently available test tools and certification processes.
- **Cyber Security Requirements:** An overview of how security is addressed in the service, including whether the service addresses specific security features, this includes version numbers and whether these security requirements are included in conformance testing.
- **Regulatory Framework:** A summary of whether the service is required or suggested as part of grid codes or other regulations.
- **Governance and Maintenance:** This section identifies the entity that manages the standard and reviews potential changes, the process used to update the standard, and information about past, present, or future revisions.
- **Relevant EPRI Reports:** A list of significant EPRI reports related to this service, this may include case studies, lab tests, government work, or other research in this area.

eXtensible Messaging and Presence Protocol (XMPP)

While HTTP provides a very common method of transporting XML-tagged messages, XMPP provides a lighter-weight alternative. In addition to native support for transporting XML content, XMPP also supports additional features, such as service discovery, that may be important in a rapidly changing IoT environment. XMPP uses a client-server model operating over long-lived TCP connections, thereby avoiding the overhead of continually creating new sessions for each message exchange (as is the case with HTTP).

XMPP was formalized as an IETF standard in 2004. The latest version of the core protocol was released in 2015.[5]

For utility applications, the value of XMPP as an alternative to HTTP has been recognized, for example, by OpenADR, which may be transported over either HTTP or XMPP. Although most OpenADR deployments use HTTP, OpenADR servers (called Virtual Top Nodes – "VTNs") are required to support both protocols to be certified as conforming to the specification. Examples of its use are given in the "Adoption" section below.

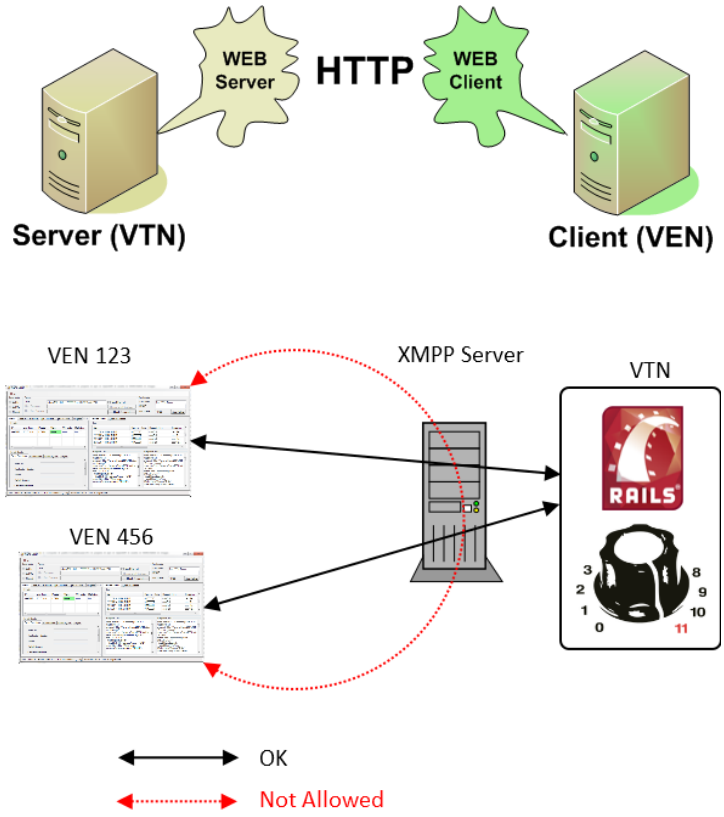


Figure 4-2
OpenADR Running over HTTP (above) and over XMPP (below)

Technical Overview

XMPP enables the exchange of relatively small pieces of structured data (called "XML stanzas") between entities. It is typically implemented using a distributed client-server architecture, wherein a client connects to a server to gain access to the network and thus to exchange XML with other entities. One XMPP server may connect to another server to enable inter-server communication; therefore, the client systems do not need to be directly connected to a server to participate in an exchange (if the servers are connected to one another). In a sense, the architecture of XMPP is similar in many ways to that of email: end-to-end communication in

[5] Internet Engineering Task Force, Extensible Messaging and Presence Protocol (XMPP): Core, RFC 6120 (https://tools.ietf.org/html/rfc6120).

XMPP is logically peer-to peer but physically client-to-server-to-server-to-client, as illustrated in the following diagram.

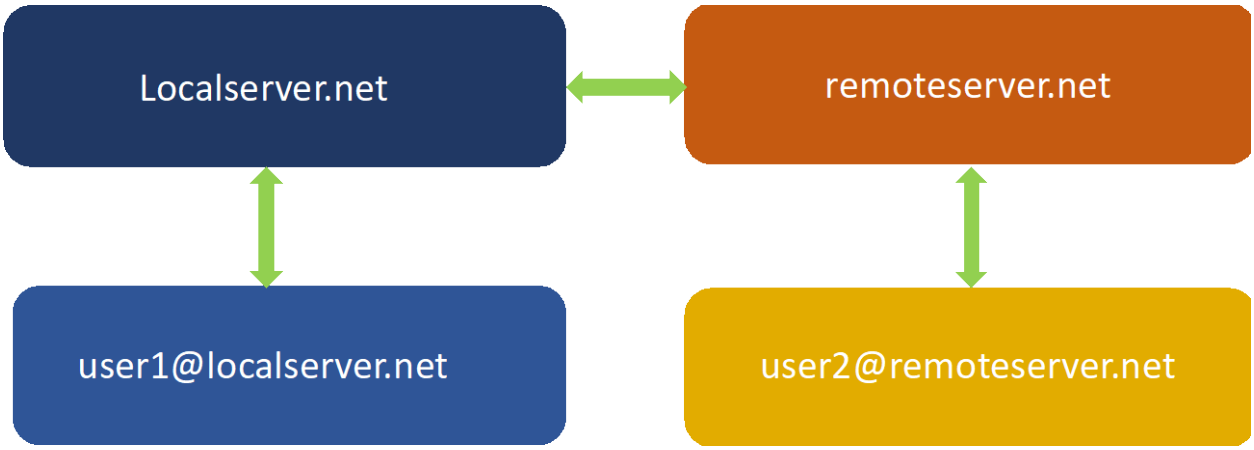


Figure 4-3
XMPP Data Flows for Remote Communications

As its name suggests, XMPP is extensible, and the payloads (XML stanzas) that it can exchange are defined by various XMPP extensions. For example, XMPP-IM[6] is an extension for XMPP that defines basic instant messaging and presence functionality.

Adoption

A European study used OpenADR to implement a Virtual Power Plant (VPP) based on battery charging stations in Germany controlled from a server in Slovenia. In this instance, it was found that OpenADR's HTTP "pull" mode required excessive bandwidth (due to the volume of client requests for information), and push mode raised security concerns (due to the need to expose the client's public IP address information). XMPP in "pull" mode also suffered from increased bandwidth and latency, so the eventual implementation used XMPP in PUSH mode for the OpenADR information exchanges.

Similarly, recent work in Japan on FastADR aggregation used OpenADR's XMPP option to transfer messages from the OpenADR VTN to twenty-five resource aggregators. XMPP is also widely used by such messaging applications as WhatsApp Messenger and Google Talk and is the basis for in-game private chat on PlayStation.

Implementation

XMPP has been used in some of the largest messaging systems, such as WhatsApp and Google Talk. Most of these deployments are built on an open-source XMPP server called ejabberd (a reference to XMPP's original name, "Jabber").

[6] Internet Engineering Task Force, Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence, RFC 6121 (https://tools.ietf.org/html/rfc6121).

Test Tools

Several commercial test tools are available for XMPP, and Apache JMeter can be used with an XMPP Sampler plugin for testing XMPP. with capabilities to test connectivity and performance of servers under load.

Cyber Security

XMPP connections are authenticated with Simple Authentication and Security Layer (SASL) and are encrypted with TLS.

Governance and Maintenance

In addition to the core protocols standardized by the IETF, the XMPP Standards Foundation (formerly the Jabber Software Foundation) actively develops open XMPP extensions. More information on the use of XMPP for IoT applications may be found on the web site of the not-for-profit XMPP Standards Foundation[7].

Relevant EPRI Reports

- *IEC 61968-5 Distributed Energy Optimization to Open Field Message Bus (OpenFMB) Mapping*. EPRI, Palo Alto, CA: 2019. 3002016145.
- *Residential Battery Energy Storage: Demand Response Opportunities with OpenADR 2.0b—Field Deployments and Performance Analysis*. EPRI, Palo Alto, CA: 2020. 3002017985.
- *Program on Technology Innovation: Evaluating IoT Messaging Protocols for DER Management.* EPRI, Palo Alto, CA: 2018. 3002014678.
- *Communication Protocol Mapping Guide 1.0, OpenADR 2.0 to ANSI/CTA-2045-A: Requirements for Exchanging Information Between OpenADR 2.0 Clients and ANSI/CTA-2045 Technologies*. EPRI, Palo Alto, CA: 2019. 3002008854.
- *Lightweight Messaging Technologies for the Energy Internet of Things: An Introduction*. EPRI, Palo Alto, CA: 2018. 3002013478.

Message Queuing and Telemetry Transport (MQTT)

MQTT is an ISO/IEC[8] and OASIS[9] standard for "publish-subscribe" messaging middleware. Like XMPP (and HTTP), it operates over TCP and is designed for use with limited storage (due to its small code footprint) and limited network bandwidth. As with XMPP, MQTT requires the use of a server for exchanging messages, though in the case of a publish-subscribe model, this server is called a "broker."

---

[7] https://xmpp.org/

[8] International Organization for Standardization, Message Queuing Telemetry Transport (MQTT) v3.1.1, ISO/IEC 20922:2016 (https://www.iso.org/standard/69466.html).

[9] OASIS, MQTT Version 3.1.1 Plus Errata 01, 2015 (http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html).

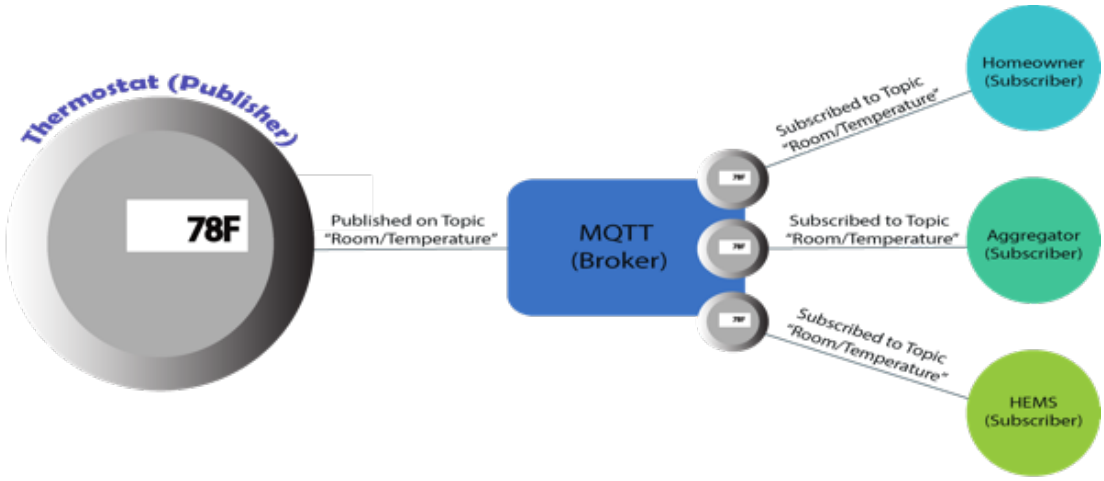


Figure 4-4
MQTT Broker and Publish/Subscribe Architecture

MQTT is well-suited for use in constrained environments as are encountered in Machine-to-Machine (M2M) and Internet of Things (IoT) networks. It is useful in situations that value a small code footprint and/or reduced network bandwidth such as might be encountered at the edges of the integrated grid. Queuing is not actually required to be supported in all situations: the presence of the phrase "message queuing" in the name is a historical artifact.

Technical Overview

The form of publish-subscribe implemented in MQTT requires the use of a message broker to track subscriptions and route messages to interested recipient nodes. There may be more than one broker in an implementation. All client nodes communicate with a broker, which maintains a list of "topics" to which client systems may subscribe. An application that wishes to "publish" some information sends it to the broker and indicates the topic to which relates. The broker then sends the information only to those clients that have subscribed to that topic. In this way, publishers do not need to keep track of the clients and their interests: the broker handles those details. Although a minimal MQTT control message can contain as little as two bytes of data, it can carry nearly 256 megabytes of data. There are fourteen defined message types used to connect and disconnect clients from brokers, to publish data, to acknowledge receipt of data, and to supervise connections between clients and servers.

MQTT is designed to run over network protocols that provide an ordered, lossless, bidirectional communication service, such as TCP. Like DDS, MQTT uses a client-server publish-subscribe interaction pattern. As with any publish-subscribe service, MQTT provides one-to-many message distribution among decoupled applications. And like DSS, MQTT is both agnostic with respect to the message payloads and offers multiple quality-of-service options.

Adoption

The first version of MQTT was written in 1999 and was submitted to OASIS for standardization in 2013. A variation of MQTT that specifically targets sensor networks (MQTT-SN[10]) can be used over lighter weight network protocols, such as UDP or Bluetooth. MQTT is used by the Amazon Web Services IoT offering and for the Microsoft Azure cloud computing IoT Hub service.

When deploying OpenADR in 2016, Austin Energy was concerned about the ability of HTTP to scale to anticipated IoT levels, particularly in terms of network bandwidth. They therefore ported OpenADR to run over MQTT and compared its bandwidth consumption with OpenADR over HTTP (both running in pull mode with 10-second polling). Testing over a 30-day period, they found a dramatic bandwidth reduction of nearly an order of magnitude (from 1,290 MB with HTTP to 152 MB with MQTT).

Implementation

Several implementations of MQTT are available, both commercial and open source. Versions are available written in Python, Erlang, Java, C, and several other languages.

Test Tools

A variety of useful tools are available for use with MQTT, such as MQTT-Spy (open source), MQTT Inspector (for iOS), and mosquito (open source). Others include tools for scalability and load testing, usage and performance measurement, and connectivity checking.

Cyber Security

MQTT sends connection credentials in plaintext and does not include any measures for security or authentication. Effective cyber security capabilities can be provided by the underlying TCP or UDP transport layers using standard measures for protecting the integrity of transferred information from interception or duplication and by the security mechanism of the infrastructure hosting the MQTT broker, such as the operating system or a firewall.

Governance and Maintenance

The original development of MQTT was done by IBM and Cirrus Link. It is now maintained by OASIS and the IEC.

Relevant EPRI Reports

- *Program on Technology Innovation: Evaluating IoT Messaging Protocols for DER Management.* EPRI, Palo Alto, CA: 2018. 3002014678.
- *IEC 61968-5 Distributed Energy Optimization to Open Field Message Bus (OpenFMB) Mapping.* EPRI, Palo Alto, CA: 2019. 3002016145.
- *Low-Power Wide-Area Networks: Overview, Characteristics, and Applications.* EPRI, Palo Alto, CA: 2018. 3002019791.

---

[10] International Business Machines, MQTT for Sensor Networks (MQTT-SN) Protocol Specification, Version 1.2, 2013 (http://mqtt.org/new/wp-content/uploads/2009/06/MQTT-SN_spec_v1.2.pdf).

- *Remote Device Management: Utility Requirements*. EPRI, Palo Alto, CA: 2019. 3002015875.
- *Lightweight Messaging Technologies for the Energy Internet of Things: An Introduction*. EPRI, Palo Alto, CA: 2018. 3002013478.

Constrained Application Protocol (CoAP)

An Internet standard[11], CoAP was designed for use on low-power devices connected to unreliable networks of the sort that might be encountered at the edges of the integrated grid. It uses protocols like those in the general Internet and allows communications between nodes on the CoAP network and nodes on the general Internet. It can also use the Internet to bridge between CoAP networks. Intended for use with wireless sensor networks, CoAP sends simple binary messages over UDP. The fixed format of the four-byte-long CoAP message header greatly simplifies information extraction.

In many ways, CoAP might be considered as a lightweight alternative to HTTP (HyperText Transport Protocol) that forms the basis of the World Wide Web. Like HTTP, CoAP is based on the REST (REpresentational State Transfer) model in which servers make resources available via a URL, and clients access these resources. Because of this similarity, CoAP feels very much like HTTP (to a software developer): for example, the code required to obtain a value from a sensor would not be much different from that used to obtain a value from a Web location. Since CoAP is agnostic with respect to the payload it is carrying (as is HTTP), it can be used with messages represented as XML, JSON, or any other data format.

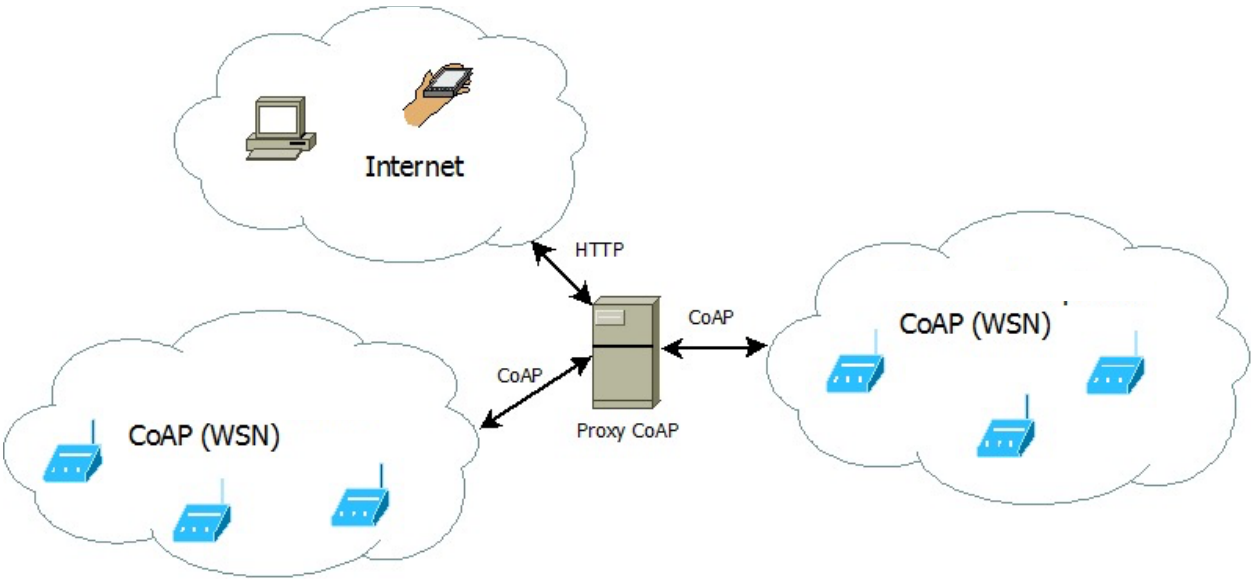


Figure 4-5
Communications between a CoAP Network and the General Internet

[11] Internet Engineering Task Force, The Constrained Application Protocol (CoAP), RFC 7252 (https://tools.ietf.org/html/rfc7252).

Although CoAP uses a simple request/response message exchange pattern, it reverses the usual assignment of client and server: the CoAP server instance is installed on the end node, while the CoAP client resides on the controller node (which typically manages several end nodes). A mapping has been defined between CoAP and HTTP, allowing standardized access to CoAP resources via HTTP.

Technical Overview

CoAP is a specialized messaging service for constrained devices. It enables those constrained devices to communicate with the wider Internet using similar protocols. CoAP is designed for use in three scenarios:

- between devices on the same constrained network (particularly low-power, lossy networks)
- between devices and general nodes on the Internet
- between devices on different constrained networks when both are connected by an internet

CoAP is also being used in other situations, such as SMS on mobile communication networks.

CoAP is intended for use in resource-constrained internet devices, such as wireless sensor network nodes, and is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity. Efficiency is very important for Internet of Things (IoT) and Machine-to-Machine (M2M) devices, which tend to be deeply embedded and have much less memory and power available than traditional internet devices. Multicast messaging, low overhead, and simplicity are extremely important for use in such applications.

The CoAP messaging model is based on the exchange of messages between endpoints. The interaction model is like the client/server model of HTTP: a CoAP request is equivalent to that of HTTP and is sent by a client to request an action from a resource on a server. The server then sends a response. But unlike HTTP, CoAP deals with these interchanges asynchronously over a datagram-oriented transport such as UDP (CoAP can run on most devices that support UDP or a UDP analogue). Figure 4-6 below compares HTTP with CoAP from a network layering perspective.

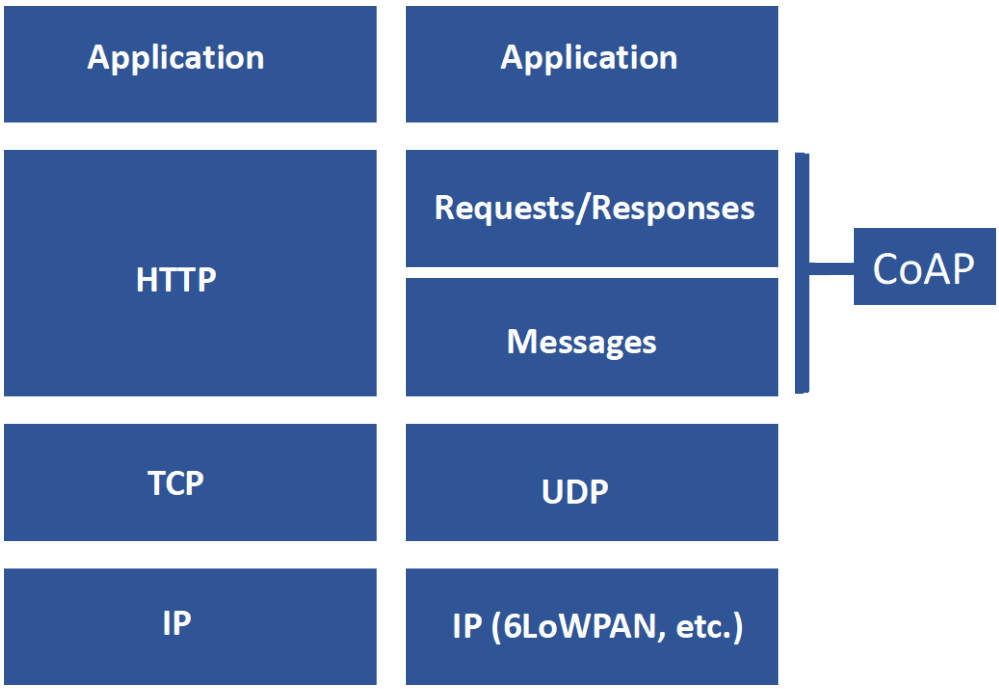


Figure 4-6
Comparison of Network Layering for HTTP (left) and CoAP (right)

CoAP is based on the exchange of compact messages that, by default, are transported over UDP (i.e., each CoAP message occupies the data section of one UDP datagram). CoAP may also be used over Datagram Transport Layer Security (DTLS). It can also be used over other transports such as SMS, TCP, or SCTP (Stream Control Transmission Protocol, which provides some of the features of both UDP and TCP and is defined in RFC 4960[12]).

Some CoAP application scenarios require the ability to address several CoAP resources as a group, instead of addressing each resource individually. For example, when turning on all the CoAP-enabled lights in a room, it would be preferable to use only a single CoAP request triggered by toggling the light switch. To address this need, the IETF has developed an optional extension for CoAP in the form of an experimental RFC describing group communication for CoAP[13].

Adoption

Although it is less than ten years old, more than thirty CoAP implementations are already in existence. Multiple versions are available written in C, Java, Python, Go, and several other languages.

---

[12] Internet Engineering Task Force, Stream Control Transmission Protocol, RFC 7252 (https://tools.ietf.org/html/rfc4960).

[13] Internet Engineering Task Force, Group Communication for the Constrained Application Protocol (CoAP), RFC 7390 (https://tools.ietf.org/html/rfc7390).

Devices and Technologies

CoAP is designed to meet the special requirements of constrained computing environments, especially as might be encountered in energy, building automation, and other machine-to-machine (M2M) applications. For example, CoAP could readily be used with messages that do not require reliable transmission (for example, to send each single measurement in a stream of sensor data). It has been designed to work on devices with as little as 10 kB of RAM and 100 KB of code space.

Implementation

CoAP is based on the exchange of messages over UDP between endpoints. CoAP request and response information is carried in CoAP messages that include either a Method Code (request) or Response Code (reply). Optional (or default) request and response information, such as the URI and payload media type are carried as CoAP options. A Token is used to match responses to requests independently from the underlying messages.

Test Tools

Interoperability tests for CoAP have been defined by the ETSI plugtest organization. Californium (a Java CoAP implementation project) contains support for this test suite. Tester implementations may be accessed via coap.me and more details are available at http://coap.technology/.

Cyber Security

CoAP relies on transport network security. By default, it runs over the secure form of UDP (called DTLS) using parameters that are the equivalent of 3072-bit RSA keys. Despite this, it can still run successfully on very small nodes.

Governance and Maintenance

The Internet Engineering Task Force (IETF) Constrained RESTful Environments Working Group (CoRE) has done the major standardization work for CoAP. To make the protocol suitable for IoT and M2M applications, various new functionalities have been added. The core of the protocol is specified in RFC 7252; important extensions are in various stages of the standardization process. More information is available at http://coap.technology/.

Relevant EPRI Reports

- *Lightweight Messaging Technologies for the Energy Internet of Things: An Introduction.* EPRI, Palo Alto, CA: 2018. 3002013478.
- *Program on Technology Innovation: Evaluating IoT Messaging Protocols for DER Management.* EPRI, Palo Alto, CA: 2018. 3002014678.
- *Blockchain: Technology Risk and Rewards for Utilities.* EPRI, Palo Alto, CA: 2017. 3002010242.

Data Distribution Service (DDS)

DDS, an Object Management Group (OMG) standard[14], was designed for "efficient and robust delivery of…information" of the sort that might be encountered in power generation and smart grid management. Unlike the request-reply mechanism used by HTTP and CoAP, DDS employs the publish-subscribe messaging pattern, in which nodes that produce information (publishers) create "topics" (e.g., temperature, location, voltage) and publish "samples" that are delivered to subscribers (nodes that declare an interest in that topic). This is illustrated in Figure 4-7.

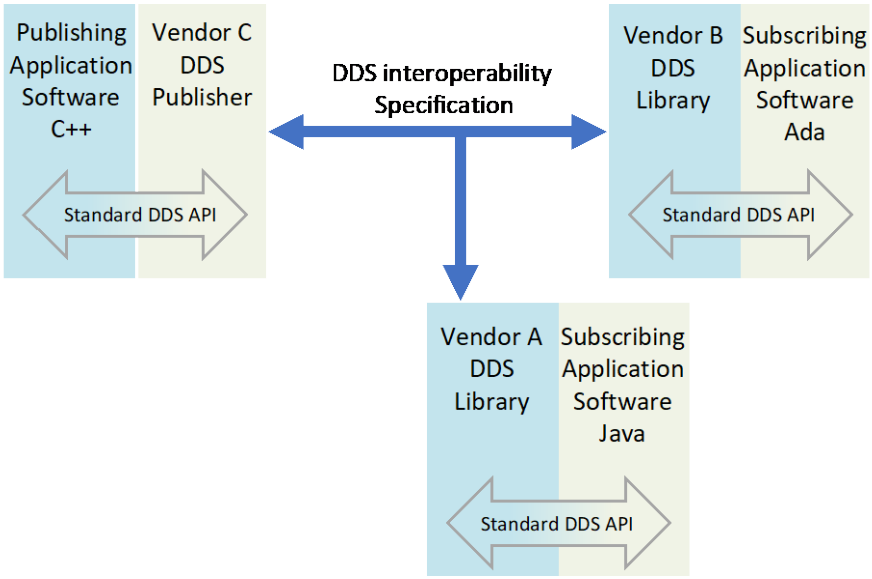


Figure 4-7
Data Distribution Service (DDS) Node Management

Technical Overview

The DDS specification describes two levels of interfaces. A lower, Data-Centric Publish-Subscribe (DCPS) interface provides for the efficient delivery of the proper information to the proper recipients, while an optional, higher, Data Local Reconstruction Layer (DLRL) allows for simple integration of DDS into the application layer. With the latest release (version 1.4), DLRL was broken out into a separate specification[15].

DDS also supports mechanisms that go beyond the basic publish-subscribe model. As a result, applications using DDS for messaging never need information about other participating applications, including their existence or location(s): DDS transparently handles message delivery without requiring intervention from the user applications to determine which nodes should receive which messages, where recipient nodes are located, and what happens if messages cannot be delivered. DDS includes quality of service (QoS) parameters that can be used to preconfigure discovery and behavior mechanisms. It also automatically handles hot-swapping of redundant publishers: if a primary publisher fails, subscribers will get the sample with the

[14] Object Management Group, Data Distribution Service (https://www.omg.org/spec/DDS/1.4).

[15] Object Management Group. Data Distribution Service + Data Local Reconstruction Layer (https://www.omg.org/spec/DDS-DLRL/).

highest priority whose data is still valid (that is, whose publisher-specified validity period has not yet expired). The system will automatically switch back to the primary publisher when it recovers.

Adoption

Commercial and open-source implementations of DDS are available. These include application programming interfaces (APIs) and libraries of implementations in Ada, C, C++, C#, Java, Ruby, and other languages.

Test Tools

Real-Time Innovations (RTI), located in Sunnyvale, California, is the largest vendor of products based on DDS. The company's Connext DDS is a software framework that includes a variety of tools and runtime services. More information is available at https://www.rti.com/.

Cyber Security

Security for DDS is provided by a separate specification[16] that adds several "DDS Security Support" compliance points to the DDS specification. The DDS Security Model is enforced by the invocation of Service Plugin Interfaces (SPIs). This DDS Security specification defines a set of built-in implementations of these SPIs that enable out-of-the box security and interoperability between compliant DDS applications. The use of SPIs allows users to customize the behavior and technologies that their DDS implementations use for information assurance, including authentication, access control, encryption, message authentication, digital signing, logging, and data tagging.

Governance and Maintenance

The DDS specification was developed starting in 2001 by Real-Time Innovations, a US government contractor, and Thales Group, a French defense company. In 2004, the Object Management Group (OMG) published DDS version 1.0 and the latest version (1.4) was published in April 2015. DDS is covered by several US patents.

Relevant EPRI Reports

- *Program on Technology Innovation: Evaluating IoT Messaging Protocols for DER Management.* EPRI, Palo Alto, CA: 2018. 3002014678.
- *IEC 61968-5 Distributed Energy Optimization to Open Field Message Bus (OpenFMB) Mapping.* EPRI, Palo Alto, CA: 2019. 3002016145.

[16] Object Management Group, DDS Security (https://www.omg.org/spec/DDS-SECURITY/1.1/PDF).

5
OTHER PROTOCOLS

The preceding sections of this report focused on open, standards-based protocols and systems that have significant support or market presence. This section discusses three other networking topics that are worth noting because they are of rising interest in the industry: two telecommunication technologies (5G cellular and low-earth-orbit satellites) and cloud-based proprietary DR protocols.

New Forms of Cellular

About every ten years a new generation of standards for mobile telephony emerges. The latest (fifth) generation ("5G") is currently superseding the preceding mixture of Mobile WiMAX, LTE, and other technologies broadly labeled "4G."

5G builds on the major changes that were introduced with "true" 4G networks, primarily the use of Internet Protocol (IP) for all services, including voice. 4G also abandoned the use of spread-spectrum radio technology, replacing it with much faster transmission and frequency equalization schemes. As was the case with earlier generations, older equipment cannot be used on 5G networks, which require the use of new devices specifically built for 5G (though the new 5G devices are also able to access 4G LTE networks).

One possible result of the transition to 5G is the potential for convergence with Wi-Fi. The significant improvement in cellular performance offered by 5G, along with its small cell size, could narrow the gap between Wi-Fi and cellular networks in dense and indoor deployments.

Meanwhile, the improved speeds of 5G will make it a stronger contender for communication with grid edge devices. It is well known that reliance on residential Wi-Fi for communication with smart grid devices can be problematic. Homeowners are often casual about reconfiguring their Wi-Fi networks, resulting in broken communication links for edge devices. For this very reason, residential devices that require a more reliable connection (such as alarm systems) often use cellular data networks, instead of Wi-Fi.

Technical Overview

Like previous generations of mobile phones, 5G is a cellular system that relies on an interconnected network of local radio transceiver stations that define individual network "cells." The edge devices connect to these stations to access the telephone network or internet.

The 5G system contains three subsystems operating at three different radio frequencies (and resulting in three different data transfer speeds). "Low-band" 5G uses the same frequencies as 4G (600–850 MHz) and each cell is similar in size and capacity. Its data rate (30–250 Mb/s) is only slightly higher than that of 4G.

The next higher level of 5G is "mid-band," which is the form most implemented today, usually in metropolitan areas. It offers 100-900 Mb/s speeds in a frequency band from 2.5–3.7 GHz (microwave region).

"High-band" 5G, while it offers the highest speeds (about 1 Gb/s, comparable to the speed of internet cable), suffers from high attenuation. The very high frequencies used for high-band 5G (25–39 GHz, millimeter waves), do not pass readily through many walls or windows.

Adoption

The major U.S. mobile carriers (AT&T, T-Mobile, U. S. Cellular, and Verizon) are all implementing 5G networks. Some carriers are not implementing low-band 5G because it offers little advantage over 4G but are positioning mid-band 5G as the entry-level service offering.

Due to the small cell size required for high band 5G, carriers are only planning to deploy it in dense urban environments or in areas of high concentration of devices (such as arenas or convention centers).

Devices and Technologies

Cellular data networks are carriers for communicating application-level protocols, and as such, have no specific connection with DR (or any other grid service). Communication modules for residential smart-grid devices will embed 5G shipsets and antennas to allow them to connect to a carrier network.

The availability of high-speed broadband communications with the 5G cellular networks may be expected to reduce latency of data transmission for DR. As a result, there may be less concern over "verbose" protocol encodings (like the uncompressed XML used by OpenADR) than there has been in the past. If promised latencies of less than 1 ms can be reliably achieved, 5G networks could be used to send data at AGC rates, making regulation service possible over a cellular network. Furthermore, a reduction in the cost per bit of data transmitted may make the use of cellular data more attractive than current systems that rely on residential Wi-Fi or FM radio to communicate DR events.

Test Tools and Certification

As a global communication standard with widespread deployments planned and underway, there is a correspondingly large market for testing tools for 5G networks and devices. Similarly, major electronics testing companies provide certification of 5G equipment.

Cyber Security

Although deployment of the vastly increased number of cellular devices enabled by 5G naturally would increase the attack surface, most cyber security concerns with 5G have not been directed at the technology itself. Rather, they have stemmed from suspicions of possible espionage stemming from the close ties that exist between Chinese 5G equipment manufacturers and the Chinese government. In response, the U.S. and several other countries now ban the use of Chinese equipment in their national 5G networks.

Regulatory Framework

As a radio-based technology, 5G networks and equipment are regulated in the U. S. by the Federal Communications Commission (FCC).

Governance and Maintenance

The 3rd Generation Partnership Project (3GPP) industry consortium sets the standards for 5G. 3GPP consists of seven "organizations partners" from Asia, Europe, and North America. In turn, the partners are made up of individual member companies, which totaled 719 at the end of 2020. Minimum standards are set by the International Telecommunications Union (ITU).

Relevant EPRI Reports and Other Articles

- *The 5G Technology Roadmap for the Utility FAN: Staying Ahead of the Technology Adoption Curve.* EPRI, Palo Alto, CA: 2019. 3002016411.
- *Quick Insights: Fifth Generation Wireless – Utility Opportunities and Challenges in the 5G Transition.* EPRI, Palo Alto, CA: 2018. 3002014789.
- *5G and Cyber Security for Utility Operational Technology Environments: Initial Assessment and Potential Outcomes.* EPRI, Palo Alto, CA: 2020. 3002017835.
- *Next Generation Wireless Local Area Network (WLAN).* EPRI, Palo Alto, CA: 2021. 3002022297.
- Hui, et al., "5G Network-Based Internet of Things for Demand Response in Smart Grid: A Survey on Application Potential," *Applied Energy,* 257 (2020) 113872. Retrieved from: https://www.sciencedirect.com/science/article/pii/S0306261919316599?via%3Dihub.

Low-Earth-Orbit Satellite Protocols

Internet access via satellites has been available to consumers for nearly twenty years. Two-way communications using these early systems suffers from the poor roundtrip latency (~600 msec) inherent in the use of satellites orbiting more than 22,000 miles away. As a result, the target consumers for these systems are mostly in locations that are not well served by terrestrial broadband providers.

Satellites with more suitable architectures for low-latency communications require shorter roundtrip times, necessitating the use of lower orbits. Since such satellites cannot be synchronized with the rotation of the earth, more (sometimes many more) are needed to provide continuous coverage. One early system, Motorola's Iridium, provided complete coverage of the earth by using 66 active satellites (with additional spares already in orbit). Placed into six low-earth polar orbits (at about 500 miles altitude), the satellites use microwave radio to access terrestrial stations and to relay data between each another. Originally intended for use with voice handsets, the service went bankrupt within a year of starting service. It is currently used by the Department of Defense.

More recently, interest in denser low-earth orbit satellite systems has grown rapidly. A leading representative of this new generation systems is Starlink, which is being constructed by SpaceX.

As with 5G cellular, there is nothing inherently DR-specific about these services. They offer a telecommunications infrastructure that could carry DR-related information and are essentially just an extension of the Internet backbone into space.

Technical Overview

Taking Starlink as an example, the company is currently implementing a constellation of 4,408 satellites planned for low-earth orbit (about 350 miles). This will provide coverage of almost the entire globe. Beta availability of the public service began in October 2020 for users in northern latitudes (between about central Oregon and northern British Columbia). In April 2021 the FCC approved Starlink's plan for the next phase of the constellation, which would place an additional 7,500 satellites into a lower orbital shell (at about 200 miles up).

By July 2021 there were more than 1,700 satellites in the Starlink constellation. As an "Internet-in-the-sky," the system can support any kind of Internet traffic, as was demonstrated in October 2019 when Elon Musk posted a tweet on Twitter via Starlink.

The lower orbits of the Starlink design reduces communication latencies and offers higher speeds than older satellite technologies. Beta users have seen speeds over 150 Mb/s and latencies of 20–40 msec. An August 2021 report found that download and upload speeds for Starlink were 80–85% those of terrestrial broadband providers, with latencies about three times longer. Compared to other satellite systems, Starlink speeds were five times faster and latencies more than an order of magnitude shorter. These results indicate that remote residential users can achieve broadband Internet speeds regardless of geographical location and cellular coverage. This may allow more rapid DR response to be achieved from remote loads.

Adoption

The Starlink system is still in beta testing. In February 2021 Starlink had over 10,000 beta users and began accepting preorders from the public. By May, more than 500,000 had paid the $99 deposit to place a preorder and in July the system had nearly 90,000 users in 12 countries.

Other satellite service providers are also beginning to respond to the IoT opportunity. In August 2021 Inmarsat announced the creation of a service that will merge new, faster GEO satellites, a small new constellation of LEO satellites, and 5G terrestrial cellular service into an integrated communications offering. OneWeb, a British satellite company, now has launched 288 LEO satellites on its way to a planned total of 648 that will be used to offer global Internet service staring next year. Most recently, Boeing received FCC permission in November 2021 to launch a constellation consisting of 132 LEO satellites and fifteen "highly-inclined" satellites: the combination of orbits is intended as a cost-effective means of providing both high speeds and low latencies.

Devices and Technologies

The Starlink satellites are relatively small (about 500 pounds each) and designed for mass production. User terminals are not handsets (as with Iridium and other systems); rather, a small "pizza-box" containing a flat, phased-array antenna is used. During the beta testing period the terminals have been priced at $499.

Starlink has applied to the FCC for permission to operate 32 ground stations in the U.S., although as of July 2020 only five had been constructed. Starlink also plans to install ground stations at Google data centers around the world.

Test Tools and Certification

Starlink is a proprietary system, and as such, there is no certification or third-party tools available to the public.

Cyber Security

Communications over the Starlink system will use a peer-to-peer network protocol that is claimed to incorporate native end-to-end encryption. Details of this have not been disclosed.

Regulatory Framework

In the U.S., the FCC regulates those portions of the microwave radio spectrum used by Starlink for communication between ground stations and satellite, while the ITU has global jurisdiction. The FCC has approved Starlink's request to communicate with 12,000 satellites and in 2019 submitted a filing to the ITU pursuant to an additional request from Starlink for 30,000 more satellites. NASA has also made requests to the FCC regarding Starlink's plans for reliably de-orbiting satellites following their five-to-seven-year lifetimes.

Governance and Maintenance

As a privately-owned, proprietary system, all governance and maintenance activities are the responsibility of Space Exploration Technologies, Inc. (SpaceX).

Relevant EPRI Reports and Other Articles

- *Resilient Communications Selection and Design.* EPRI, Palo Alto, CA: 2020. 3002018702.
- *Resilient Communication Demonstration Project: Demonstration Evaluation Report.* EPRI, Palo Alto, CA: 2020. 3002017908.
- Meloni, A., and Atzori, L., "The Role of Satellite Communications in the Smart Grid," IEEE Wireless Communications, 2017. http://ieeexplore.ieee.org/abstract/document/7909157.

Cloud-Based Proprietary Protocols

Except for the Starlink system described in the preceding paragraphs, all the communications technologies addressed thus far have been based on open, publicly available standards. Standards provide several benefits derived from their development and governance processes. However, these come at a cost in agility and therefore open standards may be seen as "stifling innovation." One benefit of proprietary protocols is that they can be quickly changed to reflect new features. They are also often related to tapping into existing markets (e.g., contracting with a major thermostat manufacturer to use their resources for grid flexibility) because the manufacturer can quickly deploy updates that work with their system.

Technical Overview

The rise of so-called "smart energy devices" and the Internet of Things present a significant opportunity. Innovative smart devices, including thermostats, pool pumps, water heaters, and electric vehicle service equipment, have all emerged. Although as standalone devices these may be somewhat more sophisticated than older models, their ability to connect to the Internet is what enables many of their truly innovative features. Rather than call them "smart devices," it might be more accurate to call them "Internet-connected" devices, for that is what differentiates them from simpler standalone devices.

The new "smart" capabilities often include one or more of the following:

- *Remote Access to Devices:* through an in-the-cloud web server, users may monitor or control their loads from any device capable of running a web browser, such as a cell phone or PC. This capability may allow remote control and scheduling, performance review, and other helpful functions. It also may allow the vendor to update the software running in the device directly over the Internet.
- *Expanded Access to Computing Resources and Data:* Vendors may leverage historical usage data from connected devices to assess trends, offer comparisons with similar residences, estimate accrued savings, and even detect anomalous behaviors related to equipment failures or other maintenance needs.
- *Protocol Conversion.* By implementing bidirectional cloud-based clients, vendors can use virtual devices to present the illusion of direct control of residential devices. This is achieved by receiving and analyzing the DR message in a standard protocol, then constructing appropriate proprietary messages for communication with the actual thermostats. For example, rather than supporting direct interpretation of prices by individual thermostats, a cloud-based client could receive price information from the utility, determine an appropriate adjustment to be made to the thermostat's schedule, and forward the changes over the vendor's proprietary network. This allows the vendor to claim compatibility with the standard DR protocol for its devices without actually implementing the standard protocol in each thermostat.
- *Voice Assistants.* By connecting to the Internet, devices can implement interfaces to voice assistants. For example, Google Nest naturally integrates with Google Assistant, while Ecobee's newer devices implement support for Amazon's Alexa assistant.
- *Advanced Analytics and Forecasts:* Combining data from external sources, such as weather forecasts, may enable the vendor to compute more efficient operating schedules to improve efficiency or reduce discomfort. The vendor may also act as a DR aggregator and earn money for itself or for the homeowner through participation in utility DR programs.

The appearance of devices in the market with these capabilities is the result of a synergistic combination of developments: 1) The use of *cloud computing* to expand the computational and data handling power available to devices without greatly increasing their actual local capabilities (and, therefore, their cost); 2) The use of *Internet connectivity* to deliver these expanded capabilities to remote devices and users at a reasonable cost (a cost that is largely borne by the homeowner, rather than the vendor); and 3) The use of *proprietary protocols* to speed time to market and allow early movers to capture market share rapidly.

As an example, consider smart thermostats. Programmable thermostats that can operate on user-defined stored schedules have been available for decades. The introduction of the Nest "learning thermostat" was a disruptive innovation that made use of existing capabilities (such as the homeowner's Wi-Fi system for basic connectivity to the Internet) as well as a new proprietary application-layer protocol that allowed remote control and data collection features to be added to the device. Using a cloud-based system kept computing requirements for the device manageable, while allowing larger computer and storage resources available in the cloud to be used to perform additional services. This architecture also allowed Nest to become a DR aggregator that

could offer services based on the loads controlled by its fleet of connected thermostats. Manufacturers offering similar devices include Ecobee and Honeywell.

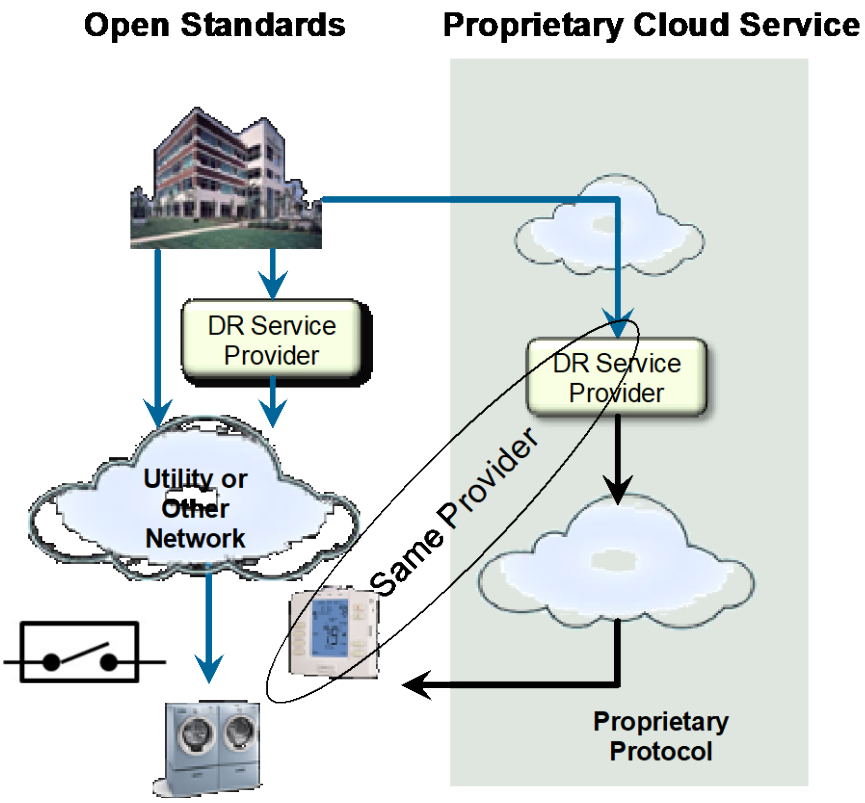


Figure 5-1
Proprietary vs. Open Access at the End Device

Adoption

Continuing with the example of the Nest thermostat, the first Nest Learning thermostat was released in early 2011 and only three years later had seen enough success that Google paid $3.2 billion in cash to acquire the company.

Devices and Technologies

Internet-connected smart thermostats may offer remote controllability, learning of customer preferences and occupancy patterns, awareness of utility TOU tariff schedules, and response to weather forecasts. They may also offer automatic response to DR events sent by aggregators or system operators. Some offer remote temperature and occupancy sensors for improved understanding of conditions in the home. These may be connected to the main thermostat via a star topology RF network (Ecobee) or Bluetooth (Google).

The thermostats connect to the vendor's cloud via customer-supplied Wi-Fi and attach to the same thermostat wires that were used with older-generation devices. They use the standard Internet protocol stack, with a proprietary application-layer protocol added. For example, both Ecobee and Nest protocol messages are expressed in JSON and run over secure HTTP.

Test Tools and Certification

These are proprietary systems and as such, there are no certification or third-party tools available to the public. Both Ecobee and Google have websites dedicated to developers who want to integrate with their respective ecosystems.

Cyber Security

Security for these systems primarily relies on the features of the underlying transport and network layers used to carry the proprietary protocols. These include standard Wi-Fi or TCP technologies such as WEP or WPA and SSL. Two-factor authentication may also be available for user authentication.

Regulatory Framework

There are no additional regulatory requirements for devices since they rely on standard residential Wi-Fi or Bluetooth networks. For a proprietary RF system like Ecobee's, appropriate licensing from the relevant communication regulator for the jurisdiction (the FCC for the US) is required.

Governance and Maintenance

As proprietary systems, all governance and maintenance activities are the responsibility of the manufacturers.

Relevant EPRI Reports

- *Program on Technology Innovation: Disruptive Innovations for Heating, Ventilation, and Air Conditioning (HVAC) Systems – 2017.* EPRI, Palo Alto, CA: 2018. 3002013866.
- *Basics of the Internet of Things: What is it, Who's Involved, and EPRI's Research.* EPRI, Palo Alto, CA: 2017. 3002000235.
- *From Innovation to Standards: Technology Evolution.* EPRI, Palo Alto, CA: 2018. 3002004840.
- *Enabling Voice Assistants for Demand Response and Demand Side Management.* EPRI, Palo Alto, CA: 2020. 3002003349.

6
CYBER SECURITY FOR RESIDENTIAL PROTOCOLS

Decarbonization of the grid will be a major driver of the energy system of the future.[17] This may be easily seen in the accelerating deployment of low-carbon renewable generation and net-zero clean energy systems. To accommodate this, the grid will need greater operational flexibility (to respond to increasing intermittency) and greater resiliency when encountering natural or man-made threats.

The success of the grid of the future depends on a widespread, stable, reliable, and secure digital infrastructure. Residential DR and DER will be important elements of this future, and decisions involving the communications solutions described in this paper will be critical to its realization.

A Cyber Security Vision

It is important to realize that any cyber security features, such as those associated with the communications technologies described in this paper, will be operating within the context of a utility's entire cyber security environment. Such a context includes numerous key factors necessary for success, including personnel, policies, procedures, and many others that transcend the technology itself. An organization's cyber security is only as strong as its weakest component, and the characteristics and features described here, while important to understand, should be viewed in that overall context.

This concept of a holistic approach to end-to-end cyber security is receiving increasing attention. IPKeys Power Partners has recently announced a monitoring service[18] to address cyber security issues that include DER and supplier clouds. And EPRI has published a vision for cyber security[19], a key goal of which is *Intrinsic Security*. Rather than treating security as a cost center, or an investment made to meet the letter of compliance-specific mandates, intrinsic security would have cyber security become an integral part of the utility's business culture, analogous to how safety is treated today.

Cyber Security Challenges of Residential DR Communications

Regardless of the specific features of any of the technologies included in this paper, there exist fundamental cyber security challenges inherent in the deployment of multiple technologies for residential communications.

---

[17] *Preparing for the 2030 Energy System: A Vision for Electric Utility Information and Communications Technologies (ICT).* EPRI, Palo Alto, CA: 2021. 3002022716.

[18] Nawy, R., "Can Grid Cybersecurity Coexist with Clouds and DERMS?." *Rural Electric Magazine,* October 2021.

[19] *Preparing for the 2030 Energy System: Why We Need a New Cyber Security Vision.* EPRI, Palo Alto, CA: 2021. 3002020794.

New Technologies

Demand response technologies can provide multiple benefits to the grid and these capabilities can be activated through both customer-facing interfaces (GUIs, web-dashboards, apps, proprietary protocols) and utility-facing interfaces (DR signals). These parallel opportunities and interfaces pose challenges that may introduce cyber security vulnerabilities.

Today's demand response programs are becoming more complex as technologies like electric vehicles and energy storage can provide both demand response and generation capabilities. DR and generation are typically addressed by different utility business processes and use different tariffs and programs. Today's program design tends to push these technologies into one bucket; however, that can change. New tariff structures can leverage these technologies to provide bi-directional benefits. In addition, new regulatory constructs created to implement FERC Order 2222 will open value streams for aggregations of DR devices to participate in bulk markets. This has led to industry discussions around how to avoid double counting simultaneous responses to both distribution and market-based services. This situation creates potential issues for data management and cyber security.

Data is becoming more important to utility system and planning. New integrated planning and operations processes will be driven by data from grid-edge DR devices.[20] Utilities will need to take care that data is harmonized so that it can be properly used for system planning and operation. The source of this data may be third parties, and utility practices must be scrutinized to ensure that data from these sources has the same level of integrity as data from internal sources. In addition, as grid operators become more dependent on aggregations of DR or DER to help stabilize the grid on both distribution and bulk systems, coordination with bulk dispatch systems also becomes important.[21,22]

In addition to data, residential technologies that can accept DR communications present some unique cyber security issues. Two examples are:

- **Parallel Interfaces:** Residential DR devices often have parallel interfaces—both utility-facing and customer-facing. Though these interfaces have different purposes—manufacturer interfaces for consumer-facing features and utility interface for grid signals—the interfaces can provide settings that may impact each other. For example, some smart inverter settings can be changed through either interface, thermostat setpoints can be changed from the customer GUI or in response to an OpenADR signal). Authentication of devices, controllers, and users may be required. Scanning from grid edge to control center, both for operational as well as for cyber security reasons, is desirable.

---

[20] *Integrated Distribution Planning: A Framework for the Future.* Smart Electric Power Alliance. 2020. https://sepapower.org/resource/integrated-distribution-planning-a-framework-for-the-future/

[21] *Systems Interoperability and Cyber Security: An EPRI FO-2222 Phase 1 Collaborative Report.* EPRI, Palo Alto, CA: 2021. 3002020597. https://www.epri.com/research/products/000000003002020597

[22] *Metering, Data and Information, and Telemetry: An EPRI FO-2222 Phase 1 Collaborative Report.* EPRI, Palo Alto, CA: 2021. 3002020596. https://www.epri.com/research/products/000000003002020596

- **Firmware**: Firmware updates in behind-the-meter systems are performed by the customer. These updates often contain patches for cyber security issues.

In summary, the introduction of new technologies and their potential parallel use naturally complicate integration with the grid. New knowledge and experience must be acquired, and programs and policies need to be adjusted to accommodate the changes. While this sort of evolution is inevitable, it nevertheless poses challenges that may introduce vulnerabilities.

Layered Cyber Security

Cyber security features can be implemented at multiple layers within a layered network architecture. Demand response protocols tend to operate at higher layers in the OSI stack and require lower-level standards (like TCP/IP) to operate. Security implemented in these lower layers help to protect the demand response protocols riding on them.

Consider a simple text message containing DR instructions. When such a message is transmitted from a system operator or aggregator to a Wi-Fi-connected residential device, security features will automatically be applied by the lower layers of the network. If the message is sent over standard secure Internet protocols (such as TCP/IP), transport-layer security (TLS) mechanisms within the network will encrypt the data using unique keys known only to the sender and receiver of the message. Once the message arrives, the residential Wi-Fi system will again encrypt the (already TLS-encrypted) message once again, using a key known only to the devices on that particular Wi-Fi network. Thus, the cleartext DR message is encrypted over the course of its journey, without any security features being present in the application-layer DR protocol. When the message arrives at the DR edge device, the Wi-Fi message will be decrypted, then the TLS message contained within the Wi-Fi message will be decrypted, allowing the text of the DR message to be understood by the end-node device. This is essentially the same mechanism used by a Wi-Fi-connected laptop in the home when performing secure web operations (such as residential banking or bill paying).

The two primary security concerns that must be addressed in a DR communication system are the following:

1. *Authentication:* Validating the claimed identities of DR users, devices, and servers. This is usually done for users using things like username/password combinations or two-factor authentication (such as with tokens or fingerprints). Device authentication usually relies on the use of security certificates (client-side, server-side, or both) issued by certificate authorities.
2. *Data Confidentiality & Integrity:* Assuring that information or data are not exposed to unauthorized parties and have not been intentionally corrupted or forged. This is usually done with encryption, which may occur simultaneously at various layers of the protocol.

A third concern may also be present, depending on the financial rules associated with payments or penalties in a DR contract:

3. *Non-Repudiation:* Providing higher levels of assurance that a DR message is legitimate (and therefore may be legally binding). This is usually provided with XML signatures encompassing the critical portions of the DR message.

Some typical cyber security methods that address these concerns may be found at various levels in the network layers. Some of these techniques used by the technologies mentioned or discussed earlier in this report are described on the following sections.

Public Key Cryptography

Authentication of systems used for residential DR is usually accomplished using pairs of public and private keys. The public keys may be shared with anyone (through a key exchange mechanism), while the private keys are kept separate. An example of this for OpenADR is illustrated in Figure 6-1.

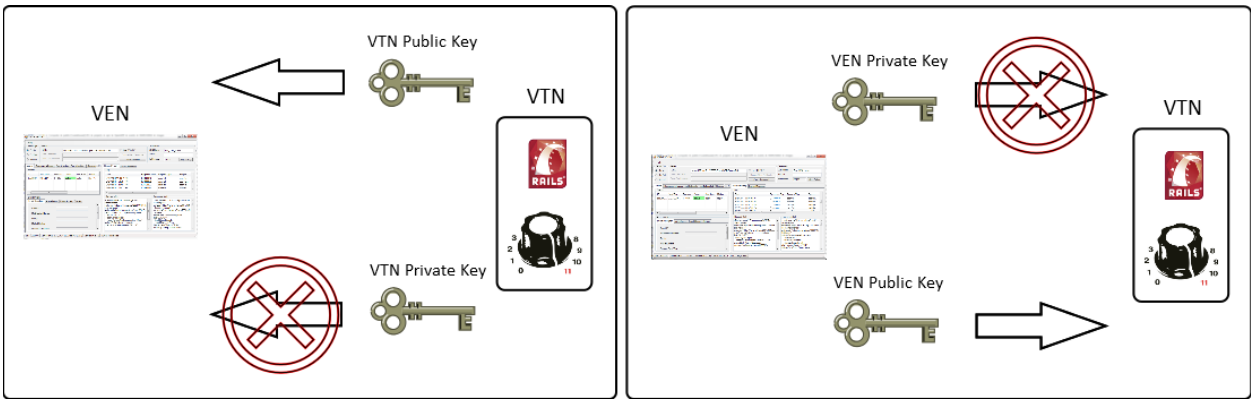


Figure 6-1
Public Key Cryptography (OpenADR Example): Public and Private Key Pairs

During normal operations the public key is used to encrypt the messages. Only the private key can decrypt them, as illustrated in Figure 6-3.

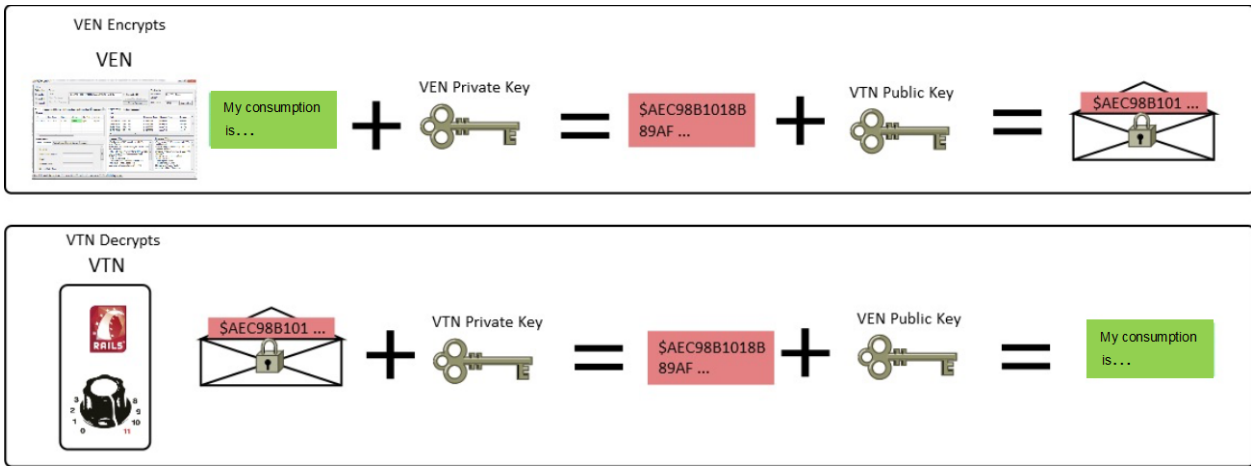


Figure 6-2
Public Key Cryptography (OpenADR Example): Encryption/Decryption Using Private/Public Keys

Device-Specific Cyber Security Certification

As described above, a holistic, end-to-end, layered approach to utility cyber security is critical for success. Nevertheless, understanding the cyber security strength of the individual components used in a system is equally important. UL, for one, has been actively expanding its

existing standards and programs in this area, with its Cybersecurity Assurance Program and the UL 2900 series of standards. The objective is to offer an IoT security rating and labeling system for networked consumer devices, provided by a trusted third party. The assessments are based on UL's "IoT Security Top 20 Design Principles" and includes both an initial assessment and biannual surveillance of devices.

Link Layer Security

Various low-level communication technologies are used in DR applications, but they usually have no exclusive connection with DR.

Bluetooth

Bluetooth is used by many "smart home" devices. For example, Google Nest uses Bluetooth to communicate between thermostats and remote temperature sensors.

- Bluetooth implements confidentiality, authentication, and encryption using custom algorithms. When devices are paired with one another, a master key is generated that relies on the PIN values used during that process. A cipher based on the master key is used for encrypting packets and guaranteeing confidentiality.

Wi-Fi

Another edge device protocol found in many residences is Wi-Fi.

- The Wi-Fi Protected Access (WPA and WPA2) wireless encryption standards replaced the older, easily breakable wireless Wired Equivalent Privacy (WEP) standard in 2003.
- Newly purchased Wi-Fi access points typically default to no-encryption (open) mode. Any devices connecting to unencrypted Wi-Fi networks can monitor and record data (including personal information) from such networks.
- Turning security on requires the user to configure the device, typically via a GUI. Successful communication using residential Wi-Fi usually requires at least a degree of management to keep the system properly configured for security.

5G

Cellular radio is sometimes used instead of residential Wi-Fi because communication goes directly from the device to the carrier network and is not affected by the resident. This can increase the reliability of the communications and is used, for example, by some home alarm systems for that reason.

- Current 4G LTE-A network security focuses on network access security and on the application domain level.
- The introduction of the new features and techniques with 5G, such as the support of massive numbers of IoT devices, device-to-device communication, vehicle-to-everything communication, software-defined network, and network function virtualization, brings challenges for the security of 5G networks. Proposals have been made to address these concerns, but the details of these are too technical to be taken up here.
- The IoT security aspect of 5G is particularly important for DR. Here, concerns have been raised over the efficiency of the mutual authentication mechanism when operated at the

massive scales forecast for the technology. Susceptibility of the authentication system to denial-of-service attacks has thus been identified as a potential problem for 5G.

Transport Layer Security

These network communication technologies are regularly used to provide secure Internet communication (including DR applications), but they have no exclusive connection with DR.

TLS/DTLS

- Secure versions of both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are available and are the primary foundation for the security of many application-layer protocols for DR. TLS (for TCP) and DTLA (for UDP) use similar concepts and synchronized version numbers for the standards.
- The most visible form of TLS can be seen when web browsers establish secure HTTP connections, identifiable by "HTTPS" in a URL (and usually also by the presence some sort of "lock" symbol in the browser's GUI). Such a connection provides privacy and data integrity. TLS encryption relies on a set of trusted certificates exchanged when the encrypted communication channel is established.
- The latest version of TLS, introduced in August 2018, is 1.3. Older application-layer standards (such as OpenADR) may still reference version 1.2. The corresponding version 1.3 of DTLS is still in development.

Application-Layer Security

Although many DR-specific application-layer protocols do not themselves contain security mechanisms, the standards for their use often mandate specific network security features, such as a minimum version of TLS, minimum encryption key lengths and encryption ciphers, and required authorization mechanisms (such as client and/or server PKI certificates).

Messaging Services

These application layer "helper" communication technologies are frequently used in DR applications, but they have no exclusive connection with DR.

XMPP

XMPP is an alternative to HTTP and generally provides a lighter weight means of transporting messages encoded using XML. XMPP connections are authenticated with Simple Authentication and Security Layer (SASL) and are encrypted with TLS.

- With SASL, applications are not limited to a single authentication mechanism. Rather, the client and server negotiate a common authentication mechanism and security level. Authentication then takes place using the agreed-upon mechanism.

- An XMPP server is considered to be secure when the following conditions are met (at a minimum):
  - The server has a server certificate
  - The server does not allow any cleartext communications, either between servers or between clients and servers

- The server supports a specific mechanism to prevent session hijacking

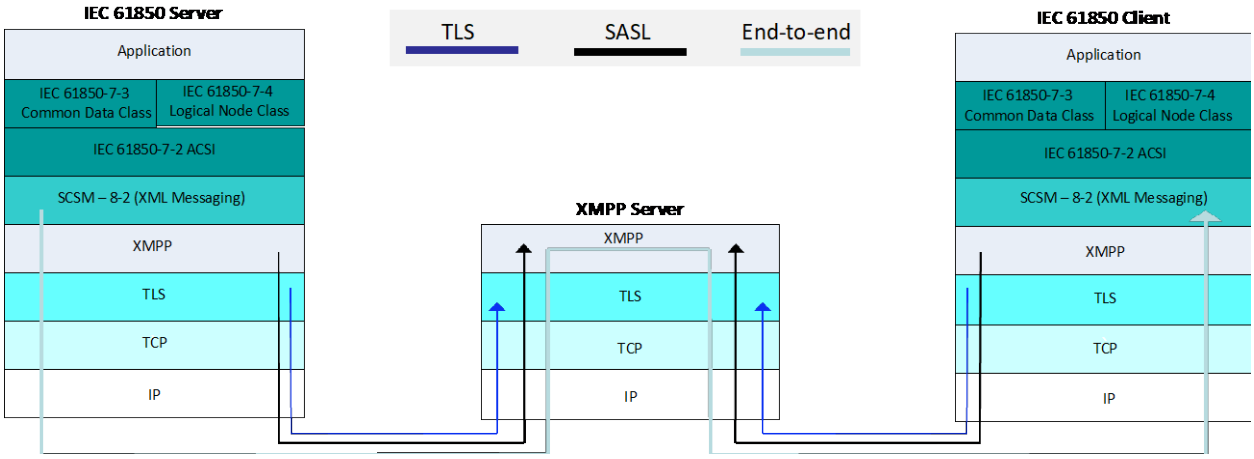


Figure 6-3
SEP2 (IEEE 2030.5) and XMPP Security

MQTT

MQTT messaging is a component of new distribution system architectures, such as Duke's OpenFMB.

- MQTT sends connection credentials in plaintext and does not include any measures for security or authentication.
- MQTT can use X.509 certificates for authentication at the transport layer of the network (TLS).This is an example of a protocol that relies on the cyber security features provided by the underlying TCP or UDP transport layers for protecting the integrity of transferred information from interception or duplication.

CoAP

CoAP is also used in the OpenFMB architecture.

- The CoAP standard calls for strong security. By default, it runs over the secure form of UDP (called DTLS) using parameters that are the equivalent of 3072-bit RSA keys.

DDS

DDS is another protocol used in OpenFMB.

- Security for DDS is provided by a separate specification that adds several "DDS Security Support" compliance points to the DDS specification.
- This DDS Security specification defines a set of built-in implementations that enable out-of-the box security and interoperability between compliant DDS applications. The mechanism uses Service Plugin Interfaces (SPIs) to allows customization of the behavior and technologies that DDS uses for cyber security (authentication, access control, encryption, message authentication, digital signing, logging, and data tagging).

DR Protocols

These application-layer protocols specifically support DR and DER-related communications.

OpenADR

In addition to specifying requirements for the security features of the network on which it is run, OpenADR also defines a higher-security option with additional requirements. The specific cryptographic algorithm and key length requirements are those contained in the latest version of NIST publication SP-800-131.

- To be certified, an OpenADR product must implement and demonstrate the use of TLS. The current version of the profile specifies TLS 1.2 and either ECC or RSA encryption (128-bit or longer).
- Both OpenADR clients and servers must implement the use of X.509v3 certificates for authentication (though this requirement can be relaxed in any given implementation). The certificates must be obtained from either Kyrio or Eonti (the OpenADR Alliance's certificate-granting partners).
- OpenADR's "high security" option uses public key cryptography to digitally sign portions of the XML message payloads. After receiving a message with a signature from a VEN, the VTN computes a "hash" of the message[23] and sends the (encrypted) hash value to the VEN. The VEN similarly computes the hash of the message it sent and checks this hash value against the (decrypted) hash value it received from the VTN. If the values match, the VTN can be sure that the message it received was indeed sent from that VEN (non-repudiation) and that the contents of the message is what was sent (integrity). This process is illustrated in Figure 6-4.

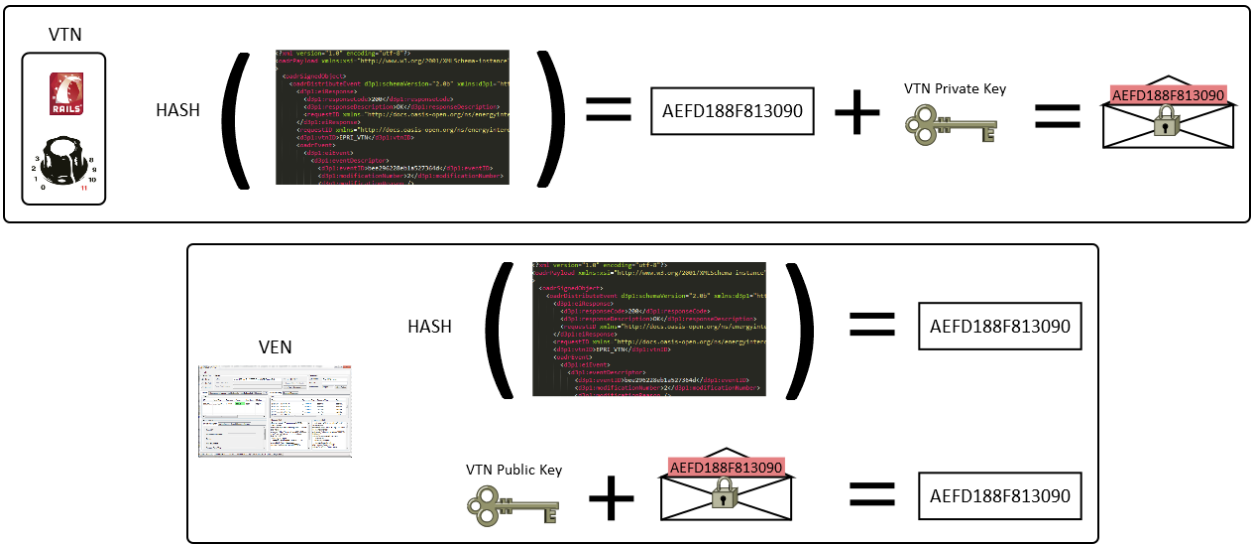


Figure 6-4
XML Signatures in OpenADR

[23] A "hash" is a one-way computation that converts a variable length string (in this case, the signed part of the XML message) into a fixed length number.

IEEE 2030.5

IEEE 2030.5 key management is based on the requirements of NIST publication 800-57.

- All transactions between clients and servers are secured using TLS.
- All devices use digital certificates to authenticate their identity.
- All data transactions between the server and device are encrypted at the transport layer using a secure cipher suite.

ANSI/CTA-2045

CTA-2045 defines requirements only for the form factors and communications between UCM modules and the devices to which they are physically connected. It relies on physical inaccessibility to provide security, and it is claimed that this eliminates any need for cyber security.

Summary

A summary of the cyber security characteristics of the protocols discussed in this report is contained in Table 6-1.

Table 6-1
Cyber Security Characteristics of Protocols for Residential DR

Protocol	Authentication	Cryptography	Authenticated Encryption	Comments
OpenADR	X.509v3 Certificates	TLS 1.2 AES (128-bit)	XML Signatures	
IEEE 2030.5	X.509v3 Certificates	TLS 1.2 AES (128-bit)	None	
CTA-2045	None	None	None	Physical Security
XMPP	SASL X.509v3 Certificates	TLS	OMEMO	
MQTT	Username/Password	TLS/DTLS	None	
CoAP	X.509v3 Certificates	DTLS	None	
DDS	X.509v3 Certificates	AES (128-bit or 256-bit)	Yes	Implemented via Plug-Ins

Additional information about EPRI's cyber security vision may be found in the references below.

Relevant EPRI Reports and Other Articles

- *Cyber Security Vision for 2030.* EPRI, Palo Alto, CA: 2021. 3002022715.
- *Grid Security of Connected Devices: Communications and Cybersecurity Assessment.* EPRI, Palo Alto, CA: 2019. 3002016154.
- *Program on Technology Innovation: Evaluating IoT Messaging Protocols for DER Management.* EPRI, Palo Alto, CA: 2018. 3002014678.
- Cao, J., et al., "A Survey on Security Aspects for 3GPP 5G Networks," *IEEE Communications Surveys & Tutorials,* **22**(1), First Quarter 2020, pp. 170-195.
- *Embedded System Security Assessment: Kyrio OpenADR Evaluation Kit—Information and Communications Technology and Security Architecture for Distributed Energy Resources Integration.* EPRI, Palo Alto, CA: 2018. 3002014145.
- NIST SP-800-131A, *Transitioning the Use of Cryptographic Algorithms and Key Lengths.* 2019.
- *Cyber Security Assessment IEEE 2030.5 Protocol for Distributed Energy Resource Integration.* EPRI, Palo Alto, CA: 2020. 3002019255.
- *PG&E Case Study – Attack Models and Security Gaps in Distributed Energy Resource Interoperability Standards: IEEE 2030.5 and 1547 Security Gaps, Impact Scenarios, and Mitigations.* EPRI, Palo Alto, CA: 2019. 3002016040.
- Nawy, R., "Can Grid Cybersecurity Coexist with Clouds and DERMS?." *Rural Electric Magazine,* October 2021.
- NIST SP-800-57, *Recommendation for Key Management,* 3 Parts, 2015-2020.
- *DNP3 Secure Authentication.* EPRI, Palo Alto, CA: 2019. 3002010607.

7
CONCLUSIONS AND NEXT STEPS

This paper has discussed three classes of networking technology related to residential DR: application protocols, messaging systems ("middleware"), and telecommunications infrastructure. Each of these differ in terms of technical evolution, market availability, and customer adoption.

Conclusions: Why These Protocols and Technologies?

The protocols and technologies contained in this report were selected for inclusion for specific reasons. The application protocols covered are leading the way for DR and DER programs around the world. The middleware messaging protocols discussed (XMPP, MQTT, CoAP, and DDS) offer alternative networking models for DR and DER programs that may result in more responsive, flexible, and robust systems. And the telecommunications solutions included (5G cellular and low-earth-orbit satellites) have the prospect of addressing some of the most common problems encountered with residential DR and DER networks: connection reliability and geographic coverage limitations.

Application Protocols

All three application protocol standards discussed (OpenADR, IEEE 2030.5, and CTA-2045) have advanced sufficiently to be included in DR and DER grid codes, manufacturer standards, and regulations[24,25]. They are recognized by national and international standards bodies (IEC, IEEE, and ANSI) and are being specified and adopted across the country and the world.

OpenADR (IEC 62746-10-1)

OpenADR is the leading protocol for standards-based DR, accommodating both utility-supplied or utility-specified devices as well as "Bring Your Own Device" programs. Its focus has been on managing DR in the form of generalized resources (via grid condition codes, prices, etc.).[26]

By emphasizing management of active power (load) while downplaying device specifics, OpenADR is analogous to a generation dispatching system that enables operators to schedule and dispatch pseudo-supply ("megawatts") when balancing supply and demand.

In the past, various mechanisms for extending or adapting the OpenADR protocol to support device-specific messages for DER have been explored. The OpenADR Alliance, "keeper" of the

---

[24] *Demand Response Interoperability Guidebook: A Repository of Information to Support Utilities in Achieving Interoperability in Demand Response Technologies*. EPRI, Palo Alto, CA: 2020. 3002018543. https://www.epri.com/research/products/000000003002018543

[25] *Mounting Importance of Communications to Monitor and Control Distributed Energy Resources*. EPRI, Palo Alto, CA: 2018. 3002013480. https://www.epri.com/research/products/000000003002013480

[26] *Common Demand Response Functions for Heating, Ventilating, and Air Conditioning (HVAC): A Summary of Demand Response Functionality Discussed in the Industry to Date*. EPRI, Palo Alto, CA: 2017. 3002011045. https://www.epri.com/research/products/000000003002011045

OpenADR specification, has recently shown increased interest in this topic. Since DER broadly includes DR, the bifurcation between DR and DER may be considered artificial and maintaining two completely different networks for managing two aspects of the same distributed resources seems inefficient.

IEEE 2030.5

In contrast to OpenADR, IEEE 2030.5 was built around information models that describe specific device types and is consequently typically used to modify the detailed behaviors or responses of such equipment (such as power factors and Volt-VAR curves in smart inverters). Although in principle IEEE 2030.5 could be used to manage "pure" DR via load control and pricing feature sets that have been defined for it, this has not received much attention. Its main appeal has therefore been to utility protection and control engineers concerned about the predictability of autonomous responses performed by the power electronics associated with distributed generation (supply) resources.

CTA-2045

Unlike both OpenADR and IEEE 2030.5, CTA-2045 is not a wide-area protocol at all. Rather, it provides a physical, electrical, and logical standard for attaching universal communication modules to smart-grid DR devices. By using an external module for network communications, the DR device itself can be built without reference to any specific DR protocol. This provides flexibility at little cost, allowing network protocol changes to be easily accomplished (by swapping modules), thereby "future-proofing" the customer's investment in the smart-grid device itself.

Because it is a local connection within the residential premises, CTA-2045 has a unique security approach: physical security of the communication module and device port is assumed, obviating the need for cyber security at the interface.

Messaging Protocols

Messaging Systems are important but often unsung components. In DR systems they may provide cyber security, message direction, or error handling, and their efficiency can have a significant performance impact on network resources.

OpenADR, for example, can be used with either HTTP or XMPP as its messaging system. In a dynamic environment in which resource availability may change frequently (such as residential DR), having a service discovery function in the DR network may be valuable: XMPP provides such a discovery feature, while HTTP does not.

The core messaging systems considered in this report (XMPP, MQTT, CoAP, and DDS) are well established, albeit not in traditional DR systems.

XMPP

XMPP is included in the OpenADR Profile B specification and its presence is required for certification of a certified Profile B VTN. Like HTTP, XMPP uses a client/server architecture, but since it uses persistent network connections, it is more efficient. When speed is an issue, XMPP has been preferred. It is easy to use with OpenADR since it is already part of the specification and certification process.

A European study[27] investigated the use of wide-area OpenADR communications with a VPP to provide frequency control for the grid. Based on a careful comparison of the standard supported messaging and deployment options (HTTP vs. XMPP and "push" messaging vs. "pull"), the investigators chose to implement OpenADR over XMPP and use push interactions to provide the highest speed and lowest latencies.

MQTT

Unlike client/server architectures (such as HTTP and XMPP), MQTT uses a publish/subscribe architecture. As a result, it can offer "discovery" services (wherein each client merely subscribes to a "topic" rather than having to register with the actual source servers). This design is particularly efficacious in a broadcast application: the information sources ("servers") do not have to know which clients have subscribed to the information they are providing, and the subscribing client systems don't need to know the identities of the sources of the information they are receiving: all the necessary addressing, routing, authentication, and other details are handled by an intermediary "broker" system. Thus, for example, a price server might publish prices for multiple locations and tariffs, but individual clients need only subscribe to those relevant or of interest to themselves.

MQTT is already supported for use with IEEE 2030.5 and is an option for OpenFMB communications. When Austin Energy grew concerned about the scalability of their growing OpenADR deployment a few years ago, they did their own port of OpenADR to run over MQTT. They found that when using the higher volume "pull" interaction mode, the bandwidth required for their MQTT deployment was only 12% of that needed for HTTP.

CoAP

Just as OpenADR's Profile A is a lightweight, reduced version of the full Profile B, so CoAP may be viewed as a lightweight, reduced version of the full Internet protocol stack. Intended for use by resource-constrained devices, it is nevertheless designed to be easily translated into HTTP for use on the regular Internet.

IoT smart grid edge devices are often small, energy constrained, and very cost sensitive. The use of a protocol like CoAP that is optimized for such devices may speed the creation and adoption of practical low-cost equipment that can still interact with standard HTTP-based DR application layer protocols.

DDS

DDS is another publish/subscribe option (like MQTT). However, the two differ in their overall architecture. As mentioned above, MQTT relies on a centralized "broker" system to manage publication topics and subscriptions thereto. This centralized design makes MQTT particularly suitable for use with hierarchical deployments (such as with OpenADR or a supporting a centralized price distribution service). DDS, on the other hand, puts more emphasis on distributed communications such as might occur between IoT nodes in a home, building, or campus. It may prove to be particularly useful, for example, in coordinating actions within a

[27] Kolenc, M., et al. "Virtual Power Plant Architecture Using OpenADR 2.0 b for Dynamic Charging of Automated Guided Vehicles." *International Journal of Electrical Power & Energy Systems,* 104, 370-382. (2019).

microgrid or other VPP, where routing information through a centralized broker would be inefficient.

Telecommunications

Telecommunications infrastructure provides the foundation upon which all DR networks are based. One of the stumbling blocks for residential DR has been dependence on the customer-supplied (and managed) home Wi-Fi network for device connectivity – known for intermittency. With the advent of 5G cellular, the speed and cost of cellular service may make it an attractive option for residential DR communications that is fast, stable, and reliable. Furthermore, areas that may receive the benefits of 5G (due to geographic distance or other coverage issues) may be able to take advantage of new LEO satellite Internet service, which will have no geographic constraints.

5G Cellular

Utility communications with residential IoT devices often has relied on local home-area networks such as Zigbee or Wi-Fi. Utility experience with such networks has been problematic: residents reconfigure, upgrade, or otherwise disrupt such networks, interrupting communications between utilities and edge devices that rely on them.

For these reasons public cellular telephone services may be more reliable than homeowner-managed residential communications and are often used in applications such as residential alarm systems. As with previous generations of cellular, the move to 5G is inevitable. If 5G can realize its promise of lower costs, higher speeds, and ubiquitous presence (at least in higher density areas), cellular communications direct to residential smart energy devices may become more attractive than Wi-Fi or other options. Utility tracking of the technical and financial evolution of 5G deployments may thus lead to faster, more reliable communications for residential DR.

Low Earth Orbit (LEO) Satellites

The geographic reach of broadband may be an obstacle to widespread DR communications. Residential users in remote locations or in areas of spotty coverage may suffer from poor radio reception or unreliable wireless connectivity. The emerging LEO satellite services promise to provide high bandwidth and low latency services across all geographies. Availability of such services could add more residential DR resources to the grid and enable them to participation in additional grid services that require faster, lower latency networks than can be reliably provisioned today.

Some Opportunities

Some exciting opportunities for improving residential DR communications may be deduced from the foregoing. For example:

- The coexistence of multiple solutions for managing DR and DER may be streamlined, reducing complexity and cost in the networks that monitor and control distributed resources. This may also provide a cyber security benefit.
- The efficiency and functionality of DR communications may be enhanced by adopting messaging systems that have proven effective in other domains, such as high-volume, low-latency text message systems.

- Emerging telecommunications platforms may offer lower costs, higher speeds, and broader geographic reach for residential DR networks in the future.

Application Layer Protocols

The industry has developed and deployed multiple application-layer protocols to manage residential distributed energy resources. Though some of these standards have been available for years and leveraged in programs and pilots, there remains opportunities to improve on their effectiveness and efficiency.

OpenADR and CTA-2045: One of the first opportunities is educational: CTA-2045 is often misunderstood as an alternative or competitor to OpenADR. Actually, they are architecturally complimentary because they address different parts of the end-to-end architecture: CTA-2045 standardizes hyper-local data exchanges over a physical port and plug that connect a communication module to a DR device. It requires another protocol (like OpenADR) to communicate between the module and the utility.[28]

Protocol Maturity Varies by Device Domains: Although the IEEE 2030.5 standard supports a DR feature set, this has not gotten traction in DR-ready devices and controllers. IEEE 2030.5 may yet become an important tool for DR management, but industry effort would be needed to increase adoption.

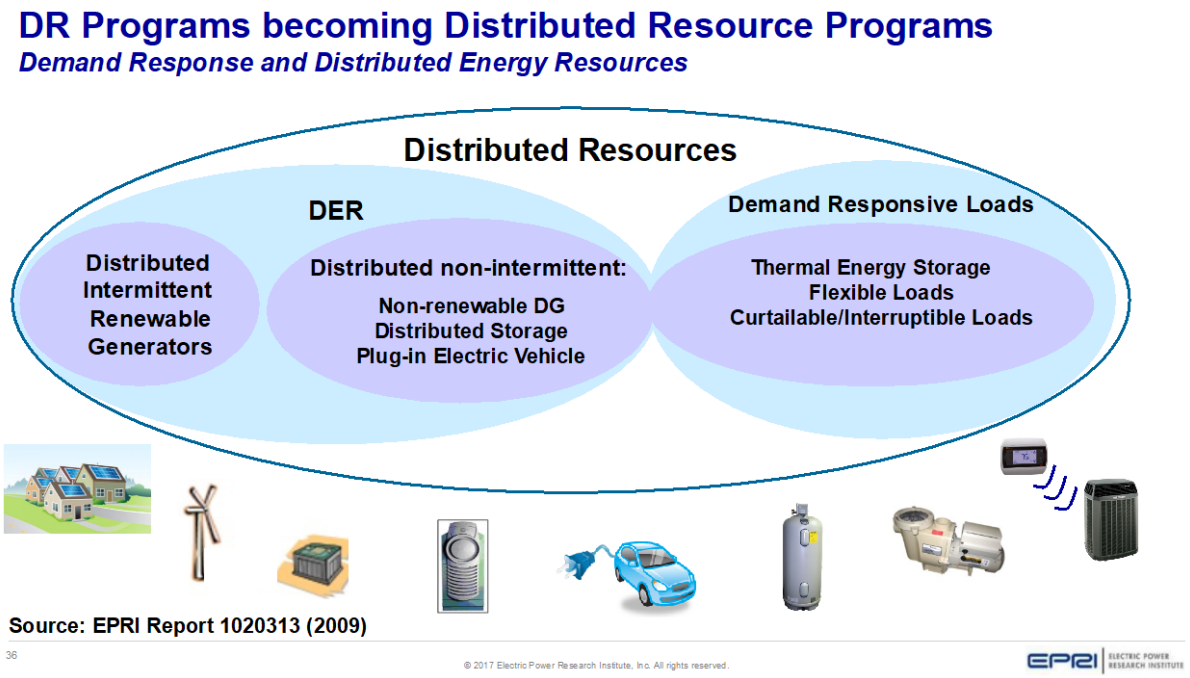


Figure 7-1
The Variety of Distributed Resources Currently Addressed by a Variety of Protocols

[28] *Communication Protocol Mapping Guide 1.0, OpenADR 2.0 to ANSI/CTA-2045-A: Requirements for Exchanging Information Between OpenADR 2.0 Clients and ANSI/CTA-2045 Technologies*. EPRI, Palo Alto, CA: 2019. 3002008854.

Aggregation Capabilities Vary. Another issue is how the protocols handle aggregation of resources. This will be a key capability in a future, federated grid.[29] California's Rule 21 defines a grid-based hierarchy for IEEE 2030.5 (with lines, substations, feeders, transformers, etc.). A flexible hierarchical architecture is inherent in OpenADR, but it is established at the time that end nodes register for communication with higher-level nodes. Neither protocol supports dynamic creation of groups or messages to manage groups of resources. Emerging standards, such as the relatively new IEC 61968-5 and the developing IEC 62746-10, define models for group management that could be added to either protocol.

Beyond that, most of the remaining questions may be addressed by careful study of the expanding deployments of residential distributed resources. Some important topics are the following:

- As the number of network nodes increases, widespread management of device authentication certificates and cyber security-related computational loads on servers may become an issue. Studies of the practical scalability of expanded communications for secure residential DR should be performed.
- As server or network capacity become better understood, the relative importance of more efficient messaging systems or higher speed telecommunications platforms will become apparent. Inefficiencies inherent in the design of HTTP and TCP may require the adoption of other networking technologies, and the related cost and efficiency gains should be measured and assessed.

Messaging Systems

The main reason for including the lighter weight messaging systems in this paper is to draw attention to the fact that the leading application protocols do not make particularly efficient use of the underlying Internet network protocol stack. The main reason is that the simplest messaging system for many protocols to adopt is that used for the World Wide Web: HTTP.

HTTP is a request/reply service that sends each message in a separate TCP session. This is somewhat akin to making a new phone call every time you wish to speak during a conversation. A more efficient way is to hold the session ("phone call") open for an extended period to allow multiple messages to be exchanged during each call (this is what XMPP does, for example).

An alternative to the request/reply service of HTTP (and its lightweight relative, CoAP) is the publish/subscribe model used by MQTT and DDS. Austin Energy ported OpenADR to run over MQTT and found very significant savings in network utilization to result.

Telecommunication Protocols

5G is the future platform for telecommunications, and it can support massive machine interconnections and transmit data very quickly, with high reliability and low latency. It will have a game-changing impact on electric utilities' grid operations networks. Therefore, utilities will have to acquire the skills required to design, build, and manage 5G platforms.

---

[29] *Federated Architecture for Distributed Energy Resources Integration*. EPRI, Palo Alto, CA: 2020. https://www.epri.com/research/products/000000003002019424

While it is always very important to consider cyber security in all use cases, "baking it in" rather than "bolting it on," it is particularly important in the case of newly introduced technologies. New services based on 5G or LEO satellites must be thoroughly investigated and understood before trusting them with business-critical communications.

Its advantages make 5G a step forward for carrying out DR in smart grids. Its advantages include massive numbers of links between flexible loads, fast data transfer speed (for remote control), robust security (for consumer privacy), high reliability (for availability), and low power consumption (for wide implementation). 5G services in a smart grid will build on the extensive and the reliable acquisition and sharing of system information on an appropriate timescale, along with massive backup storage and new computing techniques.

Next Steps

As communications standards improve to meet modern use cases for solar, energy storage, and DR systems, opportunities arise for development of test tools to ease the entry of open protocols into the market. EPRI continuously monitors and evaluates the maturity of both DR and DER communication standards[30].

Application-Layer Protocols

End-to-End Testing of Device-Integrated DR Communications

End-to-end testing of DR operations is essential. As it is, many protocols only guarantee delivery of a DR message to a smart grid device controller: what action the resource takes in response to the message is often undefined (or outside the scope of the communication protocol). For example, OpenADR 2.0b certification of a DR device only requires that it be capable of receiving an OpenADR signal; it does not require that the device be capable of responding to the signal under any specific DR use case scenario. This means that for the device to respond appropriately to OpenADR 2.0b DR messages, appropriate control logic must be programmed into the device and such control logic is often not tested during protocol compliance certification. Because of this, different smart grid devices may respond differently to the same DR signal, depending on how the device manufacturer (or an intermediate aggregator) may choose to interpret it.

Reconciliation/Coexistence of Multiple DR/DER Protocols

Future communication with residential DER (including DR) will be heterogeneous. Because different sorts of residential energy resources have been developed at different times and by different organizations, situations arise such as in California, where smart inverter-controlled devices are likely to use IEEE 2030.5 (because it is specified in Rule 21), but controllable loads are likely to use OpenADR (because it is specified in the Title 24 building codes). A likely future is that utilities will need to support multiple protocols to reach the breadth of devices on the market. This requires harmonization[31] of DER standards and the development of abstraction

---

[30] *DER Protocol Reference Guidebook – 4th Edition: Understanding the Characteristics of Communications with Distributed Energy Resource (DER) and Demand Response Technologies.* EPRI, Palo Alto, CA: 2020. 3002018544.

[31] *Harmonized Information and Communications for Distributed Energy Resources: Preliminary Guide for Grid Operators and Standards Organizations*. EPRI, Palo Alto, CA: 2021. 3002020093. https://www.epri.com/research/products/000000003002020093

layers in related tools (e.g., DERMS, ADMS) to handle the mapping of the semantics multiple protocols. This will likely include not only protocols to individual devices, but also integrations with third-party aggregators through a mixture of standardized and proprietary APIs.

Telecom Standards

5G Cyber Security Investigation

There are still issues to be studied in 5G network security, particularly around authentication and authorization. Concurrent requests for authentication or authorization from massive numbers of users may result in signaling storms, and how to handle this may become a critical issue. Also, authentication mechanisms to meet specific security and QoS requirements may cause a large amount of energy consumption for resource-limited terminals.

LEO Satellites

Exploration of LEO Satellite Internet Services

Traditional geostationary orbit satellite systems are familiar, but inherently limited in some respects. It remains to be seen if the newer LEO satellite systems can satisfy requirements for residential DR communications. Demonstrations or pilot implementations, including a laboratory integration step prior to deploying equipment to field sites, may yield useful insights. Additional demonstrations, with increasing numbers of sites deployed for lengthening periods of time, may be valuable next steps.

Wireless Protocols

Investigation of Next Gen Wireless (IEEE 802.11ax) and Next Gen Cellular (5G)

Wireless LAN technology has recently made significant advancements with the completion of Wi-FiTM 6 (IEEE 802.11ax) and the introduction of the latest security standard (WPA3). For existing and emerging wireless use cases, this next generation WLAN offers significant improvements. Furthermore, its capabilities appear to match or exceed 5G in most respects, typically at a lower cost. And while Wi-Fi 6 provides notable improvements in data throughput, the most significant advancements are improvements in efficiency: it works better with large numbers of devices and users.

Additional Research Suggestions

Other relevant research suggestions for residential DR communications include the following:

- *Testbed Implementations of Candidate IoT Protocols*—EPRI and its utility partners have a strong track record of implementing and testing emerging candidate protocols. With the continual emergence of new protocols, EPRI and/or utility testbeds may be useful for evaluating multiple protocols and accelerating utility deployments.
- *Investigate Implications of Dependence on Key Residential Smart Home Providers*—Utilities will most likely have to depend on Google, Amazon, and Microsoft as "mega-core IoT platform" providers. Facebook and Apple may also be in play as utilities pursue more

customer intimacy with beyond-the-meter connections. How these services complement (or complicate) residential DR communications may be worthy of study.

- *IoT impact on IT/OT integration*—As utilities increasingly rely on residential DR, their IT/OT convergence and integration strategies may be affected. Development and testing of integrated architectures that make control of residential resources a regular part of utility operations may become an increasingly important subject for investigation.
- *IoT cyber security design*—IoT platforms have distinctive architectural characteristics that will require special attention. EPRI has taken some steps in this direction with the Security Architecture for DER project, but more research is needed. The cybersecurity limitations of each of the protocols in this report should be investigated further against electric utility requirements.

8
BIBLIOGRAPHY

5G and Cyber Security for Utility Operational Technology Environments: Initial Assessment and Potential Outcomes. EPRI, Palo Alto, CA: 2020. 3002017835.

The 5G Technology Roadmap for the Utility FAN: Staying Ahead of the Technology Adoption Curve. EPRI, Palo Alto, CA: 2019. 3002016411.

ANSI/CTA-2045-A Water Heater Test Procedures: Information Exchange and Demand Response. EPRI, Palo Alto, CA: 2019. 3002016940.

Basics of the Internet of Things: What is it, Who's Involved, and EPRI's Research. EPRI, Palo Alto, CA: 2017. 3002010235.

Blockchain: Technology Risk and Rewards for Utilities. EPRI, Palo Alto, CA: 2017. 3002010242.

Cao, J., et al. "A Survey on Security Aspects for 3GPP 5G Networks," *IEEE Communications Surveys & Tutorials,* **22**(1), First Quarter 2020, pp. 170-195. https://doi.org/10.1109/COMST.2019.2951818.

Communication Protocol Mapping Guide 1.0, OpenADR 2.0 to ANSI/CTA-2045-A: Requirements for Exchanging Information Between OpenADR 2.0 Clients and ANSI/CTA-2045 Technologies. EPRI, Palo Alto, CA: 2019. 3002008854.

Cyber Security Assessment IEEE 2030.5 Protocol for Distributed Energy Resource Integration. EPRI, Palo Alto, CA: 2020. 3002019255.

DNP3 Secure Authentication. EPRI, Palo Alto, CA: 2019. 3002010607.

Embedded System Security Assessment: Kyrio OpenADR Evaluation Kit—Information and Communications Technology and Security Architecture for Distributed Energy Resources Integration. EPRI, Palo Alto, CA: 2018. 3002014145.

EPRI's Distributed Energy Resources Integration Toolkit: An Overview of EPRI Tools for Testing and Implementing Open Protocols. EPRI, Palo Alto, CA: 2018. 3002013623.

Enabling Voice Assistants for Demand Response and Demand Side Management. EPRI, Palo Alto, CA: 2020. 3002013349.

From Innovation to Standards: Technology Evolution. EPRI, Palo Alto, CA: 2018. 3002014840.

Grid Security of Connected Devices: Communications and Cybersecurity Assessment. EPRI, Palo Alto, CA: 2019. 3002016154.

Hui, H., et al. "5G Network-Based Internet of Things for Demand Response in Smart Grid: A Survey on Application Potential." *Applied Energy,* **257** (2020) 113872. Retrieved from https://www.sciencedirect.com/science/article/pii/S0306261919316599?via%3Dihub.

IEC 61968-5 Distributed Energy Optimization to Open Field Message Bus (OpenFMB) Mapping. EPRI, Palo Alto, CA: 2019. 3002016145.

Lightweight Messaging Technologies for the Energy Internet of Things: An Introduction. EPRI, Palo Alto, CA: 2018. 3002013478.

Low-Power Wide-Area Networks: Overview, Characteristics, and Applications. EPRI, Palo Alto, CA: 2018. 3002009791.

Meloni, A., and Atzori, L. "The Role of Satellite Communications in the Smart Grid." *IEEE Wireless Communications.* **24**(2): 50-56. April 2017. https://doi.org/10.1109/MWC.2017.1600251.

Next Generation Wireless Local Area Network (WLAN). EPRI, Palo Alto, CA: 2021. 3002022297.

NIST. *Recommendation for Key Management.* SP-800-57. 3 Parts, 2015-2020.

NIST. *Transitioning the Use of Cryptographic Algorithms and Key Lengths.* SP-800-131A. 2019.

OpenADR 2.0 Open Source Virtual Top Node (VTN) User's Manual. EPRI, Palo Alto, CA: 2017. 3002011483.

Open Source DER Outstation for DNP Application Note AN2018-001: Reference Implementation of DNP Application Note AN2018-001 – "DNP3 Profile for Communications with Distributed Energy Resources". EPRI, Palo Alto, CA: 2019. 3002015355.

Performance Test Results: CTA-2045 HVAC Thermostat: Testing Conducted at the National Renewable Energy Laboratory. EPRI, Palo Alto, CA: 2017. 3002011747.

Performance Test Results: CTA-2045 Water Heater: Testing Conducted at the National Renewable Energy Laboratory. EPRI, Palo Alto, CA: 2017. 3002011760.

Performance Test Results: CTA-2045 Electric Vehicle Supply Equipment—Testing Conducted at the National Renewable Energy Laboratory. EPRI, Palo Alto, CA: 2017. 3002011757.

PG&E Case Study – Attack Models and Security Gaps in Distributed Energy Resource Interoperability Standards: IEEE 2030.5 and 1547 Security Gaps, Impact Scenarios, and Mitigations. EPRI, Palo Alto, CA: 2019. 3002016040.

Program on Technology Innovation: Disruptive Innovations for Heating, Ventilation, and Air Conditioning (HVAC) Systems – 2017. EPRI, Palo Alto, CA: 2018. 3002013866.

Program on Technology Innovation: Evaluating IoT Messaging Protocols for DER Management. EPRI, Palo Alto, CA: 2018. 3002014678.

Reka, S. S., et al. "Future Generation 5G Wireless Networks for Smart Grid: A comprehensive Review." *Energies* **12**(11): 2140. 2019. https://doi.org/10.3390/en12112140.

Remote Device Management: Utility Requirements. EPRI, Palo Alto, CA: 2019. 3002015875.

Residential Battery Energy Storage: Demand Response Opportunities with OpenADR 2.0b—Field Deployments and Performance Analysis. EPRI, Palo Alto, CA: 2020. 3002017985.

Resilient Communication Demonstration Project: Demonstration Evaluation Report. EPRI, Palo Alto, CA: 2020. 3002017908.

Resilient Communications Selection and Design. EPRI, Palo Alto, CA: 2020. 3002018702.

Test Procedure for Validating DNP Application Note AN2018-001 in Distributed Energy Resources: Example Test Procedure for Evaluating Conformance to DNP Application Note AN2018-001 – "DNP3 Profile for Communications with Distributed Energy Resources". EPRI, Palo Alto, CA: 2019. 3002016144.

Export Control Restrictions

Access to and use of this EPRI product is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or U.S. permanent resident is permitted access under applicable U.S. and foreign export laws and regulations.

In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI product, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case by case basis an informal assessment of the applicable U.S. export classification for specific EPRI products, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes.

Your obligations regarding U.S. export control requirements apply during and after you and your company's engagement with EPRI. To be clear, the obligations continue after your retirement or other departure from your company, and include any knowledge retained after gaining access to EPRI products.

You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of this EPRI product hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI members represent 90% of the electricity generated and delivered in the United States with international participation extending to nearly 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; Dallas, Texas; Lenox, Mass.; and Washington, D.C.

Together…Shaping the Future of Electricity

10xxxxx

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com