4E Electronic Devices & Networks Annex EDNA

Guide to energy management protocols

NOVEMBER 2022

Technology Collaboration Programme
by iea

4E
Energy Efficient End-use Equipment
International Energy Agency

The Technology Collaboration Programme on Energy Efficient End-Use Equipment (4E TCP), has been supporting governments to co-ordinate effective energy efficiency policies since 2008.

Fourteen countries and one region have joined together under the 4E TCP platform to exchange technical and policy information focused on increasing the production and trade in efficient end-use equipment. However, the 4E TCP is more than a forum for sharing information: it pools resources and expertise on a wide a range of projects designed to meet the policy needs of participating governments. Members of 4E find this an efficient use of scarce funds, which results in outcomes that are far more comprehensive and authoritative than can be achieved by individual jurisdictions.

The 4E TCP is established under the auspices of the International Energy Agency (IEA) as a functionally and legally autonomous body.

Current members of 4E TCP are: Australia, Austria, Canada, China, Denmark, the European Commission, France, Japan, Korea, Netherlands, New Zealand, Switzerland, Sweden, UK and USA.

Further information on the 4E TCP is available from: **www.iea-4e.org**

4E
Electronic Devices & Networks Annex
EDNA

The EDNA Annex (Electronic Devices and Networks Annex) of the 4E TCP is focussed on a horizontal subset of energy using equipment and systems - those which are able to be connected via a communications network. The objective of EDNA is to provide technical analysis and policy guidance to members and other governments aimed at improving the energy efficiency of connected devices and the systems in which they operate.

EDNA is focussed on the energy consumption of network connected devices, on the increased energy consumption that results from devices becoming network connected, and on system energy efficiency: the optimal operation of systems of devices to save energy (aka intelligent efficiency) including providing other energy benefits such as demand response.

Further information on EDNA is available from: **www.edna.iea-4e.org**

This report was commissioned by the EDNA Annex of the 4E TCP and authored by Analytical Engines Pty Ltd. The views, conclusions and recommendations are solely those of the authors and do not state or reflect those of EDNA, the 4E TCP or its member countries.

Views, findings and publications of EDNA and the 4E TCP do not necessarily represent the views or policies of the IEA Secretariat or its individual member countries.

Guide to Energy Management Protocols

Final Report

David Coote
Analytical Engines
November 2022

Contacts

David Coote
Analytical Engines Pty Ltd

david.coote@analyticalengines.com.au

Revision History

Date	Version	Description	Author/s
10/11/2022	Release		David Coote

Disclaimer

This report is prepared by Analytical Engines Pty Ltd (AE).

AE was engaged and paid by Beletich Associates (the Operating Agent), Australian business number 52634965431, acting as the Operating Agent for the Electronic Devices and Networks Annex (EDNA) of the International Energy Agency's Energy Efficient End-Use Equipment Technology (4E) Collaboration Programme (Client).

The report is solely for the use of the Client. It is not intended to, and should not, be relied upon by anyone else.

AE does not accept any duty of care, to any other person or entity other than the Client.

The report has relied on the information provided to AE by the Client being true, accurate and complete.

It should be understood that:

- information contained in the report that has been sourced from third-parties or that has been provided to AE by the Client is assumed to be true, accurate and complete;
- information contained in the draft report is general in nature;

A copy of the report can be released on the basis that (i) it is published for general information only, and (ii) AE does not accept any duty, liability or responsibility to any person (other than the Client) in relation to the report.

Recipients of the report (other than the Client) should seek independent expert advice as this report was not prepared for them or for any other purpose.

Information contained in the report is current as at the date stated in the report and may not reflect any event or circumstances which occur after the date of the report.

All questions related to the content, or to any use of the report, should be addressed by email to David Coote at david.coote@analyticalengines.com.au

Contents

Tables

Figures

Abbreviations

Abbreviation	Full
AC	air conditioning
AC	alternating current
AMQP	Advanced Message Queueing Protocol
API	Application programming interface
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
Blockchain	An open, distributed software ledger that records transactions between two parties verifiably and permanently using cryptography
BTM	behind the meter
CHP	combined heat and power
CoAP	Constrained Application Protocol
CSIP	Common Smart Inverter Profile
COP	Coefficient of performance
CPUC	California Public Utilities Commission
CSA	Connectivity Standards Alliance
DC	direct current
DHW	domestic hot water for showers, hand washing and cleaning
DER	distributed energy resource(s)
EE	energy efficiency
EMS	energy management system; also HEMS home energy management system
ETSI	European Telecommunications Standards Institute
EV	electric vehicle
GHG	greenhouse gases
GIWH	grid interactive hot water heater
GW	gigawatt — unit of power. One billion watts
GWH	gigawatthour — unit of energy. One billion watt-hours
HHW	heating hot water for space heating
HTTP	Hypertext transfer protocol
HVAC	heating, ventilation and air-conditioning
HW(S)	hot water (service)
HVAC	heating, ventilation and air-conditioning
IEA	International Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFTTT	If This Then That

IoT	Internet of Things
ISO	International Standards Organisation
JSON	JavaScript Object Notation
kV	kilovolt — unit of voltage. 1000 volts.
kW or KW	kilowatt — unit of power
LED	light emitting diode
Li	lithium chemistry battery
LPG	liquefied petroleum gas
M2M	Machine to Machine
MJ/kg	megajoules per kilogram
MW	megawatt — unit of power. 1 million watts
MWH	megawatt hours — unit of energy. 1 million watt hours
NIST	National Institute of Standards and Technology
OASIS	Organization for Advancement of Structured Information Standards
OCF	Open Connectivity Foundation
OCPP	Open Charge Point Protocol
OECD	Organisation for Economic Co-operation and Development
OSCP	Open Smart Charging Protocol
OSI	Open Systems Interconnection
P50	minimum annual generation expected in 50% of years
PKI	Public Key Infrastructure
PPA	power purchase agreement
PV	photovoltaic
REST	representational state transfer
SCADA	supervisory control and data acquisition
SOAP	Simple Object Access Protocol
TCP/IP	transmission control protocol/internet protocol
TLS	transport layer security
TMY	typical meteorological year
TOU	time of use
UDP	User Datagram Protocol
VEN	virtual end node
VPP	virtual power plant
VTG	vehicle to grid
VTH	vehicle to home
VTN	virtual top node
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

Executive Summary

Electricity demand response/flexibility can reduce electricity demand and move demand to times when it is easier to supply. Effective demand response/flexibility can reduce the maximum electricity generation capacity required and improve economic use of existing generation capacity. Reducing required generation capacity and optimising use of existing capacity can in turn reduce the transmission and distribution infrastructure needed for a grid. These benefits can reduce customer bills and the need for government support for the electricity sector from the general budget.

As well as benefits from traditional grid load management, electricity demand response/flexibility can realise new opportunities from variable renewable generation. Ubiquitous, cheap, easily deployed, interoperable networking technology can support more flexible demand management than older methods. Using these techniques facilitates demand management at site or household level from an energy management system as well as traditional centralised control from grid operators and aggregators.

The massive decentralisation of energy generation from PV installed in communities and individual sites combined with other distributed energy resources including batteries, thermal storage using heatpumps and resistive hot-water heaters, and load management of other distributed energy resources including HVAC, pool-pumps and other devices increases demand management potential. Electric Vehicles (EVs) in particular are a challenge for grids and a significant demand management opportunity.

To assist policy makers responsible for demand management outcomes, this brief report covers aspects of application layer protocols that can be used for demand management in networked devices. Definitions (Section 1.2) are followed by an introduction to the protocol stack concept (Section 2) and some brief notes on cybersecurity (Section 3). Common energy device control functions are listed (Section 4).

Energy management application protocols are split into categories and characterised by a selection of criteria (Section 5):

- Protocols designed to support device energy management
- Protocols for EV charging
- Building, industrial and home automation protocols with some device energy management support
- Internet of Things (IoT) protocols

Energy devices that can achieve required energy management outcomes with simpler hardware interfaces can implement several open platform initiatives (Section 6).

Future work can build on this report to cover important topics including vendor lockin, mandatory device support for control and state persistence, and open access within an appropriate cybersecurity framework to energy device control and state. Animations and graphics can illustrate how application protocols work to sectoral stakeholders and other parties. Relevant physical/network layer protocols are listed (Appendix A) as are common internet stack application protocols (Appendix B) which can be used for many purposes including energy management.

1. Introduction

EDNA considers that device communication protocols have a significant impact on device energy consumption in these areas:

- **Energy management functionality can be implemented in the application layer of protocol stacks[1].** Energy management application layers are used to facilitate *systems* of devices as well as managing individual devices. Energy management functionality includes:
    - saving energy - EDNA calls this "**intelligent efficiency**"
    - responding to the needs of the grid - EDNA calls this "**demand flexibility**".
- **Protocols that reside in the physical/network layers** are essential for devices to communicate, including during periods when the device primary function is not being performed but the device is maintaining its network connection. The power used in this "network standby" mode is heavily dependant on the communications protocol used.

Physical/network layer protocols include Wifi, Zigbee, Bluetooth, Ethernet, etc. (refer Appendix A for more information). EDNA has produced a number of reports related to these protocols and their relevance to network standby power draw. These reports can be found in the publications area of the EDNA website[2].

This report is focussed on energy management protocols that reside in the application layer, which are used to facilitate intelligent efficiency and demand flexibility.

Intelligent efficiency is defined as the operation of device(s) such that they respond to the changing conditions of the external environment, in order to maximise energy savings[3].

Demand flexibility – with respect to devices – in other words 'demand flexible devices' – are defined as devices with advanced communication and control capabilities which can automatically and dynamically change energy use in response to changing electricity prices and grid system needs[3].

This report is a short guide for policy makers interested in energy management protocols used with devices to increase efficient energy usage. This focus intersects with traditional energy efficiency, demand management and demand response/flexibility as well as more recent initiatives managing distributed energy resources with site and grid level variable renewable energy.

The report includes:

- A general overview of energy management protocols including some categorisation by functionality
- Some details of market uptake of relevant protocols
- How various protocols affect device and broader energy consumption
- Protocol descriptions and relevance to energy system device management

[1] 'Layers' refers to where a protocol resides in the 'layered protocol stack'. This concept is described in more detail in Section 2.

[2] https://www.iea-4e.org/edna/publications/

[3] https://www.iea-4e.org/publications/?_sf_s=policy%20guidance%20for%20smart%20energy%20saving%20consumer%20devices. Accessed May 4th, 2022

1.1 Scope

There is an extensive range of devices that have energy consumption affected by communications protocols. This could range from include 500MW steam rankine cycle turbines to electronic consumer devices powered by tiny button batteries or ambient energy harvesting technology.

To keep scope manageable for a short guide this work will build on definitions in "More data, less energy" (IEA 2014) to exclude devices whose primary function is:

- data storage or use
- entertainment
- communication
- network connectivity
- network infrastructure.

to focus on other networked edge devices such as inverters, batteries, electric vehicles, water heating, water pumps, kitchen and laundry appliances, space conditioning (heating and cooling) equipment and lighting at residential and smaller commercial and industrial scale.

Further scope limitation exclusions are:

- specialised commercial and industrial equipment such as machine tools, industrial hydraulics and pneumatics and other.
- electricity and gas metering

However, while these devices are treated as outside scope for this report, it should be noted that common energy efficiency goals include:

- Reduce the volume of energy consumed
- Reduce the peak demand
- Move load to off-peak periods where possible.

To achieve aims such as:

- Saving customers money by:
    - reducing the volume of energy subject to a tariff
    - moving energy consumption to a cheaper tariff
    - increasing onsite consumption of behind-the-meter PV generation and storage
    - reducing critical peak demand charges.
- Reducing thermal loads and overvoltage on electricity grids.
- Reducing gas or electricity grid load to below maximum capacity for the relevant grid section.

Sites can also manage loads to avoid exceeding switchboard or grid connection (substation, transformer) maxima. Sites managing loads and PV export can also contribute to grid stability by reducing overvoltage and undervoltage.

These goals and aims can exist at:

- a grid-connected house with energy system devices including an inverter, rooftop PV, battery, heatpump and resistance hot-water systems, space conditioning heatpump and EV charger
- or at a 1GW green hydrogen plant with an onsite windfarm and solar farm, rapidly rampable PEM electrolyser, grid connection for opportunistic energy sales and purchases, onsite battery and hydrogen storage, pumps and EVs (and chargers) for onsite and road use.

Some existing energy system communications protocols – perhaps with some additions where necessary – implement use cases applicable across a range of devices beyond those covered in this report and can already be flexible enough to cope with more specialised use cases. This can have other customer benefits such as access to proven technology stacks and existing expertise, quicker implementation and reducing vendor lockin. Experience with what has contributed to the remarkable progress in the ICT sector over the last 30+ years should encourage the energy sector as it transitions to renewables to consider factors including open platforms, standardisation and plug and play user experience.

1.2 Definitions

Energy management systems are used to manage onsite networked devices at homes, offices, farms, factories and other sites to achieve outcomes including:

- minimising energy cost by:
  - load management
  - maximising financially beneficial onsite consumption of onsite PV generation
  - optimising tariff use for residual grid supply and storage
  - optimising battery and thermal storage charge and supply
  - exporting energy from a site to be paid by feedin tariffs, market spot prices and network support
- reducing grid impact of site demand and export where required or financially incentivised by an external party
- participation in aggregated/orchestrated mechanisms such as virtual power plants to support frequency control and ancillary services.

Smart grid technology supports two way communication and power flow across a grid. Typically this will involve management and interaction with distributed energy resources such as PV, thermal and battery storage, wind, despatchable devices such as pool pumps and electric vehicle chargers, demand response participating devices such as air-conditioners and other energy system devices.

Note that smart grid technologies can be deployed at national or regional grid level but also in microgrids or behind-the-meter at individual sites.

An **aggregator** will manage a cohort of energy devices across multiple sites to achieve a demand management/response outcome. Aggregators might be electricity retailers, electricity distribution services operators, grid operators (most likely in smaller grids) or entities specialising in this service.

2. Introduction to the Protocol 'Stack'

The Australian Research Data Commons[4] (ARDC) defines a communications protocol as "a set of formal rules describing how to transmit or exchange data, especially across a network." The ARDC states that a "standardised communications protocol is one that has been codified as a standard.". Regulators will find it easier to develop device demand management frameworks where there are standardised protocols available that support the functionality required. *Ad hoc* device demand management functionality which changes without notice and which may suffer from inadequate documentation complicates regulatory development of device demand management frameworks

Communications protocol developers, industry associations and standards bodies have found that developing protocols as layered stacks simplifies definition, development, testing and deployment. A protocol stack at a networked device takes data from a human or other source and passes it through each layer until it is sent by the physical layer across the network to another networked device. At the recipient device data is passed up through each layer of the protocol stack to the application layer. The application layer at the sending and recipient device is the interface to other software like email clients and web browsers. HEMS and aggregators requiring demand management services can interface with the application layer of protocols that support demand management.

Layers in the protocol stack:

- pass protocol data units upwards or downwards through the stack
- add layer specific information (encapsulation) to protocol data units going down the stack from the application layer to the physical layer
- remove the layer specific header added by the corresponding layer at the sending device (de-encapsulation) for protocol data units heading up the stack to the application layer.

As well as print textbooks, there is a wealth of online tutorials, YouTube videos[5] [6], animations, books, training manuals and other relevant material covering protocol stacks including encapsulation and de-encapsulation.

The Transport Control Protocol/Internet Protocol[7] (TCP/IP) stack is widely used in the Internet. Another influential protocol stack is Open Systems Interconnection (OSI)[8].

[4] https://ardc.edu.au/resources/standardised-communications-protocols/. Accessed 28th April, 2022

[5] https://www.youtube.com/watch?v=kCuyS7ihr_E Accessed 27th August, 2022.

[6] https://www.youtube.com/watch?v=vv4y_uOneC0

[7] https://datatracker.ietf.org/doc/html/rfc1122 Accessed 29th April, 2022

[8] https://www.iso.org/ics/35.100/x/ Accessed 29th April, 2022.

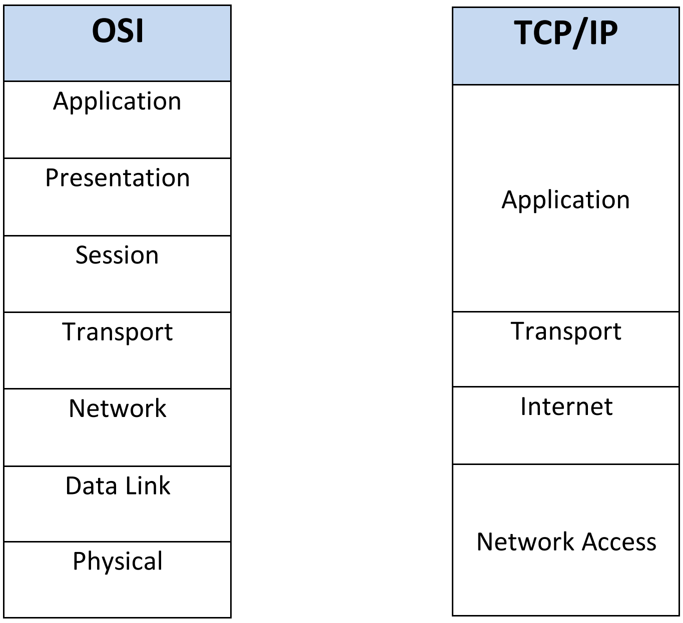

Figure 1 OSI and TCP/IP protocol stack layers

OSI Protocol Stack	
Layer	Purpose
Application	Data to and from user applications such as a web browser
Presentation	Manage information presentation including conversion to and from standard network format. Encryption and decryption occurs at this layer.
Session	Manages communications between sessions connected over the network.
Transport	Ensures complete data transfers across a network
Network	Data addressing and routing across a network.
Data Link	Reliable transmission of data between two physically connected network nodes.
Physical	Interface to network. Handles data rate, transmission type, electrical, physical and optical requirements.

Table 1 OSI protocol stack layers and purpose

TCP/IP Protocol stack	
Layer	Purpose
Application	Defines protocols applications use to exchange data.
Transport	Session and datagram communication services using TCP and UDP.
Internet	Host addressing, data packaging and routing.
Network Access	Sends and receives TCP/IP packets on the physical network.

Table 2 TCP/IP protocol stack layers and purpose

Appropriately defined and standardised application protocols like IEEE2030.5 and Open ADR can support a rich set of demand management use cases across many device types. Other protocols may support a smaller range of use cases on a more limited set of device types.

3. Cybersecurity

Cybersecurity for networked energy devices is a large area which is currently the subject of considerable attention in governments, standards bodies, trade and industry associations and other. Networked energy devices that don't implement data encryption, access control and other cryptosecurity requirements may allow access to entities with malicious intent. For example, rapidly turning on and off a large cohort of heatpumps could damage the heatpumps and cause considerable grid operation issues.

A relevant recent National Renewable Energy Laboratories (NREL) report discusses cybersecurity certification for networked grid-edge devices.[9] NREL developed the Distributed Energy Resource Cybersecurity Framework "to evaluate the cybersecurity posture of federal sites that employ distributed energy systems or plan to implement distributed energy resources (DERs) for day-to-day operations".[10] The National Institute of Standards and Technology cybersecurity framework aims to help "organizations to better understand and improve their management of cybersecurity risk"[11] Industry bodies are active in DER cybersecurity. The Sunspec Alliance DER Cybersecurity working group publish Certification Procedures for Data and Communications Security of DER and other relevant material.[12] Singapore has a cybersecurity labelling program for internet connected devices. The US has announced the intention to introduce internet connected device cybersecurity device labelling.

[9] https://www.nrel.gov/docs/fy22osti/80581.pdf Accessed August 24th, 2022
[10] https://dercf.nrel.gov/about Accessed August 24th, 2022
[11] https://www.nist.gov/cyberframework Accessed August 24th, 2022
[12] https://sunspec.org/specifications/ Accessed August 25th, 2022

4. Common energy device control functions

Devices will (or should) share some common control functions. The communications protocol stack directly or indirectly supports this commonality.

Relevant network device protocol implementations need to receive data and instructions from external agents such as Home Energy Management Systems (HEMS) and aggregators. The agents and devices also need to check and co-ordinate factors state such as when they are operational and available. Polling and pub/sub are common methods to access data, instructions and state. Polling has the software stack in the networked device regularly checking the external agent for data, instructions and relevant external agent state. Polling is often described as synchronous as the polling response is expected on receipt of the poll. In contrast, pub/sub mechanisms are typically asynchronous. A device will subscribe to a topic and go on with other processing. Once a message is published at some future time to a topic the subscribing device will be informed.

Standards such as IEEE2030.5 and OpenADR (Section 5) and EN 50631-1[13] suggest indicative demand flexibility use cases which rely on energy device control functions.

Common energy device control functions follow.

Turn off/on

A device may be turned on and off.

Register with management entity

A device may actively register with a management entity.

Device discovery

A device may be discovered on a network by a management entity which registers the device.

Start/stop device control

A device may on command enter or leave a controlled mode. Some devices under some protocols can tell a controlling entity that they are leaving the controlled mode.

Scheduling

Actions at a device may be scheduled to occur or not occur during specified periods.

Tariff information

A device with onboard scheduling or a device controlling schedules for other devices can use tariff information in scheduling.

Set device state

A networked energy system device may have configuration state that can be set by an external party.

[13] https://www.en-standard.eu/csn-en-50631-1-household-appliances-network-and-grid-connectivity-part-1-general-requirements-generic-data-modelling-and-neutral-messages/ Accessed November 9th, 2022

Report device state

A device can report current configuration and operational state on request or on a regular interval.

Update device software

Devices with software stored in writable memory may support over-the-air upgrades. This requires access protection and an update delivery chain that ensure what's installed is the upgrade without any tampering by external parties.

Setpoint set and report

Temperature setpoints are a common example of system state used to manage HVAC equipment.

Reduce/increase energy consumption

Some devices may be capable of reducing or increasing energy consumption on demand or following a schedule. The reduction might be an absolute amount or relative to or offset from some system value or parameter (such as a reduction to 75% or 50% operating capacity). This is useful for critical peak demand management in response to a grid event or to minimise critical peak demand charges.

Reduce/increase energy export

Some DER devices such as home battery systems, EV batteries and inverters can export to the grid on demand or following a schedule. A device with this capability may be told to reduce or increase export.

5. Relevant energy management protocols

5.1 Overview

For the purpose of this report, protocols used for energy management can be categorised into the following areas:

- Protocols designed to support device energy management
- Protocols for EV charging
- Building, industrial and home automation protocols with some device energy management support
- Internet of Things (IoT) protocols

As well as the energy management protocols listed in this section, there are a number of workflow/integration tools such as If This Then That (IFTTT)[14] and Node-RED[15] that can be used to build applications with networked energy devices and relevant exposed APIs to deliver energy management services. Advanced Message Queueing Protocol (AMQP)[16] could also be used to link networked energy devices in frameworks.

5.2 Protocol Characteristics Summaries

The following tables present summaries of selected protocols. More detailed protocol characterisations follow these summaries.

Designed to support device energy management							
Protocol	**Responsible Entity**	**Used for**	**Open source avail.**	**License required**	**Market presence**	**Technical ecosyst.**	**Cybersecurity support**
OpenADR	OpenADR Alliance	Smart grid	Yes	No	Established	Yes	Yes
IEEE 2030.5	IEEE	Smart grid	Yes	No	Growing	Growing	Yes
EEBUS	EEBUS Initiative	Selected smart grid use cases	No	No	Implemented by range of manufacturers	Growing	Yes

Table 3 Protocols designed to support device energy management

[14] https://ifttt.com/ Accessed May 12th, 2022
[15] https://nodered.org/ Accessed May 13th, 2022
[16] https://www.amqp.org/ Accessed May 12th, 2022

EV Charging							
Protocol	**Responsible Entity**	**Used for**	**Open source avail.**	**License required**	**Market presence**	**Technical ecosyst.**	**Cybersecurity support**
OCPP	Open Charge Alliance	Aggregated control of EV chargers	Yes	No	De-facto open standard	Yes	Yes
OSCP	Open Charge Alliance	EV charger details for OCPP server/EMS	Yes	No	Association with OCPP may help uptake.	Growing	Yes

Table 4 EV charging protocols

Building, industrial and home automation protocols with some device energy management support							
Protocol	**Responsible Entity**	**Used for**	**Open source avail.**	**License required**	**Market presence**	**Technical ecosyst.**	**Cybersecurity support**
BACnet	ASHRAE	Building automation	Yes	No	Substantial	Yes	BACnet Secure
Modbus	Modbus Organisation	Device monitoring and control	Yes	No	Substantial	Yes	Modbus/TCP Security
Matter	Connectivity Standards Alliance (CSA)	Home automation	Yes	Yes	Developing	Growing	Yes
KNX	KNX Association	Home automation	Yes	Yes	Substantial	Yes	KNX Secure

Table 5 Building, industrial and home automation protocols with some device energy management support

Internet of Things							
Protocol	**Responsible Entity**	**Used for**	**Open source**	**License required**	**Market presence**	**Technical ecosyst.**	**Cybersecurity support**
CoAP	IETF	Low-power M2M IoT	Yes	No	Established	Yes	Yes
MQTT	OASIS	Small microcontroller IoT	Yes	No	Established	Yes	Yes

Table 6 Internet of Things protocols

5.3 Protocols designed to support device energy management

Some application protocols are designed to support a range of networked device energy management use cases. These include:

- OpenADR[17,18]
- IEEE2030.5[19]
- EEBUS[20]

Descriptions

OpenADR:

- Developed by the not-for-profit OpenADR Alliance "to standardize, automate, and simplify Demand Response (DR) and Distributed Energy Resources (DER) to enable utilities and aggregators to cost-effectively manage growing energy demand & decentralized energy production, and customers to control their energy future." Open ADR defines Virtual Top Nodes (VTNs) as servers and Virtual End Nodes (VENs) as clients. VTNs can aggregate devices at utility, distribution, grid or site level.
- License required. No.
- Open source implementations. Yes.
- Conformance testing available. Yes.
- Market presence. Implemented and used across many device types including thermostats/HVAC systems, energy management systems, EV charge controllers, inverters and others. OpenADR state there are more than 200 products deployed implementing OpenADR.
- Technical ecosystem. Development and support experience available.
- Runs over: HTTP and XMPP.
- Message datatypes. Event service messages are demand response events such as prices/incentive payments, curtailment levels/direct load control and other demand response signals sent to VENs by VTNs. VENs send event service messages to VTNs to indicate whether devices and other resources will participate. Report service messages are used by VTNs and VENs to send reports containing historical, actual and forecast data including curtailment, status and availability.
- Common use. Aggregated demand response/management across networked energy devices.

[17] https://www.openadr.org/ Accessed May 12th, 2022
[18] https://webstore.iec.ch/publication/26267 Accessed August 25th, 2022
[19] https://standards.ieee.org/ieee/2030.5/5897/ Accessed May 12th, 2022
[20] https://www.eebus.org/ Accessed May 12th, 2022

- Extensible. Designed to be extensible with new devices.
- Cybersecurity. Checked as part of the compliance certification process. Uses TLS with digital certificates to authenticate communication links between OpenADR servers and clients. OpenADR maintains its own Public Key Infrastructure through a third party organisation.

IEEE2030.5:

- Developed by the IEEE as part of the IEEE2030 suite of standards for smart grids starting from the earlier ZigBee Smart Energy Profile 2. 2030.5 is referenced by the California Public Utilities Commission (CPUC) Rule 21 and Common Smart Inverter Profile (CSIP). CPUC Rule 21 mandates that generators such as wind turbines and PV systems using inverters must support an application layer protocol that can be used by utilities to manage smart inverter functions and send status information to the utility. 2030.5 supports the inverter messaging functionality required by CSIP but also supports other DER functionality. 2030.5 was designed to manage devices directly. This may change in later versions to include functionality similar to the Open ADR approach of using a site EMS or aggregator to translate demand management requirements into specific device commands.
- License required. No.
- Open source implementations. Yes.
- Conformance testing available. Yes.
- Market presence. California is a large market in its own right. Technology decisions and frameworks developed in California influence other countries and regions. Australia and several other countries are investigating use of 2030.5 based DER management approaches.
- Technical ecosystem. Some development and support experience available and likely to grow. A full implementation of the IEEE2030.5 client and a server capable of managing many clients is a complicated piece of software.
- Runs over: HTTP, TCP/IP, BlueTooth and others.
- Message datatypes. End device determines whether pub/sub or polling is used. Data compression is supported. DER information model based on SunSpec[21] and IEC 61850[22]. Core and optional function sets support pricing, device management, load control, discovery, metering and others
- Common use. Curtailing PV inverters. Broader deployment to manage DERs at town level has been trialled.
- Extensible. Designed to support range of customers and smart grid/DR programs.
- Cybersecurity. Strong focus of 2030.5. TLS with digital certificates/PKI/access control to meet National Institute of Standards and Technology (NIST) standards.

[21] https://sunspec.org/ Accessed May 12th, 2022

[22] https://webstore.iec.ch/publication/6028 Accessed 17th May, 2022

EEBUS:

- Developed by the EEBUS Initiative e.V. which states it is a "non-profit association with leading manufacturers from the sectors of networked building technology, electromobility and energy". Members mentioned on the EEBUS website include many well-known companies from these sectors. EEBUS partners include OpenADR, Open Charge Alliance and Thread. EEBUS is designed to provide an open interoperability framework for these sectors.
- License required. No.
- Open source implementations. At the time of writing no EEBUS endorsed reference open source implementations were mentioned on the EEBUS website.
- Conformance testing available. Yes
- Market presence. Implemented and used across many device types in energy management, industrial, building management and other sectors.
- Technical ecosystem. Development and support experience available.
- Runs over: UDP over IP to find Smart Home IP (SHIP) devices, TCP, Web Sockets and the SHIP Message Exchange protocol.
- Message datatypes. Smart Premises Interoperable Neutral-message Exchange (SPINE) defines device and data models including message content, how to connect SPINE devices and use cases supported. Mapping available to OpenADR.
- Common use. Aggregated control of heatpumps at multiple sites, dynamic building power limitation setpoints, HVAC and electric vehicle management.
- Extensible. SPINE toolbox designed to be extensible with new use cases and devices.
- Cybersecurity. TLS and other.

5.4 Protocols for EV charging

5.4.1 EV charging themes

Charging electric vehicles is widely forecast to drastically increase the amount of electricity consumed in many grids. Commentators have suggested apocalyptic scenarios of distribution sections and grids overwhelmed by peak loads caused by large numbers of EV chargers running simultaneously at times such as weekday evenings after the daily commute. These scenarios have been used as an argument for expensive grid upgrades. Increasing the regulated asset base in many jurisdictions flows through directly to utility/distributor revenues. Electricity customers commonly pay for grid upgrades through network tariffs. Direct government subsidy of grid upgrades from the general budget increases taxation or reduces expenditure on other programs.

Many EV models have extensive connectivity and onboard load management support. Where these are accessible through open protocols, EV charging can be an excellent use case for intelligent energy supply management from third parties whether these be onsite EMS, aggregators, electricity distributors or grid operators. Site level energy management can optimise EV charging with time-of-use or dynamic tariffs, controlled load tariffs and availability of onsite PV. Site charging can cater for multiple chargers at sites with carparks including apartment blocks, factories, offices, supermarkets and others.

Charging management can also be centralised by aggregators, distribution services organisations or at grid level where the computational load and other software issues can be managed. Centralised charging management is popular with grid operators as it facilitates transparency and a higher level of hierarchical control over EV charging. How to co-optimise onsite energy use optimisation by energy management systems with external control of EV chargers is a challenge.

Vehicle-to-grid (VTG) and vehicle-to-home (VTH) have received significant attention with mostly trial deployment at the time of writing. VTG and VTH once available and implemented by car manufacturers can use an EV battery as a networked energy device with similar use cases to behind-the-meter batteries.

How best to deploy EV charging, vehicle-to-home and vehicle-to-grid is beyond this report's scope but will be a topical, important and fascinating policy area over the next 20 years. Balancing customer and electricity sector objectives will pose challenges.

5.4.2 Protocols

Standards outside scope for this report include:

- IEC 61851[23]. Covers the hardware connection between the vehicle and charger.
- IEC 63110[24]. Developing standard for communication between charger and charging management system.
- ISO 15118[25]. Developing standard for vehicle to grid supply.
- Several vendors and other bodies including CHAdeMO[26] and Combined Charging System[27] have developed hardware and software charging solutions.
- Roaming protocols used for EVs charging at multiple charge points. As well as proprietary protocols there are open roaming protocols including Open Clearing House Protocol (OCHP)[28], Open Interchange Protocol (OICP)[29] and eMIP.[30] A recent Technical University of Eindhoven report covers these protocols.[31]
- OpenEVSE[32] have an open source hardware and software charging solution which at this point implements its own application protocol.

OpenADR, IEEE2030.5 and EEBUS all support EV charging use cases including Open Charge Point Protocol[33] mappings. CTA2045 and DRED (see Section 6.1.3) can be mapped to EV hardware charging interfaces.

[23] https://webstore.iec.ch/publication/33644 Accessed May 18th, 2022

[24] https://www.iec.ch/ords/f?p=103:38:612167375351870::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1255,23,100390 Accessed May 18th, 2022

[25] https://www.iso.org/standard/69113.html Accessed May 18th, 2022

[26] https://www.chademo.com/ Accessed May 18th, 2022

[27] https://www.charin.global/ Accessed August 24th, 2022

[28] http://www.ochp.eu/ Accessed May 20th, 2022

[29] https://assets.website-files.com/602cf2b08109ccbc93d7f9ed/60534f2e20d0f87be17ba21b_oicp-cpo-2.2.pdf Accessed May 20th, 2022

[30] https://www.gireve.com/wp-content/uploads/2019/10/Gireve_Tech_eMIP-V0.7.4_ImplementationGuide_1.0.7_en.pdf Accessed May 20th, 2022

[31] van der Kam, M., & Bekkers, R. N. A. (2020). Comparative analysis of standardized protocols for EV roaming: Report D6.1 for the evRoaming4EU project. Netherlands Knowledge Platform for Public Charging Infrastructure (NKL)

[32] https://www.openevse.com/ Accessed May 18th, 2022

[33] https://www.openchargealliance.org/ Accessed May 18th, 2022

Descriptions

Open Charge Point Protocol (OCPP):

- Developed by the Open Charge Alliance which states it is "a global consortium of public and private electric vehicle infrastructure leaders that have come together to promote open standards through the adoption of the Open Charge Point Protocol (OCPP) and the Open Smart Charging Protocol (OSCP)." OCPP1.6 supports communication between EV chargers and charging station management systems. A charging station management system may manage many EV chargers. OCPP2.0.1 improves security and adds several features including support for ISO15118.
- License required. No.
- Open source implementations. Yes.
- Conformance testing available. Yes
- Market presence. Regarded as the de-facto open standard.
- Technical ecosystem. Development and support experience available.
- Runs over. Client/server with station management systems as server and charging station as client. JSON over websockets and SOAP are supported.
- Message datatypes. Range of message types for charging station get and set configurations, setting/cancelling EV charging sessions, starting/stopping transactions, messages to EV driver covering information such as rates and tariffs and others.
- Common use. Manage multiple charging stations/EV chargers.
- Extensible. Designed to be interoperable. The device model introduced in OCPP2.0 supports compatible devices beyond EV chargers.
- Cybersecurity. TLS/PKI/certificates.

Open Smart Charging Protocol (OSCP):

- Developed by the Open Charge Alliance. OSCP2.0 informs an OCPP server or energy management system of the available charging capacity, site generation and consumption forecasts and other. As well as EV chargers, OSCP2.0 is designed to support other distributed energy resources including PV, batteries and heatpumps.
- License required. No.
- Open source implementations. Yes.
- Conformance testing available. Yes
- Market presence. Association with OCPP may help uptake.
- Technical ecosystem. Development and support experience available.
- Runs over. JSON through a REST interface.
- Message datatypes. Range of message types for forecasts, errors and other.
- Common use. Notify managing agent of resource forecast.

- Extensible. Range of devices and forecasts now supported.
- Cybersecurity. TLS/PKI/certificates.

5.5 Building, industrial and home automation protocols with some device energy management support

Some application protocols support energy management within a broader remit. Examples detailed below include:

- BACnet[34] - Building Automation Controls Network
- Modbus[35]
- Matter[36]
- KNX[37]

Other protocols such as the Energy Flexibility Interface (EFI)[38] and the Open Connectivity Foundation (OCF)[39] IoT specification may develop material support and deployment in the energy management space. Some protocols have seen adoption primarily in one country. such as Echonet Lite[40] in Japan.

New home automation vendor association protocols such as Home Connect[41] can support device energy management. Home Connect is defined by a consortium of companies including Bosch, Siemens and others to control household appliances including ovens, cleaning robots, dishwashers, freezers, washing machines, refrigerators, coffee machines and others. A Home Connect device energy management example would be running a washing machine when there is excess onsite PV generation or a cheap tariff. To be used for energy management outcomes requires customer support for washing clothes etc outside an on demand model.

Descriptions

BACnet:

- Original protocol developed by ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) for building automation. Controlling and monitoring space conditioning elements such as boilers and AC units is a typical application. BACnet Interoperable Building Blocks (BIBBS) define the standard behaviours of devices in a BACnet environment including services supported. Devices change dynamically between master and slave.
- License required. No.

[34] http://www.bacnet.org/ Accessed May 12th, 2022
[35] https://www.modbus.org/specs.php Accessed May 12th, 2022
[36] https://csa-iot.org/all-solutions/matter/ Accessed May 12th, 2022
[37] https://www.knx.org/knx-en/for-professionals/index.php Accessed May 12th, 2022
[38] https://flexible-energy.eu/efi-energy-flexibility-interface/ Accessed May 21st, 2022
[39] https://openconnectivity.org/ Accessed May 21st, 2022
[40] https://echonet.jp/english/ Accessed May 21st, 2022
[41] https://www.home-connect.com/global Accessed May 12th, 2022

- Open source implementations. Yes.
- Conformance testing available. Yes
- Market presence. Implemented and used across many device types in energy management, industrial, building management and other sectors.
- Technical ecosystem. Development and support experience available.
- Runs over UDP/IP, serial RS-485 over MS/TP (Master Slave Token Passing) and slower networks for devices with lower requirements.
- Message datatypes. Range of message types for alarms and events, faults, maximum and minimum limits and other.
- Common use. Notify change of value at a device.
- Extensible. Vendors can extend the standard protocol with non-standard objects.
- Cybersecurity. A new version of the BACnet standard adds BACnet Secure Connect (BACnet/SC).

Modbus:

- Original protocol developed by Modicon (now Schneider Electronics) in 1979 for serial communication between a master and slave devices. As well as communication from the slaves to the master the master can also write to the slaves.
- License required. No.
- Open source implementations. Yes.
- Conformance testing available. Yes
- Market presence. Commonly used across many device types. Particularly industrial systems but also AC units at residential scale upwards, inverters and other distributed energy resources meeting the SunSpec standard and others.
- Technical ecosystem. Development and support experience available.
- The Modbus RTU (remote terminal unit) and ASCII versions run over serial links. The Ethernet version runs over TCP.
- Message datatypes. Range of data types defined for Modbus.
- Common use. Slave updates master with relevant information.
- Extensible. Vendors using Modbus have considerable freedom in how they define the data layout. Some vendors have defined protocol extensions that have seen some uptake.
- Cybersecurity. Modbus/TCP Security uses Transport Layer Security.

Matter:

- Home automation interoperability standard with support announced by a wide range of companies including Google, Schneider, Apple, Amazon, Samsung and others through the Connectivity Standards Alliance (CSA). Initially running on several protocols. (See Thread description in Appendix A.)

- License required. Yes.
- Open source implementations. Yes.
- Conformance testing available. Yes.
- Market presence. Implementations becoming available at time of writing.
- Technical ecosystem. Development and support experience available will increase if the protocol is successful.
- Runs on. IP. Local and cloud supported.
- Message datatypes. For true interoperability Matter will need to support device and underlying protocol message types.
- Common use. Interoperably connect networked home automation devices from many vendors.
- Extensible. Designed to support new devices meeting the standard.
- Cybersecurity. CSA state range of security approaches supported.

KNX:

- Well-established home automation interoperability protocol standardised in Europe, USA and China. Products implementing KNX available from wide range of companies.
- License required. The KNX Engineering Tool Software has licenses ranging from a free demo to higher cost versions. This tool is used to configure devices. Note devices may come pre-configured from the vendor or may self-configure.
- Open source implementations. Yes.
- Conformance testing available. Yes.
- Market presence. Broad adoption in the home automation sector.
- Technical ecosystem. Development and support experience available.
- Runs on. KNX IP, KNX Powerline, KNX Twisted Pair and KNX Radio Frequency. KNX IP over Ethernet uses UDP. Can gateway to other systems.
- Message datatypes. Small data packets containing address, data and control information.
- Common use. Connects sensors, actuators and modules such as room temperature controllers from different vendors.
- Extensible. Designed to support new devices meeting the standard.
- Cybersecurity. KNX Secure supports a range of security approaches.

5.6 Internet of Things (IoT) protocols

Some application protocols support energy management within a broader remit. Examples detailed below include:

- CoAP[42] - Constrained Application Protocol
- MQTT[43]

Descriptions

CoAP:

- Internet Engineering Task Force (IETF) protocol for machine to machine applications including smart energy and building automation on low-power networks using low-power computing platforms such as micro-controllers with limited RAM and ROM. Standardised server resource discovery.
- License required. No.
- Open source implementations. Yes.
- Conformance testing available. ETSI have defined CoAP testing standards.
- Market presence. Implementations available from range of IoT vendors.
- Technical ecosystem. Development and support experience available.
- Runs over UDP.
- Message datatypes. Smaller data packets than HTTP. Data compression techniques such as bitfields used.
- Common use. Client/server model with similarities to HTTP including use of GET, POST, PUT and DELETE messages.
- Extensible. Designed to work with other protocols. Device message data formats can be updated.
- Cybersecurity. Datagram Transport Layer Security used.

[42] https://coap.technology/ Accessed May 12th, 2022
[43] https://mqtt.org/ Accessed May 12th, 2022

MQTT:

- Pub/Sub many-to-many protocol standardised by OASIS (Organization for the Advancement of Structured Information Systems) for small microcontrollers in automotive, logistics, manufacturing, smart home, consumer products and other sectors.
- License required. Limited offering on free plan. Paid plan required to offer full commercial service.
- Open source implementations. Yes.
- Conformance testing available. ETSI have defined MQTT testing standards.
- Market presence. Implementations available from range of IoT vendors.
- Technical ecosystem. Development and support experience available.
- Runs on TCP. MQTT-SN defines a UDP mapping for MQTT.
- Message datatypes. Clients must understand MQTT message formats without message metadata.
- Common use. Information from many clients passed through a central broker.
- Extensible. MQTT topics defined a hierarchical data layout which can be flexibly defined for a different device types.
- Cybersecurity. Transport Layer Security.

6. Device hardware interfaces that minimise required onboard software stack

6.1.1 Description

Implementing a full protocol stack on a device like a hot-water heater or an AC unit to support application layer interaction with a local or remote entity raises issues including:

- Protocol stack energy overhead
- Cybersecurity
- Protocols supported limited to the implementation
- Updating software with new versions of the current implementation or a new implementation
- CPU and memory cost.

Various control approaches have sought to avoid these issues by, for example, using hardware such as timers for hot-water systems or simple on/off control elements operated by utilities during periods of low demand on the grid.

Hardware interface solutions can raise other issues:

- Non-standardisation replicates work over multiple platforms. This cost needs to be recouped
- Vendor lockin can restrict third-party access to these devices. A related issue is interface devices designed only to support control from a utility, restrict the use of onsite control in energy management systems to, for example, maximise PV onsite consumption, dynamic tariffs and other use cases
- Limited functionality supported can restrict use cases. For example, a simple on/off device communicating with a utility would not support setpoints for a resistance element in a hot-water heater which restricts load-management options.

Industry and standards associations have developed solutions that specify a simplified set of controls that can be used by a more fully-featured software stack to drive device energy management.

These solutions include:

- Consumer Technology Association standard CTA-2045[44]
- Demand Response Enabling Device (DRED, Australian Standard 4755)[45]
- SG Ready initiative[46]

An application protocol can manage energy devices by using lower levels of the protocol stack to control a device through these interfaces. For example, an application layer protocol use case interfacing to a SG Ready compatible heatpump might tell a heatpump to operate for a specified 2

[44] https://standards.cta.tech/apps/group_public/project/details.php?project_id=192

[45] https://infostore.saiglobal.com/en-au/Standards/AS-NZS-4755-1-2017-99622_SAIG_AS_AS_209429/

[46] https://www.waermepumpe.de/normen-technik/sg-ready/

hour period. Software controlling an AC unit might use the DRED interface to run the AC unit at no more than 50% of its maximum continuous rating.

While supporting limited functionality with upgrades difficult to implement, these initiatives:

- Require minimal energy to support device energy management
- Are protocol agnostic.
- Local energy management system or other agent can support protocols as required
- Minimise device energy management interface installation
- Reduce device cybersecurity requirements which are now primarily managed by local or remote agent
- Standardised interface facilitates open platform and standard implementations.

6.1.2 CTA-2045

The Consumer Technology Association (CTA) states that:[47]

> "ANSI/CTA-2045 specifies a modular communications interface (MCI) to facilitate communications with residential devices for applications such as energy management. The MCI provides a standard interface for energy management signals and messages to reach devices."

The CTA-2045 socket can be connected to a management platform for local or remote control.

Devices implementing CTA-2045 can support:

- load up
- load shed
- critical peak event
- grid emergency
- time-of-use tariffs
- real-time pricing.

This range of device use cases can be controlled by OpenADR, IEEE2030.5 and other software stacks with a suitable application protocol and physical and link layer capability to interface with the socket.

CTA-2045 has been used in several US demand management programs for HW heaters. Implementations for EV charging and other use cases are becoming commercially available.

[47] https://standards.cta.tech/apps/group_public/project/details.php?project_id=192. Accessed 15th March, 2022

6.1.3 Demand Response Enabling Device

Australia has developed the Demand Response Enabling Device (DRED) as defined in the AS/NZS 4755 standards. Devices such as resistive hot-water heaters, air-conditioners and pool-pumps supporting DRED Demand Response Modes from the following list can be managed by onsite or offsite platforms mapping application layer use cases to the DRED DRMs.

AS/NZS 4755 defines these demand response modes (DRM):

- DRM 0: Disconnect
- DRM 1 Do not consume power
- DRM 2 Do not consume at more than 50% of a reference value
- DRM 3 Do not consume at more than 75% of a reference value
- DRM 4 Start or increase load
- DRM 5 Do not export power to the grid
- DRM 6 Do not export at more than 50% of a reference value
- DRM 7 Do not export at more than 75% of a reference value
- DRM 8 S Start or increase export to grid

The physical interface to the DRED controlled device is specified in the standard. Appliance manufacturers may supply an adaptor that can communicate with an onsite or offsite platform to implement DRED functionality.

There is also an AS/NZS standard for inverter DRED support.

DRED has seen limited international uptake. If Australia mandates DRED compliance for appliances sold in Australia, manufacturers wishing to sell in Australia may need to support DRED as well as any international standards.

6.1.4 SG Ready initiative

The Bundesverband Warmepumpe e. V. (German Federal Heatpump Association) state that Smart Grid Ready labelling is awarded for systems in Germany, Austria and Switzerland.

SG Ready devices are required to support 2 or more of 4 operating states which control energy consumption. The operating states are driven by two contacts which are each set to on or off.

- Operating state 1: Switched off
- Operating state 2: Normal energy efficient mode
- Operating state 3: Recommended to run in boost mode possibly during low tariff period or taking advantage of onsite PV
- Operating state 4: Start command working with tariffs and with options including higher temperature in the storage tank and using the room temperature – for relevant devices - as a reference variable.

A the time of writing the SG Ready interface supports a useful but limited set of use cases primarily in AC units and heatpumps used to heat water. SG Ready is implemented on a range of heatpumps made by German and other manufacturers and AC units from several manufacturers.

Appendix A Relevant physical/network layer protocols

The layers below the application layer in the TCP/IP stack and the bottom 4 layers in the OSI stack are referred to by EDNA as the physical/network layers. These layers collectively support the application oriented functionality in the layers above.

There is a wealth of academic, institutional, government and other authoritative information covering the physical/network layers. Physical/network layer relevance for this report is to support application layer protocols communicating with energy devices and the network standby energy consumption. The EDNA report "Network Standby Power Basics"[48] covers networked device protocol standby energy consumption topics in detail. The EDNA report "Energy Efficiency of the Internet of Things"[49] discusses the following protocols used for the physical layer:

- ANT+[50]
- Bluetooth And Bluetooth Smart (AKA Bluetooth Low Energy)[51]
- DECT ULE (ultra low energy)[52]
- Z-Wave[53]
- ZigBee[54]
- EnOcean[55]
- Wi-Fi[56]
- LowPower Wo-Fi Wi-Fi HaLow™ [57]
- Ethernet[58]
- LoRa[59]

The EDNA report also covered IEEE 802.15.4-2011 but this has been superseded by IEEE 802.15.4-2020[60].

A recent protocol development is Thread[61] which the Thread Group state "is a low-power and low-latency wireless mesh networking protocol built using open and proven standards." The Matter

[48] https://www.iea-4e.org/edna/tasks/task-5-network-standby-power-basics/ Accessed 3rd May, 2022

[49] https://www.iea-4e.org/wp-content/uploads/publications/2016/04/Energy_Efficiency_of_the_Internet_of_Things_-_Technical_Report_FINAL.pdf Accessed 4th May, 2022

[50] https://www.thisisant.com/ Accessed 4th May, 2022

[51] https://www.bluetooth.com/ Accessed 4th May, 2022

[52] https://www.etsi.org/technologies/dect Accessed 4th May, 2022

[53] https://z-wavealliance.org/ Accessed 4th May, 2022

[54] https://csa-iot.org/all-solutions/zigbee/ Accessed 4th May, 2022

[55] https://www.enocean.com/en/ Accessed 4th May, 2022

[56] https://www.wi-fi.org/ Accessed 4th May, 2022

[57] https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-halow Accessed 4th May, 2022

[58] https://standards.ieee.org/ieee/802.3/7071/ Accessed 4th May, 2022

[59] https://lora-alliance.org/ Accessed 4th May, 2022

[60] https://standards.ieee.org/ieee/802.15.4/7029/ Accessed 4th May, 2022

[61] https://www.threadgroup.org/ Accessed 7th May, 2022

application protocol (see Section 5) can run on Thread. There is an open source implementation[62] of Thread with a permissive license. Thread/Matter is supported by a large range of companies. There is a Thread certification process for third-party products.

[62] https://openthread.io/ Accessed 7th May, 2022

Appendix B Common Internet stack application protocols

These protocols can be used for energy management at devices without any specific energy management use cases defined for the protocol.

Some open platform application protocols are used for generic support of use cases from a sweep of problem domains. While not developed specifically for energy management, benefits of using these protocols may include:

- Flexible data and control application layer contents
- Widespread availability on multiple CPUs, micro-controllers, platforms and operating systems
- Broad, deep technical experience
- Well-proven, well-tested protocols

Using these protocols raises issues including:

- User defined shared, accurate application layer data layout and definition is required for network nodes to communicate using these protocols. This contrasts with a well-designed application protocol used in part or primarily for energy management with standardised application layer contents.
- General purpose protocols may cater for functionality not needed for energy management which may complicate system configuration and implementation. Deploying device energy management as simple plug-and-play may encourage electricity customers to adopt demand response/flexibility at scale.

Relevant protocols include:

- HTTP/HTTPS - Hyper Text Transfer Protocol[63]/Secure[64, 65]
- WebSocket[66]
- telnet[67]
- FTP - File Transfer Protocol[68]
- SNMP – Simple Network Management Protocol[69]
- SOAP – Simple object access protocol[70]

[63] https://httpwg.org/specs/rfc7231.html Accessed May 5th, 2022
[64] https://datatracker.ietf.org/doc/html/rfc2817 Accessed May 10th, 2022
[65] https://datatracker.ietf.org/doc/html/rfc2818 Accessed May 10th, 2022
[66] https://datatracker.ietf.org/doc/html/rfc6455 Accessed May 5th, 2022
[67] https://datatracker.ietf.org/doc/html/rfc854 Accessed May 5th, 2022
[68] https://datatracker.ietf.org/doc/html/rfc959 Accessed May 5th, 2022
[69] https://www.rfc-editor.org/info/std62 Accessed May 5th, 2022
[70] https://datatracker.ietf.org/doc/html/rfc4227 Accessed May 5th, 2022

Descriptions

HTTP/HTTPS:

- Primarily designed as a half-duplex simple protocol for information sent from a server after a request by a client. Various workarounds and updates implement increased functionality.
- License required. No.
- Open source implementations. Yes.
- Market presence. Ubiquitous. Implemented on platforms with minimal processing power and tiny amounts of memory up to supercomputers
- Technical ecosystem. Extremely well-supported. Deep, broadly spread knowledgeable development expertise available
- Commonly runs over TCP
- Stateless: New connection established whenever client makes request from server
- Message datatypes. Range supported.
- Common use. Client retrieves relatively static data from server.
- Extensible. The ubiquity of HTTP has encouraged development of HTTP2 and other initiatives to add functionality.
- Widely used APIs using HTTP include XMLHTTPRequest, Fetch and many flavours of REST (Representational State Transfer).
- Extensively used cybersecurity support with HTTPS

Websocket:

- Full duplex communications between networked entities with stateful connection once established.
- License required. No.
- Open source implementations. Yes.
- Market presence. Used in some realtime environments such as gaming and stockmarkets. HTTP upgrades and web development frameworks may affect broader uptake.
- Commonly runs over TCP
- Full duplex and either side of the connection can send data whenever available without workarounds like HTTP long-held requests. Can implement Publish-Subscribe (Pub-Sub) messaging pattern.
- Persistent connection once established. Continues until either side ends the connection. Once connection established more efficient than HTTP and can reduce latency.
- Message datatypes. Text and binary.
- Common use. Client retrieves frequently changing data from resource.

Telnet:

- Simple command line interface to check TCP connections to networked device. Can be used for applications but other superior alternatives are available.
- License required. No.
- Open source implementations. Yes.
- Market presence. Many platforms support a telnet client.
- Cybersecurity. Data including passwords/usernames transferred in clear. Secure shells commonly used instead of telnet.

FTP:

- Transferring files between networked devices.
- License required. No.
- Open source implementations. Yes.
- Market presence. Ubiquitous. Implemented on platforms with minimal processing power and tiny amounts of memory up to supercomputers
- Technical ecosystem. Well-supported. Broad user and developer experience.
- Commonly runs over TCP
- Common use. Client retrieves relatively static data from server.
- Extensible. Versions with user interfaces and other functionality.
- Cybersecurity improved with Secure FTP.

SNMP:

- Managing computing servers and network devices in communications networks.
- License required. No.
- Open source implementations. Yes.
- Market presence. Used in corporate and telecommunications networks to manage switches, servers and routers. Later versions of the protocol have seen limited market uptake.
- Technical ecosystem. Specialised protocol.
- Commonly runs over UDP (User Datagram Protocol)
- Common use. Get and Set configuration data on a managed device. Get operational data such as device utilisation.
- Extensible. The Management Information Base (MIB) can be extended by hardware and software vendors.
- Cybersecurity improved in later versions.

SOAP:

- Exchanging XML information between networked entities.
- License required. No.
- Open source implementations. Yes.
- Market presence. Used in a wide range of use cases in multiple sectors.
- Technical ecosystem. SOAP is designed to be simple to learn and implement. XML experience is relatively common but JSON uptake is increasing.
- Runs over variety of transports including HTTP.
- Common use. Implementing web services.
- Extensible. Can define message types to suit required use case but communicating entities must agree on message contents, layout etc Sector and use case specific XML formats have been developed and used.
- Cybersecurity can include lower layer support such as TLS/PKI/certificates and other. Can also use XML encryption.