FINAL

Evaluating international standards for electric vehicle chargers

For SA Department for Energy and Mining

December 2021

George Wilkenfeld and Associates
with
Auseng Pty Ltd

GEORGE WILKENFELD AND ASSOCIATES Pty Ltd
ENERGY POLICY AND PLANNING CONSULTANTS
PO Box 460 Katoomba NSW 2780 Sydney Australia Tel (+61 2) 4782 1155
geosanna@ozemail.com.au

Contents

FIGURES

Executive Summary

The share of plug-in electric vehicles (EVs) in the Australian light vehicle fleet is low at present but projected to increase rapidly. Rapid growth in EV numbers together with unconstrained charging behaviour would place pressure on the electricity distribution network and could result in rising costs to both EV owners and other electricity users.

As Australia is still an immature EV market, with limited public and at-work charging infrastructure, the best indications of charging behaviour come from overseas studies or from surveys of the intentions of Australian EV adopters.

Data from the UK and the USA suggests that many EV owners will install fixed Electric Vehicle Supply Equipment (EVSE) in their garages or next to their homes. EVSEs are hard-wired to the power supply, so they must be installed by a qualified electrician. They will almost certainly be the largest load in a dwelling – up to 15 kW if single phase, and up to 30 kW if three phase.

EVSE suppliers contacted for this project estimated that the share of home EV charging in Australia using EVSEs ranges from 30% to 50%, with the balance using standard general purpose outlets. Once the Australian EV market matures, it is likely that about two thirds of home charging energy – i.e. about half of *all* EV charging energy – will utilise via home EVSEs.

There is a significant risk that unmanaged EV charging will have a negative impact on the electricity network. There are several ways to manage this risk, including structuring tariffs to incentivise charging when there is excess renewable energy and demand is low (e.g. in the middle of the day) and discouraging it when demand is high (e.g. during the evening peak).

Even with cost-reflective tariffs, there are likely to be times when pricing incentives alone will not be enough to manage EV charging demand, leading to events such as spiking wholesale prices, power quality problems or local distribution congestion.

EV owners may wish to participate voluntarily in managed charging or demand response programs, in return for commercial financial incentives. Establishing such a capability quickly, economically and on a large scale will depend partly on the inherent demand response capabilities of EVSEs. Open demand response standards allow customers who choose to participate in demand response markets to do so easily, and *opt-in and out* of demand response offerings without being locked into particular service arrangements and usually without the need for installing extra equipment

Accordingly, the South Australian government is seeking to introduce demand response capability requirements for electric vehicle chargers. It commissioned this study, with the following terms of reference:

> For electric vehicle chargers intended for residential applications and capable of managing the charging and/or discharging to the grid at SAE Level 2 or IEC Mode 3, identify open, non-proprietary international product standard(s) or parts of standard(s), that support equivalent demand response capabilities to any or all of AS/NZS 4755 DRMs 0,1,2,3,4,5 and 8.
>
> For the identified international standard(s) or parts of standard(s):

- advise on levels of compliant EV charger models in the current Australian market;
- advise on availability of testing report templates to verify compliance against the standard;
- advise whether the preferred DR standard requires compliance with specific communications standards;
- draft a technical requirement based on the identified standard(s) or parts of standard(s), for adoption in South Australia as a mandatory technical standard for electric vehicle chargers
- for non-compliant models in the current Australian market, advise on estimated manufacturer costs to achieve compliance.

Our findings on the Terms of Reference are as follows. Note that the project did not cover high-power direct current (DC) chargers.

Open, non-proprietary international product standards

There are many standards and protocols impacting on EV charging and chargers. Those which can support some degree of demand response (DR) capability are summarised in Table 2. They are at different stages of maturity and completeness, and only one has been adopted at scale by EVSE suppliers: OCPP 1.6.

The standards provide platforms for exchanging information, including secure DR messaging, between a remote agent or charging system operator and the EVSE. An EVSE that complies with a standard should be able to receive these messages (via a range of connection pathways). Whether they can correctly interpret them and signal to the EV the maximum power or current to be made available to the EV's on-board charge controller (OBCC) will depend partly on the actual design of the EVSE and partly on how it is set up by the installer.

Some EV manufacturers have systems that manage DR by communicating directly with the OBCC, but managing the EVSE to restrict or prevent charging will take precedence. It also means that the DR capability remains effective irrespective of the brand of EV connected.

Some EVs are capable of discharging energy to the grid ("V2G"). Additional capabilities and protections are required in Electric Vehicle Supply and Discharge Equipment (EVSDE) to manage two-way energy flows. At present very few EV models support V2G, and there are no commercially available EVSDEs on the Australian market. The EV industry does not expect V2G to develop quickly in the residential sector, although it may become economic in EV fleets, if all garaged at the one location.

The terms of reference cite AS/NZS 4755 as the benchmark for evaluating DR capability. That standard does not cover EVSEs at present, but may do so in future. It sets out clearly defined DR modes for any electrical product. Applied to EVSEs, DRM 0 is a safety disconnect, DRM 1 prevents charging, DRM 2 and 3 constrain the rate of charging and DRM 4 initiates charging (if an EV capable of accepting charge is connected to the EVSE).

Both EVSEs and EVSDEs can be capable of DRMs 0 to 4, but only EVSDEs can be capable of DRMs 5 to 8. DRM 5 prevents discharging, DRM 6 and 7 constrain the rate

of discharge and DRM 8 initiates discharge (if an EV capable of discharge is connected to the EVSE).

Only two DRMs are essential for an EVSE to be able to participate effectively in managed charging or demand response: a no-charge mode and a constraint mode. The no-charge mode corresponds to DRM 0 or DRM 1: in fact, most EVSEs achieve cessation/prevention of charging by opening the electrical contactor; in effect a combined DRM 0/1.

Depending on their design and the installer settings, an EVSE could constrain charging flexibly (anywhere between 0% and 100% of a reference value) or in one or more discrete steps (say 25%, 50% and 75% of a reference value). Experience with existing DR programs, such as PeakSmart for air conditioners, suggests that the availability of a constraint DRM is an important factor in enrolling consumers in a DR program, because the aggregator does not have to immediately resort to DRM0/1.

DRM 4 (turn load on if not charging, increase rate of charge) is not of great value for EVSEs. As users will typically plug the EV in and let it charge until full – not rest at partial charge states – EVs will rarely be in a position to respond to DRM4. They will most likely be either fully charged or not connected at all.

Conclusions

The intent of adopting a standard is to ensure that a complying EVSE or EVSDE can accept DR operational instructions (OIs) and obtain the required action by the EV. The international standards evaluated enable the transmission, receipt and interpretation of OIs (in various formats) but none provide for testing that the message is actually passed on to and correctly actioned by the EV. In this respect there is no international standard which would, on its own, achieve demand response outcomes to the same level of confidence as the AS/NZS 4755 framework.

Therefore it would be prudent to allow for testing with an actual EV or an electrical analogue of an EV. Otherwise a standards-compliant EVSE may still be unable to deliver a firm DR capability.

OCPP 1.6 and 2.0.1 and ANSI/CTA 2045 can be used in conjunction with a range of “upstream” communications platforms, including OpenADR and IEEE 2030.5. Complying EVSEs rarely specify or restrict the platform. The choice of platform would be up to remote agents, but they can be confident that the DR messaging would get through to standard-compliant EVSEs (barring communication disruptions).

OCPP 1.6 is the only standard with widespread support by EVSEs currently on the market. It is backed by a testing and certification scheme administered by the Netherlands-based Open Charge Alliance, the industry consortium which publishes the standard. It can replicate DRMs 1 to 4 but not DRMs 5 to 8, as it does not support V2G.

This does not mean that all EVSE models complying with OCPP 1.6 are able to action all DR messages. Analysis of the wiring diagrams and installer instructions from a number of EVSE installation manuals indicates that some can only be set to action one of DRMs 1,2 and 3, some can be set to action two and some to action all three (See Table 1). Where fewer than 3 DRMs are supported, in some cases DRM1 is automatic and the installer sets the other (e.g. a level of constraint that could correspond to either DRM2 or DRM3). In other cases the installer can choose NOT to set DRM1 if they wish.

The actual DR capability of an OCPP 1.6 compliant EVSE needs to be specifically certified by the supplier, and must be capable of being verified in independent testing. The method of test could be based on the AS/NZS 4755 framework, which provides for testing that a complying electrical product actually responds as required.

The installer's setup of an OCPP-compliant EVSE (e.g. through dipswitch settings) will be the final determinant of its actual DR capability. This means installers will need to know how to set up that particular model of EVSE to make it DR-capable, and certify that they have done it.

Table 1 DRMs supported by EVSE models according to standards compliance

	OCPP 1.6	CTA 2045	Proprie-tary	No DR standard	Total models
Models capable of three DRMs	6	3	0		9
Models capable of two DRMs	0		2		2
Models capable of one DRM	10				10
Models probably capable of at least DRM1 (a)	9		3		12
Models probably incapable of DRMs	0			13	13
TOTAL MODELS	25	3	5	13	46

(a) Not enough conclusive information in public domain, but likely to support at least DRM1

ANSI/CTA-2045 differs from the other standards in that it provides for a plug-in universal communications module (UCM), which functions like the Demand Response Enabling Device (DRED) in AS/NZS 4755.1. Different UCMs support different messaging platforms; the most common one uses OpenADR 2.0. ANSI/CTA-2045 is mainly used for water heaters and thermostats, but it is supported by at least one brand of EVSE. All UCM-equipped EVSEs would be able to replicate DRMs 1 to 4 and DRMs 5 to 8 would be possible if the EVSE were specifically designed for V2G.

The other standards are less mature, and consequently have negligible takeup in the EVSE industry, although this is expected to change over the coming years.

OCPP 2.0.1 provides for V2G, but is not backwards compatible, so DR platforms and programs built for OCPP 1.6 will not be inter-operable with OCPP 2.0.1 compliant EVSEs (or vice versa). It is expected that as OCPP 2.0.1 develops it will be consistent with IEC 15118. IEC 15118 is specifically designed to support V2G, but key parts remain to be completed and it will require more complex communications with the EV than offered by the IEC 61851 compliant "control pilot" wire that is wrapped in with the EV charging cable.

IEEE 2030.5 was developed in the USA to enable utility management of the end user energy environment, including demand response. It is widely used for controlling PV inverters, and is the default standard adopted by the California Energy Commission under Rule 21 (although other standards can also be used).[1] It is applicable to V2G EVSDEs, as they also use inverters. However, the number of EVSEs (even in the USA) claiming IEEE 2030.5 compliance is negligible.

[1] California's Public Utilities Commission Rule 21 mandates that generating facilities that utilise inverter based technologies to interconnect with utility grids must support an application layer communications protocol. This protocol is used by the utilities to configure advanced inverter functions and receive operating state information from the inverters.

Interest in IEEE 2030.5 is growing in Australia. Standards Australia has started a project to adopt it as an AS/NZS standard, and at the same time develop an Australian Implementation Guideline. An early draft of the Guideline includes an Annex describes how IEEE 2030.5 can accept and pass on OIs for the DRMs in AS/NZS 4755, including combination of OIs that request power quality responses. While promising, the work is still at an early stage.

OpenADR (adopted as IEC 62746) is widely used for conveying dynamic energy pricing information and DR requests from remote agents to building energy systems and charging point operators, but is not designed to issue direct DR OIs to EVSEs or other end use products. However, it can be used in combination with OCPP 1.6-compliant EVSEs to achieve that purpose.

BSI PAS 1878:2021 *Energy smart appliances –System functionality and architecture – Specification* is more like a regulatory standard than a technical standard. It prescribes an architecture in which a Demand Side Response Service Provider (DSRSP) interfaces with a Customer Energy Manager (CEM; a functional or physical unit) which interfaces in turn with an Energy Smart Appliance (ESA). OpenADR is listed as one option for managing "Interface A" between the DSRSP and the CEM, but the standard for "Interface B" between CEM and appliance is left open. This is the opposite of the AS/NZS 4755 approach, where interaction with and performance of the appliance is highly prescribed, but the "upstream" platform is left open. It remains to be seen whether EVSE products claiming conformance with BSI PAS 1878:2021 come on the market, and how they can be tested.

Table 2 Summary of standards reviewed

Standard or Protocol	V1G or V2G	Maturity	Market adoption	Suitable for Reg use in SA
OCPP 1.6	V1G only	Mature	High	Immediate
ANSI/CTA-2045	V2G possible	Mature	Low	Immediate
OCPP 2.0.1	V2G supported	Developing	None yet	Near term
IEEE 2030.5	V2G supported	Mature	Low	Near term
IEC 15118	V2G supported	Developing	None yet	Longer term
OpenADR/IEC 62746	V2G supported	Mature	Low	Not on its own
BSI PAS 1978 (UK)	V2G optional	Developing	None yet	Not on its own

Compliance levels and costs

Of the 47 home EVSE model variants identified on the Australian market, 27 are claimed to comply with OCPP 1.6, three support ANSI/CTA-2045 and four support proprietary messaging protocols. The remainder are basic or "dumb" EVSEs with no communications capability. It is likely that all OCPP 1.6-compliant EVSEs would support a no-load DRM (0/1) if set up to do so at installation, but not all will support a constraint mode (DRM 2/3).

In our discussions with EVSE suppliers, the quoted price difference between basic and OCPP 1.6 compliant varied from about $500 to zero, with the most common value around $200. This was about the same price as the charging cable connecting the EV to the EVSE. The price differences are more reflective of market positioning and commercial strategy than actual manufacturing or licensing fees. The EV market leader, Tesla, has decided to phase out its basic EVSE model entirely, and has priced the smart variant equal to the basic model. In a market where all models have to be smart, suppliers charging price premiums would be at a commercial disadvantage, so prices of smart EVSEs could be expected to fall.

Testing and Certification

The Open Charge Alliance (OCA) has developed a testing tool for OCPP 1.6 and is currently developing one for OCPP 2.0.1. At present six test laboratories around the world offer OCPP testing and certification services. A manufacturer seeking certification would need to bear the cost of the test and pay a certification fee of several thousand Euros to OCA. At present only two brands of home EVSEs are certified, neither of which are available in Australia.

There are also US-based testing and certification programs for IEEE 2030.5 and OpenADR, and the OpenADR Alliance is developing a certification program for ANSI/CTA 2045. At present there is nothing to prevent or deter an Australian EVSE supplier claiming compliance with any standard, apart from the Trade Practices Act. If compliance were mandated, proponents could be required to make a declaration of compliance in the first instance, in the knowledge that the SA Technical Regulator could commission tests for those standards that are backed by testing and certification.

As stated above, such testing would only verify that a complying EVSE or EVSDE can receive and interpret the relevant DR instructions, but not that the message is actually passed on to and correctly actioned by the EV. If regulations describe a further test with an actual EV or an electrical analogue of an EV, this would put suppliers on notice to verify this for themselves, and enable Regulators to commission such a test should they wish to do so.

Suitability for Regulatory Adoption

The report concludes with preliminary proposals relating to the installation of EVSEs and EVSDEs in South Australia. A draft Technical Regulator Guideline detailing the provisions has been prepared as a separate document.[2]

The standard most suitable for early adoption is clearly OCPP 1.6. It would ensure that all EVSEs sold in SA would have at least a minimum DR or “smart charging” capability. While the standard only covers charging, the likely slow development of V2G would give time to assess the development and market adoption of other standards.

ANSI/CTA 2045 offers considerable flexibility, and while its use in EVSEs is limited at present it is mature and testable and would offer another compliance option.

The regulatory proposal includes “Deemed to Comply” provisions to enable the Technical Regulator to adopt other standards that may be proposed by suppliers, including IEEE 2030.5, OCPP 2.0.1 or IEC 15118, should they develop more quickly than expected. It also sets out a response test in which the EVSE or EVSDE is connected to an actual EV or EV analogue.

*****

[2] Technical Regulator Guideline Minimum Technical Standard for Installation of Electric Vehicle Supply Equipment (EVSE) for residential use, Version X, YYYY 2022 (Draft 2)

Glossary

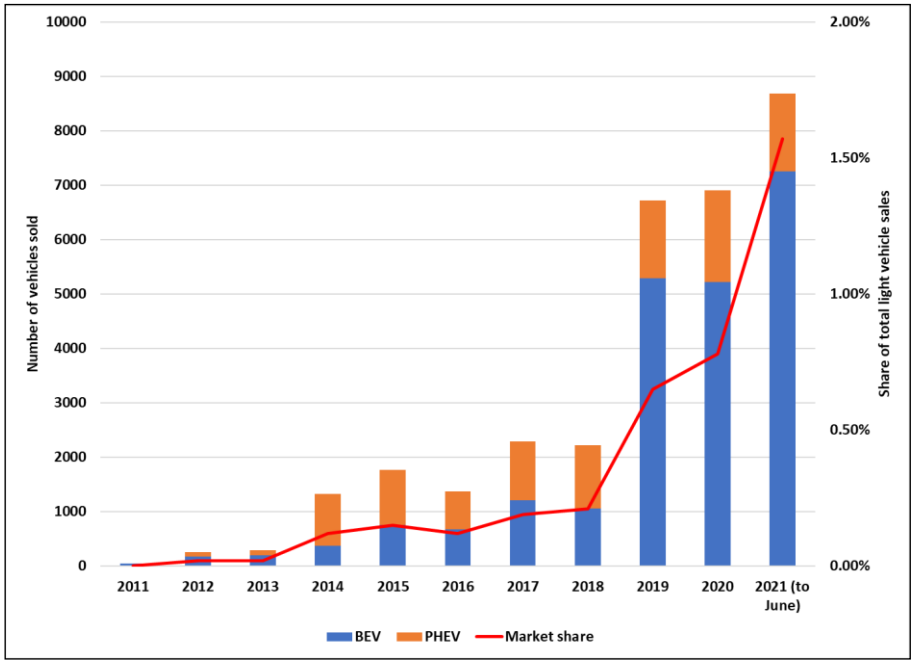
ARENA	Australian Renewable Energy Agency
AS/NZS	Australian Standard/New Zealand Standard
BEV	Battery electric vehicle
CTA	Consumer Technology Association
DEM	Department of Energy and Mining
EESS	Electrical Energy Storage System
EP	Electrical product
EV	Electric vehicle
EVCS	Electric Vehicle Charging Station
EVSE	Electric Vehicle Supply Equipment
EVSDE	Electric Vehicle Supply and Discharge Equipment
GIP	Grid-interactive Port
IEA	International Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers (USA)
ISO	International Standardization Organisation
MCI	Modular Communications Interface
OBCC	On-board charge controller
OCA	Open Charge Alliance
OCPP	Open Charge Point Protocol
OI	Operational instruction
OTR	Office of the Technical Regulator (SA)
PHEV	Plug-in hybrid electric vehicle
RA	Remote Agent
SAE	Society of Automotive Engineers (USA)
SAPN	SA Power Networks
UCM	Universal Communications Module (ANSI/CTA 2045)

1. Background

Electric Vehicle Charging

The share of plug-in electric vehicles (EVs) in the Australian light vehicle fleet is low at present but projected to increase rapidly.[3] Estimates of the rate of growth vary widely, and will be sensitive to both government policy settings and the strategies of global vehicle manufacturers. The EV percentage of light vehicle sales has been rising sharply since 2018 (Figure 1), and it is likely that the long-predicted market shift toward EVs has begun.

Figure 1 EV sales, Australia



Source: EVC 2021

Rapid growth in EV numbers together with unconstrained charging behaviour would place pressure on the electricity distribution network and could result in rising costs to both EV owners and other electricity users.

There are several ways to manage this risk, including structuring tariffs to incentivise charging when there is excess renewable energy and demand is low (e.g. in the middle of the day) and discouraging it when demand is high (e.g. during the evening peak). However, relatively few householders have chosen time-of-use tariffs, and the time periods are too rigid fixed to permit signalling of dynamically changing prices.

Even with cost-reflective tariffs, there are likely to be times when pricing incentives alone will not be enough to manage EV charging demand, leading to events such as

[3] Plug-in electric vehicles (PHEVs) include those in which electricity is the sole energy source (sometimes called Battery EVs or BEVs) and those powered partly by an internal combustion engine and partly be batteries, generally called Plug-in Hybrid EVs or PHEVs. Fuel Hybrid vehicles are powered exclusively by petroleum fuels and have an internal combustion engine. They have a large traction battery capacity (recharged though regenerative braking or an on-board dynamo) and a fully or partly electric drivetrain, but as they cannot be plugged in they are not considered EVs for the purpose of this study.

spiking wholesale prices, power quality problems or local distribution congestion. At those times more direct control of charging may be required. Establishing such a capability quickly, economically and on a large scale will depend on the inherent physical capabilities of the EV Supply Equipment (EVSE) as well as on user choices and permissions regarding the temporary sharing of control.

High-power public and commercial charging stations are not likely to contribute to these problems, for a number of reasons:

- Each installation will require interaction between the operator (or host building owner), the local distribution network service provider (DNSP) and the electricity retailer, so the impacts can be anticipated and factored into the initial connection charges and the energy price structure;
- Groups of high-power stations will be connected directly to the high voltage (>1kV) network which has greater capacity and resilience than the low voltage network; and
- Real-time price variations can be signalled directly to charging station users, who can make their decisions about charging accordingly.

The options for managing charging at the user's place of residence, whether at a detached house or the parking area of an apartment building, will be constrained by the "mode" or "level" of charging and the related hardware. Charging "modes" or "levels" are classified differently in IEC and SAE (US) standards (Table 3). The definitions in IEC 61851:2017 *Electric vehicle conductive charging systems – Part 1- General requirements* are:

- Mode 1 is a method for the connection of an EV to a standard socket-outlet of an AC supply network, utilizing a cable and plug, both of which are not fitted with any supplementary pilot or auxiliary contacts.
- Mode 2 is a method for the connection of an EV to a standard socket-outlet of an AC supply network utilizing an AC EV supply equipment with a cable and plug, with a control pilot function and system for personal protection against electric shock placed between the standard plug and the EV..
- Mode 3 is a method for the connection of an EV to an AC EV supply equipment permanently connected to an AC supply network, with a control pilot function that extends from the AC EV supply equipment to the EV.
- Mode 4 is a method for the connection of an EV to an AC or DC supply network utilizing a DC EV supply equipment, with a control pilot function that extends from the DC EV supply equipment to the EV.

In Modes 1,2, and 3 AC power is delivered to the EV, which has an on-board charge controller (OBCC) to convert AC to DC to charge the batteries. In Mode 4, typically used by public charging stations, high voltage, high current DC power is supplied direct to the EV battery, bypassing the EV's OBCC.[4] By definition, IEC Mode 3 charging involves a dedicated EV Charging Station: the stationary part of EV supply equipment

[4] Lower power Mode 4 EVSEs with inbuilt rectifiers limited to about 25 kW DC are available for home charging use. (A rectifier converts AC to DC, i.e. it acts in the opposite way to an inverter).

(EVSE) connected to the supply network.[5] SAE Level 2 AC charging could in theory be undertaken either via a 3 phase GPO or an EVSE.

Single phase Mode 1 or Mode 2 charging can be used with any standard 10A GPO or a 15A GPO (wired direct to the switchboard on a dedicated circuit), but gives the longest charging times. The impact on the network is limited, and no greater than other domestic plug loads. If householders choose to use these modes, the most readily available strategy would be a mandatory time-of-use tariff structure.

Table 3 Charging mode and level definitions

Standard		Supply	Max Amps	Max Volts	Max kW	Typical kW (a)
IEC 61851-1:2017	Mode 1	1P AC	16	250	4	
		3P AC	16	480	7.7	
	Mode 2	1P AC	32	250	8	
		3P AC	32	480	15.4	
	Mode 3	1P AC	No Max	No Max	NA	3.7-7.4
		3P AC	No Max	No Max	NA	11-22
	Mode 4	DC	No Max	No Max	NA	150-200
SAE 1772:2017	Level 1	AC	12	120	1.44	
		AC	16	120	1.92	
	Level 2	AC	80	240	19.2	
	Level 1	DC	80	1000	80	
	Level 2	DC	400	1000	400	

(a) Typical charging rates quoted for EVSEs available in Australia (Table 5) Shaded cells indicate range of capabilities of EVSEs within scope of this report.

Householders could use high-power Mode 1 or Mode 2 charging if they have a 3-phase supply and install a standard 3-phase outlet (4 or 5 pin) in the garage or outside near the EV parking spot. The change from a single to a three-phase supply must be done by a qualified electrician, who will need to get approval from the DNSP.

The cost of a new 3-phase supply would be a natural deterrent if the sole purpose were to allow unconstrained 3-phase EV plug charging. Is more likely that the first EV adopter in a dwelling will either settle for Mode 1 charging or install a hard-wired EVSE capable of Mode 3 charging. (They may also choose to install a 15A GPO for more rapid Mode 1 charging, but that would pass up other advantages of an EVSE, such as convenient cable tethering and, potentially, “smart charging”). It also means that from a metering perspective the EV use is indistinguishable from other loads.

As Australia is still an immature EV market, with limited public and at-work charging infrastructure, the best indications of charging behaviour come from overseas studies or from surveys of the intentions of Australian EV adopters.

A UK analysis of 8.3 million charging events during 2018 indicates that about 75% of EV charging energy was drawn from residential supply (Table 4). A separate US study also estimated that 75% of charging occurs at home (NBER 2021).[6] The analysis did not differentiate by charging mode.

[5] In this report the fixed unit in a Mode 3 charging arrangement is called the EVSE in line with industry practice, although according to IEC 61851 it is the fixed part of the EVSE, which also includes the flexible cables connecting to the EV.
[6] The UK study also analysed the load shape for residential charging, and estimated that the average load from home charging events peaked at 0.42 kW per EV between 7 and 8 pm on week nights. The COAG Decision RIS projected

Table 4 Estimated charging energy by location, UK 2018

Charging location	Average annual kWh			Share of total EV GWh
	BEV	PHEV	All EV	
Residential	1860	1050	1310	74.6%
Work	360	210	260	14.7%
Slow/fast public	140	80	100	5.8%
Rapid public	260	0	90	4.8%

Source: Element Energy (2019)

The breakdown of charging activity in Table 4 is supported by a recent Australian literature review, which found that:

> EV users and potential users show similar preferences for charging locations, with home charging (or overnight charging near home when home charging is not available) being the preferred location. The second most popular charging location is the workplace or other commute related charging points (e.g., public transport hubs, park and ride facilities), followed by other destination charging locations (e.g., supermarkets, retail centres). End-route service station charging is the least desirable and utilised charging location for urban settings. However, service station charging is perceived as essential in travel corridors to enable long-distance trips and reduce range anxiety (University of Melbourne, 2021).

The review also found that:

> According to USA large scale data sets, even though some EV users only have Level 1 charging in their homes, the penetration of Level 2 charging is rapidly increasing as this seems to be users preferred residential option. Compared to BEV drivers, PHEV drivers are more likely to be using Level 1 charging at home. Workplace and other destination charging also predominantly occur using Level 2 chargers.

The US data suggests that many users will progress to SAE Level 2 (IEC Mode 3) EVSEs over time. EVSE suppliers contacted for this project estimated that the share of home EV charging in Australia that takes place using EVSEs ranges from 30% to 50%, with the balance being Mode 1 or Mode 2. Once the Australian EV market matures, it is likely that about two thirds of home charging energy – i.e. about half of *all* EV charging energy – will take place via home EVSEs.

The EVSE Market

The International Energy Agency (IEA) estimates that in 2020 there were about 10 million light EVs in use worldwide, and 9.5 m private EVSEs (as distinct from public charging stations): 7 m installed at residences and 2.5 m at workplaces (IEA 2021). This equates to 0.95 EVSEs per light EV. Their average power rating was estimated at 4.2 kW, projected to rise to 5.2 kW by 2030.

Globally, the value of the EVSE market is projected to rise to US$ 11.3 billion in 2027, by which time the global EV market is projected to reach US$ 802 billion.[7] It is not clear

that the average contribution to summer maximum demand in SA at about 0.11 kW per EV in 2020, rising to 0.45 kW in 2036.

[7] https://www.statista.com/statistics/1254535/global-electric-vehicle-supply-equipment-market-forecast/

whether this value includes Mode 4 public charging stations, which are many times the price of Mode 3 EVSEs.

Home EVSEs appear to have a low priority with the Australian EV industry, which is focussed on encouraging EV sales through government subsidies and public charging infrastructure (EVC 2021). If the local EV market follows the patterns of more mature markets, then over time about 75-80% of private EV owners will acquire a fixed EVSE, even if they manage initially with the Mode 1 or 2 charging cables supplied with their EV, combined with public and at-work charging.

If the trends in Figure 1 continue, then about 15,000-17,000 EVs will be sold in calendar 2021. With a one-year lag to EVSE purchase, this suggests about 11,000-14,000 units in 2022.

Table 5 lists 47 model variants of Mode 3 EVSEs available in Australia, from 14 brands. Brand shares are hard to obtain, but it is estimated that the largest selling brands are Tesla (by virtue of its dominance of the EV market), EO, Wallbox and Delta. EVSEs are relatively straightforward to build, and there is at least one locally made Mode 3 model (Jetcharge Chargemate, which supports OCPP 1.6J). Tritium, based in Brisbane, is a world-scale manufacturer of Mode 4 public charging stations, but does not make Mode 3 EVSEs.

Of the 45 model variants, 27 are claimed to support OCPP 1.6 (mainly 1.6J), 3 support ANSI/CTA-2045 and 4 support proprietary messaging protocols. Only 13 are “basic” models, but these are said to account for the majority of sales. Based on our discussions with suppliers, we estimate that a third to a half of EVSEs sold will have OCPP 1.6 capabilities.

V2G and other developments

A widely discussed developments in EV charging is “vehicle to grid” (V2G).[8] In this mode, energy stored in the battery of an EV is transferred to the grid. Both the EV and the EVSE need to be capable of V2G. At present, the only V2G-capable vehicles available in Australia are the Nissan Leaf ZE1 and the Mitsubishi Outlander PHEV. There are no V2G-capable EVSEs currently on the Australian market, although at least one model is advertised as “on order”.[9] The ARENA EV trials include two with V2G research components (see Table 16) and both are stalled pending the arrival of V2G-capable EVSEs from overseas suppliers.

The largest selling EV brand in Australia, Tesla, does not support V2G. It designs its vehicle batteries to suit vehicle operating cycles: a relatively small proportion of the battery’s energy capacity is used and replenished (“cycled”) each day, but the power flows during vehicle operation are very high. By contrast, a home battery may cycle its total energy capacity more than once every day, but at much lower power compared with a vehicle.

Energy discharged from an EV battery to the grid would need to be converted from DC to AC. If the inverter were in the EV itself it could in theory discharge energy into the grid without an EVSE (e.g. direct to a suitably rated GPO) but under current connection

[8] “V1G” is sometimes used as shorthand terminology for one-way charging from the grid.
[9] Quasar V2G https://evse.com.au/product/v2g-vehicle-to-grid-charger/

rules the EV inverter would have to meet the same requirements as PV inverters: AS/NZS 4777.2. It is not likely that any global EV manufacturer will do so.

The EV could transfer DC current to a V2G EVSDE which would include an inverter, presumably meeting AS/NZS 4777.2. There are no such EVSDEs certified for use in Australia, although the arrival of one model has been announced.[10]

The view in the industry is that deployment of V2G is several years away, and if it happens at scale it will not be in homes but in commercial fleets, where a number of vehicles can be connected to charging stations at predictable times.

Premises with solar PV are increasingly installing home energy management systems (HEMS) which monitor PV input and, when this exceeds the dwelling load, switch on discretionary loads such as pumps, water heaters or stationary batteries to use energy that would otherwise be discharged to the grid. If solar feed-in tariffs are lower than the purchase tariff the householder is financially better off by using the energy when available.

An EVSE could be one of the loads subject to “solar management” but EV charging is less reliable as an energy store because at the time of energy availability the EV may be either absent or fully charged. Nevertheless, some EVSEs are being advertised as “solar compatible” in that they are able to monitor both the PV inverter and the house load, once appropriately connected and installed. (At least one model of electric water heater has a similar capability). An external HEMS or “solar diverter” could serve the same function, and would be more flexible in that it could manage a number of loads, not just the EVSE.

At present, all home charging is “conductive” in that the electrical energy is transmitted to the EV via a conductor cable. An alternative is inductive charging based on the principle of magnetic resonant coupling – the ability to transmit electricity wirelessly by creating a magnetic field between two circuits, a transmitter and a receiver. This method of charging is now common for mobile phones and other low-power devices, and is being developed for EV charging.[11]

The EV is parked over a coil embedded in the floor of the garage, or a charging mat, and the current turned on. The receiver loop in the underside of the EV become energised and transfers the energy to the battery. If the energy is supplied from the grid it would need to be managed in the same way as conductive charging – either limited in power so that it does not exceed the capacity of GPOs, or managed through an EVSE.

There are standards for conductive charging, including SAE J2954,[12] but EVs that are able to be charged wirelessly should also be able to be charged conductively by SAE J1772 plug-in chargers. If wireless home charging becomes widespread, it is possible that existing EVSEs, sockets and cables could be retained, and plugged into the inductive charging equipment rather than a cable direct to the EV. However, that would complicate the communications pathway between the EVSE and the EV, which utilises a pilot wire bundled with the conductor cable to signal to the OBCC, among other things, the maximum current available.

[10] The UK-made Wallbox Quasar “bi-directional charger” https://jetcharge.com.au/services/vehicle-to-grid
[11] https://www.powerelectronicsnews.com/wireless-charging-technology-for-evs/
[12] Wireless Power Transfer for Light-Duty Plug-in Electric Vehicles and Alignment Methodology J2954:2020

At present home EVSEs appear to be installed either at the time of EV acquisition or later at the instigation of the EV owner. At the present level of maturity of the EV market it possible that when EV owners move they will take the EVSE with them to reinstall at their new address, given that the probability of the new owner also having an EV is so low. Over time this will change, and an EVSE will have a similar value to other fixed appliances such as dishwashers or air conditioners.[13] Fortunately nearly all EVSEs are capable of use with any brand of EV, so there are no technical impediments to leaving them connected in the dwelling.

The 2022 revisions to the National Construction Code propose to:

> Introduc[e] new provisions designed to make retrofit of DER equipment over the life of a building easier. These provisions require space to be left on electrical distribution boards for DER circuit breakers and for cable trays to connect distribution boards to car park spaces in Class 2 buildings. Class 2 buildings will also be required to install charge control devices to ensure EVs will only be charged when there is available electrical capacity in the building. Without this requirement, Class 2 buildings would be required to size their electricity supply to support 100% of car parking spaces being used to charge EV at times of peak demand. This would at least double the required electrical supply capacity for the building.[14]

In effect this would make some form of EVSE demand response mandatory for the shared car parks in Class 2 dwellings (apartments), although not in Class 1 (detached and attached houses).

Demand Response for EVSEs

EVSE is a common term in the EV industry. It was initially adopted in IEC standards for products involved in EV charging only, at a time when EV discharge to grid was only a remote possibility. IEC 61851-1:2017 defines an EVSE as:

> "equipment or a combination of equipment, providing dedicated functions to supply electric energy from a fixed electrical installation or supply network to an EV for the purpose of charging"

For Mode 3 charging, the EVSE includes the fixed Charging Station as well as any flexible cables for connecting the EV, whether the cables are permanently attached to the charging station or detachable. EVSEs designed to manage discharge from the EV to the grid are still rare and there is not yet a standard convention for naming them. Some documents call them "bi-directional EVSEs." Electric Vehicle Supply *and Discharge* Equipment (EVSDE) would be a more convenient way to distinguish them in regulation, and this is the term adopted here.

EVSEs within the scope of this report must be hard-wired to the power supply, so they must be installed by a qualified electrician. They will almost certainly be the largest load in a dwelling – up to 7.6 kW if single phase, and up to 22 kW if three phase.

[13] When dishwashers were first introduced they were luxury goods, and often moved with their owners. Over time they have become common fixtures that are more often left with the dwelling.
[14] https://consultation.abcb.gov.au/engagement/ncc-2022-public-comment-draft-stage-2/supporting_documents/Summary%20of%20changes.pdf

We have identified 46 models of EVSE available in Australia, either from the EV manufacturer, specialist EV charging companies or by mail order, generally from the USA or the UK (see Table 5). Nearly all have the following characteristics:

- There are both single phase and three phase variants of each model, with identical appearance, dimensions and features. According to the suppliers, the only difference between them is the rating of the electrical conductor.
- The maximum charge rate is usually selectable: typically 3.6 or 7.2 kW for a single phase installation and 11 or 22 kW for a three phase installation. The installer will usually select the setting based on the capacity of the supply and the EVSE's power circuit, but in some cases the setting can be changed by the user.
- There are both basic variants without communications or external control capabilities (sometimes called "dumb" or "basic" EVSEs) and "smart" variants which support what the industry calls "smart charging".

In our discussions with EVSE suppliers, the quoted price difference between basic and smart variants varied from about $500 to zero, with the most common value around $200. This was about the same cost as adding a charging cable if not included in the original EVSE bundle. However, the price differences are reflective of market positioning and commercial strategy rather than actual manufacturing or licensing fees. The EV market leader, Tesla, has decided to phase out its basic EVSE model entirely, and has priced the smart model equal to the basic model. In a market where all models have to be smart, suppliers charging price premiums would be at a commercial disadvantage, so prices of smart EVSEs could be expected to fall.

The "smart" variants are generally claimed to be compliant with Open Charge Point Protocol (OCPP) version 1.6, and are capable of establishing communications via Ethernet, Wifi, 4G, 5G, Bluetooth or some other means (these will be discussed later). They are mainly intended for the user to set up a charging regime that suits their needs while minimising energy costs, but can also provide a pathway for charging to be managed by a remote agent.

With a "dumb" EVSE the user simply plugs in the EV, the charging session commences immediately and is modulated by the EV's OBCC, but constrained within the maximum amperage parameter that it reads from the EVSE via the control pilot conductor. The session will run to full charge unless interrupted by a supply power failure, the disconnection of the cable to the EV or if the user switches off the EVSE. This pattern of operation is sometimes called "unmanaged charging."

The capabilities of a "smart" EVSE can be utilised in two ways:

- User-managed charging: the user programs the EVSE with allowable or preferred charging time periods (usually reflecting the tariff structure) and/or operating envelopes (maximum load limits over given time periods). The main difference from unmanaged charging is that the maximum amperage constraint that is initially set by the EVSE's mode of installation may be reduced (down to zero if necessary) by the user, or perhaps by a user-set algorithm that includes parameters such as a target time for reaching full charge.
- Remotely-managed charging: a "remote agent" (RA) authorised by the user may program the charging times and operating envelopes remotely, and/or

exercise “demand response” during emergency periods, by limiting charging or discharging power levels (down to zero if necessary), initiating charging when there is excess energy and discharging when there is a shortage. From the viewpoint of the RA, this pattern of operation may be called “orchestrated charging”. For some EV brands, the user communicates their managed charging preferences direct to the EV via their smartphone app, but the remote agent can still manage the EVSE and so exercise a degree of control over the charging process.

The extent to which a “smart EVSE” can exercise these capabilities depends on its ability to receive instructions, interpret and execute them, as described and documented in technical standards. Some manufacturers prefer to follow proprietary standards which they keep private for commercial reasons, while others follow public standards. From the viewpoint of RAs , EVSEs that follow public standards offer lower cost opportunities for building up a portfolio of demand responsive EV charging that can be monetised in energy, demand and ancillary service markets. Their capabilities are known, and EVSEs from different manufacturers can be accessed and managed in the same way.

It should be noted that compliance with a particular protocol or standard does not in itself guarantee that an EVSE can exercise a useful demand response capability. In some cases the unit is able to receive signals conforming to that standard – provided it is connected to a communications network - but is not configured (by design or by the way it is installed) to act on some signals. Therefore further testing may be required to confirm that even fully standards-compliant EVSE models are able to manage demand during EV charging, if directed to do so.

Table 5 EVSE Models available in Australia

Brand	Model	Variant	Mod identifier	Network comms interfaces	Rating	Supplier	Price	OCPP?	IEC 61851?	Other
Delta	AC Max	1P	EIAW-E4KTSE5A04	With 4G & Ethernet	7.4 kW	NHP		1.6	61851-1	
		3P	EIAW-E11KTSE5A04	With 4G & Ethernet	11 kW	NHP		1.6	61851-1	
		3P	EIAW-E22KTSE5A04	With 4G & Ethernet	22 kW	NHP		1.6	61851-1	
Delta	DC Wallbox	3P	EVDE25D4DUM	Ethernet (standard) + 4G	25 kW	NHP		1.6	61851-1, 61851-23	
Delta	AC Mini Plus	1P	EVPE3225MWN	Ethernet (standard) + Wifi	7.4 kW	NHP		1.5, 1.6	61851-1, 61851-22	
		1P	EVPE3220MUN	Ethernet (standard) + 3G	7.4 kW	NHP		1.5, 1.6	61851-1, 61851-22	
Schneider	EV Link Smart Wallbox	3P Key	EVB1A22PKI	Ethernet (RJ45)	7.4-22 kW	JetCharge	$1,856	1.5, 1.6	61851-1, 61851-22	With EV link
		3P RFID	EVB1A22PRI	Ethernet (RJ45)	7.4-22 kW	JetCharge		1.5, 1.6	61851-1, 61851-22	With EV link
Schneider	EV Link Wallbox	1P	EVH2S3P04K		3.7 kW	evse.com.au			61851-1, 61851-22	
		1P	EVH2S7P04K		7.4 kW	evse.com.au			61851-1, 61851-22	
		3P	EVH2S11P04K		11 kW	evse.com.au			61851-1, 61851-22	
		3P	EVH2S22P04K		22 kW	evse.com.au			61851-1, 61851-22	
Siemens	Versicharge	1P	US2:VC30GRYHW	CTA2045 interface (no module)	1.8-7.2 kW	Siemens			61851-21-2	
		1P	US2:VC30GRYU	CTA2045 interface (no module)	1.8-7.2 kW	Siemens			61851-21-2	
		1P	US2:VCSG30GRYUW	With CTA2045 module (Wifi)	1.8-7.2 kW	Siemens			61851-21-2	
		1P	US2:VCSG30GCPUW	OCPP and Wi-Fi VersiCharge	1.8-7.2 kW	Siemens		1.6	61851-21-2	
ABB	Terra AC Wallbox	1P	TAC-W4-S-0	Wifi, Bluetooth, 3G, 4G, Ethernet	3.7 kW	JetCharge		1.6	61851-21-2	
		1P	TAC-W7-T-0	Wifi, Bluetooth, 3G, 4G, Ethernet	7.4 kW	JetCharge		1.6	61851-21-2	
		3P	TAC-W11-G5-R-0	Wifi, Bluetooth, 3G, 4G, Ethernet	11 kW	JetCharge		1.6	61851-21-2	
		3P	AC-W22-T-0	Wifi, Bluetooth, 3G, 4G, Ethernet	22 kW	JetCharge		1.6	61851-21-2	
JetCharge	Chargemate	1P	Chargemate 3P22	Wifi, Ethernet, Modbus	7.2 kW	JetCharge		1.6J	61851-1, 61851-22	Aust made
		3P	Chargemate 3P22	Wifi, Ethernet, Modbus	22 kW	JetCharge		1.6J	61851-1, 61851-22	Aust made
QUBEV		1P			7.2 kW	JetCharge	$950			
Wallbox	Pulsar Plus	1P			7.2 kW	JetCharge	$1,550	1.6J		
		3P			22 kW	JetCharge		1.6J		
Wallbox	Commander 2	1P		Wifi, Ethernet, Bluetooth	7.2 kW	JetCharge	$2,490	1.6J		
		3P			22 kW	JetCharge		1.6J		
WallPod		1P			7.2 kW	JetCharge	$1,150			
		3P			22 kW	JetCharge				
Ocular	Home	1P	OC1101		7.6 kW	evse.com.au	$950			
		3P	OC1102		22 kW	evse.com.au	$1,150			
Ocular	IQ	1P	IOCAH10R-7	Wifi, Ethernet, Optional 4G	7 kW	evse.com.au		1.6J	61851-1, 61851-22	
		3P	OCAH10R-22	Wifi, Ethernet, Optional 4G	22 kW	evse.com.au		1.6J	61851-1, 61851-22	
Keba	Commerial	3P	EBA P30 a-series		22 KW	evse.com.au	$2,310			
	Commerial - Smart	1P	EBA P30 X-series	UDP interface for smart home au	7.4 kW	evse.com.au	$2,420	1.6		
	Commerial - Smart	3P	EBA P30 X-series	UDP interface for smart home au	22 kW	evse.com.au	$3,500	1.6		
EO	Universal	1P			7 kW	evse.com.au	$1,450			Proprietary
EO	Universal	3P			22 kW	evse.com.au	$1,800			Proprietary
OpenEVSE	Model 3	1P	Advanced series - Kit		7.4 kW	Mail order				
Tesla	Wall Connector	1P	Gen 2	(being phased out)	2.3-7.4	Tesla	$780			
		3P	Gen 2	(being phased out)	11-16.5	Tesla	$780			
		1P	Gen 3	Wifi	2.3-7.4	Tesla	$780	1.6		
		3P	Gen 3	Wifi	11-16.5	Tesla	$780	1.6		
Zappi		1P			7 kW	EvolutionAustrali	$1,545			Proprietary
		3P			22 kW	EvolutionAustrali	$1,880			Proprietary
EV-NRG	Smart Pioneer	1P			7.4 kW	EV-NRG				Proprietary

This project

The South Australian government is seeking to introduce demand response capability product requirements for residential electric vehicle chargers.

Dynamic and flexible energy demand provides direct benefits for customers who participate in demand response aggregation markets. The benefits of a strong uptake of demand response opportunities will also flow to non-participants in demand response programs through reduced wholesale electricity prices and improved electricity network security.

The volume of energy that could be managed through introduction of South Australian demand response product requirements for electric vehicle chargers could reduce load at times of maximum network peak by 47MW by 2036.

In November 2019 COAG Energy Ministers agreed that:

> *Controllers capable of managing the charging and/or discharging to the grid of EVs, that are intended for residential applications and capable of charging at SAE Level 2 or IEC Mode 3, to comply with any of the following standards:*
>
> - *AS/NZS 4755.3.4 (when published); or AS/NZS 4755.2 (when published); or*
> - *an equivalent international standard, if an E3 technical working group determines by mid-2022 that there is one that provides equivalent capabilities to AS/NZS 4755.*
>
> *Compliance with AS/NZS 4755 DRMs 0, 1,2,3,4,5 and 8 to be required (6 and 7 optional), or the equivalents in the other approved standard, for EV chargers supplied or offered for supply from 1 July 2026. 15. A Determination to give effect to the above to be made by 1 July 2024.*

Energy Ministers noted that some jurisdictions with imminent network-related issues requiring more controllable devices in the power system may consider an earlier implementation or additional measures using local regulation.

In March 2021 the South Australian government released a consultation paper on 'Proposed Demand Response Capabilities for Selected Appliances in South Australia and Proposed Amendments to Local Energy Performance Requirements for Water Heaters', proposing that:

> *All electric vehicle chargers supplied or offered for supply from 1 July 2024 to comply with AS/NZS 4755.3.4 (when published), or AS/NZS 4755.2 (when published) or an equivalent international standard if determined by the South Australian Office of the Technical Regulator. Compliance with 4755 DRMs 0, 1, 2, 3, 4, 5 and 8 will be required, or any equivalent DRMs in an international standard approved by the South Australian Office of the Technical Regulator.*

During consultations on the above demand response requirements, the electric vehicle industry and other stakeholders indicated that use of existing international standards would be a preferred mechanism to implement open, non-proprietary demand response capability product requirements.

Consequently, in June 2021 the SA Department for Energy and Mining (DEM) invited tenders for a project to evaluate international standards for electric vehicle chargers. The project was awarded to George Wilkenfeld and Associates Pty Ltd in association with Auseng Pty Ltd.

Terms of Reference

The client's terms of reference are:

> For electric vehicle chargers intended for residential applications and capable of managing the charging and/or discharging to the grid at SAE Level 2 or IEC Mode 3, identify open, non-proprietary international product standard(s) or parts of standard(s), that provide equivalent demand response capabilities to any or all of AS/NZS 4755 DRMs 0,1,2,3,4,5 and 8.
>
> For the identified international standard(s) or parts of standard(s):
>
> - advise on levels of compliant EV charger models in the current Australian market
> - advise on availability of testing report templates to verify compliance against the standard
> - advise whether the preferred DR standard requires compliance with specific communications standards
> - draft a technical requirement based on the identified standard(s) or parts of standard(s), for adoption in South Australia as a mandatory technical standard for electric vehicle chargers
> - for non-compliant models in the current Australian market, advise on estimated manufacturer costs to achieve compliance.
>
> Where the AS/NZS 4755 framework does not cover electric vehicle chargers, assume the DRM tests for electrical energy storage systems [as set out in AS/NZS 4755.3.5 and AS4755.2 Appendix D] will apply.
>
> The supplier is required to deliver:
>
> - Draft and final project plans:
> - Draft and final report on international standards, levels of compliant product and testing templates.
> - Presentation of draft and final report findings to DEM
> - Presentation of draft report findings to E3

There were weekly progress meetings (via video conference) with the DEM project team.[15] DEM advised that any regulation would be implemented via electrical installations rules, rather than legislation targeting product supply.

In our view some aspects of the regulatory requirements would be much the same under either installation or supply regulations:

[15] Attended by the DEM project manager (Craig Walker), the consultant team (George Wilkenfeld and Peter Seebacher) and SA DEM team (Justin Ward, Ian Furness, Darren Hornby).

- The required capabilities of the EVSEs to be supplied or installed would need to be defined in regulations, in a way that can be verified by the regulator; and
- Liable parties (suppliers and installers) would need to be able to identify products that comply – whether by markings on the product (e.g. standards marks), information in the documentation or by reference to a list of complying products maintained by the regulator or other party.

Having completed the research, however, it seems that the use of installation rules has an advantage in that the actual capability of EVSEs to achieve demand response may depend on the settings that the installer selects, even if the EVSE complies with a given standard.

The general principles for regulation set out in Chapter 4 of this report were agreed with DEM and it is understood that the SA Office of the Technical Regulator (OTR) has the head of power to gazette a technical demand response standard.

Work Program

We undertook the following tasks:

- Reviewed the publicly available documents, commentary and analysis on EVSE standards;
- Assessed which parts are directly relevant (noting that many are multi-part standards);
- Obtained copies of the relevant parts; and
- Evaluated each standard/part against the criteria in Table 9.

We contacted a number of stakeholders regarding the project, including:

- EVSE suppliers;
- Managers of current ARENA-sponsored EV charging trials (see Table 16);
- Other groups in Australia investigating EVSE standards, including selected members of the *Vehicle-Grid Integration Standards Taskforce;* and
- EV industry experts; and
- International standards experts.

The stakeholders interviewed are listed in Annex B.

Report Overview

This introductory section gives a background to the project and an overview of home EV charging and how it may evolve in Australia, based on discussions with the EVSE industry and the documented experience of more mature EV markets.

Section 2 presents an initial list of “open, non-proprietary international product standard(s)” that have the potential to support equivalent demand response capabilities to AS/NZS 4755. As there is no published part of AS/NZS 4755 that actually covers EVSEs, this section clarifies how AS/NZS 4755 defines demand response modes and how the same outcomes could be delivered through other standards. This section also presents a list of evaluation criteria based on the capabilities in AS/NZS 4755.

Section 3 present the findings on the terms of reference.

Section 4 sets out the main provisions of a “technical requirement based on the identified standard(s) or parts of standard(s), for adoption in South Australia as a mandatory technical standard for electric vehicle chargers”. The actual draft requirements are contained in a separate document, *Technical Regulator Guideline: Minimum Technical Standard for Electric Vehicle Supply Equipment and Deemed to Comply Provisions.*

Annex A presents detailed analyses of each candidate standard and evaluates them against the criteria in Section 2. Annex B lists persons and organisations consulted. Annex C lists a number of ARENA-funded project that will yield useful information on the suitability for adoption in Australia of some of the standards evaluated in this report.

2. Key Issues

Standards of interest

In 2019 AEMO's Distributed Energy Integration Program (DEIP) established a Vehicle-Grid Integration Standards Taskforce. The Taskforce report (DEIP 2021) focussed on three key areas:

1. **Charging Interoperability**: how different charging configurations might influence interoperability standards, and whether any specific configurations might limit interoperability opportunities. The Taskforce concluded that many international standards are available that specify communications pathways between the electricity system and EVs via EVSE, however no single set of standards has yet become dominant worldwide. Communications direct to the vehicle are mainly managed through bespoke, privately-owned systems.

2. **Energy and services market integration**: where standards might help enable participation of EVs in energy and services markets. The Taskforce concluded that: "most regulation of device performance and communication protocols is implemented via market rules; however a noteworthy exception is Australian Standard AS/NZS 4755. This demand response standard is of interest to the Taskforce due to a recent Council of Australian Governments (COAG) recommendation to expand its scope to include EVSE.

    - Communications standards like IEEE 2030.5, OpenADR, and ISO 15118 could work with AS 4755.2 to provide a complete interoperable demand response framework for EVs, including communications, information exchange, response specification, cybersecurity requirements, and test procedures.
    - Industry, government, and the relevant standards committees need to work together to establish a clear pathway to meet the requirements of the 2019 COAG Regulation Impact Statement (RIS) decision to apply AS/NZS 4755, or an equivalent international standard, to some categories of EVSE from 2026. This work should include engagement with the E3 technical working group which will be established to determine, by mid-2022, whether an equivalent international standard can be used in place of AS/NZS 4755." (DEIP 2021)

3. **Disturbance performance and grid support**: whether current and emerging feature sets of EVs and EVSE could play a role in supporting grid operation, and whether standards might influence or enable this capability. The Taskforce concluded that: "AS/NZS 4777.2 is an established standard applicable to bidirectional V2G inverters, including both stationary and on-vehicle inverters. However, no established Australian or international standards have been identified in relation to disturbance performance and grid support capability for unidirectional chargers, which will likely make up the majority of the charging fleet for many years to come." (DEIP 2021)

The Taskforce examined a number of international standards and identified those relevant to each of the three key focus areas. For the present project, the primary focus area is Energy and Services Market Integration but a secondary focus is Charging Interoperability, because establishing communications with a Remote Agent is necessary to give effect to the DR capabilities of the EVSE. Table 6 lists the international standards identified by the Taskforce as relevant to its first two focus

areas. We have added a number of documents that we consider also relevant (shown in italics). All of the documents in Column 2 of Table 6 are evaluated the present report.

Table 6 International Standards of interest

Standard	1. Charging Interop-erability (a)	2. Energy & services integration(a)
ISO 15118-1:2019 Road vehicles — Vehicle to grid communication interface — Part 1: General information and use-case definition (and other parts?)	✓	✓
SAE J3072 Interconnection Requirements for Onboard, Utility-Interactive Inverter Systems	✓	
IEC 61851-1 Ed. 3.0b:2017 Electric Vehicle Conductive Charging System - Part 1: General Requirements (and other parts?)	✓	
OpenADR IEC 62746-10-1:2018 Systems interface between customer energy management system and the power management system - Part 10-1: Open automated demand response	✓	✓
IEEE 2030.5 (SEP 2.0) Standard for Smart Energy Profile Application Protocol; *Common Smart Inverter Profile – Australia V1.0; Common Smart Inverter Profile (Sunspec)*	✓	✓
IEC 61850:2021 Communication networks and systems for power utility automation (several parts?)	✓	
OCPP Open Charge Point Protocol *1.6 and 2.0.1*	✓	✓
IEC 63110–1 ED1: Protocol for Management of Electric Vehicles charging and discharging infrastructures (in development)	✓	
IEC 63119-1:2019 Information exchange for electric vehicle charging roaming service - Part 1: General	✓	
SAE J2931 Digital Communications for Plug-in Electric Vehicles	✓	
ANSI/CTA-2045 Modular Communications Interface for Energy Management	✓	✓
BSI PAS 1878:2021 Energy smart appliances –System functionality and architecture – Specification	✓	✓

(a) Focus areas in DIEP (2021) Documents in italics have been added for the present study.

The Vehicle-Grid Integration Standards Taskforce report did not consider the EVSE standards from China, which is now the world's largest EV producer and EV market. China has its own standards for EVSEs, GB/T 18487.1–2015 Electric vehicle conductive charging system–part 1: general requirements. This categorises charging modes 1, 2 and 3 in a similar way to IEC 61851-1:2017 (see Table 3) with adjustments for China's standard grid voltages: 220V single phase and 380V three-phase.

As global demand grows, it is inevitable that a large share of EVSEs arriving in Australia will be manufactured in China. However, as with other electrical equipment, Chinese manufacturers would have no trouble in supplying products built to any required standard, provided the global market is large enough to make it worthwhile.

There have been studies on harmonising the requirements of GB/T 18487.1–2015 and SAE J1772:2017 so that US-made EVs are interoperable with GB/T 18487.1–compliant EVSEs (Zhang, 2021).

In the USA, EVSE manufacturers appear to be converging to the use of OCPP for communications between EVSEs and charging system operators. A 2019 survey found that:

> The industry appears to be coalescing around OCPP (including OSCP) with at least 66% (29) of managed charging-capable EVSE manufacturers integrating it. Of those 29 vendors, 8 paired the equipment with OpenADR 2.0 as well. The second most common standard is ISO/IEC 15118… (SEPA (2019)

A follow-up survey in 2021 found that the trend to OCPP continues, with 81% of managed charging-capable EVSE manufacturers integrating it (SEPA 2021).

In Australia, 9 of 14 brands identified offer OCPP-capable models.

IEEE 2030.5 is widely used for DR of inverter appliances. Its predecessors, SEP1 and SEP2 are extremely widely used. Its use for EVSE will be assisted by California Rule 21. Some interpret this rule to mean that IEEE 2030.5 is mandatory, but it in fact a default standard, and alternatives are also allowed.

Demand Response Modes

The Terms of Reference refer to “open, non-proprietary international product standard(s) or parts of standard(s), that provide equivalent demand response capabilities to any or all of AS/NZS 4755 DRMs 0,1,2,3,4,5 and 8.”

In the AS/NZS 4755 suite of standards the way in which each type of electrical product (EP) complies with each DRM is specified in a sub-part of the standard.[16] There is no sub-part covering EVSEs or EVSDEs, but the nearest EP type is *Grid-connected electrical energy storage (EES) systems (EESS)*, which include stationary batteries, covered in Appendix D of 4755.2.[17] The relevant DRMs are described in Table 7. Both EVSEs and EVSDEs can be capable of acting with the EV to achieve DRMs 0 to 4, but only EVSDEs can be capable of DRMs 5 to 8.

Table 7 Demand response modes in AS 4755.2 (Electrical Energy Storage Systems, Appendix D)

DRM	General description of the required EESS response
0	Open the disconnection device, if present
1	Do not import energy [through the GIP (a) of the EESS] but control and auxiliary functions may continue
2	When importing energy [through the GIP of the EESS], limit rate to ≤ 50 % of the import reference value
3	When importing energy [through the GIP of the EESS], limit rate to ≤ 75 % of import reference value Provide power quality support if the EESS is capable
4	Increase the import of energy [through the GIP of the EESS] subject to other active DRMs and if able to import energy through the grid interactive port. If not importing at time of OI 4 received then start importing energy through the GIP.
5	Do not export energy [through the GIP]
6	When exporting energy [through the GIP], limit rate to ≤ 50 % of the export reference value
7	When exporting energy [through the GIP], limit rate to ≤ 75 % of the export reference value Provide power quality support if the EESS is capable
8	Increase the export of energy [through the grid interactive port] subject to other active DRMs and if able to export energy [through the grid interactive port]. If not exporting at time OI 8 received then start exporting energy [through the GIP]

Source: AS 4755.2 Public Commenting Draft. (a) Phrases in square brackets would not apply if installation does not have a distinct grid-interactive port (GIP).

The grid interactive port (GIP) referred to in Table 7 is defined as the point of connection in an EESS or other system where—

a) electromagnetic energy may be supplied to or received from the grid;
b) the device or network variables may be observed or measured; and

[16] *AS 4755.2 Demand response capabilities and supporting technologies for electrical products Part 2: Demand response framework and requirements for communication between remote agents and electrical products*, currently at the public comment stage, is part of the AS/NZS 4755 framework.
[17] Appendix A covers Air Conditioners, Appendix B covers swimming pool pump controllers, Appendix C covers electric water heaters. AS/NZS 4755.3.4 Part 3.4: G*rid-connected charge/discharge controllers for electric vehicles* was released for public comment in 2013 but not published.

c) the flow of electromagnetic energy may be controlled by the demand response controller

The reason for defining energy flows though the GIP rather than to or from the EESS itself is because an EESS may be configured so that it can charge from PV, say, and discharge to the house supply even if the connection to the grid (the GIP) is open (i.e. no energy can flow). AS4755.2 DRMs are not intended to affect any flows of energy behind the meter other than those involved in an interaction with the grid. The same principle would apply to an EVSE that continues to charge the EV from on-site PV, or to an EVSDE with PV-management capabilities.

DRM0 applies if the product has a "device which meets the requirements of an automatic disconnection device in AS/NZS 4777.2" where it was introduced as a precautionary measure to protect line workers from PV or battery discharge at times when they would expect the grid to be de-energised. It would significantly increase the safety of EVSDE installations, but is less necessary for EVSEs, which by definition cannot discharge. Nevertheless, several EVSEs activate a "no-load" state (DRM1) by opening the contactor, so in effect DRM0 and DRM1 are combined. DRM1 is supported by all DR standards.

DRM2 and DRM3 were originally included in AS/NZS 4755 as operating power limits that are simple for consumers to understand and relatively straightforward for manufacturers to build, whether the products have single-speed motors and basic controls or variable speed drives and complex controls. They are also simple for remote agents (RAs) to explain when recruiting DR program participants: "we can guarantee you will have 50% of the energy service [DRM2] or 75% [DRM3] except on the rare occasions when we have to interrupt the service for brief periods [DRM1]".

Other DR standards are able to set variable power limits across the full range from 100% (no constraint) down to 0% (effectively DRM1), passing through 75% (DRM3) and 50% (DRM2) on the way. However, the question is the reference value "x% of what". There are two approaches to reference value in AS/NZS 4755:

- Fixed reference value: the maximum power of the EP when operating at full load; or
- Dynamic reference value: the actual operating power of the EP over the period immediately preceding a DR event. Where the EP starts operating during the DR event, and so has not immediate operating history, there are various rules for determining the dynamic reference value.

A fixed reference value is simpler to verify, but does not deliver a demand reduction if the EP is operating at low power when the DR event starts: e.g. if it is already operating at 40% power then it needs to do nothing under DRM2 (with the proviso that it must not *increase* its power level to 50%). In AS4755.2, water heaters and air conditioners are subject to fixed reference values.[18]

A dynamic reference value is intended to deliver a response even at low power. It is especially valuable for products with a high maximum power rating which routinely operate at a fraction of that level, such as EVSEs. In AS4755.2, pool pump controllers and EESS are subject to variable reference values. The way in which DR standards define reference value will be an important aspect of the evaluation.

[18] Air conditioner DR was originally defined in relation to a fixed reference (in AS/NZS 4755.3:2008 and 2012), then a variable reference (AS/NZS 4755.3.1:2014) and reverted to a fixed reference in AS4755.2.

Some DR standards specify that a complying EP must be capable of receiving, interpreting and acknowledging receipt of DR instructions, but do not specify how the instructions are translated into a verifiable response. It is possible for products to comply but still be designed or installed in ways that prevent all or some responses.

AS/NZS 4755 defines power quality support as the ability to provide or draw reactive power (vars). Additional instructions would need to be given with a DRM3 (or DRM7) instruction in order to support this capability. As with DRM0, this capability is based on AS/NZS 4777.2. Other DR standards, if they offer this capability at all, may do so via a separate instruction set.

DRM4 is in effect a request to the EP to turn on if not operating, or increase load if already operating. Unlike DRM1, it cannot be a directive because there are layers of safety and functional conditions to be met. Operation must not present a human safety risk, must not damage the EP (e.g. by forcing it to store energy beyond its safe limit) and must not lead to energy waste (e.g. by turning on cooling in unoccupied houses). For EVSEs DRM4 would be subject to further conditions: whether an EV is connected at all, and if so whether it is fully charged when a DRM4 event starts. As users will typically plug the EV in and let it charge until full – not rest at partial charge states – EVs will rarely be in a position to respond to DRM4. Another way to achieve a "load on" function during renewables-abundant or low-price periods is to invoke DRM1 beforehand and release it at those times.

DRMs 5 to 8 apply to EVSDEs only. DRM5 is equivalent to DRM1, except that it prevents discharging rather than charging. Some EVSDE DR standards may use the same instructions for both DRM1 and DRM5: e.g. a "0% power" instruction may prevent flows of energy in either direction. This would represent less control flexibility than AS4755.2 where inflow and outflow limits can be set independently.

DRMs 6 and 7 are equivalent to DRMs 2 and 3, and present the same reference value issues. The equivalent capabilities in other DR standards will be evaluated, even though the COAG Energy Council and DEM have decided not to mandate DRM 6 or 7.

DRM 8 is a request to discharge energy stored in the EV. It can be combined with DRMs 6 and 7, or a continuous range (e.g. "please export but limit to X% of a reference value"). As with DRM4, fulfilment of such a request is subject to a layer of conditions, including having an EV connected at the time, adequate charge in the EV and no user over-rides in place. For example, a user who regularly permits their EVSE to provide grid support (in return for some incentive, presumably) may have an important appointment in the morning, may have already charged their EV and not want to risk a discharge, and so will set an override to DRM8 only (but not other DRMs).

The way in which DR standards enable users to set over-rides also varies. AS4755.2 has different over-ride rules for different EPs. Appendix D specifies that, for stationary EESS, "no DRM shall be subject to a user override" (Clause D.2.4). This is based on the principle that activation of DR capability is optional, at the discretion of the EP owner/user and revocable by arrangement with the RA. The RA's exercise of DR over a stationary battery is likely to be minimally disruptive, and probably not even noticed. By contrast, the exercise of DR over an air conditioner, a water heater or an EVSE may well inconvenience the user and so should be subject to over-ride, but the way in which this is exercised should balance the interests of the user and the RA who is compensating the user for the right to initiate DR under agreed conditions. AS4755 manages this balance by limiting over-rides to certain DRMs, or to be exercised only once per day or per operating cycle, and to be accessed via a deliberate set of user operations rather than easily pre-programmable.

Evaluation Criteria

Maturity of Standard

The maturity of a standard is one indicator of whether the inevitable gaps and errors of the first versions have been resolved. Some of the standards in Table 6 have already gone through several revisions, whereas the operative parts of IEC 63110 have not yet been published. In some standards later versions are not backwards compatible, so products built to different versions behave differently.

Another indication of stability and longevity is the body responsible development and maintenance. Standards issues by recognised agencies such as the IEC and the ISO are subject to formal processes of drafting and review, which indicate a certain level of consensus and acceptability, but on the other hand may not keep up with the speed of technological development. Other standards, developed by industry associations such as the OpenADR Alliance and the Open Charge Alliance, are sometimes adopted as IEC or ISO standards.

Scope

Some standards cover DR support capabilities for any electrical product, some for a range of specified products including EVSEs, some specifically for EVSEs and some specifically for other products, although they may be adapted for EVSEs. Some cover one-way energy flows only, while others cover two-way flows as well (i.e. V2G).

Another key aspect of the scope is whether it covers the DR of the EVSE only, the means of communicating with the EVSE or both. With respect to communications, is the standard structured according to the Open Systems Interconnection (OSI) model, and if so which of the 7 layers are covered?

Adoption and Usage

Some DR standards have been referenced in legislation. In the USA for example, IEEE 2030.5 is referenced in California Rule 21. OpenADR 2.0b is referenced in California Rule 24, Mandatory Requirements for Demand Management in Buildings. ANSI/CTA 2045 is a mandatory requirement for water heaters in Washington State.

Other standards are being widely adopted by industry, even without regulation – OCPP 1.6 is a notable example. In the UK, OCPP 1.6 (or higher) compliance is required for EVSEs that qualify for the Electric Vehicle HomeCharge Scheme.[19]

Interfaces

A demand responsive EVSE must be physically able to receive information from an RA (the “upstream interface”). This may be defined in terms of OSI layers, or pathways such as 3G, 4G, Ethernet, WiFi or Bluetooth. It must also be able to communicate DR requests or conditions to the EV (the “downstream interface”), usually via the pilot conductor cable. An important aspect of the upstream interface is the management of potential conflicts between instructions from the RA and the user or from different RAs.

Other standards required/supported for end-to-end operation

[19] The scheme subsidises 75% of the cost of buying and installing a home EVSE, up to £350 value. https://www.gov.uk/government/publications/electric-vehicle-homecharge-scheme-minimum-technical-specification/electric-vehicle-homecharge-scheme-minimum-technical-specification

The EVSE is only one element in a DR framework linking the RA to the EV. It may be compatible with some types of interfaces or standards needed to complete the system but not others. Adopting a given standard for the EVSE may therefore imply the necessity to adopt, or preclude, other standards in the system as a whole. In some cases pairs of standards may need to be inked in regulations.

Proprietary/patent content

Mandating the use of a standard is problematic if it embodies proprietary technology or is subject to outstanding patent applications. This could create uncertainty and risk for standards users, and expose them, and perhaps the regulating body, to legal challenges or demands for royalties or compensation.

Main functions, settings and capabilities

AS 4755.2 includes the following minimum capabilities for electrical products, which standards committee EL-054 considers essential in a DR framework.

- the capability to receive commands from a remote agent; other DR standards may specify the ability of the EVSE to receive and respond to commands, but do not distinguish the origin, and so are not able to give priority to an RA over a user, or indeed other RAs.
- Entering responsive and non-responsive states; where a user enrolled in a DR program wishes to their involvement, the RA can exclude the product from future DR events.
- Time delay/scheduling capability for start/end event; the RA can instruct the product to modify operation immediately, at a specified clock time or a specified interval.
- Randomisation of start/end of a DR event, to prevent power surges on the network. If product-level randomisation capability of this kind is not present in a standard itself, we will need to assess whether there would be “natural” randomisation in the DR framework as a whole, e.g. if all EVSEs are given the same charging start and stop times, will the fact that the instruction has to be actioned by the on-board charge controllers of different brands of EVs, all in the different states of charge, be sufficient to damper surges?
- User over-ride provisions. Are these mentioned in the standard at all, or could they be introduced in the DR framework as a whole?

Preservation/deletion of settings (privacy)

Internet-connected electrical products are liable to monitor and record their activity, and this information could be used for privacy breaches and even criminal actions – for example, to know when houses are empty for long periods and so vulnerable to break-ins. Also, when equipment is reused and re-installed there should be no record of the activities of the previous owner or location.

Command formats required/supported

Some standards support different variants (OCPP terms them “flavours”) which need to be addressed in different ways. These may create different categories of EVSE which need to be managed differently and so reduce the value of an ostensibly open standard.

Equivalence of Demand Response Modes

The terms of reference require identification of standard(s) or parts of standard(s), that "provide equivalent demand response capabilities to any or all of AS/NZS 4755 DRMs 0,1,2,3,4,5 and 8", all of which are described in detail in the preceding section. It is necessary to evaluate how, and to what the extent, each standard supports equivalent outcomes.

Other inbuilt DR capabilities

There may be other valuable DR features beyond those that are equivalent to AS4755 DRMs.

Feedback pathways

Some DR business models require information feedback from the electrical product to the RA. A standard may specify that the EVSE may, or must be capable of establishing a feedback pathway to communicate information to the RA. It may also specify the categories of information to be communicated, e.g.

- The present operating status of the EVSE, e.g. 'Standby' or 'Charging';
- If charging, the power level (instantaneous or over a recent period);
- DR events under way, recently executed or logged for future execution;
- Power levels during DR events;
- Whether user override has been activated; and
- Indication of communication failure when the electrical product is no longer sending or receiving signals.

Cyber-Security

A fundamental requirement of an electric product that is capable of being remotely managed is that only authorised remote agents can exercise that management. This requires a clear process by which the product and the RA verify each other's identity and establish secure channels of communication.

Documentation, Certification and Testing

Some EVSE suppliers claim that certain models comply with specified standards. Some standards specify how compliance may be verified, but others leave it to third parties to devise compliance tests. If so, have any such tests been carried out, how reliable are the testing authorities and is there a simple way for the regulator to access the test reports? Are all specified requirements tested or just a subset? These questions need to be put to suppliers in a systematic way, so the regulator can formally register those models and maintain a current list of complying products.

A regulatory program also requires the capability for the regulator to commission verification tests from a trusted independent test laboratory.

ESVE brands and & models claiming compliance

Are there actual products on the market that meet that standard? Is the number of such products increasing or decreasing? Are there brands or jurisdictions committed to one or other standard?

Suitability for regulatory adoption (alone or in association)

Annex A analyses each of the standards of interest in terms of the evaluation criteria above. At the end it should be possible to make an overall assessment of the suitability of the standard for regulatory adoption.

3. Conclusions

Summary of Evaluations

The intent of adopting a standard is to ensure that a complying EVSE or EVSDE can accept DR operational instructions (OIs) and obtain the required action by the EV. The international standards evaluated enable the transmission, receipt and interpretation of OIs (in various formats) but none provide for testing that the message is actually passed on to and correctly actioned by the EV. In this respect there is no international standard which, on its own, would achieve demand response outcomes to the same level of confidence as the AS/NZS 4755 framework.

Therefore it would be prudent to allow for testing with an actual EV or an electrical analogue of an EV. Otherwise a standards-compliant EVSE may still be unable to deliver a firm DR capability.

The assessment of each standards against the evaluation criteria are summarised in Table 9. The detailed descriptions and assessment are in Annex A.

OCPP 1.6 and 2.0.1 and ANSI/CTA 2045 can be used in conjunction with a range of "upstream" communications platforms, including OpenADR and IEEE 2030.5. Complying EVSEs rarely specify or restrict the platform. The choice of platform would be up to remote agents, but they can be confident that the DR messaging would get through to standard-compliant EVSEs (barring communication disruptions).

OCPP 1.6 is the only standard with widespread support by the Mode 3 EVSEs currently on the market. It is backed by a testing and certification scheme administered by the Netherlands-based Open Charge Alliance, the industry consortium which publishes the standard. OCPP can transmit signals which should, if actioned, replicate DRMs 1 to 4 but not DRMs 5 to 8, as it does not support V2G.

This does not mean that all EVSE models complying with OCPP 1.6 are able to action all DR messages. Analysis of the wiring diagrams and installer instructions from a number of EVSE installation manuals indicates that some can only be set to action one of DRMs 1,2 and 3, some can be set to action two and some to action all three (See Table 8). Where fewer than three DRMs are supported, in some cases DRM1 is fixed and the installer sets the other (e.g. a level of constraint that could correspond to either DRM2 or DRM3). In other cases the installer can choose NOT to set DRM1 if they wish. In other words, the installer's setup of an OCPP-compliant EVSE will be the final determinant of its actual DR capability.

Table 8 DRM supported by EVSE models according to standards compliance

	OCPP 1.6	CTA 2045	Proprie-tary	No DR standard	Total models
Models capable of three DRMs	6	3	0		9
Models capable of two DRMs	0		2		2
Models capable of one DRM	10				10
Models probably capable of at least DRM1 (a)	9		3		12
Models probably incapable of DRMs	0			13	13
TOTAL MODELS	25	3	5	13	46

(a) Not enough conclusive information in public domain, but likely to support at least DRM1

ANSI/CTA-2045 differs from the other standards in that it provides for a plug-in universal communications module (UCM), which functions like the Demand Response Enabling Device (DRED) in AS/NZS 4755.1. Different UCMs support different messaging platforms; the most common one uses OpenADR 2.0. ANSI/CTA-2045 is mainly used for water heaters and thermostats, but it is supported by at least one brand of EVSE. All UCM-equipped EVSEs would be able to replicate DRMs 1 to 4 and DRMs 5 to 8 would be possible if the EVSE were specifically designed for V2G.

The other standards are less mature, and consequently have negligible take-up in the EVSE industry, although this is expected to change over the coming years.

OCPP 2.0.1 provides for V2G, but it is not backwards compatible, so DR platforms and programs built for OCPP 1.6 will not automatically cover OCPP 2.0.1 compliant equipment (or vice versa). It is expected that as OCPP 2.0.1 develops it will be consistent with IEC 15118. IEC 15118 is specifically designed to support V2G, but key parts remain to be completed and it will require more complex communications with the EV than offered by the IEC 61851 compliant "control pilot" wire that is wrapped in with the EV charging cable.

IEEE 2030.5 was developed in the USA to enable utility management of the end user energy environment, including demand response. It is widely used for controlling PV inverters, and is the default standard adopted by the California Energy Commission under Rule 21 (although other standards can also be used).[20] It is applicable to V2G EVSDEs, as they also use inverters. However, the number of EVSEs (even in the USA) claiming IEEE 2030.5 compliance is negligible.

Interest in IEEE 2030.5 is growing in Australia. Standards Australia has started a project to adopt it as an AS/NZS standard, and at the same time develop an Australian Implementation Guideline. An early draft of the Guideline includes an Annex describes how IEEE 2030.5 can accept and pass on OIs for the DRMs in AS/NZS 4755, including combination of OIs that request power quality responses. While promising, the work is still at an early stage.

OpenADR (adopted as IEC 62746) is widely used for conveying dynamic energy pricing information and DR requests from remote agents to building energy systems and charging point operators, but is not designed to issue direct DR OIs to EVSEs or other end use products. However, it can be used in combination with OCPP 1.6-compliant EVSEs to achieve that purpose.

BSI PAS 1878:2021 *Energy smart appliances –System functionality and architecture – Specification* is more like a regulatory standard than a technical standard. It prescribes an architecture in which a Demand Side Response Service Provider (DSRSP) interfaces with a Customer Energy Manager (CEM; a functional or physical unit) which interfaces in turn with an Energy Smart Appliance (ESA). OpenADR is listed as one option for managing "Interface A" between the DSRSP and the CEM, but the standard for "Interface B" between CEM and appliance is left open. This is the opposite of the AS/NZS 4755 approach, where interaction with and performance of the appliance is highly prescribed, but the "upstream" platform is left open. It remains to be seen

[20] California's Public Utilities Commission Rule 21 mandates that generating facilities that utilise inverter based technologies to interconnect with utility grids must support an application layer communications protocol. This protocol is used by the utilities to configure advanced inverter functions and receive operating state information from the inverters.

whether EVSE products claiming conformance with BSI PAS 1878:2021 come on the market, and how they can be tested.

Table 9 Evaluation Against Criteria

Assessment Criteria	OCPP 1.6	OCPP 2.0.1	CTA 2045	IEEE 2030.5	IEC 15118	OpenADR/ IEC62756	PAS 1878
Status & Maturity	Mature	Developing	Mature	Mature	Developing	Mature	Developing
Able to manage charging	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Able to manage discharging	No	Yes	Possible(a)	Yes	Yes	Yes	Yes
Other standards required for end-to-end operation	TCP/IP	TCP/IP	Yes - comms	TCP/IP	Yes - several	XML, TCP/IP	PAS 1879, OpenADR etc
Proprietary/patent content	None	None	Possible	Possible	Possible	Possible	Possible
Ability to receive commands from one remote agent	Yes	Yes	Yes	Yes	Multiple RAs	Yes	Yes
Entering responsive and non-responsive states	Possible (b)	Possible (b)	Yes	Yes	No	No?	No?
Time delay/scheduling capability for start/end event	Yes (b)	Yes	Yes	Yes	Yes	Yes	Yes
Randomisation of start/end	No	No	Optional	Yes	No	Yes	Yes
User over-ride facilities	No (a),(b)	No (a),(b)	Yes	Yes	Yes	Yes	Yes
Preservation/deletion of settings (privacy)	Can clear	Can clear	Possible	Possible	Yes	No	Yes
Command formats required/supported	See details	See details	See details	See details	See details	See details	See OpenADR
DRM 0 equivalence	×	? (a)	✓	✓	×	×	×
DRM 1 equivalence	✓	✓	✓	✓	✓	✓	✓
DRM 2 equivalence	✓ (as A or W)	✓ (as A or W)	✓	✓	✓	✓	✓
DRM 3 equivalence	✓ (as A or W)	✓ (as A or W)	✓	✓	✓	✓	✓
DRM 4 equivalence (if chargeable EV connected)	✓	✓	✓	✓	✓	✓	✓
DRM 5 equivalence	×	✓	? (a)	✓	✓	✓	✓
DRM 6 equivalence	×	✓	? (a)	✓	✓	✓	✓
DRM 7 equivalence	×	✓	? (a)	✓	✓	✓	✓
DRM 8 equivalence (if dischargeable EV connected)	×	✓	? (a)	✓	✓	✓	✓
Other inbuilt DR capabilities	NA	NA	Yes	Possible	Reactive pwr	Yes	UK meters
Feedback pathways	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Secure provisioning	Yes	Yes	Possible	?	Yes	Yes	Yes
Access control	Yes	Yes	Yes	Yes	Yes	Yes	No
Firmware update provisions	No	Yes	Yes	Yes	Yes	No	Yes
Registration (network)	Yes	Yes	Yes	Yes	Yes	Yes	No
Communications security	Yes	Yes	Yes	Yes ?	Yes	Yes	Yes
Provisions for documenting/reporting compliance	Yes (d)	Coming	Coming	Yes (d)	Yes (d)	Yes (d)	No
Provisions for testing compliance	Yes (d)	Not yet	Yes	Yes (d)	Not yet	Yes (d)	No
Availability of testing and certification facilities	Yes (d)	Not yet	Coming	Yes (d)	Not yet	Yes (d)	No
EVSE market adoption	High	None yet	Low	Low	None yet	Low	None yet
Suitability for regulatory adoption	Immediate	Near term	Immediate	Near Term	Longer Term	Not on its own	Not on its own

(a) Depends on design or configuration of EVSE (b) Depends on combination or sequence of RA instructions (c) Depends on user settings or actions (d) Does not extend to testing actual DR

Findings on Terms of Reference

There are no existing EVSE or EVSDE DR-related standards that would exactly meet all the requirements and features of AS/NZS 4755. Of the two standards that are in use (and which are supported by actual available models):

1. A product that complies with OCPP 1.6 can be managed by a remote agent to replicate DRMs 1,2,3 and 4; and

2. A product that complies with CTA2045 can accept a communications module which would be able to pass on the operational instructions for DRMs 1,2,3,4 and perhaps 5 and 8, using a wide range of pathways (including OpenADR, OCPP, etc.). It would be up to the future aggregator or remote agent to deliver their preferred module to the user. The module and its capabilities are outside the scope of the initial product standard, so a CTA2045-complant EVSE would be "potentially DR-capable" rather than "DR-capable"

A regulation that requires EVSEs to comply with either (1) or (2) would exclude "dumb" EVSEs from the SA market and ensure that every EVSE installed is actually or potentially DR-capable. Publishing a Performance Specification as well would give suppliers the opportunity to come up with other novel solutions.

Compliance levels and costs

Of the 47 home EVSE model variants identified on the Australian market, 27 are claimed to comply with OCPP 1.6, three support ANSI/CTA-2045 and four support proprietary messaging protocols. The remainder are basic or "dumb" EVSEs with no communications capability.

In our discussions with EVSE suppliers, the quoted price difference between basic and OCPP 1.6 compliant varied from about $500 to zero, with the most common value around $200. This was about the same price as the charging cable connecting the EV to the EVSE. The price differences are more reflective of market positioning and commercial strategy than actual manufacturing or licensing fees. The EV market leader, Tesla, has decided to phase out its basic EVSE model entirely, and has priced the smart variant equal to the basic model. In a market where all models have to be smart, suppliers charging price premiums would be at a commercial disadvantage, so prices of smart EVSEs could be expected to fall.

Testing and Certification

The Open Charge Alliance has developed a testing tool for OCPP 1.6 and is currently developing one for OCPP 2.0.1. At present six test laboratories around the world offer OCPP testing and certification services. A manufacturer seeking certification would need to bear the cost of the test and pay a certification fee of several thousand Euros to OCA. At present only two brands of home EVSEs are certified, neither of which are available in Australia.

There are also US-based testing and certification programs for IEEE 2030.5 and Open ADR. At present there is nothing to prevent or deter an Australian EVSE supplier claiming compliance with any standard, apart from the Trade Practices Act. If compliance were mandated, proponents could be required to make a declaration of compliance in the first instance, in the knowledge that the Regulator could commission tests for those standards that are backed by testing and certification.

As stated above, such testing would only verify that a complying EVSE or EVSDE can receive and interpret the relevant DR instructions, but not that the message is actually passed on to and correctly actioned by the EV. If regulations describe a further test with an actual EV or an electrical analogue of an EV, this would put suppliers on notice to verify this for themselves, and enable Regulators to commission such a test should they wish to do so.

Suitability for Regulatory Adoption

The standard most suitable for early adoption is clearly OCPP 1.6. It would ensure that all EVSEs sold in SA would have at least a minimum DR or “smart charging” capability. While the standard only covers charging, the likely slow development of V2G would give time to assess the development and market adoption of other standards.

ANSI/CTA 2045 offers considerable flexibility, and while its use in EVSEs is limited at present it is mature and testable and would offer another compliance option.

4. Regulatory Proposal

A draft Technical Regulator Guideline has been drafted, as a separate document.[21] The main provisions are below. It is proposed to include "Deemed to Comply" provisions to enable the Technical Regulator to adopt other standards that may be proposed by suppliers, including IEEE 2030.5, OCPP 2.0.1 or IEC 15118, should they develop more quickly than expected. It also sets out a response test in which the EVSE or EVSDE is connected to an actual EV or EV analogue

Installer Requirements

An installer shall not install or connect an EVSE or an EVSDE of a type that is within the scope of these Guidelines unless:

1. The product complies with either the Minimum Technical Standards (Part 6 of these Guidelines) or the Deemed to Comply Provisions (Part 7 of these Guidelines); and
2. The product is of a brand and model that has been registered with the Technical Regulator; and
3. The installer configures the EVSE (in accordance with the manufacturer's instructions) so that it is able to respond correctly to a signal to turn load off and to a signal to limit charging power or current to 40-60% of the unconstrained charging limit.
4. The installer registers the location of the installation, once completed.

The listing of the brand and model on the register of the Technical Regulator may be taken as evidence that the product complies with clause (1) above.

Minimum Technical Standards

Demand Response

An EVSE shall comply with:

a. Open Charge Point Protocol (OCPP) 1.6, edition 2 FINAL, 2017-09-28 (or higher)[22]; or
b. ANSI/CTA-2045-B:2021 *Modular Communications Interface for Energy Management* [23]*; or*
c. A standard that the Regulator has "Deemed to Comply."

An EVSDE shall comply with a standard that the Regulator has "Deemed to Comply."

For clarity, both SOAP and JSON versions of OCPP 1.6 are acceptable.

Other minimum technical standards may be added by the Regulator in future revisions of these Guidelines.

Remote Communications Capabilities

An EVSE or EVSDE that complies with OCPP (any version) must have internet capability (the ability to share data via the World Wide Web) and an on-board

[21] Technical Regulator Guideline Minimum Technical Standard for Installation of Electric Vehicle Supply Equipment (EVSE) for residential use, Version X, YYYY 2022 (Draft 1)
[22] Downloadable from https://www.openchargealliance.org/protocols/ocpp-16/
[23] Downloadable from https://shop.cta.tech/products/modular-communications-interface-for-energy-management

communication port that can be used for a physical connection to another device (e.g. via Ethernet, USB and RS-232). If an EVSE or EVSDE can communicate wirelessly in a manner similar to an on-board communication port (for example by providing a secure Application Programming Interface or API over Wifi) that can be used for a connection to another device, this may be utilised in lieu of a physical communication port.

An EVSE that complies with ANSI/CTA-2045-B:2021 will have a port that accepts a standard size communications module, that may be configured for OCPP, OpenADR or other protocols. It will be open to remote agents or others to supply or arrange for the supply of modules that conform with their own systems.

Table 10 summarises the compliance options for EVSEs and EVSDEs.

Table 10 Compliance Options

Compliance options	EVSE and EVSDE, with regard to EV charging from grid	EVSDE, with regard to EV discharging to grid
Option 1	OCPP 1.6 V2 or higher	NA
Option 2	ANSI/CTA 2045-B	NA
Option 3	Meets “Deemed to Comply”	Meets “Deemed to Comply”

Verification of Demand Response

Irrespective of the Compliance Option in Table 10, the EVSE or EVSDE shall be capable of responding to and implementing at least the following:

- An instruction from a Remote Agent to cease or prevent charging (corresponding to either DRM 0 or DRM 1); and
- An instruction from a Remote Agent to constrain the rate of charge in accordance with DRM2; or
- An instruction from a Remote Agent to constrain the rate of charge to between 40% and 60% of the maximum rate of charge set at the time of installation of the EVSE.

The implementation of these DRMs shall be capable of being tested when the EVSE is connected to an actual EV or to an EV analogue load.

Deemed to Comply Provisions

The Regulator may deem a brand and model of EVSE or EVSDE to comply if, in the Regulator’s view, it meets the following requirements.

1. The product is capable of being set (with the consent of the user/owner) so that an authorised remote agent can take direct control for a period, over-riding the user settings.

2. The product is capable of being set so that, if it is accessible to more than one remote agent at a time, it is clear which agent has priority.

3. The user may override some individual demand response events, but not DRM 0, 1 or 5 (or their equivalent).

4. The EVSE or EVSDE supplier must nominate one or more means of communication, and be willing to supply the hardware and software that enables a remote agent to establish secure communication with the product.

5. Once communication is established, the remote agent must be able to send, and the product must be able to respond to, at least the following commands:

For EVSEs and EVSDEs:
a. Safety disconnect [equivalent to DRM0]
b. No charging [equivalent to DRM1]
c. Constrain charging levels, to one of:
- 50% [DRM2] and/or 75% [DRM3] of a reference value;
- over a continuous reduction range (e.g. 0-100% of a reference value), or
- a maximum current or power level.
d. Request charge [DRM4]
In addition, for EVSDE only:
e. No discharge to grid [DRM5]
f. Request discharge [DRM8][24]

6. The reference value/s for reductions in charging levels shall be stated by the supplier. The reference may be a fixed value (e.g. the maximum current set at the time of installation), a dynamic value (e.g. the average power consumed or sent out over a 5 min period prior to the product entering a DRM) or some other measurable value.

7. The EVSE or EVSDE must be capable of receiving and storing commands for later action, even if received when it is not charging or discharging.

8. Commands shall be capable of being changed or deleted by the remote agent.

9. To avoid demand surges on the network, the EVSE or EVSDE itself, or the system of which it is a part, shall be capable of establishing time delays between the receipt of a command from a remote agent and—

   a. a target time to commence and cease demand response (i.e. a delay capability); and
   b. randomization with regard to the commencement and cessation of demand response, such that demand response events do not result in mass simultaneous change in the operating mode of all products of the same model type.

10. The supplier must provide (and submit to the Regulator) documentation on the product's demand response capabilities and how to access them, for the use of prospective purchasers, users and installers.

11. The EVSE or EVSDE shall be capable of responding immediately to an emergency command to switch off load, whatever the time delay or randomisation settings.

12. The supplier must provide documentation on its cyber-security provisions to the Regulator (e.g. evidence of TLS certificate and Certification Authority arrangements).

13. It must be possible for the Regulator to randomly select an individual sample unit and to verify that it complies with the above, once the specified mode of communication has been set up (e.g. in a test laboratory). Suppliers must be prepared to disclose all information and settings needed for testing.

[24] Note that DRMs 6 and 7 may also be within the capability of an EVSDE, but are optional.

In addition to the mandatory requirements above, an EVSE or EVSDE may offer additional capabilities, such as power quality support or other demand response features, provided they do not conflict with the mandatory requirements.

*****

References

AGL (2021) AGL Electric Vehicle Orchestration Trial; Lesson Learnt Report 1, May 2021

ANSI/CTA-2045-B *Modular Communications Interface for Energy Management*, Consumer Technology Association, February 2021

DEIP (2021) Distributed Energy Integration Program - Electric Vehicles Grid Integration, Vehicle-Grid Integration Standards Taskforce – Key Findings, May 2021

Element Energy (2019) Electric Vehicle Charging Behaviour Study Final report for National Grid ESO 29th March 2019

EPRI (2012) Update: CEA Standard Modular Communication Interface for Residential Demand Response, Brian Seal, Technical Executive EPRI, 27 March 2012

EPRI (2017) Performance Test Results: CTA-2045 Electric Vehicle Supply Equipment Testing Conducted at the National Renewable Energy Laboratory, Technical Update, October 2017

EVC (2021) State of Electric Vehicles, Electric Vehicles Council, August 2021

GB/T 18487.1–2015. 2015 Electric vehicle conductive charging system–part 1: general requirements Standards Press of China

IEA (2021) Global EV Outlook 202: Accelerating ambitions despite the pandemic, International Energy Agency, 2021

IEC 61851-1 Edition 2 2017-02 Electric vehicle conductive charging system – Part 1: General requirements

IEC 62746-10-1:2018 Systems interface between customer energy management system and the power management system - Part 10-1: Open automated demand response (OpenADR)

IEEE 2030.5 Standard for Smart Energy Profile Application Protocol

ISO 15118-1:2019 Road vehicles — Vehicle to grid communication interface — Part 1: General information and use-case definition

Jemena (2021) Jemena Dynamic Electric Vehicle Charging Trial Project; Lessons Learnt Report #1, May 2021

NBER (2021) Low Energy: Estimating Electric Vehicle Electricity Use, National Bureau of Economic Research (USA) Working Paper 28541, February 2021

Neaimeh and Andersen (2020) Mind the gap – Open Communication Protocols for Vehicle Grid Integration, Myriam Neaimeh and Peter Bach Andersen, Energy Informatics, 2020 3:1

NREL (2017) *Performance Test Results: CTA-2045 Electric Vehicle Supply Equipment Testing Conducted at the National Renewable Energy Laboratory*, Technical Update, October 2017

OCPP 1.6 Open Charge Point Protocol 1.6 Ed 2:2017

OCPP 2.0.1 Open Charge Point Protocol 2.0.1:2020

Origin (2021) Origin EV Smart Charging Trial Interim Report, June 2021

REVS (2021) Interim Social Report from the Realising Electric Vehicle-to-grid Services (REVS) trial, May 2021

SEPA (2019) A Comprehensive Guide to Electric Vehicle Managed Charging, Smart Electric Power Alliance, May 2019

SEPA (2021) The State of Managed Charging in 2021, Smart Electric Power Alliance, November 2021

Skycentrics (2019) Open Standards: Why they matter and how to implement them (CTA-2045 & OADR), ACEEE Hot Water Forum March 12, 2019

University of Melbourne (2021) Electric Vehicle Uptake and Charging; A Consumer-Focused Review, 28 April 2021

Zhang, X et al (2021) Analysis and Testing of U.S.-China Key Technology for Charging Interoperability of Electric Vehicles, IOP Conf. Series: Earth and Environmental Science 701 (2021) 012073

ANNEX A. Detailed Evaluation of Standards

The following evaluations are based on our reading of the published standards, supported by internet research and discussions with experts, users and in some cases authors of the standards. As each standard uses different terminology, acronyms are spelled out when first introduced.

OCPP 1.6

Open Charge Point Protocol (OCPP) 1.6 2nd edition is a part of a suite of communication protocols, with certification requirements, published by the Open Charge Alliance (OCA).[25] OCPP development started in 2009 and it is now used in many countries. It is not recognised as a standard by official bodies. The suite consists of a technical specification, implementation guidelines and compliance requirements.

OCPP 1.6 is mainly used to communicate between a Charging Station, which consists of one or more EVSEs, and a Charging Point Management System (CPMS) but can be used for other applications. The protocol describes the message formats and rules that are required to exchange messages between an EVSE and CPMS where the underlying technologies are already provisioned. OCPP 1.6's standard data transfer can control loads and convey many measured values ("measurands") for both export and import. OCPP 1.6 offers vendor-specific data transfer (with a compatibility warning – this may be used to extend the standard control options).

In summary, OCPP1.6 comprises:

- 3 documents to the standard: general, json and SOAP
- 9 parts: including messages, firmware, and profiles
- 2 actors: charge point and central system
- Operations initiated by charge point or central system
- Fundamental DR capabilities that allow the RA to control the EVSE
- Main specification plus two "flavours" – SOAP and JSON
- 6 Profiles: a core of OCPP 1.5 features, firmware management, authorization, reservation, smart charging and remote trigger
- 3 charging profiles: ChargePointMaxProfile, TxDefaultProfile and TxProfile
- Transport mechanism: FTP, FTPS, HTTP and HTPPS
- Security levels: SS/TLS (HTTPS)
- Test tool (in development)
- Implementation certification.

The is no DR outcome confirmation process.

[25] https://www.openchargealliance.org

Maturity

There have been several OCPP versions leading to OCPP 1.6 and to OCPP 2.0.1 (which is covered in the next section). These are summarised in Table 11. The indications that OCA no longer maintains OCPP version 1.2 or 1.5 are:

- There is no Errata Management in the Technology Working Group
- OCA does not publish application notes or white papers for OCPP 1.2/1.5
- OCA does not organize OCPP 1.2/1.5 Interoperability Test events ("plugfests")
- OCA does not provide Conformance Testing Tools for OCPP 1.2/1.5
- There is no Certification Program for OCPP 1.2/1.5

Table 11 OCPP Suite of Protocols

Protocol	Date	Comment	Overview				
			Use cases	Mess-ages	data types	Config. keys	Test cases
OCPP 1.2	2010	No longer maintained					
OCPP 1.5	2012	No longer maintained SOAP still used		24x2	42	15	
OCPP 1.6	2015	Both SOAP & JSON	60	28x2	49	43	
OCPP 1.6 2nd Edition	2017	Current version					
OCPP 2.0	2018	No longer maintained JSON	116	65x2	129	85	260
OCPP 2.0.1	2020	Current; JSON only					

The documents related to OCPP1.6 are listed in Table 12. The technical specification must be used in conjunction with one of the transport protocols.

Table 12 Parts of OCPP 1.6

Document	Comment	Published
ocpp-1.6 edition 2.pdf	Technical specification	28/09/2017
ocpp-1.6-errata-sheet.pdf	Technical specification errata (V4.0)	23/09/2019
ocpp-j-1.6-specification.pdf	Transport Protocol: JSON implementation guide	08/01/2015
ocpp-j-1.6-errata-sheet.pdf	Transport Protocol: JSON implementation errata	04/12/2019
ocpp-s-1.6-specification.pdf	Transport Protocol SOAP implementation guide	28/09/2017
ocpp-s-1.6-errata-sheet.pdf	Transport Protocol SOAP implementation errata	04/12/2019

The two implementation variants (or "flavours") are:

- OCPP-J - JSON / websockets: where the message format is JSON. Communication takes place over a websocket connection. This technology starts with an HTTP connection that is "upgraded" to a websocket connection which is a bidirectional tunnel for communication that is typically between the CSMS and Charging Station. In this case the Charging Station initiates the connection which has several key advantages.
- OCPP-S - SOAP / XML: where the message format is XML. Communication using "SOAP calls", which are worldwide standardised HTTP request / responses either initiated by the CSMS (e.g. setting a Charging Profile) or

initiated by the Charging Station (e.g. an Authorization request when a user swipes an RFID card).

In OCPP 2.0.1 the SOAP variant was dropped, because it was infrequently used in practice due to the larger messages (XML is more bulky than JSON) and firewall issues (websockets vs. SOAP). In practice, most Charging Stations are OCPP-J as per the OCPP 1.6 2nd edition specification using Websocket connections.

Scope

OCPP 1.6 is mostly seen as an application protocol for communication between Charging Stations and a Charging Point Management System (CPMS – sometimes called Central Systems in the documents). The protocol provides formal descriptions of the digital message formats and rules for actions and responses from both sides. It does not define the communication technology and it will work on all TCP/IP based systems. OCPP provides all necessary functionality and its deployment does not depend on other application layer protocols.

OCPP 1.6 is a means to convey demand response requirements from a remote agent (RA) to an EVSE for actioning as a demand response (DR).

An OCPP 1.6 deployment can be fully tested and certified. It is important to appreciate that the test is of the communications system not the actual DR outcome. As there is no test for DR outcomes in OCPP, it would have to be added.

OCPP 1.6 is mostly deployed to control EVSE charging but it is capable of controlling any resources that are suitably enabled, including PC inverters. For EVSEs, a standard implementation of OCPP 1.6 only covers charging.

Current Usage

OCPP is used in over 20 countries, with most deployments in Europe. New charge points in the UK must meet the Electric Vehicle Home Charge Scheme's minimum technical requirements for data communication protocols which are "The charge point must be able to be accessed remotely, through a data communication protocol and communication technology, by utilising the Open Charge Point Protocol (OCPP) version 1.6 (or above), or equivalent."[26] OCPP is also well supported in the USA (SEPA 2021) and appears to be the global EVSE industry's communications protocol of choice.

Interfaces

OCPP 1.6 requires an underlying physical structure to support an internet connection which is not specified. An OCPP 1.6 implementation requires a HTTP interconnection between the EVSE and the RA that is supported by the underlying internet protocol layers. The JSON implementation uses the full-duplex websockets.

Other standards required/supported for end-to-end operation

The OCPP 1.6 suite is self-contained and does not require any other software to support it other than what is normal for a web based protocol. However, the use of Operational Instructions (IOs) expressed as a percentage of prior load will require additional capability or a sequence of operations (see below).

[26] https://www.gov.uk/government/publications/electric-vehicle-homecharge-scheme-minimum-technical-specification/electric-vehicle-homecharge-scheme-minimum-technical-specification

Proprietary/patent content

OCPP is an open standard but OCA charges fees for compliance certification which covers a conformance test and performance measurements.

Main functions, settings and capabilities

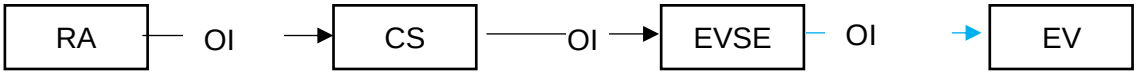
Operation Instructions for Demand Response can be communicated via OCPP as charging schedules and profiles defined by time, maximum power or maximum current). OCPP 1.6 profiles include smart charging. Smart charging in turn has three types of charging profiles as described in the following table. As illustrated in the example code below, TxProfile has the necessary functionality for communicating AS4755 defined load DRs.

Profile		use case	Useful for DR
TxDefaultProfile	Local Smart Charging	Charging Stations have charging limits controlled locally by a Local Controller, not the CSMS.	✓
TxProfile	Central Smart Charging	the CSMS has the ability to influence the charging power or current of a specific EV, the total allowed energy consumption on an entire Charging Station or a group of Charging Stations. May be used to override existing profiles	✓
ChargingStationMaxProfile	Internal Load Balancing	Internal load balancing within the ChargingStation, where the Charging Station controls current/power per EVSE.	✗

DRMs which limit charging power are expressed as a percentage reduction from the existing load (i.e. the “reference value”): limit to 0% (equivalent to DRM1 in AS 4755); limit to 50% (DRM2) and limit to 75% (DRM3).

OCPP allows only for charging limits to be expressed in Amperes or Watts, not percentages. The EVSE then communicates the Amp or Watt limit to the EV plugged in for charging. However there are several options for achieving the desired DRM, some based on the internal metering of the EVSE:

Option 1: RA does not read the meter and simply reduces the allowed load limit until the required demand reduction is detected by monitoring elsewhere in the system.



Option 2: Where the EVSE has the necessary software capability (indicated as C), it can monitor its meter and convert a DRM request to the required limit, referencing its dynamic charging state at the time.

Option 3: The Central System (CS) monitors the power of the EVSE (or group of EVSEs) and when RA requests, sends out operating envelope limited to the required percentage.

Option 4: Use power measured with CS based meter and convert the OI at the EVSE

Option 5: Use power measured with EVSE based meter and convert the OI at the CS

Note: the meter is read using functions such as MeterValues.req which contains the field definition of the MeterValues.req Protocol Data Unit (PDU) sent by the Charge Point to the Central System.

Capability to receive commands from a remote agent

The OCCP 1.6 protocol provides full capability to deliver load OI's from the RA to the EVSE, subject to the RA acting as (or establishing a business arrangement with) the Central System operator.

Entering responsive and non-responsive states

AS/NZS 4755 defines this state is a reversible condition of the electrical product in which it remains connected but does not respond to commands from the remote agent. The ability to make the electrical product responsive or non-responsive is intended to permit remote agents to enrol or suspend a customer from a demand response tariff or program without physically removing equipment.

In OCPP a charge point can enter an offline state in which it continues to operate on its own but does not respond to external commands. A charge point can also become unavailable where it does not allow charging. A central system can request that the charge point change its availability (SS5.2 ChangeAvailability.req).

It would be difficult for users to control responsiveness directly. They could disrupt the communications but this would not guarantee that the end device would cease executing its profile. The RA would need to over-write the profile so there is no DR and then refrain from issuing further commands.

Time delay/scheduling capability for start/end event

The charging profile allows for setting times for starting and ending events. Implementations are required to use ISO 8601 notation, fractions of seconds and time zone offsets. OCPP does not specify timing delay requirements for messages. Timing of messages is greatly influenced by the underlying network used. A GPRS network has different timing characteristics compared to a land-line. As OCPP does not require any specific type of network, but leaves this open for the Charging System operator (CSO) to select, OCPP cannot require timing constraints. A CSO can learn the latency of a given system by, for example, starting with a 30 second timeout on message requests, and tuning it for the network used.

Randomisation of start/end

Randomisation does not appear to be within the scope of OCPP. If response co-ordination and high ramping rates become a problem, a measure of diversity could be achieved through the code that converts OI power requirements to Amps or Watts

User over-ride provisions

There are no provisions for user over-ride of the EVSE in OCPP 1.6. The commencement and termination of charging by a user needs to be authorized by the charge point which in turn may get authorization from the central system so it is unlikely that a second RA could exercise control. If the entity stopping the transaction is different from the one that initialised the event then they will be asked for authorisation.

The user could however defeat or modify charging profiles in the following ways:

- To over-ride charging load reduction OIs (DRMs 1,2 and 3) the user would need to have an arrangement with the RA;
- To over-ride an OI for the EVSE to commence charging (DRM 4) users who have direct control of the EV (via a proprietary app, as for Tesla) could prevent charging even if the EV is connected and would otherwise charge.

Preservation/deletion of settings (privacy)

OCPP1.6 allows charging profiles and authorisation caches to be cleared. It needs to be confirmed if these are consistent with AS4577.2 requirements: that the manufacturer of the electrical product and the remote agent should follow the guidelines of ISO/IEC 27001 (IT and management Security Techniques) and ISO/IEC 27019 (energy processes) and national privacy principles. This question may extend to how the RA and CSO manage data, and how the EVSE would be set up to reflect those privacy objectives.

Command formats required/supported

This section focuses on the transmission of operational instructions for “Smart Charging” – that part of OCPP which enables loads to be controlled at specific times. OCPP1.6. It does not consider items such as the transport layer and heartbeats.

The charging power or current limits are determined by sending energy transfer limits at specific points in time to a Charging Station. Those limits are combined in a ChargingProfile which holds the ChargingSchedule that defines of charging power or current limits, start times and durations. There are three Smart charging profiles:

Profiles	Description
ChargePointMaxProfile	For load balancing
TxDefaultProfile	Sets policies such as don’t charge for a day
TxProfile	Overrules the default charging profile

Each charging profile has a number of attributes including transaction ID, the charging profiles, period of validity, and the charging schedule. The charging schedule is a list of charging periods, conveying duration, StartSchedule, ChargingRateUnits, ChargingSchedulePeriod and minimumCharging rate.

For demand response, the RA sends a SetChargingProfile command (SS5.16) via the CS. The contents of the charging profile would contain the required charge limit and the time of its implementation. The units (Watts or Amps) need to be selected via ChargingRateUnitType.

The following table (based on section 3.12.7 of the 2015-10-08 version of OCPP1.6) illustrates a JSON SetChargingProfile command for a charging schedule starting at midnight with 1kW limit, increasing to a 6kW limit at 8am and finally a 5kW limit at 8PM

ChargingProfile			
chargingProfileId	100		
stackLevel	0		
chargingProfilePurpose	TxProfile		
chargingProfileKind	Recurring		
recurrencyKind	Daily		
chargingSchedule	(List of 1 ChargingSchedule elements)		
	ChargingSchedule		
	duration	86400 (= 24 hours)	
	startSchedule	2013-01-01T00:00Z	
	chargingRateUnit	W	
	chargingSchedulePeriod	(List of 3 ChargingSchedulePeriod elements)	
		ChargingSchedulePeri	
		od	
		startPeriod	0 (=00:00)
		limit	1000
		numberPhases	1
		startPeriod	28800 (=08:00)
		limit	6000
		numberPhases	1
		startPeriod	72000 (=20:00)
		limit	5000
		numberPhases	1

Equivalence of Demand Response Modes

The standard (not vendor specific) data transfer methods has two paths to achieve DR outcomes from issued OIs: absolute (A or W limit) or relative (% reduction). Absolute outcomes are readily achievable because OCPP1.6 communicates limits in amperes or Watts. In this case the OI would be conveyed without knowledge of the existing load on the EVSE.

The charging profile table above indicates how this would be done using Watts. For example, to set the power to the values in the above table the code to be issued by the RA could be:

```
“csChargingProfiles”: {
     “chargingProfileId”: 100,
     “chargingProfileKind”: “Absolute”,
     “chargingProfilePurpose”: “TxProfile”,
     “chargingSchedule”: {
         “chargingRateUnit”: “W”,
         “chargingSchedulePeriod”: [
             {
                “limit”: 1000.0,
                “startPeriod”: 0
             },
             {
                “limit”: 6000.0,
                “startPeriod”: 6000
             },
             {
                “limit”: 5000.0,
                “startPeriod”: 7200
```

```
            },
            “duration”: 10000
            },          ],
      “stackLevel”: 0,
      “transactionId”: ZZ,
      “validFrom”: “start time”,
      “validTo”: “end time”
}
```

Note: Time is in seconds from midnight. 24hrs = 86,400 seconds.

Ways in which relative demand response outcomes could be achieved were described previously. The ability of OCPP 1.6 to simulate AS/NZS 4755 DRMS using standard messaging is summarised in the following table. OCPP does not support power quality support.

OI	DRM	OCPP 1.6 equivalent
0	Disconnect	×
1	No primary load	✓
2	Constrain load (50%)	✓
3	Constrain load (75%)	✓
4	Request load	✓only if EV connected and requests energy
5	No export to grid	×
6	Constrain export (50%)	×
7	Constrain load (75%)	×
8	Request export	×

Feedback pathways

This section refers to information feedback from the electrical product to the RA. A standard may specify that the EVSE may, or must be capable of establishing a feedback pathway to communicate information to the RA. It may also specify the categories of information to be communicated as given in the following table.

Categories of information to be communicated	**OCPP 1.6**
The present operating status of the EVSE, e.g. ‘Standby’ or ‘Charging’	✓ (Status)
If charging, the power level (instantaneous or over a recent period)	✓
DR events under way, recently executed or logged for future execution	✓
Power levels during DR events	✓
Whether user override has been activated	✓ (reason)

Indication of communication failure when the electrical product is no longer sending or receiving signals AS 4755.2 identifies communications pathway requirements and possible architectures that rely on TCP/IP, HTPP and cloud based solutions. OCPP 1.6 does enable such pathways. In a broader sense this may also refer to communications or information pathways in general.

Communications

The common deployment architecture indicates OpenADR being the main source of connection to the demand response provider but intermediary systems such as those operated by an aggregator can use other means to reach endpoints.

Information: The charge point opens a TCP connection to the central system. Over this, OCPP uses HTTP with websockets for bidirectional information exchange. This

requires messaging to include information about the nature of the request or response which is achieved through three call types: send a message, receive a message or error. A call is a wrapper of 4 elements: message Type ID, unique, action and payload. The payload is a response to the action and is the actual OCPP message.

Cyber-Security

AS4755.2 requires that the demand response system not exacerbate threats to the security and reliability of the electricity system. It covers the following areas under cyber-security.

AS4755.2 (Draft) Sections		Title	Comment	OCPP1.6 See Notes
General	4.1			
Device identification	4.2	Permanent embedded unique identifier (UID)		?
Access management for electrical products	4.3			
	4.3.1	Provisioning states	Update credentials, reset, delete data	✓
	4.3.2	Electrical product ready for provisioning	Before registration and after deregistration	✓
	4.3.3	Provisioning	Mutual authentication using credentials or encryption	✓
	4.3.4	Completion of provisioning	EP only act	✓
	4.3.5	Credentials	Transfer encryption keys, username and password	✓
	4.3.6	Role-based access control	As per table below in "Access control"	✓
	4.3.7	Secure boot	An encrypted secure boot process	✓
	4.3.8	Electrical product firmware maintenance	Capability to accept firmware updates.	✓
	4.3.9	Security event logging	Log of failed updates	✓
Field gateway device	4.4	Comms security	Transfer encryption keys, username and password	
Communications Security	4.5	Public-key infrastructure shall conform with IEC 62351-9.	Public-key infrastructure shall conform with IEC 62351-9.	?
Common information model (CIM)	4.6	Meet requirements of IEC 61968-9.	Meet requirements of IEC 61968-9.	?

Note 1: These requirements can apply to the OCPP1.6 implementation or the way that implementation is used. Often the answer depends on the implementation and does not indicate a limit in capability. The ✓ mark indicates that to some extent these requirements can be met by either component. The actor can make change but that does not mean that they are permitted to do so.? indicates that at the time of writing no clear answer was evident.

Note 2: Protection measures against cyber-attacks are not described in the technical specification but the JSON implementation (SS6.2.3) covers two security approaches:

- Network level encryption and authentication measures
- TLS encryption and charge point authentication.

OCPP1.6 JSON security provides:

- authentication of the Charge Point to the Central System (using HTTP Basic Authentication- CP username(ID) and password (20byte key stored on CP))
- encryption of the connection between Charge Point and Central System (Transport Layer Security (TLS))

- authentication of the Central System to the Charge Point (with a TLS certificate)

OCPP1.6 JSON security does not provide:

- A guarantee that the meter values are not tampered with between the meter and the Central System
- Authentication of the driver
- Protection against people physically tampering with a charge point.

Secure provisioning

AS4755.2 cyber-security requirement for secure provisioning which involves bringing the electrical product under the management of the RA for the purposes of demand response. The following capabilities shall be supported by the electrical product:

	AS4755.2 required Capabilities	**OCPP1.6**
(a)	EP shall be capable of having its credentials updated.	✓
(b)	EP shall have a factory reset capability located on or accessible from the EP.	
(c)	Factory reset shall delete all data except for data required to maintain the safety and system performance of the EP.	✓
NOTE	Any data from the EP that may identify the previous owner or user, location, log events or communication information should be purged	✓
	The EP shall not be able to prevent RA from revoking cryptographic keys used to maintain the trust relationship, and from deregistering the EP.	See Note

Note: Cryptographic keys should not be sent over the channel and it is preferable to install the authorization key on the charge point during manufacture or installation so the key is not sent over the channel it is meant to secure.

During provisioning, the EP or field gateway device and the RA shall be capable of mutual authentication, using the capabilities listed below.

	AS 47455.2 Mutual authentication capability	**OCPP1.6**
(a)	Credentials unique to each individual EP or field gateway device; NOTE The same credentials may not be issued or used among multiple EPs, even if they are of the same model.	✓
(b)	A one-time cryptographically secure pseudorandom number generator to generate the access token for that individual EP, to establish the trust with the RA; or	✓
(c)	provisioned relevant credentials for cryptographic message signing, EP authentication and secure connections.	
	The RA provisioning process shall update the RA registration details of the EP and/or field gateway device	✓

Access control

In addition to the cyber security areas mentioned above there are specific role based access requirements in AS4755.2. AS4755 defines and authorized person as a person, other than the user, who is authorized by the remote agent or the supplier of the electrical product to access, install or adjust parts or functions of the electrical product not accessible to the user. Access control has a number of requirements including those for role based access control.

AS4755.2 Section 4.3.6 Roles	**RA access Rights**		**EP communications manager access**		**Owner/user access**	
	AS4755.2	OCPP1.6	AS4755.2	OCPP1.6	AS4755.2	OCPP1.6
Reset demand response communication credentials	False	✓	True	✓	False	?
Modify/add users to demand response roles	False	✓	True	✓	False	?
Start-up/shut down operating system of EP or field gateway device	False	✓	False	✓	True	✓

Reboot EP or field gateway device	False	✓	True	✓	True	✓
Initiate or request a firmware upgrade for EP or field gateway device	False	✓	True		True	××
Factory reset of EP or field gateway device	False	✓	False	✓	True	×
Manage field gateway device	False	✓	True	✓	True	×
View system/event logs	True	✓	False	✓	True	×
View system statistics (e.g. capacity, performance)	True	✓	False	✓	True	✓

AS4755.2 requires that the electrical product shall maintain a log of the occurrence and time of, at the least, the following types of events, in a form that is accessible to an authorized person:

	Event	**OCPP1.6**
(a)	Failed validations of device updates and firmware.	✓
(b)	Initiated/failed firmware updates.	✓
(c)	Device power cycling, start-up and shutdown events.	✓
(d)	User-initiated resets.	✓

NOTE if optional feedback pathway is supported then the RA shall be able to access this log.

While the OCPP technical specification does not specify security provisions the JSON implementation does cover two security approaches as described below.

Firmware update provisions

AS4755 requirements for a firmware update are:

	AS4755.2. Section 4.3.8 Capability	**OCPP1.6**
(a)	Capable of being initiated by an authorized person (pushed), or by the EP itself via a periodical check of a software publication point (pulled).	✓
(b)	Cryptographically verifiable by the authorized person before it is release.	✓
(c)	Cryptographically verified by the EP or trusted field gateway device it is applied.	✓
(d)	Applied within the period specified by the authorized person (or immediately on receipt by the EP if no period is specified).	✓
(e)	Capable of confirming successful installation and operation (via either push or pull), once applied.	✓
(f)	Capable of being delivered remotely.	✓

OCCP1.6 allows for firmware and diagnostic transfers. When the Central System requests a Charge Point to download new firmware, the request includes the URL where the firmware can be downloaded. The URL also contains the protocol which must be used to download the firmware. The supported transfer protocols are controlled by the configuration key SupportedFileTransferProtocols. FTP, FTPS (recommended), HTTP, HTTPS (CSL). To ensure that the correct firmware is downloaded, it is recommended that the firmware is also digitally signed.

Registration (network)

There are two registration processes: network registration and registering a Charge Point.

In AS4755.2 the term registration is used in the context of a Registration Authority.

In OCPP1.6 registration refers to the Central System acceptance of the Charge Point. Network. Registration requirements are covered under Security and Provisioning. There are several steps in the network registration process and either the Charge point or the Central System can initiate a boot notification which initiates a registration

response. This contains the field definition of the BootNotification.req PDU sent by the Charge Point to the Central System. RegistrationStatu: This contains information about the Charge Point has been registered within the System Central. A value can be accepted or pending.

Communications security

AS4755.2 requires that communications shall be cryptographically protected. If public key infrastructure is utilized in the EP communication, it shall conform to the requirements of IEC 62351-9.

While there are no security provisions in the OCPP1.6 technical specification, both the SOAP and JSON transport protocols rely on network level security (encryption with SSL/TLS and client side certificates).

OCPPJ over WebSockets has the following security objectives:

- To create a secure cryptographic communication channel between the Central System and Charge Point.
- To provide mutual authentication (identify parties) between the Charge Point and the Central System.
- To provide a secure firmware update process by allowing the Charge Point to check the source and the integrity of firmware images, and by allowing non-repudiation of these images.
- To allow logging of security events to facilitate monitoring the security of the smart charging system.

The following table describes the authentication process:

Authentication	Authentication is the process of confirming an identity or attribute. When speaking about authentication one should distinguish between user authentication (e.g. sender/receiver) and message authentication.
Message authentication	Messages should be protected against unauthorized modifications. The message should always be sent together with an authentication tag providing its authenticity. Such an authentication tag can be the second output of an authenticated cipher such as AES-CCM or AES-GCM or a message authentication code.
Password authentication	The user proves his/her identity using a password or PIN.

Note: From OWASP - Transport Layer Protection Cheat Sheet. https://www.owasp.org/index.php/ Transport_Layer_Protection_Cheat_Sheet#Extended_Validation_Certificates"

Documentation, Certification and Testing

A complete certification system requires provisions for documenting and reporting compliance, provisions for testing compliance and the availability of testing and certification facilities (including physical or software “Testing Tools”).

All of these are available for OCPP 1.6 edition 2 (but not earlier versions of OCPP). Certification testing involves:

- Conformance tests to evaluate correct implementation: the product is tested against the appropriate OCPP Compliance Testing Tool (for OCPP 1.6. this was published in May 2015); and

- Measurement of the performance parameters stated by the vendor in a Protocol Implementation Conformance Statement (PICS).

There are three certification profiles: Full Certificate, Subset Certificate and Security Certificate. Charging Stations (EVSEs) can receive either a full certificate or a subset certificate. Testing Smart Charging capabilities, which provide the basis for demand response, is mandatory for a Full Certificate but optional for a Subset Certificate. Three laboratories currently undertake compliance testing: DNV-GL, KSGA and Dekra. Only two home EVSE brands have been certified: Alfen and EVBox.

Functionality	**Full Certificate OCPP 1.6 For Charging Station and CSMS**	**Subset Certificate OCPP 1.6 For Charging Station**
Core	Mandatory	Mandatory
Firmware Management	Mandatory	Optional
Smart Charging	**Mandatory**	**Optional**
Reservation	Mandatory	Optional
Local Authorisation List Management	Mandatory	Optional
Remote trigger	Mandatory	Optional

ESVE brands and & models claiming compliance

Of the 46 model variants listed in Table 13, 25 are claimed to support OCPP 1.6 (mainly 1.6J), 3 support ANSI/CTA-2045 and 5 support proprietary messaging protocols.

Table 13 Summary of EVSE Brands and Standards Compliance

	Number of models	OCPP 1.6 compliant	CTA2045 compliant	Other DR platforms
ABB	4	4		
Delta	6	6		
EO	2	0		Proprietary
EV-NRG	1	0		Proprietary
JetCharge	2	2		
Keba	3	2		
Ocular	4	2		
OpenEVSE	1	0		
QUBEV	1	0		
Schneider	6	2		
Siemens	4	1	3	
Tesla	4	2		
Wallbox	4	4		
WallPod	2	0		
Zappi	2	0		Proprietary
Total models	**46**	**25**	**3**	**5**

This does not mean that all models are able to action all OCPP DR messages. Analysis of the wiring diagrams and installer instructions from a number of EVSE installation manuals indicates that some can only be set to action one of DRMs 1,2 and 3, some can be set to action two and relatively few to action all three (See main text)

OCPP 2.0.1

Open Charge Point Protocol OCPP 2.0.1 edition is part of a suite of communication protocols, with certification requirements, published by the Open Charge Alliance (OCA). The parts of the suite are listed in Table 11. OCPP 2.0.1 supports control and measurement of both import and export energy flows. Like OCPP 1.6, OCPP 2.01 also allows customisation.

OCPP 2.0.1 describes information exchange between a Charging Station Management System (CSMS) and Charging Station (CS). Its main use is to enable the CSMS to manage and to authorize users of the CS. OCPP 2.0.1 uses a three tier physical model: CSMS, CS/EVSE and connectors. The two key parts of OCPP 2.0.1 are a data model and an information model. The device model specifies how CS describes itself to the CSMS. The information model describes the messaging and specification/schemas.

The information model is divided into functions one of which is Smartcharging which can be used for DR. Deployments need to be carefully considered so that inadvertent occurrences such as third party interactions do not impact the DR outcomes. OCPP 2.0.1 only describes a JSON implementation. It enables parties to extend existing commands with custom attributes or add new custom commands.

OCPP 2.0.1 is not backwardly compatible: an OCPP 2.0.1 compliant device cannot run OCPP 1.6 or even OCPP 2.0.27 It also relies on direct vehicle to grid communications (not required by OCPP 1.6) and has been designed to support the ISO 15118 standard for this purpose, with mapping of OCPP to ISO 15118 terminology. However, the standard's authors expect that the majority of EVs will continue to only support the control pilot signals specified in IEC61851.

It is also important to note that OCPP 2.0.1 does not appear to be complete, with scope left for some identified mechanisms to be evolved such as the Device Management Monitoring which replaces the MeterValueRequest. Security options available in this version include client side certificates.

In summary, OCPP 2.0.1 comprises:

- 4 documents: introduction, specification, json and schemas
- 4 main parts: Intro, architecture & topology, specification, J schemas and implementation. There are two additional parts in development: certification and test cases.
- 3 Actors: charging station management system (CSMS), charging station (CS)/EVSE and connector
- Resources for fundamental DR capabilities that allow the RA to control the EVSE
- 6 Profiles: core (all OCPP1.5 features), firmware management, authorization, reservation, smart charging and remote trigger
- 3 extensions to 1.6's Smart Charging

[27] "After the release of OCPP 2.0, issues were found that could not be fixed by issuing errata to the specification text only, as has been done with OCPP 1.6, but these required changes to the protocols machine-readable schema definition files *that cannot be backward compatible*."

- 4 Smart Charging profiles including TxProfile
- Support for ISO 15118
- Transport mechanism: FTP, FTPS, HTTP and HTPPS
- 3 Security Profiles: unsecured HTTP, TLS with Basis Authentication and TLS with client side certificates
- Test tool is in development.

There is no DR outcome certification process.

Maturity

OCPP 2.01.1 development started in 2020 and is not yet completed; there are indications in the document that a new edition is planned in the near future. The communication suite consists of four main parts, listed in the table below. The protocol describes the message formats and rules for exchanging messages between an EVSE and CSMS where the underlying technologies are already provisioned.

A testing tool being developed for OCPP 2.0.1 was being trialled in September 2021. When completed, it will be released and the certification for OCPP 2.0.1 will also be opened. The version will be OCPP 2.0.1 with the latest errata release might be in the September 2021 version or a later version. The most used document for information in this report is Part 2 the specification.

Scope

OCPP 2.01 is mostly intended as an application protocol for communication between the Charging Station Management System (CSMS) and Charging Stations (CS). This communication protocol provides formal descriptions of the digital message formats and rules for actions and responses from both sides. It is a prospective means of conveying demand response requirements from a remote agent (RA) to and EVSE. for actioning as a demand response (DR).

Part	Document	Description
0	OCPP-2.0.1_part0_introduction.pdf	Introduction – overview of suite
1	OCPP-2.0.1_part1_architecture_topology.pdf	Architecture & Topology
	OCPP-2.0_part1_errata.pdf	
2	pdfOCPP-2.0.1_part2_specification.pdf	**Specification:** Use Cases and Requirements, Messages, Data Types and Referenced Components and Variables
	OCPP-2.0.1_part2_appendices.	**Appendices:** Security Events, Standardized Units of Measure, Components and Variables
	OCPP-2.0_part2_errata.pdf	
3	OCPP-2.0.1_part3_JSON_schemas.zip	**Schemas**
4	OCPP-2.0.1_part4_ocpp-j-specification.pdf	Implementation Guide JSON
	OCPP-2.0_part4_errata.pdf	
	Changelog OCPP 2.0 - 2.0.1.pdf	changes between version 2.0 and 2.0.1 of OCPP
5	To be developed?	Certification Profiles
6	To be developed?	Test Cases

Main focus

While OCPP 2.0.1 is primarily intended for two way communication between a CSMS and a Charging Station, it is capable of controlling any resources that are suitably enabled. For example, the Device Model deals with products such as transformers or stand-alone battery packs.

Current Usage

Unlike OCPP 1.6, the use of OCPP 2.0.1 is currently very limited. There are no EVSE or EVSDE products in Australia that claim compliance with OCPP 2.0.1, and for the present is not possible to test or certify products as compliant.

Interfaces

Like OCPP 1.6, OCPP 2.0.1 requires an underlying physical structure to support an internet connection. An OCPP 2.0.1 implementation requires a HTTP interconnection between the EVSE and the RA that is supported by the underlying internet protocol layers. The JSON implementation uses websockets.The commencement and termination of charging by a user needs to be authorized by the charge point which in turn may get authorization from the central system so it is unlikely that a second RA could exercise control. If the entity stopping the transaction is different from the one that initialised the event then they will be asked for authorisation.

Other standards required/supported for end-to-end operation

The OCPP 2.0.1 suite is self-contained and does not require any other software to support it other than what is normal for a web based protocol. However, the use of Operational Instructions (IOs) expressed as a percentage of prior load will require additional capability or a sequence of operations (see below).

Proprietary/patent content

OCPP is an open standard but OCA charges fees for compliance certification.

Main functions, settings and capabilities

OCPP 2.0.1 is a protocol specification for a communications messaging system. The specification does not define the communication technology. Any technology will do, as long as it supports TCP/IP connectivity. The basic functionalities of OCPP 2.0.1.are summarised in the following table.

	Functional Blocks	
A.	Security	Including client side certificates
B.	Provisioning	
C.	Authorization	
D.	Local Authorization List Mgmt.	
E.	Transactions	Start/Stop & Metervalues
F.	Remote Control	Start/Stop/Unlock
G.	Availability	
H.	Reservation	
I.	Tariff and Cost	
J.	Metering	
K.	Smart Charging	
L.	Firmware Management	OTA Firmware updates
M.	ISO 15118 Certificate Mgmt	Communications from EVSE to EV
N.	Diagnostics	
O.	Display Message	

P.	Data Transfer	
	Charge Point configuration	
	Status Information	

Operation Instructions for Demand Response can be communicated via OCPP as charging schedules and profiles defined by time, maximum power or maximum current). There are four Smart Charging profiles, as described listed in the following table.

Purpose		use case	Useful for DR
ChargingStationMaxProfile	Internal Load Balancing	Internal load balancing within the ChargingStation, where the Charging Station controls current/power per EVSE.	×
TxProfile	Central Smart Charging	the CSMS has the ability to influence the charging power or current of a specific EV, the total allowed energy consumption on an entire Charging Station or a group of Charging Stations	✓✓
TxDefaultProfile	Local Smart Charging	Charging Stations have charging limits controlled locally by a Local Controller, not the CSMS.	✓
ChargingStationExternal Constraints	External Smart Charging Control Signals	Other actors participate such as DSO signals (e.g. via IEC61850-7-420], IEC60870-5-104], DNP3 or OpenADR [OPENADR]) or signals from a Building / Home Energy Management System.	Perhaps for connectivity with OpenADR

DRMs which limit charging power are expressed as a percentage reduction from the existing load (i.e. the “reference value”): limit to 0% (equivalent to DRM1 in AS 4755); limit to 50% (DRM2); and limit to 75% (DRM3).

As with other parts of OCPP, 2.0.1 allows only for charging limits to be expressed in Amperes or Watts, not percentages. The EVSE then communicates the Amp or Watt limit to the EV plugged in for charging. However there are several options for achieving the desired DRM, some based on the internal metering of the EVSE (see diagrams in previous section on OCPP 1.6).

Note: A Charging Station can return values of measurands such as the meter value it receives a TriggerMessageRequest with requestedMessage set to: MeterValues.

Capability to receive commands from a remote agent

The OCCP 2.0.1 protocol provides full capability to deliver load OI's from the RA to the EVSE, subject to the RA acting as (or establishing a business arrangement with) the Central System operator. A possible exception is DRM 0 (disconnect).

Entering responsive and non-responsive states

AS/NZS 4755 defines this state is a reversible condition of the electrical product in which it remains connected but does not respond to commands from the remote agent. The ability to make the electrical product responsive or non-responsive is intended to permit remote agents to enrol or suspend a customer from a demand response tariff or program without physically removing equipment.

In OCPP a charge point can enter an offline state in which it continues to operate on its own but it not respond to external commands. A charge point can also become unavailable where it does not allow charging. A central system can request that the

charge point change its availability (G03 ChangeAvailability.req). A charging station can request a transaction to stop by sending a RequestStopTransaction to the CSMS.

It would be difficult for users to control responsiveness directly. They could disrupt the communications but this would not guarantee that the end device would cease executing its profile. The RA would need to over-write the profile so there is no DR and then refrain from issuing further commands.

Time delay/scheduling capability for start/end event

The charging profile allows for setting times for starting and ending events.

OCPP does not specify timing delay requirements for messages. Timing of messages is greatly influenced by the underlying network used. A GPRS network has different timing characteristics compared to a land-line. As OCPP does not require any specific type of network, but leaves this open for the Charging System operator (CSO) to select, OCPP cannot require timing constrains. A CSO can learn the latency of a given system by, for example, starting with a 30 second timeout on message requests, and tuning it for the network used

Randomisation of start/end

Randomisation does not appear to be within the scope of OCPP. If response co-ordination and high ramping rates become a problem, a measure of diversity could be achieved through the code that converts OI power requirements to Amps or Watts

User over-ride provisions

There are no provisions for user over-ride of the EVSE in OCPP 2.0.1. The user could however defeat or modify charging profiles in the following ways:

- To over-ride charging load reduction OIs (DRMs 1,2 and 3) the user would need to have an arrangement with the RA;
- To over-ride an OI for the EVSE to commence charging (DRM 4) users who have direct control of the EV (via a proprietary app, as for Tesla) could prevent charging even if the EV is connected and would otherwise charge.

Preservation/deletion of settings (privacy)

Privacy extends to how the organisation manages data, as well as the device behaviour, which would be set up to reflect the privacy objectives. It needs to be confirmed if these are consistent with AS4577.2 requirements: that the manufacturer of the electrical product and the remote agent should follow the guidelines of ISO/IEC 27001 (IT and management Security Techniques) and ISO/IEC 27019 (energy processes) and national privacy principles.

Information is kept at several locations, e.g. the Charge Point retains a username and password that can be requested – both appear to be factory set. OCPP 2.0.1 has commands to clear the authorisation cache, the charging profile and customer information. Customer information is cleared using the CustomerInformationRequest with a clear flag set. The CSMS is able to send a message to the Charging Station to clear customer information which may be used for compliance with local privacy laws.

Command formats required/supported

This section focuses on the transmission of operational instructions for “Smart Charging” – that part of OCPP which enables loads to be controlled at specific times. It does not consider items such as the transport layer and heartbeats.

The charging power or current limits are determined by sending energy transfer limits at specific points in time to a Charging Station. Those limits are combined in a ChargingProfile which holds the ChargingSchedule that defines of charging power or current limits, start times and durations. There are four Smart charging profiles:

ProfileProfilePurpose	**Description**
ChargePointMaxProfile	For load balancing
TxDefaultProfile	Sets policies such as don’t charge for a day
TxProfile	Overrules the default charging profile
ChargingStationExternal Constraints	When an external system, not the CSMS, sets a charging limit or schedule, the Charging Station uses this purpose to report such a limit/schedule.

Each charging profile has a number of attributes including transaction ID, the charging profiles, period of validity, and the charging schedule. The charging schedule is a list of charging periods, conveying duration, StartSchedule, ChargingRateUnits, ChargingSchedulePeriod and minimumCharging rate.

For demand response, the RA sends a SetChargingProfile command via the CS. The contents of the charging profile would contain the required charge limit and the time of its implementation. The units (Watts or Amps) need to be selected via ChargingRateUnitType.

The charging schedules are structured in the same way as for OCPP 1.6 (JSON - see previous example of a SetChargingProfile command for a charging schedule starting at midnight with 1kW limit, increasing to a 6kW limit at 8am and a 5kW limit at 8PM).

Equivalence of Demand Response Modes

The standard (not vendor specific) data transfer methods has two paths available to achieve DR outcomes from issued OIs: absolute (A or W limit) or relative (% reduction). Absolute outcomes are readily achievable because OCPP 2.0.1 communicates limits in amperes or Watts. In this case the OI would be conveyed without knowledge of the existing load on the EVSE.

The charging profile table would be similar to that for OCPP 1.6 (see the previous section). The ability of OCPP 2.0.1 to simulate AS/NZS 4755 DRMS is summarised in the following table.

OI	DRM	OCPP 2.0.1 equivalent
0	Disconnect	×
1	No primary load	✓
2	Constrain load (50%)	✓
3	Constrain load (75%) and export reactive power	✓
4	Request load	✓only if EV connected and requests energy
5	No export to grid	✓
6	Constrain export (50%)	✓
7	Constrain load (75%) and consume reactive power	✓
8	Request export	✓

Feedback Pathways

This section refers to information feedback from the electrical product to the RA. A standard may specify that the EVSE may, or must be capable of establishing a feedback pathway to communicate information to the RA. It may also specify the categories of information to be communicated as given in the following table.

Categories of information to be communicated	OCPP 2.0.1
The present operating status of the EVSE, e.g. 'Standby' or 'Charging'	✓
If charging, the power level (instantaneous or over a recent period)	✓
DR events under way, recently executed or logged for future execution	✓
Power levels during DR events	✓
Whether user override has been activated	✓

AS 4755.2 identifies communications pathway requirements and possible architectures that rely on TCP/IP, HTPP and cloud based solutions. OCPP 2.0.1 does enable such pathways. In a broader sense this may also refer to communications or information pathways in general.

Communications: The common deployment architecture indicates OpenADR being the main source of connection to the demand response provider but intermediary systems such as those operated by an aggregator can use other means to reach endpoints.

Information: OCPP 2.0.1 provides for bi-directional information exchange. The charge point opens a TCP connection to the central system. Over this, OCPP uses HTTP with websockets for bidirectional information exchange. This requires messaging to include information about the nature of the request or response which is achieved through three call types: send a message, receive a message or error. A call is a wrapper of 4 elements: message Type ID, unique, action and payload. The payload is a response to the action and is the actual OCPP message.

Cyber-Security

AS4755.2 requires that the demand response system does not exacerbate threats to the security and reliability of the electricity system. AS4755.2 covers the following areas under cyber-security.

AS4755.2 (Draft) Sections		Title	Comment	OCPP2.0.1 See Notes
General	4.1			?
Device identification	4.2	Permanent embedded unique identifier (UID)		
Access management for electrical products	4.3			
	4.3.1	Provisioning states	Update credentials, reset, delete data	✓
	4.3.2	Electrical product ready for provisioning	Before registration and after deregistration	✓
	4.3.3	Provisioning	Mutual authentication using credentials or encryption	✓
	4.3.4	Completion of provisioning	EP only act	✓
	4.3.5	Credentials	Transfer encryption keys, username and password	✓
	4.3.6	Role-based access control	As per table below in "Access control"	✓
	4.3.7	Secure boot	An encrypted secure boot process	✓

	4.3.8	Electrical product firmware maintenance	Capability to accept firmware updates.	✓
	4.3.9	Security event logging	Log of failed updates	✓
Field gateway device	4.4	Comms security	Transfer encryption keys, username and password	✓
Communications Security	4.5	Public-key infrastructure shall conform with IEC 62351-9.	Public-key infrastructure shall conform with IEC 62351-9.	?
Common information model (CIM)	4.6	Meet requirements of IEC 61968-9.	Meet requirements of IEC 61968-9.	?

Note: These requirements can apply to the OCPP 2.0.1 implementations or the way that implementation is used. Often the answer depends on the implementation and does not indicate a limit in capability. The ✓ mark indicates that to some extent these requirements can be met by either component. The actor can make changes but that does not mean that they are permitted to do so.? indicates that at the time of writing no clear answer was evident.

The three levels of OCPP Security profiles for Charging Station and/or CSMS authentication and Communication Security are given in the following table.

Profile	**Charging Station Authentication**	**CSMS Authentication**	**Communication Security**
1. Unsecured Transport with Basic Authentication	HTTP Basic Authentication	-	-
2. TLS with Basic Authentication	HTTP Basic Authentication	TLS authentication using certificate	Transport Layer Security (TLS)
3. TLS with Client Side Certificates	TLS authentication using certificate	TLS authentication using certificate	Transport Layer Security (TLS)

The following improvements have been added to harden OCPP against cyber-attack. Security options are available in this version include client side certificates.

- Key management for Client-Side certificates: OCPP uses a number of public private key pairs for its security to manage the keys on the Charging Station, messages have been added to OCPP
- Secure firmware updates
- Security event log

Secure Provisioning

AS4755.2 cyber-security requirement for secure provisioning which involves bringing the electrical product under the management of the RA for the purposes of demand response. The following capabilities shall be supported by the electrical product:

	AS4755.2 required Capabilities	**OCPP2.0.1**
(a)	EP shall be capable of having its credentials updated.	✓
(b)	EP shall have a factory reset capability located on or accessible from the EP.	
(c)	Factory reset shall delete all data except for data required to maintain the safety and system performance of the EP.	✓
NOTE	Any data from the EP that may identify the previous owner or user, location, log events or communication information should be purged	✓
	The EP shall not be able to prevent RA from revoking cryptographic keys used to maintain the trust relationship, and from deregistering the EP.	See Note

Note: Cryptographic keys should not be sent over the channel and it is preferable to install the authorization key on the charge point during manufacture or installation so the key is not sent over the channel it is meant to secure.

During provisioning, the EP or field gateway device and the RA shall be capable of mutual authentication, using the capabilities listed below.

	AS 47455.2 Mutual authentication capability	OCPP2.0.1
(a)	Credentials unique to each individual EP or field gateway device; NOTE The same credentials may not be issued or used among multiple EPs, even if they are of the same model.	✓
(b)	A one-time cryptographically secure pseudorandom number generator to generate the access token for that individual EP, to establish the trust with the RA; or	✓
(c)	provisioned relevant credentials for cryptographic message signing, EP authentication and secure connections.	
	The RA provisioning process shall update the RA registration details of the EP and/or field gateway device	✓

AS4755 Access management for electrical products provisioning requirements are given in the next section.

The security of deployment of OCPP 2.0.1 depends on several factors including the way it is set up and additional matters such as the use of TSL.

OCPP 2.0.1 Terminology	Description	OCPP2.0.1
Authentication	Authentication is the process of confirming an identity or attribute. When speaking about authentication one should distinguish between user authentication (e.g. sender/receiver) and message authentication.	
Message authentication	Messages should be protected against unauthorized modifications. The message should always be sent together with an authentication tag providing its authenticity. Such an authentication tag can be the second output of an authenticated cipher such as AES-CCM or AES-GCM or a message authentication code.	
Password authentication	The user proves his/her identity using a password or PIN.	

Access Control

In addition to the cyber security areas mentioned above there are specific role based access requirements in AS4755.2. AS4755 defines and authorized person as a person, other than the user, who is authorized by the remote agent or the supplier of the electrical product to access, install or adjust parts or functions of the electrical product not accessible to the user. Access control has a number of requirements including those for role based access control.

OCPP 2.0.1 has many options to authorise changes to charging profiles. Authorization options include: EV Driver using RFIDTecharging. PIN-code, Contract Certificates, ISO 15118 External Identification Means (EIM), GroupId and Stop Transaction with a Master Pass. There is also Offline Authorization when the Id is unknown.

AS4755.2 Section 4.3.6 Roles	RA access Rights		EP communications manager access		Owner/user access	
	AS4755.2	OCPP2.0.1	AS4755.2	OCPP2.0.1	AS4755.2	OCPP2.0.1
Reset demand response communication credentials	False	✓	True	✓	False	?
Modify/add users to demand response roles	False	✓	True	✓	False	?
Start-up/shut down operating system of EP or field gateway device	False	✓	False	✓	True	✓
Reboot EP or field gateway device	False	✓	True	✓	True	✓
Initiate or request a firmware upgrade for EP or field gateway device	False	✓	True		True	××
Factory reset of EP or field gateway device	False	✓	False	✓	True	×
Manage field gateway device	False	✓	True	✓	True	×
View system/event logs	True	✓	False	✓	True	×

View system statistics (e.g. capacity, performance)	True	✓	False	✓	True	✓

Note. The ticks and crosses in the above table are indicative only – there is a fair degree of flexibility in what capabilities various actors are allowed. ? indicates that at the time of writing no clear answer was evident.

AS4755.2 requires that the electrical product maintain a log of the occurrence and time of, at the least, the following types of events, in a form that is accessible to an authorized person:

	Event	**OCPP2.0.1**
(a)	Failed validations of device updates and firmware.	✓
(b)	Initiated/failed firmware updates.	✓
(c)	Device power cycling, start-up and shutdown events.	✓
(d)	User-initiated resets.	✓

NOTE if optional feedback pathway is supported then the RA shall be able to access this log.

Firmware update provisions

AS4755 requirements for a firmware update are:

	AS4755.2. Section 4.3.8 Capability	**OCPP2.0.1**
(a)	Capable of being initiated by an authorized person (pushed), or by the EP itself via a periodical check of a software publication point (pulled).	✓
(b)	Cryptographically verifiable by the authorized person before it is release.	✓
(c)	Cryptographically verified by the EP or trusted field gateway device it is applied.	✓
(d)	Applied within the period specified by the authorized person (or immediately on receipt by the EP if no period is specified).	✓
(e)	Capable of confirming successful installation and operation (via either push or pull), once applied.	✓
(f)	Capable of being delivered remotely.	✓

OCPP 2.0.1 has sophisticated firmware update provisions including secure firmware update capabilities with defined deployment requirements. It also provides for non-secure firmware updates. It describes how to publish and unpublish a firmware file on a local controller.

Registration (network)

There are two registration processes: network registration and registering a Charge Point.

In AS4755.2 the term registration is used in the context of a Registration Authority. For example "Supplier provides certificates from Certificate and/or Registration authority responsible for issuing UIDs/certificates or “The RA provisioning process shall update the RA registration details of the EP and/or field gateway device or, as an example, owner/user may access the website of the EP communications manager to request registration."

The network link is established in the normal fashion including an initial exchange of HTTP requests and responses. Network registration requirements are covered under security and provisioning.

In OCPP 2.0.1 registration refers to the Central System acceptance of the Charge Point. There are several steps in the registration process and either the Charge point or the Central System can initiate a boot notification which initiates a registration response. There are a few nuances to registration including that a Charging Station

Operator may choose to configure a Charging Station to accept transactions before the Charging Station is accepted by a CSMS.

Communications security

AS4755.2 requires that communications shall be cryptographically protected. If public key infrastructure is utilized in the EP communication, it shall conform to the requirements of IEC 62351-9.

There are many security provisions in OCPP 2.0.1. General information is available in the specification and detailed information in ENISA (European Network and Information Security Agency) OCPP Security.

OCPPJ over WebSockets has the following security objectives:

- To create a secure cryptographic communication channel between the Central System and Charge Point.
- To provide mutual authentication (identify parties) between the Charge Point and the Central System.
- To provide a secure firmware update process by allowing the Charge Point to check the source and the integrity of firmware images, and by allowing non-repudiation of these images.
- To allow logging of security events to facilitate monitoring the security of the smart charging system.

The security of deployment of OCPP 2.0.1 depends on several factors including the way it is set up and additional matters such as the use of TSL. The following table describes the authentication process:

Authentication	Authentication is the process of confirming an identity or attribute. When speaking about authentication one should distinguish between user authentication (e.g. sender/receiver) and message authentication.
Message authentication	Messages should be protected against unauthorized modifications. The message should always be sent together with an authentication tag providing its authenticity. Such an authentication tag can be the second output of an authenticated cipher such as AES-CCM or AES-GCM or a message authentication code.
Password authentication	The user proves his/her identity using a password or PIN.

Note: From OWASP - Transport Layer Protection Cheat Sheet. https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Extended_Validation_Certificates"

Documentation, Certification and Testing

A complete certification system requires provisions for documenting and reporting compliance, provisions for testing compliance and the availability of testing and certification facilities (including physical or software “Testing Tools”).

A testing tool being for OCPP 2.0.1 was being trialled in September 2021. Like the OCPP 1.6 Compliance Testing Tool, it is intended to test systems implementing OCPP 2.0.1 for the conformance to the guidelines specified in the OCPP 2.0.1 specification. The tool can test the compliancy of both charge point and Central System. When a test for testing charge point is executed, the tool can be configured as Central System and vice versa.

Three laboratories currently undertake OCPP 1.6 compliance testing: DNV-GL, KSGA and Dekra can provide OCPP Device Under Test (DUT) certification. It is expected that the same laboratories will offer OCPP 2.0.1 certification when available.

The certification testing has two categories:

- Conformance tests: To evaluate correct implementations, the DUT is tested against the appropriate OCPP Compliance Testing Tool.
- Performance measurements: Laboratory performance parameters to be stated by the vendor in the Protocol Implementation Conformance Statement (PICS).

As with OCPP 1.6, there is no provision for testing the actual demand responses of the EVSE.

Current Usage

At present there are no EVSEs claiming compliance with OCPP 2.0.1.

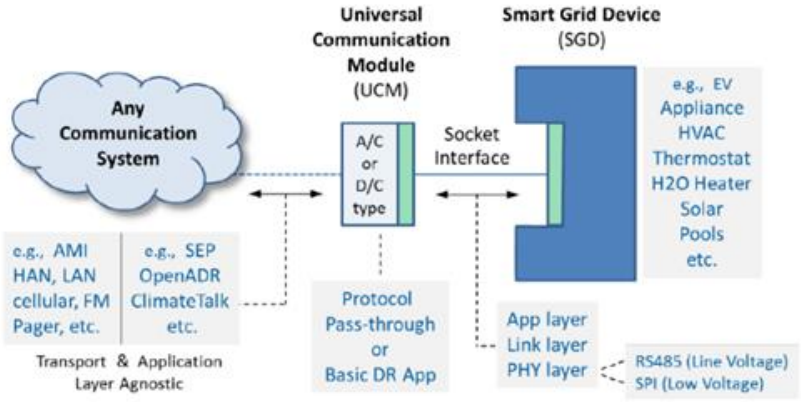
ANSI/CTA 2045-B

ANSI/CTA 2045-B describes a modular communication interface (MCI) for demand response communications. While it defines both hardware and software the technology and protocols of the communications system of which the UCM is part is out of scope. An MCI has two physical components: a removable Universal Communications Module (UCM) and a socket interface. They come in two physically different forms: low voltage DC with an SPI interface and AC with an RS-485 interface. The MCI application layer messaging system has two options: protocol pass-through or Basic/Intermediate DR. The scope of 2045-B is limited to the interface between the UCM and the smart grid device (SGD). The development of 2045 was supported by the US Electric Power Research Institute (EPRI) and a consortium of appliance manufacturers (USNAP).

Its architecture corresponds to AS/NZS 4755.1 in that the communications module, like the AS/NZS 4755 Demand Response Enabling Device (DRED) is physically separate from the electrical product, so the same product can be sold anywhere and retrofitted with a range of modules by the local utility or aggregator. In fact, EPRI acknowledges AS/NZS 4755 as one of the precedents for the standard (EPRI 2012).

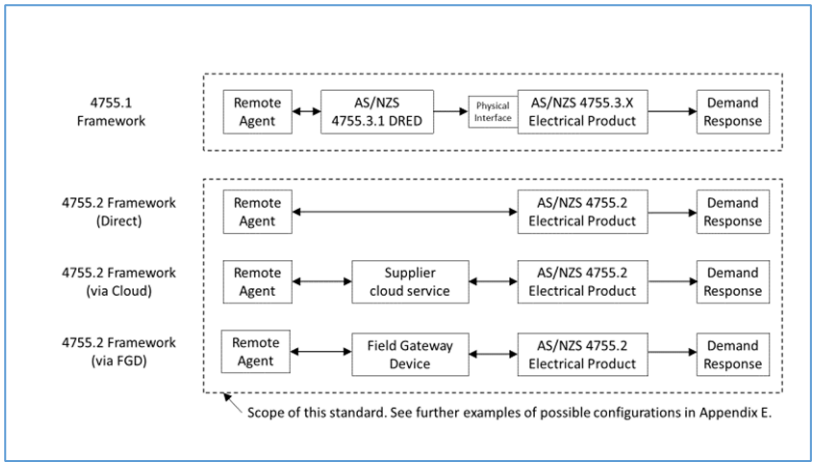
Figure 2 illustrates the general architecture of CTA-2045. It is virtually identical to the AS/NZS 4755.1 framework (Figure 3), and its scope is analogous to the combined scope of 4755.1 and 4755.3.X.

Figure 2 Scope of ANZI/CTA 2045



Source: CTA 2045

Figure 3 Scope of AS/NZS 4755



Source: Draft AS4755.2

In summary, the main features of the ANSI/CTA 2045-B suite are:

- 1 document
- 2 physical form factors (AC and DC)
- 2 serial communications protocols
- A simplified implementation process
- Basic and intermediate DR messaging
- 9 Pass through options (including SEP 1.0 and OpenADR)
- Security relies on applications that use it
- Does not encourage randomisation
- Several certification levels and requirements (SGD and UCM).

Maturity

The standard was originally published in 2013 as CEA 2045 Modular Communications Interface for Energy Management by the US Consumer Electronics Association (CEA). It was endorsed by the American National Standards Institute (ANSI) and when the CEA later changed its name to the Consumer Technology Association (CTA) later versions of the standard were badged ANSI/CTA 2045 (called CTA 2045 in short). An amended version, ANSI/CTA-2045-A, that clarified issues identified in the field, reorganized the data-link layer and added new features and functions was published in 2018. The latest version, ANSI/CTA-2045-B, was published in February 2021.

Year	Version	Name
2013	CEA 2045	Modular Communications Interface for Energy Management
2014	ANSI/CTA-2045.1 R-2020	*MCI for Firmware Transfer Message Set*, July 2014, www.cta.tech
2014	ANSI/CTA-2045.2	*MCI for Generic Display Message Set*, July 2014, www.cta.tech
2017	CEA 2045-2017 (ANSI)	Amendment - reorganized the data-link layer, and added new features and function
2018	ANSI/CTA-2045-A	Modular Communications Interface for Energy Management
2019	ANSI/CTA-2045.3 R-2019	*MCI for Thermostat Message Set*, August 2014, www.cta.tech
2021	ANSI/CTA-2045-B	Modular Communications Interface for Energy Management

Scope

The three parts of the ANSI/CTA-2045 modular interface (MCI) are: a physical interface, a communications protocol and an application layer messaging system. The MCI allows messages to pass across the interface to the end device. The methods that the SGD and the UCM undertake to "discover" each other's capabilities are described. The UCM and the system it participates govern the demand response.

Physical/Electrical interface: details the mechanical, electrical, and logical characteristics of a socket interface. As seen in Figure 3, this interface connects the Universal Communications Module (UCM) to the Smart Grid Device (SGD) in a standard way. Two physical form factors are presently defined for the module (Figure 4): one where the module draws AC (100-240V) power from the electrical product to

which it is attached, and the other DC, for use where the end device has no AC power source or when a smaller socket size is required. Electrical product device manufacturers may choose either, and communications module providers who wish to cover all products may offer two module versions.

Communications protocol: The serial communications across the UCM accommodates a variable payload and may act to simply pass-through information such as OpenADR commands.

Application layer: Allows basic and intermediate DR messages that are defined in CTA-2045-B to be actioned. This is "where the demand response commands live", for example “operate at reduced load for 4 hours”; “the grid price is high”; “consume more energy if possible.” However, the standard was designed to accommodate other standards such as OpenADR, SEP 2.0 (IEEE 2030.5), BACnet, etc. The standard anticipates the creation of new DR application languages. The data link layer of CTA-2045 allows the UCM to discover which of these languages the end device prefers, and then to use that language.

Figure 4 CTA-2045 AC and DC universal communications modules (UCM)

Source: Skycentrics

Adoption and Usage

The standard provides for the discovery of 47 identified product types, including:

- Electric Vehicle
- Electric Vehicle Supply Equipment – general (SAE J1772)
- Electric Vehicle Supply Equipment – Level 1 (SAE J1772)
- Electric Vehicle Supply Equipment – Level 2 (SAE J1772)
- Electric Vehicle Supply Equipment – Level 3 (SAE J1772)

The following products are available with CTA 2045 interfaces, and the compliance of production models supplied by manufacturers has been tested by EPRI (EPRI 2017):

- Electric Vehicle Supply Equipment (Siemens)
- Thermostat (Emerson)
- Solar Inverter (Fronious)
- Pool Pump (Pentair)
- Water Heaters (AO Smith)
- Battery Storage (PowerHub systems)

In 2019, Washington State in the US passed legislation requiring that “(1) An electric storage water heater, if manufactured on or after January 1, 2021, may not be installed, sold, or offered for sale, lease, or rent in the state unless it complies with the following design requirement:

(a) The product must have a modular demand response communications port compliant with: (i) The March 2018 version of the ANSI/CTA–2045-A communication interface standard, or equivalent and (ii) the March 2018 version of the ANSI/CTA-2045-A application layer requirements.
(b) The interface standard and application layer requirements required in this subsection are the versions established in March 2018, unless the department adopts by rule a later version."[28]

There are several models of compliant electric resistance and heat pump water heaters available in the USA, including from the largest US suppliers, A.O.Smith and Rheem. To date, the only EVSE manufacturer that makes CTA 2045-compliant models is Siemens (see below).

Interfaces

The form factors of permitted connectors are defined. The physical communications interface on the electrical product may be either an RS-485 based serial interface (for an AC module) or an SPI serial data interface (for a DC module). As the specified AC service voltage is 120/240V its operation at 230V for Australia would need to be verified. Modules must be capable of being inserted and or removed without switching off the electrical product ("hot-swappable").

Other standards required/supported for end-to-end operation

This specification stands alone and is not dependent on other specifications other than underlying comms protocols. Implementation of a DR solution when pass-through is used will require other software to deliver end to end DR solutions.

Proprietary/patent content

CTA 2045 itself is an open standard. It is possible that some of the "pass-through" protocols listed in Table 14 – including new ones that may be enabled under the "future assignment" categories – could involve proprietary material, licenses or royalties. The hardware may be protected by patents. CTA allows patented material and has processes to manage IP.[29]

The RA that selects and distributes the modules to be used by EPS under their control would have the option of using wholly open standard protocols or proprietary/patented protocols to access the module if they wish, but this would not affect the EP.

Capability to receive commands from a remote agent

A CTA 2045 compliant product can be designed to respond to either a basic set of DR applications, or to respond to the "pass-through" of a number of identified protocols (see Table 14). The "payload" portion of the message can transport a range of protocols, with the "Message Type" field indicating which protocol.

In its simplest mode of operation, the modular communications interface provides for physical layer diversity and allows application layer and network layer protocols used in the communications system to pass-through directly to the end device. In such a mode of operation, the UCM need not understand the content of the messages or parse them in any way, but the end device must be capable of accepting and understanding the protocol that is passed through..

[28] https://app.leg.wa.gov/rcw/default.aspx?cite=19.260.080
[29] https://standards.cta.tech/kwspub/rules/

Alternatively the UCM could be designed to respond to OpenADR or any other of the protocols in Table 14 (over a range of transport layers), undertake all processing of commands, start/stop times etc. and interact with the electrical device through a set of generic DR commands only (similar to the AS/NZS 4755.1 architecture). The main producer of modules advocates the OpenADR/generic DR command approach (Skycentrics 2019).

Table 14 CTA 2045 Message Type Field

Message Type	Message Type	Description
0x00 to 0x05	0x00 to 0xFF	Reserved for vendor proprietary use
0x06	0x00 to 0xFF	Reserved to avoid confusion with link layer ACK
0x07	0x00 to 0xFF	For Future Assignment
0x08	0x01	Basic DR Application (at least partially supported by all devices)
0x08	0x02	Intermediate DR Application
0x08	0x03	Data-Link Messages
0x08	0x04	Commissioning and Network Support Messages
0x08	0x05 to 0xFF	For Future Assignment
0x09	0x01	USNAP 1.0, Pass-Through
0x09	0x02	ClimateTalk, Pass-Through
0x09	0x03	Smart Energy Profile 1.0, Pass-Through
0x09	0x04	Smart Energy Profile 2.0 over IP, Pass-Through
0x09	0x05	OpenADR1.0 over IP, Pass-Through
0x09	0x06	OpenADR2.0 over IP, Pass-Through
0x09	0x07	Generic IP Pass-Through (IP packets self-identify version so both IPV4 and IPV6 are covered)
0x09	0x08	ECHONET Lite Pass-Through
0x09	0x09	KNX Pass-Through
0x09	0x0A	LonTalk Pass-Through
0x09	0x0B	SunSpec Modbus Pass-Through
0x09	0x0C	BACnet Pass-Through
0x09	0x0D to 0xFF	For Future Assignment
0x0A to 0x14	0x00 to 0xFF	For Future Assignment
0x15	0x00 to 0xFF	Reserved to avoid confusion with link layer NAK
0x16 to 0xEF	0x00 to 0xFF	For Future Assignment
0xF0 to 0xFF	0x00 to 0xFF	Reserved for vendor proprietary use

Main functions, settings and capabilities

2045-B allows pass-through and Basic DR (SS10.4). Basic DR events are:

- None, End Shed / Run Normal
- Shed
- Critical Peak Event
- Grid Emergency
- High Relative Price
- Low Relative Price
- Load Up
- Price Stream

The following table indicates event scheduling. Table 15 describes each event.

ITEM	Mandatory/Optional
Event ID	M
Start Time UTC seconds since 1/1/2000	M
Event Duration in minutes	M
Duty Cycle	M
Start Randomization in minutes	O
End Randomization in minutes	O
Criticality	O
Duty Cycle Period in minutes	O

Table 15 CTA 2045 Basic DR Application Command Set

Description	Opcode 2	Usage
Shed	Event duration	Sent from the UCM to the EP when a load shed event begins. If other load management commands are attempted but not accepted by the EP, then the UCM must fall back to this Opcode. Priority: High
End Shed/Run Normal	Not used	This command must be sent once from the UCM to the EP when a load shed or other curtailment event ends, regardless of whether the Event Duration is provided for informational purposes. Priority: High
Basic Application ACK	ACK'ed Opcode1	Acknowledge successful receipt and support of previous command. This message does not imply that the EP will alter its state according to the command sent by the UCM. The UCM should query the operational state to determine whether the command has taken effect.
Basic Application NAK	Reason	Reject previous command. Sent from either EP or UCM to the other when any of the following reasons occur. 0x00 = No reason given 0x01 = Opcode1 not supported; 0x02 = Opcode2 invalid; 0x03 = Busy; 0x04 = Length Invalid; 0x05 = Customer Override is in effect; 0x06 to 0xFF Reserved
Request for Power Level	Percent Setting	Sent from the UCM to the EP to request that its average Power Level (relative to the full rating of the device) be reduced to a level between 0 and 100% of full value on a 7 bit precision scale. Priority: High
Present Relative Price	Relative Price Indicator	Sent from the UCM to the EP when a change in relative price occurs to inform of the new relative price. Priority: Low
Next Period Relative Price	Relative Price Indicator	Sent from the UCM to the EP when a change in relative price occurs to inform of the relative price in the next future period. Priority: Low
Time Remaining in Present Price Period	Event Duration	Sent from the UCM to the EP when a change in price occurs to inform of the duration of the present price period. Priority: Low
Critical Peak Event	Event Duration	Critical Peak Event is in Effect (Critical Peak Events are intended to represent events that occur only a few times per year, on system peak days, for a maximum duration determined by the terms of the program) Sent once from the UCM to the EP when a critical peak price event goes into effect. If NAK'ed, send Opcode 0x01. Priority: High
Grid Emergency	Event Duration	A Grid Emergency is occurring. Sent once from the UCM to the EP when a grid emergency event goes into effect. If NAK'ed, send Opcode 0x01. Priority: High
Grid Guidance	Guidance Indicator	Sent from the UCM to the EP to provide an arbitrary indication of whether energy consumption is preferred or not. Guidance Indicator: 0x00 = Bad Time to Use Energy; 0x01 = Neutral; 0x02 = Good/Preferred Time to Use Energy; 0x03 to 0xFF = Reserved Priority: Low
Outside Comm Connection Status	Connect Status Code	Sent from the UCM to the EP when outside communication status is gained or lost. When in the "communicating" state, this command is resent every 1 to 5 minutes so that EPs may know that the UCM is still attached and working. Connect Status Code: 0x00 = No/Lost Connection; 0x01 = Found/Good Connection; 0x02 = Poor/Unreliable Connection; 0x03 to 0xFF = Reserved

Description	Opcode 2	Usage
Customer Override	0 = No Override, 1 = Override	Sent from either the EP or UCM anytime a customer chooses to change its override state. Also sent immediately after acknowledging receipt of any load reduction message if the customer's preference is set to override.
Query: What is your operational state?	0x00 (Not Used)	Sent from the UCM to the EP
State Query Response	Operating State Code	Sent from the EP to the UCM in response to an Opcode 0x12 query. In some cases, as determined by the EP, this message may be sent spontaneously not in response to Opcode 0x12. If EP sends this message, the UCM should respond with a Basic Application ACK.
Sleep	0x00	Sent from the EP to the UCM to inform it that the EP is idle, that information from the UCM is not needed, and that the UCM may shift into a low power state, if exists. This command assumes that the UCM will be provided with a "Wake" command before it will be expected to operate. Usage assumes the UCM can hear "Wake" messages while in "Sleep" mode.
Wake / Refresh Request	0x00	Sent from the EP to the UCM to end a "Sleep" period and to request that all messages related to currently valid connection status, price, time, and/or load curtailment be sent. UCMs that previously received a "Sleep" message shall provide up-to-date grid information within 10 seconds of receipt of a "Wake" signal. How UCMs function internally during Sleep periods in order to be able to support this capability is up to the UCM provider.
Simple Time Sync	Time value	When supported, this command is sent from the UCM to the EP on the hour. Time Value: Bits 7..5 = Weekday (0 = Sunday, 6 = Saturday) Bits 4..0 = Hour* of Day (0 to 23). *This is the local hour, including DST where applicable, for display on the EP clock as-is.
Load Up	Event Duration	This command is the opposite (complement) of the "Shed" command. It requests that the EP run now, and continue as possible. The assumption of this command is that energy is not wasted, but rather that things like thermal devices will cycle on and operate until the maximum stored energy state is reached. Sent from the UCM to EP at the beginning of the event. Priority: High
Pending Event Time	Time Until Event	Used to inform the EP (and possibly the user) that a DR event will occur in the near future.
Reboot	Type of reset	Request made by either UCM or EP for the other device to perform a reboot. Opcode 2 0x00 = Soft reboot; 0x01 = Reset to factory defaults (restore factory default configuration and then reboot); 0x02 to 0xFF Reserved After this command is acknowledged, both UCM and EP must return to startup conditions.

Randomisation of start/end

Randomisation of start and stop times by the electrical product is an optional capability, but the standard recommends that it be left to the communications system, or the UCM. The Format StartCycling() – Request has a Start Randomization in minutes and an End Randomization in minutes. The default is zero and the set values offset the start or end by a number of seconds randomly chosen between 0 and the Start or End value.

User over-ride provisions

The SGD is required to be capable of sending a Customer Override message to the UCM. The RA receives a Customer Override from either the SGD or UCM whenever a user chooses to change its override state. It is also sent immediately after acknowledging receipt of any load reduction message if the customer's preference is set to override. Figure 5 illustrates an EVSE with an override button on the consumer interface, allowing opt-out of control events that are in progress or that may occur in the next 12 hours.

Preservation/deletion of settings (privacy)

There appears to be no privacy setting requirements. This may be the role of the applications that sit on top of this platform.

Command formats required/supported

The standard defines a set of Basic DR application commands and explains how they are supported by the CTA-2045-B interface. Understanding the Basic DR commands is important, because even advanced communications modules and devices that may normally use more complex demand response protocols, are required to be able to fall back to a few required Basic DR messages in the event that the device to which they are connected is not capable of the same advanced functionality.

The Basic Demand response message payloads (defined in Table 15) cover:

- event duration less than 10min for spinning reserve
- shift for greater than 10min
- End Shed/
- Request for Power Level
- Customer Override
- Load Up
- Reboot

Feedback Pathways

If a feedback pathway is established via the UCM, the following information can be communicated to the RA.

Categories of information to be communicated	**CTA 2045**
The present operating status of the EVSE, e.g. 'Standby' or 'Charging'	✓ (Activation status)
If charging, the power level (instantaneous or over a recent period)	✓
DR events under way, recently executed or logged for future execution	✓
Power levels during DR events	✓
Whether user override has been activated	✓

Cyber-security

Network security is supported through the selected transport protocol, such as Wi-Fi, ZigBee, HomePlug, Z-Wave, LonWorks, etc., in addition to network or application layer security.

The standard requires that if present, security to be handled above the link layer (network, transport, application) and is outside the scope of the specification. The serial interface between a UCM and an SGD supports end-to-end security at the application layer and/or at the IP / network layer. It is not encrypted at the link layer. The Basic and Intermediate DR applications' messages identified in CTA-2045-B do not employ any security mechanisms.

AS4755.2 (Draft) Sections		**Title**	**Comment**	**CTA 2045**
General	4.1			
Device identification	4.2	Permanent embedded unique identifier (UID)		✖
Access management for electrical products	4.3			
	4.3.1	Provisioning states	Update credentials, reset, delete data	?
	4.3.2	Electrical product ready for provisioning	Before registration and after deregistration	?
	4.3.3	Provisioning	Mutual authentication using credentials or encryption	?
	4.3.4	Completion of provisioning	EP only act	?
	4.3.5	Credentials	Transfer encryption keys, username and password	?
	4.3.6	Role-based access control	As per table below in "Access control"	✓
	4.3.7	Secure boot	An encrypted secure boot process	?
	4.3.8	Electrical product firmware maintenance	Capability to accept firmware updates.	✓
	4.3.9	Security event logging	Log of failed updates	?
Field gateway device	4.4	Comms security		
Communications Security	4.5	Public-key infrastructure shall conform with IEC 62351-9.		?
Common information model (CIM)	4.6	Meet requirements of IEC 61968-9.		?

Access Control

An optional translation function is specified for connection to another communications medium is the connection to an energy management system access-network supplied by a service provider. This second medium is outside the scope of this standard. The specification does utilise the ability to Set User ID.

AS4755 defines and authorized person as a person, other than the user, who is authorized by the remote agent or the supplier of the electrical product to access, install or adjust parts or functions of the electrical product not accessible to the user Access control has a number of requirements including those for role based access control.

AS4755.2 Section 4.3.6 Roles	RA access Rights		EP communications manager access		Owner/user access	
	AS4755.2	CAT 2045	AS4755.2	CTA 2045	AS4755.2	CTA 2045
Reset demand response communication credentials	False	×	True	×	False	×
Modify/add users to demand response roles	False	✓	True	✓	False	✓
Start-up/shut down operating system of EP or field gateway device	False	✓	False	✓	True	✓
Reboot EP or field gateway device	False	✓	True	✓	True	✓
Initiate or request a firmware upgrade for EP or field gateway device	False	✓	True		True	✓
Factory reset of EP or field gateway device	False	✓	False	✓	True	✓
Manage field gateway device	False	✓	True	✓	True	✓
View system/event logs	True	✓	False	✓	True	✓
View system statistics (e.g. capacity, performance)	True	✓	False	✓	True	✓

AS4755.2 requires that the electrical product maintain a log of the occurrence and time of, at the least, the following types of events, in a form that is accessible to an authorized person:

	Event	CTA-2045
(a)	Failed validations of device updates and firmware.	×
(b)	Initiated/failed firmware updates.	×
(c)	Device power cycling, start-up and shutdown events.	✓
(d)	User-initiated resets.	✓

NOTE if optional feedback pathway is supported then the RA shall be able to access this log.

Firmware update provisions

CTA-2045-B does have firmware upgrade capability. Items related to firmware reporting are covered in the specification include year, month date, firmware minor or major. The specification refers to the external document ANSI / CTA-2045.1 for firmware commands.

Registration (network)

The use of full encapsulated pass-through mode and internet pass-through probably means that the network registration is taken care of by other actors, but there are commands to join and leave a network:

- Join Network: Sent to the UCM to instruct it to join the network for which it is configured
- Leave Network: Sent to the UCM to instruct it to leave the network.

Communications security

AS4755.2 requires that communications shall be cryptographically protected. If public key infrastructure is utilized in the EP communication, it shall conform with the requirements of IEC 62351-9. 2045 does not provide any security beyond that provided by application that uses this platform such as encryption within the IP packet embedded in the serial message. There are some noteworthy observations:

The serial interface between a UCM and an SGD supports end-to-end security at the application layer and/or at the IP / network layer. It is not encrypted at the link layer. For

certain application protocols, such as the Basic DR, it is not encrypted. In this case, the socket interface is treated as a protected local interface like any other wired connection between circuit boards inside a product.

If the communication on the communications network (PLC, wireless, etc.) is encrypted, as it may be in a secured Wi-Fi or ZigBee HAN for example, the decryption may occur in the communications module or be passed through to the SGD, if supported.

In the case of more advanced protocols, like internet pass-though, encryption may exist within the IP packet embedded in the serial message. For example, if the communications network is Wi-Fi, then a Wi-Fi communications module may receive an IP packet wirelessly, strip-off any 802.11 phy/mac part, insert the IP packet as the "Payload" in the message structure and send it on through to the electrical product. In this case, the communications module would be serving as a phy/mac translator and would know nothing of the packet's content, which may or may not be encrypted. The UCM would only know whether or not the electrical product is accepting or not acknowledging the messages.

Equivalence of Demand Response Modes

The "shed" and "critical peak" events can achieve equivalence to DRM2 to or DRM3, but do not correspond exactly. The response required by the EP to both "shed" and "critical peak" commands is a reduction in power level. Critical Peak events are distinguished from Shed Events only in that they are intended to be used only a few times a year (in association with Critical Peak DR programs) and therefore may result in a more aggressive response, if set by the EP manufacturer.

In the case of an EVSE that supports CTA 2045, the reference value from which power is to be reduced is the maximum power level set in the EVSE by the installer, based on their knowledge of the capacity of the site power supply. The curtailment relative to the reference value, on receipt of "shed" or "critical peak" may be pre-set in the module or sent as a "Request for Power Level" command. One EVSE interprets the "shed" command as limiting power to 50% of the reference value, and the "critical peak" as limiting to 25% (but with the proviso that curtailed power level must not fall below any safety parameters, such as the 6A charging level recommended in SA J1772 standard. For example, if the installed sets the reference maximum power at 22.5A, 25% of that value would be 5.625A. to keep to the minimum safe level, the EVSE would limit charging to 6A (EPRI 2017).

A "grid emergency" command is equivalent to DRM0. The EVSE opens the contactor, and no charging takes place for the duration of the event, and this cannot be over-ridden by the user (unlike "shed" and "critical peak" events). This is more severe than DRM1, but achieves a similar outcome.

DRM4 is a request for the EVSE to commence charging, if connected to an EV which has the capacity to take charge. This could be achieved by sending first a (low priority) "grid guidance" signal indicating that "this is Good/Preferred Time to Use Energy." If this does not get the desired response it could be followed up by a (high priority) "Load Up" command.

OI	DRM	CTA 2045 equivalent (for EVSEs)
0	Disconnect	✓ Grid Emergency event
1	No primary load	✓Grid Emergency event
2	Constrain load (50%)	✓ Critical Peak event or Request for Power level
3	Constrain load (75%) and export reactive power	✓Load Shed event or Request for Power level
4	Request load	✓Grid Guidance or Load Up event (only if EV connected and wants energy)
5	No export to grid	? (depends on EVSE design)
6	Constrain export (50%)	? (depends on EVSE design)
7	Constrain load (75%) and consume reactive power	? (depends on EVSE design)
8	Request export	? (depends on EVSE design)

Other inbuilt DR capabilities

CTA 2045 is a very flexible system. Additional capabilities include:

- Set temperature;
- Autonomous cycling;
- Monitoring EP operation and power levels
- Duration of events signalling, so EP can plan response (if it has logic).

The SGD manufacturer may offer an energy efficient mode of operation.

The pricing related commands in Table 15 can be used for curtailment or load shedding purposes or they may be used only for the purpose of display to the end user. The “Relative_Price_Indicator” may be simply used as an indication of how high or low the energy price for the period is relative to normal. As a simple ratio, it may be directly converted to percentages for customer presentation or preference settings.

The intent of the Opcode 0x07 is that it be sent from the UCM to the EP at the beginning of each new price period. It reflects the price that has just become effective. The intent of the Opcode 0x08 is to provide a forward-looking indication of the relative price in the next future period. If available and supported, UCMs provide EPs with both the present (0x07) and next (0x08) indicators. EPs may support neither, one, or both, at their discretion.

Signalling future events does not seem to be possible, but perhaps these can be stored in comms module and commands sent to EP when time to execute and terminate.

Documentation, Certification and Testing

The OpenADR alliance is planning to offer certification of products to CTA 2045. Complying products can be branded as “EcoPort compliant.”[30]

EPRI has tested the one EVSE model that claims CTA compliance, and has published a report demonstrating that it complies (EPRI 2017).

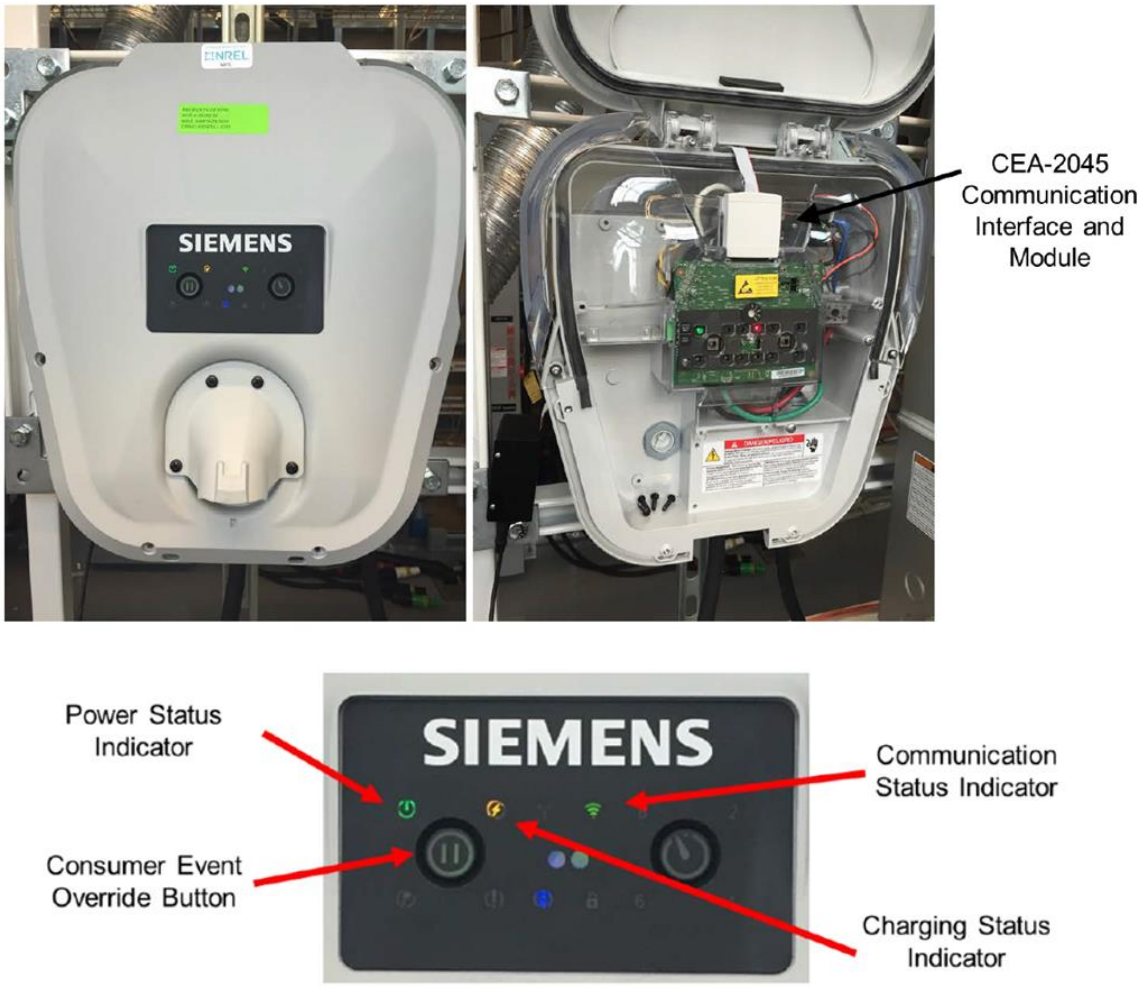
[30] EcoPort Certification & Branding (openadr.org)

ESVE brands and & models claiming compliance

There are only two EVSE models known to be compliant: the Siemens US2:VC30GRYHW, which is sold with an interface but without a module, and the US2:VCSG30GRYUW, which is supplied with a module that connects to Wifi. Figure 5 illustrates the latter, with the module fitted (shown right) and the consumer control panel (below). The three lights below the brand name are power status indicator, charging status indicator and communications status indicator. The button on the left is the Consumer Event Override, which allows consumers to opt-out of control events that may be in effect or may occur in the next 12 hours.

The Charging Status Indicator is illuminated when the EVSE is charging a vehicle and blinks when a control or event is in effect that alters the EVSE's normal mode of operation in any way.

Figure 5 EVSE with CTA 2045 module and consumer interface



Source: EPRI (2017)

IEEE 2030.5

The widely used standard IEEE 2030.5 connects servers with resources or clients. Function sets such as metering, pricing, distributed energy resources (DER) and demand response/load control (DRLC) describe device behaviour. EVSE is a defined device type and the standard enables DR communications between a remote agent and the EVSE.

The standard defines an application layer protocol with TCP/IP that provides functions including demand response and load control, pricing, energy usage information (e.g., meter data) and distributed energy resources, including V2G. Generally, lower layer protocols are not covered except where there is direct interaction with the application protocol. The standard covers messages, errors and security.

Resources and functions are organised according to three categories: Support, Common and Smart Energy. Smart Energy resource functions include DER (client devices for generation and storage and servers hosting DER programs) and DRLC (server devices for devices that support load control and servers exposing load control events). An event is an instance of a resource with defined duration to which users can opt-in or opt-out. Because multiple simultaneous events are allowed they have priority attributes.

All IEEE 2030.5 devices are required to maintain compliance to these documents:

- IEEE Std 2030.5
- IEEE 2030.5 XML Schema Definition (XSD) (sep.xsd in the supplemental material of IEEE Std 2030.5)
- IEEE 2030.5 WADL (sep_wadl.xml in the supplemental material of IEEE Std 2030.5).

Standards Australia is currently considering a proposal to adopt IEEE 2030.5 as an AS/NZS standard, and also to develop an Australian Common Smart Inverter Profile, possibly as a guide rather than as a full standard.

In summary, the features of IEEE 2030.5 are:

- 1 document standard
- 7 main parts:
    1. Application support: RESTful, HTTP 1.1, XML, HTTP over TLS
    2. Security: TLS 1.2, authentication and certificates
    3. Discovery: Service and resource discovery
    4. Support Resources: resources and function sets:
        - Operational information to end devices
        - Services for end devices to support operations
    5. Common Resources: non-domain specific resources (files etc)
    6. Smart Energy Resources: behaviours and function set definitions
    7. Manufacturer Specific Resources: rule and mechanisms for proprietary extensions

- Information model that is organised into function sets represented by sub-packages
- 23 packages including the DRLC package and the DER package (energy back to grid)
- DRLC has end device control for shifting, randomisation etc.
- Transport mechanism: HTTP 1.1
- Security TLS 1.2
- Test tool is indicated by Sunspec.

There is no DR outcome certification process.

Maturity of Standard Published or in development?

After many years of development this would be considered a relatively well-developed and stable standard. IEEE 2030.5-2013 evolved from SEP 2. In 2009, 2030.5 became the US National Institute of Standards and Technology (NIST) standard for home energy management devices and in 2015 it became the Californian Public Utilities Commission (CPUC) protocol of choice for DER communications. The key versions are listed in the following table.

Year	Version	Name
2008	SEP 2	ZigBee Smart Energy Profile 2 initiated in 2008
2013	IEEE 2030.5-2013	Standard completed and adopted as IEEE 2030.5 in 2013
2018	IEEE 2030.5 -2018	IEEE Standard for Smart Energy Profile Application Protocol

Scope

IEEE 2030.5 defines a TCP/IP based application layer protocol together with functions in the transport and Internet layers. Its purpose is to enable demand response (matching supply with demand), load control, time of day pricing and management of distributed generation, smart thermostats, meters, plug-in electric vehicles, smart inverters, and smart appliances. It provides capabilities for consumers to manage their energy.

Current Usage

IEEE 2030.5 is used for demand response of many appliances. Its predecessors, SEP1 and SEP2 are widely used. Its use for EVSE will be assisted by CA Rule 21. Some interpretations of this rule are that IEEE 2030.5 is mandatory but it is the default, and alternatives are also allowed.[31]

[31] The Californian Energy Commission (CEC) states: To ensure these utilities can communicate with all distributed energy resources, the Smart Inverter Working Group Phase 2 selected a default communications protocol, Institute of Electrical and Electronics Engineers (IEEE) 2030.5, that all installations must support although other communication protocols are permitted. California Rule 21 codified these communication requirements with distributed energy resources manufacturers given a short time to implement the IEEE 2030.5 communication protocol.
PG&E state: The default application-level protocol shall be IEEE 2030.5 (i.e., Smart Energy Profile 2.0 (SEP 2)) as defined in the California IEEE 2030.5 Implementation Guide, **but other application-level protocols may be used** by mutual agreement of the parties including IEEE 1815/DNP3 for SCADA real-time monitoring and control and IEC 61850.
SUNSPEC leaves the last part out and claims: California Rule 21 requires that Distributed Energy Resources in Investor Owned Utility regions must utilize the IEEE™ 2030.5-2018 networking standard in the manner described in the

Common Smart Inverter Profile – Australia (CSIPA) is intended to be the Australian Implementation Guide for IEEE 2030.5. It includes an "Annex C - DRED Communications" which maps the Operational Instructions in AS/NZS 4755 to IEEE 2030.5 DERControls. The document has no official status at present, but there is a proposal before Standards Australia to develop it into a Handbook (not a full standard), which could nevertheless be called up in regulations. [32] This standard is supported by NIST, EPRI and SAE

Interfaces (physical)

This application layer protocol uses TCP/IP to provide functions in the transport and Internet Layers. It does not require any other resources. Security attributes cover managing registration and access control but access to them and their ultimate functionality is left to the implementer.

Other standards required/supported for end-to-end operation

Three documents comprise the full definition of IEEE 2030.5 and all IEEE 2030.5 devices are required to maintain compliance to these documents:

- IEEE 2030.5
- IEEE 2030.5 XML Schema Definition
- IEEE 2030.5 WADL.

The standard calls up over 30 normative refences.

Proprietary/patent content

The core product does not appear to have patented content. However, manufacturers are allowed to make propriety extensions in accordance with stated rules. IEEE indicates that patent rights might exist and make no assurances about this.

Main functions, settings and capabilities

The 2030.5 specification describes an application that enables a RA to provide DR control over the EVSE. Functions are available for randomisation and an override function that can be enabled through a button available to users.

Two Smart Energy function sets DRLC and DER have features for controlling an EVSE. The Australian Common Smart Inverter Profile uses the DER feature set which supports two relevant control modes: Mode 2 = opModConnect (connect/disconnect—implies galvanic isolation) and Mode 7 = opModFixedW (charge/discharge setpoint). Together these two modes provide all required demand response modes.

Capability to receive commands from a remote agent

IEEE 2030.5 is platform for communicating instructions and information between actors including a RA and EVSE.

Entering responsive and non-responsive states

Probably due to its ZigBee legacy, there is an auto shut down mode (sleeping), for devices which spend most of their time off line and only connect if they need to.

Time delay/scheduling capability for start/end event

Common Smart Inverter Profile (CSIP). The test specification for this certification is the SunSpec Common Smart Inverter Profile Conformance Test Procedure.

[32] Comments to Standards Australia were due by 14 September 2021. The work would be undertaken by committee EL-062 *Smart Grids*. The Handbook would contain test procedures to verify performance.

The following commands enable event time control: Start Time, Duration, Specified End Time, Scheduled Period, Effective Start Time, Earliest Effective Start Time, Effective End Time, Effective Scheduled Period, Duration Randomization, Effective Duration, Overlapping Event, Start Randomization.

Randomisation of start/end

DRLC is one of two primary function sets to use randomisation. There are two randomisation commands.

- Start Randomization: The bound on the amount of time to be used when randomizing the commencement of an Event.
- Duration Randomization: The bound on the amount of time to be used when randomizing the completion of an Event.

User over-ride provisions

IEEE 2030.5 allows for override the end user (e.g., a button press).

- An EndDeviceControl is used to provide control parameters to a DRLC client. An EndDeviceControl can always be overridden by the user.
- If an Event is in progress and an override occurs, the client SHALL respond to the override without randomization.
- After the override Duration time of an EndDeviceControl has elapsed, the client device SHALL return to execution of the EndDeviceControl for the remaining Effective Scheduled Period.
- Client devices MAY allow users to override an EndDeviceControl for a longer duration than event overrideDuration, in which case they SHOULD provide a warning for non-compliance if the drProgramMandatory flag is set to true.
- When overriding an event, client devices SHOULD provide a duration for the override using the drOverrideDuration attribute found in the DrResponse object. This is useful for service providers and energy management systems (EMSs) in understanding for how long the client device will override the event and when it can expect the client device to return to shedding load.

Preservation/deletion of settings (privacy)

There are rules under the Manufacturing certificate lifecycle requirements for the management of certificates and how to retire those certificates and associated public keys. It needs to be confirmed if these are consistent with AS4755.2 requirements: that the manufacturer of the electrical product and the remote agent should follow the guidelines of ISO/IEC 27001 (IT and management Security Techniques) and ISO/IEC 27019 (energy processes) and national privacy principles.

Command formats required/supported

The IEEE 2030.5 model is organized into function sets, represented by sub-packages. However, all structures are defined inside a single namespace. There are data packages that can be from 8bit to 160bit long. There is a DRLC function set with capabilities with options for implementation such as a reduction in kW. The information model defines a range of instructions for load control such as:

- loadAdjustmentPercentageOffset attribute (PerCent) [0..1] where the value change requested for the load adjustment percentage. The value should be subtracted from the normal setting, or if loadShiftForward is true, then the value should be added to the normal setting.

- randomizeDuration attribute (OneHourRangeType) [0..1] Number of seconds boundary inside which a random value must be selected to be applied to the associated interval duration, to avoid sudden synchronized demand changes. If related to price level changes, sign may be ignored. Valid range is −3600 to 3600. If not specified, 0 is the default.

Equivalence of Demand Response Modes

The Australian Common Smart Inverter Profile provides mapping in section 5.2.4 DER Controls and DER Default Control Requirements provides information on the relevant DER controls.

Grid DER Support Functions	IEEE 2030.5 DERControls	IEEE 2030.5 DefaultDERControls
Ramp Rate Setting		setGradW
		setSoftGradW
Connect/Disconnect	opModEnergize	opModEnergize
Real Power Output Limit Control	opModMaxLimW	opModMaxLimW
Site Export Limit (in Watts)	opModExpLimW	opModExpLimW
Site Import Limit (in Watts)	opModImpLimW	opModImpLimW
Max generation limit	opModGenLimW	opModGenLimW
Max load limit	opModLoadLimW	opModLoadLimW

The document *Common Smart Inverter Profile – Australia V1.0, August 2021* (CSIPA) includes an optional Annex C DRED Communications. It treats the DRED (Demand Response Enabling Device) as a DER (Distributed Energy Resource) EndDevice and utilises the existing DERControl function set and maps AS/NZS 4755 DRM controls for appliance DRED to the DERControl properties used for BESS control.

The DRED EndDevice is treated as a load that can be reduced by applying a DRM control percentage (as listed in the table below. This is a subset of the OperationaModeStatus mapping in Table C2 of CSIPA, which also maps to combinations of AS/NZS 4755 DRMs, including those combinations which invoke power quality support).

AS4755 Operating Instruction	AS4755 DRM	Operational Mode Status	DERControl Property	DERControl Property Value	Lower Limit	Upper Limit
OI 0	DRM 0	100	opModConnect	False	-	-
OI 1	DRM 1	101	opModFixedW	0 %	-30.00	-0.01
OI 2	DRM 2	102	opModFixedW	-50 %	-60.00	-30.01
OI 3	DRM 3	103	opModFixedW	-75 %	-90.00	-60.01
OI 4	DRM 4	104	opModFixedW	-100 %	-100.00	-90.01
OI 5	DRM 5	105	opModFixedW	0 %	0.00	30.99
OI 6	DRM 6	106	opModFixedW	50 %	31.00	60.99
OI 7	DRM 7	107	opModFixedW	75 %	61.00	90.99
OI 8	DRM 8	108	opModFixedW	100 %	91.00	100.00

OI	DRM	IEEE 2030.5
0	Disconnect	✓
1	No primary load	✓
2	Constrain load (50%)	✓
3	Constrain load (75%)	✓
4	Request load	✓
5	No export to grid	✓
6	Constrain export (50%)	✓
7	Constrain load	✓
8	Request export	✓

Note: Some DRMs can only be actioned if an EV is connected and in is in a state of charge that permits charging or discharging.

Other inbuilt DR capabilities

IEEE 2030.5 is a flexible platform. The available commands to be communicated can be mixed and matched to provide different DR outcomes.

Feedback pathways

Bi directional information exchange is used.

Categories of information to be communicated	**2030.5**
The present operating status of the EVSE, e.g. 'Standby' or 'Charging'	✓ (connect status, inverter status)
If charging, the power level (instantaneous or over a recent period)	✓ (metering Log Events)
DR events under way, recently executed or logged for future execution	✓
Power levels during DR events	✓
Whether user override has been activated	✓ (DrResonse drOverrideDuration)

Cyber-Security

The IEEE 2030.5 communications protocol uses the internet protocol. Security covers the application and lower layers. TLS 1.2 is specified and this has known weaknesses with TLS 1.3 preferred. There is control on access to resources that is based on authentication levels and address information. The following table lists key security items that are covered by IEEE 2030.5.

IEEE 2030.5 IEC 61850 Requirement
Group Assignments
Group Management
Autonomous Controls
Cyber-Security
Registration
Enrolment
Device Discovery
DER Config Reporting
DER Information and Status
DER Performance
Capabilities Reporting

The default security policy involves authentication, certificates and registration. It is difficult to ascertain whether the AS4755.2 security requirements would be met.

Section		Title	Comment	2030.5
General	4.1			
Device identification	4.2	Permanent embedded unique identifier (UID)		✓
Access management for electrical products	4.3			
	4.3.1	Provisioning states	Update credentials, reset, delete data	✓
	4.3.2	Electrical product ready for provisioning	Before registration and after deregistration	?
	4.3.3	Provisioning	Mutual authentication using credentials or encryption	?
	4.3.4	Completion of provisioning	EP only act	?
	4.3.5	Credentials	Transfer encryption keys, username and password	?
	4.3.6	Role-based access control	As per table below in "Access control"	?
	4.3.7	Secure boot	An encrypted secure boot process	?
	4.3.8	Electrical product firmware maintenance	Capability to accept firmware updates.	?
	4.3.9	Security event logging	Log of failed updates	?
Field gateway device	4.4	Comms security		?
Communications Security	4.5	Public-key infrastructure shall conform with IEC 62351-9.		?
Common information model (CIM)	4.6	Meet requirements of IEC 61968-9.		?

Access control

AS4755 defines an authorized person as a person, other than the user, who is authorized by the remote agent or the supplier of the electrical product to access, install or adjust parts or functions of the electrical product not accessible to the user Access control has a number of requirements including those for role based access control.

From the perspective of a client or host (represented by an IP address) obtaining information from the server, IEEE 2030.5 has authorisation controls for resource access as part of security considerations with an access control list to authorise client access to resources and access privileges. IEEE 2030.5 standard makes a distinction between authentication and authorization Certificates provide a mechanism to authenticate an identity. Once authenticated (by proving possession of the associated private key, and by having the certificate chain to a known root of trust), that identity (or the service, person, or application associated with that identity) can be authorized to access resources, the ability to assume a role (e.g., system operator, general user), or perform various functions. The matrix for this is:

Authentication		Server		
		Native IEEE2030.5 application	Generic server	Self-signed
Client	Native IEEE 2030.5 application	IEEE 2030.5 Cert-Indef	Optional OCSP	Not allowed
	Generic client	Optional OCSP	Not specified here	Not specified here
	Self-signed	Signature validation	Not specified here	Not specified here

An authenticated certificate by itself does not generally grant authorization. Specific applications that accept the certificate MAY grant implicit authorization to access any resource under the purview of the application, but usually authorize access based on the identity represented by the certificate (e.g., an access control list entry). The following tables describe both the authentication and authorization uses of certificates described by this profile:

	Native IEEE2030.5 application	**Generic server**	**Self-signed**
Native IEEE 2030.5 application	ACL	ACL or public resources (server specific)	Not allowed
Generic client	ACL or public resources	Not specified here	Not specified here
Self-signed	ACL or public resources	Not specified here	Not specified here

Draft AS 4755.2 S4.3.6 Roles	**RA access Rights**		**EP communications manager access**		**Owner/user access**	
		2030.5		**2030.5**		**2030.5**
Reset demand response communication credentials	False	✓	True	Optional	False	×
Modify/add users to demand response roles	False	✓	True	?	False	?
Start-up/shut down operating system of EP or field gateway device	False	✓	False	?	True	Note 2
Reboot EP or field gateway device	False	?	True	?	True	?
Initiate or request a firmware upgrade for EP or field gateway device	False	✓	True	?	True	?
Factory reset of EP or field gateway device	False	Note 3	False	?	True	×
Manage field gateway device	False	✓	True	?	True	Note 2
View system/event logs	Note 4	✓	False	?	True	?
View system statistics (e.g. capacity, performance)	True	✓	False	?	True	?

Note 1: ? Not sure at time of writing
Note 2: Override: A local act by the end user (e.g., a button press).
Note 3: There is no explicit reference to this in the Standard.
Note 4; For logging security events

The electrical product shall maintain a log of the occurrence and time of, at the least, the following types of events, in a form that is accessible to an authorized person:

	Capability	**2030.5**
(a)	Failed validations of device updates and firmware.	×
(b)	Initiated/failed firmware updates.	×
(c)	Device power cycling, start-up and shutdown events.	✓
(d)	User-initiated resets.	✓

NOTE if optional feedback pathway is supported then the RA shall be able to access this log.

Firmware update provisions

There are methods for monitoring files associated with updating firmware and to determine if any firmware files need to be updated. There is also a non-mandatory request for vendors to provide a trust store for firmware updates.

Registration (network)

Section 6.9 Registration describes an out-of-band procedure to convey client registration information a priori to the server that houses a resource that will subsequently be accessed by the client. The registration information is the client's SFDI and optionally, PIN, which uniquely identifies the client in the given context. Authentication and registration involve HTPP(s) requests and subsequent responses.

Communications security

AS4755.2 requires that communications shall be cryptographically protected. The SFDI and LFDI are derived from public information (i.e., a Certificate), therefore can potentially be recreated by an eavesdropper.

In IEEE 2030.5, depending on the underlying physical network, messages may be encrypted at lower layers, in addition to the security features provided specifically for the application layer, which are required for use over all networks. Securing transactions between clients and servers is based on HTTP over TLS version 1.2 The TLS records are then transported using TCP. The TLS handshake mechanism provides mutual authentication based on device certificates or self-signed certificates. TLS records provide encryption and message authentication using the AESCCM mode of operation. Access control lists allow or deny use of resources based on authentication level and address information. A registration list is used for authorizing clients.

Documentation, Certification and Testing

The Consortium for SEP2 Interoperability (CSEP) has developed test and certification programs. Interoperability test occur monthly over the internet. Independently, Sunspec provides certification packages for use by test labs. This is for IEEE 2030.5 clients, gateways, aggregators and servers. Certification is applicable to software running on embedded devices and cloud services alike.

Provisions for documenting/reporting compliance

There do not appear to be any documentation or reporting requirements for the delivery of instructions or DR outcomes. There are compliance requirements for the use of certificates and RFC 5280 and IEEE 802.1

Availability of testing and certification facilities

Sunspec does indicate that there are testing facilities available but again these are likely to be for the software not the DR outcomes.

ESVE brands and & models claiming compliance

The only model of EVSE known to be certified to IEEE 2030.5 is the AeroEnvironment EVSE-RS 1.0, which was certified in 2016.[33] This is not available in Australia.

[33] . https://www.qualitylogic.com/wp-content/uploads/2017/01/IEEE2030-5-Conformance-Report-AeroVironment-EVSE-RS-1.pdf.

ISO 15118

ISO 15118 *Road Vehicles – Vehicle to Grid Communications Interface* covers all OSI (Open Systems Interconnection) elements between the controllers of an EVSE and the EV. ISO 15118 was initially designed to complement IEC 61851-1 with IP based bi-directional communications. (The High Level Communications option required compliance with IEC 61851-1).

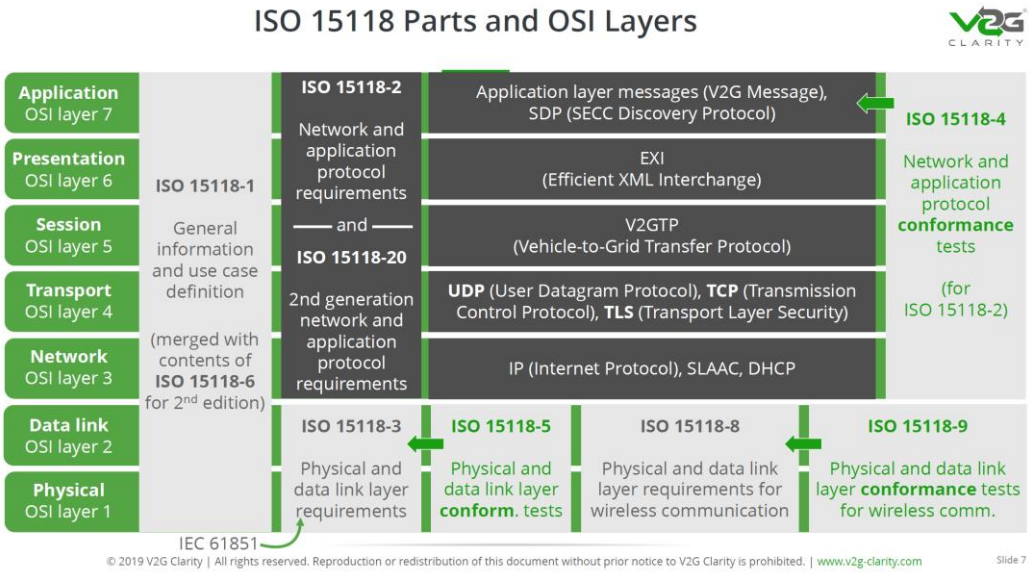
- In summary, the features of ISO 15118 are:
- 6 main parts/standards covering: physical, data link and compliance
- Covers plug and play communications between EVSE and EV
- Covers all parts of OSI model
- Issues identified with governance, technology and operations
- Test protocols

There is no DR outcome certification process.

Status and Maturity

ISO and IEC began working together on the standard in 2010, and a Plug & Charge section was released in 2014. By 2018, no automakers had a functional implementation of the standard. As of 2019 and 2020, several Public Key Infrastructure issues remained unsolved for application the standard as intended.

The following diagram describes the evolutionary paths.



- ISO 15118 Part 1 covers all layers.
- ISO 15118 Part 2 covers the processes involved at layers 1 and 2, but not a description of the physical connection.
- ISO 15118 Part 3 covers the physical and data link
- ISO 15118 Part 4 covers compliance

- ISO 15118 Part 8 covers the physical and data for wireless
- ISO 15118 Part 20, yet to be published, may be more able to answer the type of questions that we might ask of an operational standard.

ISO 15118-20 is currently being developed by ISO/TC 22/SC 31 Data communication which started work in 2014. This standard will define the latest requirements for:

- Test protocols
- Interfaces and gateways (including those for nomadic devices)
- Data formats
- Standardized data content

ISO 15118-20 will cover three type of charging services: alternating current (AC), direct current (DC), wireless power transfer (WPT).

- Check for available charging services - ServiceDiscovery
- Mutually exchange charging limits - ChargeParameterDiscovery request .The structure of this data is similar to the charging and discharging schedule, which the charging station can propose to the EV
- Calculate and send a power profile to the charging station- ChargeParameterDiscovery
- Control the charging process in the charging loop - AC_BidirectionalControl

Scope of Standard

Described as a “plug & charge” standard, ISO 15118 suite specifies communication between an EV and the EVSE. It identifies the entities responsible for the communications as the Electric Vehicle Communications Controller (EVCC) and the Supply Equipment Communications Controller (SECC). The suite describes a communications system that may be used to convey information, including charging control and schedules, between the EVCC and SECC. It describes everything from the physical interface to the information model.

Standard	Name	Description
ISO 15118-1	General information and use-case definition	Published in April 2013 (Worth noting: publication of ISO 15118-1 Ed. 2 is planned for Q4/2019)
ISO 15118-2	Network and application protocol requirements – core of standard	Status: Published in April 2014
ISO 15118-3	Physical and data link layer requirements	Status: Published in May 2015
ISO 15118-4	Network and application protocol conformance test	Status: Both published in February 2018
ISO 15118-5	Physical and data link layer conformance test	
ISO 15118-6	General information and use-case definition for wireless communication (out of commission, merged with 2nd edition of ISO 15118-1)	OUT OF COMMISSION Moved to part 1 This means ISO/DIS 15118-6 can be ignored. Status: To be published as part of ISO 15118-1 Edition 2 by end of 2019

ISO 15118-7	Network and application protocol requirements for wireless communication (out of commission, moved to ISO/DIS 15118-20)[11]	Moved to part 20 The anticipated publication date for ISO 15118-20 is the end of 2019 or the beginning of 2020. Status: There is no document behind ISO 15118-7 (although the title remains out of commission)
ISO 15118-8	Physical layer and data link layer requirements for wireless communication	Status: Published in March 2018
ISO 15118-9	is called “Physical and data link layer conformance test for wireless communication”.	Status: No publication date available yet
ISO 15118-20	2nd generation network and application protocol requirements	Status: at November 2021 it was at Approval stage. Publication is the next stage

Current Usage

It has been reported that Opel Ampera-e, Porsche Taycan, Lucid Air, Ford Mustang Mach-E, Volkswagen ID.4 and the Rivian R1T EVs use “plug & charge”. Coritech, a charging station manufacturer, includes ISO 15118 in its approved standards list.

There are close ties between OCPP, ISO 15118 and IEC 61851. OCPP 2.0 Part 2 – Specification: April 2018 states "In order to control the amount of power that an EV may draw from a Charging Station, some form of vehicle to grid communication is necessary. OCPP has been designed to support the ISO 15118 standard for communication between the EV and Charging Station (EVSE). However, it is anticipated that for the coming years, the majority of EVs will only support the control pilot PWM signal IEC61851, so care has been taken to support smart charging with this as well." (p252/400)

Interfaces (physical)

Part 3 of the standard describes the physical connection between the EVCC and the SECC including circuit examples for PLC injection. 15118 allows multiple actors to exercise control over charging but charging is via a contract between the SECC and the user or vehicle that involves a contract ID so this probably limits assess to the charging control.

Signal coupling

The signal coupling interface technical requirements are described in detail. There are two levels of communication

- Basic signalling: vehicle stats, control pilot handling for safety and initialization of the charging process
- High-level Communication for identification, payment, load levelling and value-added services (compliant with IEC 61851-1).

Other standards required/supported for end-to-end operation

This standard refers to other standards to communicate instructions and information to the RA. The High Level Communications option requires compliance with IEC 61851-1. Part 3 lists other standards which it states are indispensable for the application of this document. They are:

IEC 61851-1 2010	*Electric vehicles conductive charging system*	*Part 1 General requirements*
IEC 61851-21 2001	*Electric vehicles conductive charging system*	*Part 21 Electric vehicle requirements for conductive connection to an a.c./d.c. supply*
IEC 62196-2 2011	*Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles*	*Part 2 Dimensional compatibility and interchangeability requirements for a.c. pin and contact-tube accessories*
DTR TC69-221	*System using a PWM function*	
ISO/IEC 15118-1	*Road vehicles – Vehicle to grid communication interface*	*Part 1 General information and use-case definition*
ISO/IEC 15118-2	*Road vehicles – Vehicle to grid communication interface*	*Part 2 Network and application protocol requirements*

Proprietary/patent content

The standard states that patent rights are identified in the introduction or on-line and www.iso.org/patents. The introduction makes no comment. The following routine caution is provided: “Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.”

Ability to receive commands from a remote agent

A minimum capability in AS 4755 is the ability to action commands from a single remote agent at a time. Other DR standards may specify the ability of the EVSE to receive and respond to commands, but do not distinguish the origin, and so are not able to give priority to a single RA over a user, or indeed other RAs.

The role of ISO 15118 is to pass information from the SECC and not the RA directly.

Entering responsive and non-responsive states

There do not appear to be commands to enter responsive or non-responsive modes. For mode 3 charging there is a period of initialisation when the cable is plugged preceding charging events – this implied that there are non-responsive modes during these periods.

Time delay/scheduling capability for start/end event

Time delays and power levels are handled with a loop. The protocol defines a departure time which indicates when the user intends to unplug the car.

Randomisation of start/end

This capability does not appear to be covered in Parts 1, 2 and 3.

User over-ride provisions

The charging loop may be disrupted (with interrupts) by an EVCC or user. For example, the standard indicates that the when a user returns to their car they have the capability to initiate an end to charging.

Preservation/deletion of settings (privacy)

The protection of privacy requires that data shall only be readable by the intended addressee and private information only transferred when necessary. Retained device information would be reset when profiles are updated.

Command formats required/supported

The commands available support reading the power used and setting the maximum power. Power can be controlled with Pmax values within a range of 0 to 200kW.

Equivalence of Demand Response Modes

The equivalence to AS4755 DR modes is indicated in the following table. These would be achieved by setting the limit in accordance with the required DR.

OI	DRM	ISO 15118
0	Disconnect	× the contactor is not for power
1	No primary load	✓
2	Constrain load (50%)	✓
3	Constrain load (75%) and export reactive power	✓ can reduce reactive power
4	Request load	✓
5	No export to grid	✓
6	Constrain export (50%)	✓
7	Constrain load (75%) and consume reactive power	✓can reduce reactive power
8	Request export	✓

Note: The reactive power capability works firstly by the EVCC indicating to the SECC that reactive power compensation is possible and then the SECC can request it with a reactive power compensation value.

Feedback pathways

ISO 15118 provides for feedback of the following categories of information. It also anticipates a situation where a user returns to an EV that is in a charging session and wants to drive away before the session has ended.

Categories of information to be communicated	15118.2
The present operating status of the EVSE, e.g. 'Standby' or 'Charging'	✓ (charger status code)
If charging, the power level (instantaneous or over a recent period)	✓
DR events under way, recently executed or logged for future execution	✓
Power levels during DR events	✓
Whether user override has been activated	✓ (see note)

Cyber-Security

ISO 15118 has many security considerations covering:

- Confidentiality – Authorisation and encryption
- Data integrity – processes against data manipulation (modification and hacking)
- Authentication – entity authentication and data origin authentication
- Non-repudiation - accountability with third party
- Reliability – service availability and working correctly

The rules for certificates require that wall boxes (EVSEs) come with manufacturer-installed certificates and that Private Operator Root Certificates are installed in all vehicles. Certificates are checked when TLS communications commence. These rules require OCPP connection certificate-based authentication and authorization takes place at the Charging Station.

The standard also covers "man-in-the-middle theft" where certificates are compromised, and indicates that new certificates can be deployed using the automatic OEM Provisioning Certificate.

Draft AS 4755.2 Section	Title	Comment	ISO 15118

General	4.1			
Device identification	4.2	Permanent embedded unique identifier (UID)	They refer to EVSEID but it may be changeable	?
Access management for electrical products	4.3			
	4.3.1	Provisioning states	Update credentials, reset, delete data	✓
	4.3.2	Electrical product ready for provisioning	Before registration and after deregistration	✓
	4.3.3	Provisioning	Mutual authentication using credentials or encryption	✓
	4.3.4	Completion of provisioning	EP only act	?
	4.3.5	Credentials	Transfer encryption keys, username and password	✓
	4.3.6	Role-based access control	As per table below	✓
	4.3.7	Secure boot	An encrypted secure boot process	✓
	4.3.8	Electrical product firmware maintenance	Capability to accept firmware updates.	✓
	4.3.9	Security event logging	Log of failed updates	?
Field gateway device	4.4		Transfer encryption keys, username and password	✓
Communications Security	4.5		As per table below in "Access control"	✓
Common information model (CIM)	4.6		An encrypted secure boot process	?

An assessment of 15118-2 by Digcert, Chargepoint and eonTi found: "Within each major assessment area (governance, technology, operations), the team identified shortfalls of underdeveloped or ad hoc policies and requirements." They identified particular issues with certificate based authentication and secure communications[34].

Access Control

AS4755 defines an authorized person as a person, other than the user, who is authorized by the remote agent or the supplier of the electrical product to access, install or adjust parts or functions of the electrical product not accessible to the user Access control has a number of requirements including those for role based access control. This does not align with the architecture of ISO 15118, where the EV itself has a role to play.

Draft AS4755.2, S.4.3.6 Roles	**RA access Rights**		**EP communications manager access**		**Owner/user access**	
		ISO 15118		ISO 15118		ISO 15118
Reset demand response communication credentials	False	?	True	×	False	×
Modify/add users to demand response roles	False	?	True	✓	False	×
Start-up/shut down operating system of EP or field gateway device	False	?	False	✓	True	✓
Reboot EP or field gateway device	False	?	True	✓	True	✓
Initiate or request a firmware upgrade for EP or field gateway device	False	?	True	✓	True	✓

[34] Practical Considerations for Implementation and Scaling ISO 15118 into a Secure EV Charging Ecosystem 2019

Factory reset of EP or field gateway device	False	?	False	?	True	?
Manage field gateway device	False	?	True	?	True	?
View system/event logs	True	?	False	?	True	?
View system statistics (e.g. capacity, performance)	True	?	False	✓	True	✓

Logging Events

AS 4755.2 requires an electrical product to maintain a log of the occurrence and time of, at the least, the following types of events, in a form that is accessible to an authorized person:

	Capability	ISO 15118
(a)	Failed validations of device updates and firmware.	×
(b)	Initiated/failed firmware updates.	×
(c)	Device power cycling, start-up and shutdown events.	✓
(d)	User-initiated resets.	✓

NOTE if optional feedback pathway is supported then the RA shall be able to access this log.

Firmware update provisions

Firmware can be updated remotely (Provisioning certificates and installation requests).

Registration (network)

The process of the EV joining a logical network of the EVSE is described.

Communications security

AS4755.2 requires that communications shall be cryptographically protected. If public key infrastructure is utilized in the EP communication, it shall conform with the requirements of IEC 62351-9. 2045 does not provide any security beyond that provided by application that uses this platform such as encryption within the IP packet embedded in the serial message.

The IP communications has security requirements such as the application of TLS.

Documentation, Certification and Testing

15118 defines conditions to test the electrical characteristic of the transmitted signal but there does not appear to be testing associated with DR outcomes.

Provisions for documenting/reporting compliance

There are several conformance reporting requirements.

ISO 15118-4	ISO 15118-4: Network and application protocol conformance test	Status: Both published in February 2018
ISO 15118-5	ISO 15118-5: Physical and data link layer conformance test	

Provisions for testing compliance

The requirements for testing compliance are covered in ISO 15118.4.

Availability of testing and certification facilities

Testing and certification facilities for Australia could not be identified. Deka in Germany and Kinetics (global) offer testing services.

ESVE brands and & models claiming compliance

Coritech, a charging station manufacturer that offers V2G Fast Chargers, includes ISO 15118 in its approved standards list.[35] There is no known Mode 3 EVSE that claims ISO 15118 compliance.

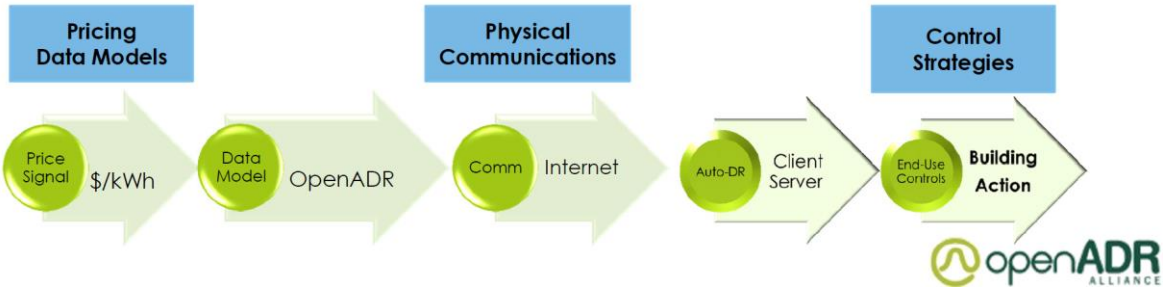
[35] https://coritech.com/v2g-architecture

IEC 62746-10-1:2018 (OpenADR 2.0 Profile Specification B)

Originally developed by the OpenADR Alliance, OpenADR 2.0 Profile Specification B (Open Automated Demand Response Communications Specification) is now an IEC standard IEC 62746-10-1:2018 (Systems interface between customer energy management system and the power management system – Part 10-1: Open Automated Demand Response).

IEC 62746-10-1(E) specifies a DR data model and services. It covers pricing, distributed energy resource (DER) communications and the characteristics of a DR interface. The model introduces virtual top nodes (VTNs) that are servers which publish information about events and automated virtual end nodes (VENs) that subscribe to the information and respond to it – an end node could be an aggregator but it is not a resource itself and it does communicate information about its resources to the top node. An important feature of 62746 is that it does not make assumptions of specific DR, market strategies, contacts or agreements.

The following diagram indicates the intended role of OpenADR. It is primarily intended to enable DR based on price signals, but also offers a set of DR commands and the ability to pass messages containing operational instructions that the RA can define.



In summary, the features of Open ADR are:

- 1 document standard
- 3 Actors: electricity service providers, aggregators and end users (EVSE).
- Resources: Provides fundamental DR capabilities that allow the RA to control the EVSE
- 4 Services: register, event, report and opt
- 2 Feature sets: a and b
- Transport mechanism: HTTP or XMPP
- 2 Security levels: Standard (TLS) and high (XML signatures)
- Test tool (in development).

There is no DR outcome certification process.

Maturity of Standard

IEC 62746-10-1:2018 originated from OpenADR2.0b which is the results of nearly 20 years of development. The evolution of OpenADR is given in the following table:

Year	Version	Comments
2002		Research by LBNL/CEC
2007	OpenADR 1.0 Commercialisation	PG&E, SEC, SDG&E
2009	OpenADR specification v1.0	Three profiles a and b and c
2012	OpenADR 2.0	
2014	IEC PAS 62746-10-1:2014 withdrawn	IEC PAS 62746-10-1:2014-02 originally designated as OpenADR 2.0b profile
2015	OpenADR 2.0	Profile Specification B Profile
2018	IEC 62746-10-1:2018	Systems interface between customer energy management system and the power management system - Part 10-1: Open automated demand response

OpenADR functionality is designed for continual evolution and it allows new profiles to be added if required by the market.

Scope

IEC 62746-10-1 specifies a message exchange interface covering a minimal data model and services for DR, pricing, and DER communications using a common language and communications such as the internet. Features of IEC 62746-10-1 are referred to in terms of “system”, “technology,” or “service”. It does not specify “bit structures” as some communications protocols do, but instead relies upon existing open standards such as XML and Internet Protocol (IP) as the framework for exchanging DR signals.

Its main parts are:

- A communications data model, a set of data models that describe information communicated in message payloads a set of services for performing various functions and operations for the exchange of the data models.
- A transport mechanism - a set of transport mechanisms (protocols) for implementing the services. The transport mechanisms rely upon standard-based IP communications such as HTTP and XML Messaging and Presence Protocol (XMPP).
- Security mechanisms - a set of security mechanisms (levels) for securing each of the transport mechanisms.
- A set of XML schemas.
- A test tool.

To reduce overheads for simple applications such as thermostats a light version OpenADR2.0a is also defined, but this has not been adopted as an IEC standard.

Current Usage

There appears to be some use of OpenADR for EV control but it is mostly used for other products. Californian Title 24 lists many products for load control. The list does not currently include relevant EV or EVSE requirements, but these would be captured by the general statements given below.

The Californian Title 24, Mandatory Requirements for Demand Management in Buildings - for the 2019 Building Energy Efficiency Standards states[36]:

[36] Title 24, Part 6, and Associated Administrative Regulations in Part 1. Section 110.12 – Mandatory Requirements for Demand Management Buildings - for the 2019 Building Energy Efficiency Standards https://www.energy.ca.gov/programs-and-topics/programs/building-energy-efficiency-standards

1. All demand responsive controls shall be either:
   a) A certified OpenADR 2.0a or OpenADR 2.0b Virtual End Node (VEN), as specified under Clause 11, Conformance, in the applicable OpenADR 2.0 Specification; or
   b) Certified by the manufacturer as being capable of responding to a demand response signal from a certified OpenADR 2.0b Virtual End Node by automatically implementing the control functions requested by the Virtual End Node for the equipment it controls.
2. All demand responsive controls shall be capable of communicating using one or more of the following: Wi-Fi, ZigBee, BACnet, Ethernet, or hard-wiring.
3. Demand responsive controls may incorporate and use additional protocols beyond those specified in Sections 110.12(a)1 and 2.
4. When communications are disabled or unavailable, all demand responsive controls shall continue to perform all other control functions provided by the control.
5. Demand responsive control thermostats shall comply with Reference Joint Appendix 5 (JA5), Technical Specifications for Occupant Controlled Smart Thermostats.

Examples of IEC 62746-10-1 (OpenADR2b) applications include:

Country	Example
Japan	OpenADR required from Utility to aggregator, under consideration also to DER systems
Korea	Multiple Korean manufacturers building and certifying OpenADR systems in preparation for trials and deployments
US & Canada	Multiple deployments in California, Nevada, Hawaii, other US states, Canada
	California building energy standards - Title 24
China	CEPRI validated as OpenADR test facility to simplify deployment
Europe	ENERA project (http://www.energie-vernetzen.de/en/index.html);
	Pilots in several other countries (e.g. UK - http://www.greentechmedia.com/articles/read/is-europe-ready-for-automated-demand-response);
	USEF (http://www.usef.info/Home.aspx) implementing OpenADR as transport
	Vattenfall OpenADR evaluation
	Denmark project (http://greentechcenter.dk/uk/projects/demand-response-capacity-management.aspx)
	California Rule 24 use for products such as lighting.

Interfaces (physical)

OpenADR refers to software interfaces and not physical interfaces. The lowest level considered is the transport layer for implementing services. The network, link and physical layers are taken care of in the underlying technologies that are part for the current purposes of WiFi or Ethernet.

Other standards required/supported for end-to-end operation

OpenADR does not require any other software to establish IP based connectivity. However, some deployments involve other systems for end to end deployment. The State of California views the architecture as flexible and that multiple paths will exist with multiple protocols such as OCPP 1.6J. There are some commands that are used in the OpenADR 2.0 Demand Response Program Implementation Guide which appear to require the OASIS Energy Interoperation 1.0 schema.

Proprietary/patent content

The necessary security certificates must be purchased and so while the standard is open its implementation is not. A disclaimer states: Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

Main functions, settings and capabilities

OpenADR is described in terms of feature sets, services, capabilities, payloads and events. OpenADR has two feature sets (a and b). Feature set "a" is very limited but it has a simple deployment. Feature set "b" has more capabilities and it is the version that is described here. An EVSE acting as an OpenADR VEN would be able to receive commands from a RA acting as the VTN and communicate information between them using services that pass payloads. The following table lists the key services in the IEC 62746-10-1:2018 main feature set: EiRegisterParty, EiEvent, EiReport, and EiOpt together with three additional ones. EiEvent (DR) and EiOpt (opt-in or opt-out)would provide the required functionality for EVSE DR.

Key Services		**Description**
Register:	EiRegisterParty	Registration identifies entities in advance of interactions with other parties in various roles such as VEN and VTN.
Event:	EiEvent	The core DR event functions and information models for price-responsive DR. This service is used to call for performance under a transaction. The service parameters and event information distinguish different types of events: reliability events emergency events, price events, regulation events and possibly other types in the future.
Report:	EiReport	The Report service enables feedback to the server in order to provide periodic or one-time information on the state of a resource.
Opt:	EiOpt	Overrides the EiAvail; addresses short-term changes in availability to create and communicate Opt-in and Opt-out schedules from the VEN to the VTN.
Report only VEN		The B profile has a sub-profile for VENs called Report Only, for use with say a meter
Transport Protocols		VENs can either support HTTP or XMPP, or may support both. VTNs must support both HTTP and XMPP.
Security levels		Supported security details are outlined in Clauses 8 and 9. The following security levels apply to OpenADR 2.0b. a) Standard Security – mandatory b) High Security – optional

The following elements/signals to define a DR event: time, notification time, randomisation, ramp up, duration, active state, recovery and completed state.

Capability to receive commands from a remote agent

An IEC 62746-10-1 VEN can receive commands from a remote agent (VTN). It is worth noting that when a VEN has overlapping events its behaviour is undefined and it is up to the DR deployment to define the required behaviour.

Entering responsive and non-responsive states

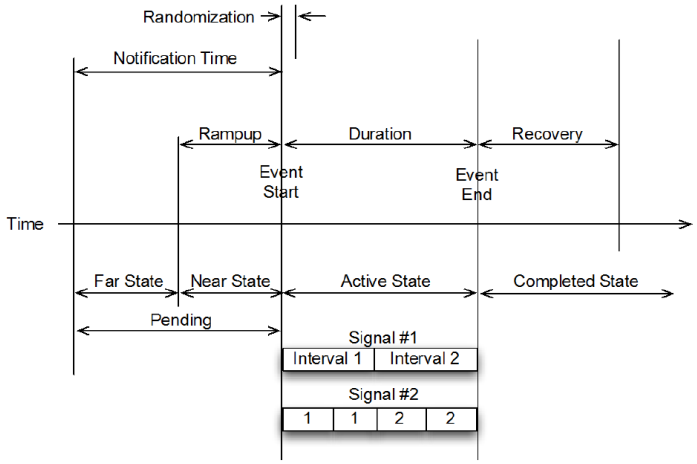
One interpretation of this mode of operation is giving notice to the client that it will enter a DR event. The period before the event starts is called the notification time. There are several related situations:

- VEN clients are requested to use presence packets to notify subscribed entities of their online and offline status.
- VTN clients might choose to use the roster as a mechanism to track presence of online VEN clients
- If a VEN deliberately terminates its XMPP connection (e.g., due to a controlled shutdown, not an unexpected connectivity loss) it shall first send an ‘unavailable’ notification.
- The available event signals do not appear to include an instruction for the client to deliberately go into a non-responsive state. For failures, OpenADR has rules

for communicating with non-responsive end nodes to reduce communications burden due to retrying (doubling the quiescent interval). If the service is intentionally unavailable then the quiescent path is not activated.

Time delay/scheduling capability for start/end event

Both VTN and VEN are required to have awareness of the current time. Time synchronization requirements are determined by the specific implementation and demand response program. A single eiActivePeriod defines the start time and duration of the event. The timing of major events is shown in the following figure. Events such as randomize is achieved through using the tolerance object in the eiActivePeriod.



Randomisation of start/end

Event start times can be randomized using the tolerance object in the eiActivePeriod. The sub-element Startafter defines a randomization time window used by the VEN to select a random value that is added to the start time of the event. If the start time of a one-hour event is 3:00pm and the randomization window is 5 minutes, if the VEN selected 3 minutes as the random value then the event would start at 3:03pm and would end at 4:03pm.

User over-ride provisions

Opt-Out - Provides opt-out or override function to any participants for a DR event if the event comes at a time when changes in end-use services are not desirable.

The OpenADR 2.0 B profile specifies the EiOpt service to create and communicate Opt-In and Opt-Out schedules from the VEN to the VTN. These schedules define temporary changes in the availability, and may be combined with longer term availability schedules and the Market Context requirements to give a complete picture of the willingness of the VEN to respond to EiEvents received by the VEN.

Opt is a specified service and overrides the EiAvail; addresses short-term changes in availability to create and communicate Opt-in and Opt-out schedules from the VEN to the VTN. EiOpt payloads can create or cancel an event. Opt-Out - Provides opt-out or override function to any participants for a DR event if the event comes at a time when changes in end-use services are not desirable.

Preservation/deletion of settings (privacy)

There does not appear to be any specific function to deal with the preservation and deletion of device retained information. The reporting payload does include identifying information such as end node ID but it is unclear if this can be tied to an actual user.

Command formats required/supported

The following list summarises key points in using OpenADR 2.0b:

1. OpenADR 2.0b services are independent of transport mechanisms.
2. OpenADR 2.0b services make no assumption of specific DR electric load control strategies that might be used within a DR resource
3. Profile b is much more sophisticated than profile a
4. Not all devices need to support all OpenADR capabilities.
5. Feature sets - Both VTN and VEN shall have awareness of the current time.
6. There are four OpenADR 2.0 services tow important for EVSE are:
    a. The Event service is the core of DR event functions and information models normally for price responsive DR The service is used to call for performance under a transaction
    b. The Opt Overrides the EiAvail; addresses short-term changes in availability to create and communicate Opt-in and Opt-out schedules from the VEN to the VTN.
7. Report Only VENs - some devices, such as meters, do not have the ability to shed load.
8. Transport Mechanism Supported transport mechanisms are as follows. .
    a. a) HTTP is mandatory for VTNs; VENs shall either support HTTP or XMPP
    b. b) XMPP is mandatory for VTNs; VENs shall either support HTTP or XMPP
9. The following security levels apply to OpenADR 2.0b.
    a. a) Standard Security – mandatory
    b. b) High Security – optional
10. Event Interactions Events are generated by the VTN and sent to the VEN using the oadrDistributeEvent payload containing one or more events described by the oadrEvent element.
11. Either a PUSH or PULL interaction pattern may be used.
12. For push, the VTN will deliver events to the VEN using an oadrDistributeEvent payload.
13. In PULL mode, the oadrDistributeEvent will be sent from the VTN to the VEN as response to an oadrPoll
14. Event start times can be randomized using the tolerance object in the eiActivePeriod.
15. The eiEventSignal:signalName, eiEventSignal:signalType, and eiEventSignal:itemBase attributes are used to describe the signal. (See table next page).

Equivalence of Demand Response Modes

There are two ways the signalling can be used. Use the 8 bit signalPayload command to directly transmit AS4755 commands. This option was developed for Standards Committee EL-054 during the drafting of AS4755.2. but not included in the draft released for public comment in 2021.

An alternative is to use existing commands to achieve the required DR. Usable DR commands are shown in the following table where XXX represents Real, Apparent, and Reactive versions of power or energy. Note that some commands refer to charge or discharge.

Signal category	Name (signalName)	Type (signalType)	Units (itemBase)	Allowed values	Description
Simple levels	SIMPLE	level		0,1,2,3	0=normal; 1=moderate; 2=high; 3=special.
Demand charge	DEMAND_CHARGE	price	currency/kW	any	This is the demand charge ex-pressed in absolute terms
	DEMAND_CHARGE	priceRelative	currency/kW	any	This is a delta change to the existing demand charge
	DEMAND_CHARGE	priceMultiplier	None	any	This is a multiplier to
dispatch storage resources	CHARGE_STATE	setpoint	energyXXX (1)	any	This is used to either charge or discharge a certain amount of energy from a storage resource until its charge state reaches a certain level.
	CHARGE_STATE	delta	energyXXX (1)	any	This is the delta amount of energy that should be contained in a storage resource from where it currently is.
	CHARGE_STATE	multiplier	None	0,0 < 1,0	This is the percentage of full charge that the storage re-source should be at.
set the load to values ex-pressed in terms of desired load	LOAD_DISPATCH	setpoint	powerXXX (1)	any	Dispatch loads to a specific amount
	LOAD_DISPATCH	delta	powerXXX (1)	any	Dispatch loads to some offset from an agreed upon baseline – could be current power consumption.
	LOAD_DISPATCH	multiplier	None	any	Dispatch loads as multiple of power against some agreed upon baseline. Could be current power consumption.
	LOAD_DISPATCH	level	powerXXX	integer value from -10 to +10	This is used to specify the load
set the load control to values relative to load controller and its output capacity. This does not re-quire the VTN or the VEN knowing precisely what the load consumption level is, but are expressed in ways that the VTN can know that the signal values will either increase or decrease the load consumption regardless of the specific type of device that is performing the load control. These can be used for some aspects of direct load control by mapping these general instructions to specific load control commands in the VEN without the VTN needing to know precisely what device	LOAD_CONTROL	x-loadControlCapacity	None	0 – 100 % (0,0 – 1,0)	This is an instruction for the load controller to operate at a level that is some percentage of its maximum load consumption capacity. This can be mapped to specific load controllers to do things like duty cycling. Note that 1,0 refers to 100 % consumption. In the case of simple ON/OFF type devices then 0 = OFF and 1 = ON.
	LOAD_CONTROL	x-loadControlLevelOffset	None	integer value, Pos-itive or negative	Discrete integer levels that are relative to normal operations where 0 is normal operations. The higher the setpoint the less load is consumed.
	LOAD_CONTROL	x-loadControlSetpoint	None	any value	Load controller set points. Generic controller set points and can be mapped at the VEN side to something as simple as specific

may be consuming the signal.					thermostat temperature set points.
	LOAD_CONTROL	x-loadCon-trolPercen-tOffset	None	any per-centage, both posi-tive and negative	Percentage change from normal operations. The lower the percentage the less load is consumed.

The equivalence to AS4755 DR modes is indicated in the following table. These could be achieved either by using either in-built capabilities or the signalPayload to carry the 8bit OI.

OI	**DRM**	**IEC 62746-10-1:2018**
0	Disconnect	✓
1	No primary load	✓
2	Constrain load (50%)	✓
3	Constrain load (75%) and export reactive power	✓
4	Request load	✓
5	No export to grid	✓
6	Constrain export (50%)	✓
7	Constrain load (75%) and consume reactive power	✓
8	Request export	✓

Note: Some DRMs can only be actioned if an EV is connected and is in a state of charge that permits charging or discharging

Other inbuilt DR capabilities

The DR controls that are available are:

- Setpoint - amount of energy reduction that was offered by a resource into a program. This is used to either charge or discharge a certain amount of energy from a storage resource until its charge state reaches a certain level.
- Delta - this is the delta amount of energy that should be contained in a storage resource from where it currently is.
- Multiplier level offset - the higher the setpoint the less load is consumed.
- Setpoint - Load controller set points.
- PercentOffset - Percentage change from normal operations.

Feedback pathways

This covers communications and information pathways.

Communications: The common deployment architecture indicates OpenADR being the main source of connection to the demand response provider but intermediary systems such as those operated by an aggregator can use other means to reach endpoints.

Information: OpenADR provides bi-directional information exchange

The Report service enables feedback to the server in order to provide periodic or one-time information on the state of a resource.

Categories of information to be communicated	IEC 62746-10-1
The present operating status of the EVSE, e.g. ‘Standby’ or ‘Charging’	✓
If charging, the power level (instantaneous or over a recent period)	✓
DR events under way, recently executed or logged for future execution	✓
Power levels during DR events	✓
Whether user override has been activated (a VEN can optout)	✓

Cyber-Security

OpenADR Cyber Security section was reviewed by NIST, SGIP and IEC. As a result, the OpenADR Alliance has:

- Implemented Server and Client certificates
- Made usage of TLS1.2 mandatory for certification
- Made additional security (XML wrappers) optional
- Established a Certificate Authority (Kyrio/DigiCert – formerly Symantec)

There are two levels of security for the VTN and VEN, the standards level is mandatory and the highest level optional.

- Standard Security – mandatory. The ‘Standard’ security uses TLS for establishing secure channels between a VTN and a VEN for communication.
- High Security – optional ‘High’ security additionally uses XML signatures providing non-repudiation for documentation purposes (e.g., a signed OpenADR event may be stored in a database for later documentation that an event has actually been received.

OpenADR 2.0b has two Transport Mechanisms

1. HTTP is mandatory for VTNs; VENs shall either support HTTP or XMPP
2. XMPP is mandatory for VTNs; VENs shall either support HTTP or XMPP.

In both cases:

- TLS and Cipher Suites that require TSL1.2 (not 1.3). Note that a VTN or VEN may be configured to support any TLS version and cipher suite combination based on the needs of a specific deployment
- Client certificates for HTTP client authentication. If no client certificate is supplied, or if the certificate is not valid the server shall terminate the connection during the TLS handshake.

All XMPP clients are required to support SSL/TLS and authentication as defined in section 13.8 and 13.9.4 of 1290 [RFC6120]. Clients are also required to implement Simple Authentication and Security Layer SASL EXTERNAL in order to use certificate authentication as defined in [RFC6120].

Certificate Authorities: The OpenADR 2.0 Certificate Policy and the OpenADR/NetworkFX partnership govern the OpenADR Security Certificates. These are claimed to be "low cost" to manufacturers. OpenADR Alliance Certificate Policy OpenADR-CP-I01-131101 provides additional information on security.

Draft AS 4755.2 Section		Title	Comment	IEC 62746
General	4.1			
Device identification	4.2	Permanent embedded unique identifier (UID)	Makes use of UID but not sure if embedded	?
Access management for electrical products	4.3			
	4.3.1	Provisioning states	Update credentials, reset, delete data	✓
	4.3.2	Electrical product ready for provisioning	Before registration and after deregistration	?
	4.3.3	Provisioning	Mutual authentication using credentials or encryption	✓
	4.3.4	Completion of provisioning	EP only act	?
	4.3.5	Credentials	Transfer encryption keys, username and password	✓
	4.3.6	Role-based access control	As per table below in "Access control"	✓
	4.3.7	Secure boot	An encrypted secure boot process	✓
	4.3.8	Electrical product firmware maintenance	Capability to accept firmware updates.	✓
	4.3.9	Security event logging	Log of failed updates	✓
Field gateway device	4.4	Comms security		
Communications Security	4.5	Public-key infrastructure shall conform with IEC 62351-9.		?
Common information model (CIM)	4.6	Meet requirements of IEC 61968-9.		?

Secure provisioning

AS4755.2 cyber-security requirement for secure provisioning involves bringing the electrical product under the management of the RA for the purposes of demand response. The following capabilities shall be supported by the EP:

	AS4755.2 required Capabilities	IEC 62746
(a)	EP shall be capable of having its credentials updated.	✓
(b)	EP shall have a factory reset capability located on or accessible from the EP.	
(c)	Factory reset shall delete all data except for data required to maintain the safety and system performance of the EP.	✓
NOTE	Any data from the EP that may identify the previous owner or user, location, log events or communication information should be purged	✓
	The EP shall not be able to prevent RA from revoking cryptographic keys used to maintain the trust relationship, and from deregistering the EP.	See Note

Note: Cryptographic keys should not be sent over the channel and it is preferable to install the authorization key on the charge point during manufacture or installation.

AS4755.2 requires during provisioning, the EP or field gateway device and the RA shall be capable of mutual authentication. Provisioning is part of the OpenADR registration services

AS4755.2	Mutual authentication capability	IEC62746
(a)	Credentials unique to each individual EP or field gateway device; NOTE The same credentials may not be issued or used among multiple EPs, even if they are of the same model.	✓

(b)	A one-time cryptographically secure pseudorandom number generator to generate the access token for that individual EP, to establish the trust with the RA; or	✓
(c)	provisioned relevant credentials for cryptographic message signing, EP authentication and secure connections.	
	The RA provisioning process shall update the RA registration details of the EP and/or field gateway device	✓

Access control

AS4755.2 defines an authorized person as a person, other than the user, who is authorized by the remote agent or the supplier of the electrical product to access, install or adjust parts or functions of the electrical product not accessible to the user. Access control has a number of requirements including those for role based access.

Draft AS4755.2 S 4.3.6 Roles	**RA access Rights**		**EP communications manager access**		**Owner/user access**	
		IEC 62746-10-1:2018		IEC 62746-10-1:2018		IEC 62746-10-1:2018
Reset demand response communication credentials	False	✓	True	?	False	?
Modify/add users to demand response roles	False	✓	True	?	False	?
Start-up/shut down operating system of EP or field gateway device	False	✓	False	?	True	✓
Reboot EP or field gateway device	False	✓	True	?	True	?
Initiate or request a firmware upgrade for EP or field gateway device	False	✓	True		True	?
Factory reset of EP or field gateway device	False	✓	False	?	True	?
Manage field gateway device	False	✓	True	?	True	?
View system/event logs	True	✓	False	?	True	?
View system statistics (e.g. capacity, performance)	True	✓	False	?	True	?

Note: "?" indicates that at the time of writing no clear answer was evident. Often the answer depends on the implementation and does not indicate a limit in capability.

The electrical product shall maintain a log of the occurrence and time of, at the least, the following types of events, in a form that is accessible to an authorized person:

		Capability	IEC 62746-10-1:2018
(a)		Failed validations of device updates and firmware.	?
(b)		Initiated/failed firmware updates.	?
(c)		Device power cycling, start-up and shutdown events. – Note 2	✓
(d)		User-initiated resets. – Note 2	✓

NOTE 1: if optional feedback pathway is supported then the RA shall be able to access this log.
NOTE 2: Recovery steps are outlined for when a device is being powered up and resent.

Firmware update provisions

There does not appear to be any over the wire or OTA firmware upgrade method specified – this is consistent with the understanding that this is a data model.

Registration (network)

There are two registration processes: the network and registering a VEN.

- Registering on network. This is taken care of as per normal IP connectivity processes.
- Registering a VEN. Makes use of EiRegisterParty payloads. Where the VTN becomes “aware” of the VEN.

Communications security

AS4755.2 requires that communications to be cryptographically protected.

IEC 62746 requires TLS be used to encrypt all traffic, regardless of the authentication method used. The client shall always validate the server’s TLS certificate given during the handshake. Client certificates are required to be used for HTTP client authentication. The entity initiating the request (the client) shall have an X.509 certificate that is validated by the server during the TLS handshake. If no client certificate is supplied, or if the certificate is not valid (e.g., it is not signed by a trusted CA, or it is expired) the server shall terminate the connection during the TLS handshake.

Documentation, Certification and Testing

OpenADR covers conformance and interoperability and has procedures to validate conformance of data models. Interoperability covers test specifications, cases and procedures, tools and compliance. The OpenADR Alliance has partnered with several international test houses to provide testing services to members of the Alliance. The certification process is described at https://www.openadr.org/certification-process.

OpenADR 2.0 specifies the mandatory and optional attributes required to meet broader interoperability, testing and certification requirements. Mandatory service requirements include, for example, that a VEN be capable of producing TELEMETRY_USAGE reports. Extensions beyond defined capabilities are allowed, however they are required to be tested as part of certification.

The IEC itself does not provide any attestation of conformity.

Provisions for testing compliance

For the purpose of device development, the OpenADR Alliance always tests the interface between a VTN and a VEN, where either node can be the device under test. Intelligence built into the systems not related to the OpenADR 2.0 message exchange is not part of the OpenADR Alliance testing program.

The authoritative requirements for implementation of OpenADR VENs and VTNs are defined in the OpenADR schema and conformance rules. Later sections, separate from the conformance rules, provide context and implementation examples but do not contain the full breadth of implementation requirements.

Conformance

In order to claim conformance to the profile specification, a VTN, VEN or VTN/VEN combination shall conform to all statements made in IEC62746-10-1 as well as the OpenADR 2.0 PICS document.

Availability of testing and certification facilities

There are OpenADR test certified test facilities in nine countries. They are listed at https://www.openadr.org/certification-process.

ESVE brands and & models claiming compliance

The list of OpenADR certified product includes about 50 charging systems but no individual EVSEs.

BSI-PAS 1878

PAS (Publicly Available Specification) 1878 *Energy smart appliances –System functionality and architecture – Specification* was published by the British Standards Institution (BSI) in May 2021.

It is not a standard but a fast tracked technical specification for the demand response of domestic energy smart appliances (ESAs). It is to be read with PAS 1879:2021 *Smart appliances – Demand side response operation – Code of practice*, which covers Demand Side Response Service Providers (DSRSPs). Smart EV charge points are a focus.

A PAS is not to be regarded as a British Standard and will be withdrawn in the event it is superseded by a British Standard.

PAS 1878 describes requirements for DR control, system technical specifications for a DSR system (including appliances), DSR services, operational models and cyber security. There are specific requirements for smart EV charge points reporting and importantly they include that smart EV charge points are not required to support V2G functionality.

In summary, the features of PAS 1878 are:

- 1 document standard
- 5 Actors: Smart energy appliance, customer energy manager, demand side response service providers, manufacturers, and home energy management system.
- Resources: Provides fundamental DR capabilities that allow the RA to control the EVSE through defined interfaces.
- At least 4 Services: can use OpenADR
- 3 Interfaces: A,B and C
- Transport mechanism: HTTPS, secure websockets and XMPP
- Comprehensive security requirements

There is no test tool and no DR outcome certification process.

Scope

The PAS defines an Energy Smart Appliance (ESA) and describes standardised control of ESAs, subject to explicit consumer consent. The ESA is required to broadcast its immediate capabilities to the DSRSP via the customer energy manager/ESA gateway (CEM/ESAG). The DSRSP then sends requests to the ESA to implement one of its capabilities and implement its demand response.

The PAS:

- Specifies requirements and criteria that an electrical appliance needs to meet in order to perform and be classified as an ESA;
- Specifies attributes, functionalities and performance criteria for an ESA; and
- Identifies that DSRSP are responsible for compliance through the verification processes provided in the document.

The PAS covers:

- functional requirements of ESAs for DSR-based activities;
- the ESA system architecture for DSR-based activities, including
    - communication links and object functionalities and,
    - in particular, the interfaces between the CEM and the ESA and between the CEM and the DSRSP;
- the ESA operational sequence of DSR-based activities,
    - communication protocols
    - relevant ESA lifecycle considerations; and
- compatibility with British smart meter technologies.

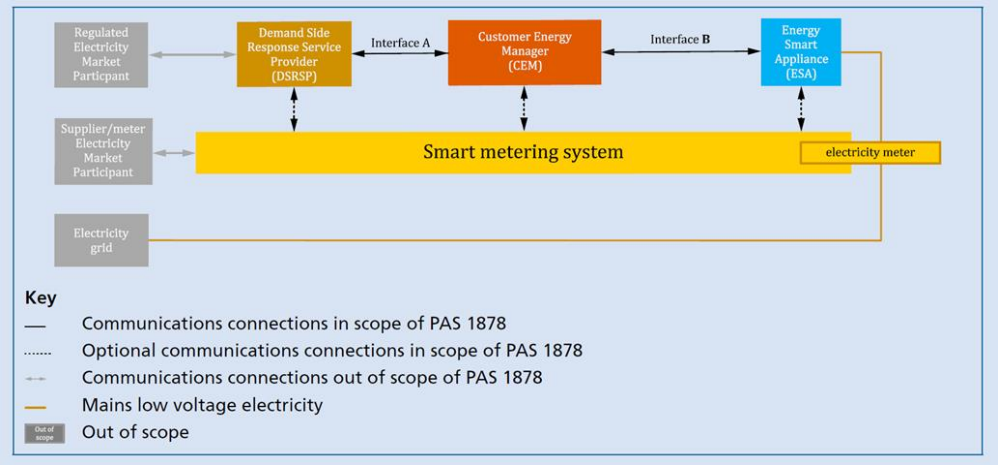
The PAS applies the following criteria in defining the requirements that are to be met by an ESA performing DSR-based activities:

- Interoperability ;
- Data privacy;
- Grid stability; and
- Cyber security.

Figure 6 illustrates the system architecture. PAS 1878 specifies OpenADR as the default option for Interface A, while indicating that other possible candidates include the IEC 61850 series, BS IEC 62746-10-1: 2018 and EEBus.

No approved option is named for Interface B, although OCPP 2.0.1 is mentioned in the references.

Figure 6 BSI PAS 1878:2021 System Architecture



ESAs currently covered include smart EV chargepoints (EVSEs), electric heating, ventilation and air conditioning (HVAC), domestic battery storage, wet appliances and cold appliances, but the ESA classification is not limited to these appliances.

Current Usage

Being a relatively new document, there is no evidence of its use as yet.

Interfaces (physical)

The physical layer of the ESA is not specified but there is a requirement that the status of the physical link to the CEM be indicated. The interface to the metering system would is defined in informative Annex D. References to physical interfaces are given in the following table.

Definition	Description
local physical interface	interface on the ESA or CEM that can only be accessed physically (e.g. USB port, UART, JTAG port
local user interface	interface on the ESA or CEM used for user interaction that can only be accessed physically (e.g. buttons, keypad, speaker, touchpad, screen)
network logical interface	logical interface or protocol operating over the network physical interface that connects the ESA or CEM to other entities on a communications network
network physical interface	hardware interface that physically connects the ESA or CEM to a communications network (e.g. Ethernet, radio transceiver)

PAS 1878 describes the three communications interfaces:

Interface	Start	End
A	DSR Service provider	CEM
B	CEM	ESA
C	CEM	HEMS

It describes two mandatory and three optional physical network interfaces:

Interface	Mandatory/optimal
B (CEM to ESA)	M
Manufacturer to CEM or Service provider	M
Remote user	O
External (weather)	O
Smart metering System	O

Other than meeting security requirements there are to be no restrictions on the ESA connecting to other CEMs but it is only allowed to connect to one at a time.

Other standards required/supported for end-to-end operation

PAS 1978 is intended to be read in conjunction with PAS 1879:2021 *Energy smart appliances – Demand side response operation – Code of Practice*, which provides recommendations for the provision of DSR services by service providers.

The PAS mandates that any implementation of Interface A shall support the use of OpenADR and shall always revert to the use of OpenADR in order to guarantee interoperability. This PAS does not restrict the use of other protocols to implement Interface A and mandates that all such implementations shall meet the requirements of Clauses 5 and 6 of this PAS.

Proprietary/patent content

There does not appear to be any declaration in this regard. The architecture does include options that might in turn include proprietary content.

Main functions, settings and capabilities

PAS 1878 says more about the system architecture than about the information the system conveys. AS4577.2 Operational instructions could be communicated over this messaging system using OpenADR or other protocols that offer similar utility.

Capability to receive commands from a remote agent

PAS 1878 specifies communications requirements between the DSRSP, CEM and ESA as well as other actors so it has the capability to receive commands from a remote agent. CEM and ESA are allowed to only register with one DSRSP at a time.

Entering responsive and non-responsive states

PAS 1878 does not specify such states and OpenADR does not appear to include an instruction for the client to go into a responsive or non-responsive state.

Time delay/scheduling capability for start/end event

This capability would be at least similar to that provided by OpenADR.

Randomisation of start/end

There are several references to randomisation. The ESA is required to be capable of applying a randomized offset to the start time in the range 0 seconds to 1800 seconds. The consumer override function must be able to override the randomized offset, if activated by the consumer. The CEM/ESA may not incorporate randomized offsets when creating the Most Delayed and Least Delayed power profiles, as these will be used to provide fast-responding DSR services.

User over-ride provisions

PAS 1878 specifies an optional Remote User Interface, which must, as a minimum, provide access to information and controls required consumers to engage in DSR services and allow them to provide their preferences for CEM or ESA operation and DSR service provision. The remote user interface shall give the consumer the ability to manually override, in real-time, current and planned DSR operations.

Preservation/deletion of settings (privacy)

This PAS has a number of privacy requirements including the need for consumer consent for access to personal information and control over data. Relevant data privacy standards and guidelines are referenced such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. There is also a requirement that the end user is able to remove personal identifiable information by means including a factory reset.

Command formats required/supported

The interface command formats are provided for OpenADR, the details of which are provided in the OpenADR review in the present report.

Equivalence of Demand Response Modes

The equivalence to AS4755 DRMs is covered in the OpenADR review. Two options are available: using the 8 bit signalPayload command or simply using predefined OpenADR instructions. Both allow the AS4755.2 IOs to be communicated.

The availability of AS5755 modes are indicate din the following table. These would be achieved by setting the limit in accordance with the required DR which are form the OpenADR section.

OI	DRM	PAS 1878
0	Disconnect	✓
1	No primary load	✓
2	Constrain load (50%)	✓
3	Constrain load (75%) and export reactive power	✓
4	Request load	✓
5	No export to grid	✓
6	Constrain export (50%)	✓

7	Constrain load (75%) and consume reactive power	✓
8	Request export	✓

Note: Some DRMs can only be actioned if an EV is connected and is in a state of charge that permits charging or discharging

Other inbuilt DR capabilities

PAS 1878 enables additional DR related capabilities that may be made possible due to its communications options. For example, systems are required to be compatible with the UK smart metering system – this enables the ESA to partake in wider activities. There is the capability to convey information and control signals related to power production and frequency response capabilities.

Feedback pathways

PAS 1878 supports the feedback from the ESA of the following categories of information.

Categories of information to be communicated	**PAS 1878**
The present operating status of the EVSE, e.g. 'Standby' or 'Charging'	✓
If charging, the power level (instantaneous or over a recent period)	✓
DR events under way, recently executed or logged for future execution	✓
Power levels during DR events	✓
Whether user override has been activated	✓ (if available)

Cyber-Security

BIS PAS 1878 has numerous cyber-security requirements as specified in section 6. This covers general cyber-security requirements, key generation, product design, manufacturing and supply chain, privacy, certificates, protocols and configurations.

Interface A must conform to all OpenADR security requirements and specifications. TLS v1.3 or later with X.509 certificates shall be used over Interface A. The set of TLS criteria specified in the table below are required to be used over Interface A.

Criteria	**Version**
Protocol	TLS v1.3 (or later)
Protocol Ciphers	TLS_ECDHE_RSA_WITH_ AES_128_GCM_SHA256
Client Certificate Hash Algorithm	SHA256
Server Certificate Key	RSA 2048 bit
Server Certificate Hash Algorithm	SHA256

AS4755.2 requires that the demand response system does not exacerbate threats to the security and reliability of the electricity system. AS4755.2 covers the following areas under cyber-security.

AS4755.2 Section 4		**Title**	**Comment**	**PAS 1878**
General	4.1			
Device identification	4.2	Permanent embedded unique identifier (UID)	Does not appear to be a requirement	?
Access management for electrical products	4.3			

	4.3.1	Provisioning states	Update credentials, reset, delete data	✓
	4.3.2	Electrical product ready for provisioning	Before registration and after deregistration	?
	4.3.3	Provisioning	Mutual authentication using credentials or encryption	?
	4.3.4	Completion of provisioning	EP only act	?
	4.3.5	Credentials	Transfer encryption keys, username and password	✓
	4.3.6	Role-based access control	As per table below in "Access control"	✓
	4.3.7	Secure boot	An encrypted secure boot process (S6.9)	✓
	4.3.8	Electrical product firmware maintenance	Capability to accept firmware updates.	✓
	4.3.9	Security event logging	Log of failed updates	✓
Field gateway device	4.4		Cryptographic requirements and comms security	✓
Communications Security	4.5		Public-key infrastructure shall conform to IEC 62351-9.	?
Common information model (CIM)	4.6		Meet requirements of IEC 61968-9.	?

Secure provisioning

AS4755.2 cyber-security requirement for secure provisioning involves bringing the electrical product under the management of the RA for the purposes of demand response. The following capabilities shall be supported by the EP:

	AS4755.2 required Capabilities	**PAS 1878**
(a)	EP shall be capable of having its credentials updated.	✓
(b)	EP shall have a factory reset capability located on or accessible from the EP.	
(c)	Factory reset shall delete all data except for data required to maintain the safety and system performance of the EP.	✓
NOTE	Any data from the EP that may identify the previous owner or user, location, log events or communication information should be purged	✓
	The EP shall not be able to prevent RA from revoking cryptographic keys used to maintain the trust relationship, and from deregistering the EP.	?

During provisioning, the EP or field gateway device and the RA shall be capable of mutual authentication, using

AS4755.2	**Mutual authentication capability**	**PAS 1878**
(a)	Credentials unique to each individual EP or field gateway device; NOTE The same credentials may not be issued or used among multiple EPs, even if they are of the same model.	✓
(b)	A one-time cryptographically secure pseudorandom number generator to generate the access token for that individual EP, to establish the trust with the RA; or	✓
(c)	Provisioned relevant credentials for cryptographic message signing, EP authentication and secure connections.	✓
	The RA provisioning process shall update the RA registration details of the EP and/or field gateway device	✓

Access control

AS4755 defines and authorized person as a person, other than the user, who is authorized by the remote agent or the supplier of the electrical product to access, install or adjust parts or functions of the electrical product not accessible to the user Access control has a number of requirements including those for role based access control. Passwords to authenticate consumers or others actors to access secure storage areas are not recommended. It would appear that registration is not within the scope of BIS PAS 1878 but it is covered in BIS PAS 1879. PAS 1879 covers authorization to enroll in a service under data privacy, consumer relationship management and cyber security but the requirements are very general.

Firmware update provisions

PAS 1879 has several minimum requirements for firmware updates, certificate management information (new certificates, certificate revocation), mutual authentication and indication of de-registration. Section 6.10 provides the following requirements.

- The ESA shall connect to its manufacturer (or service provider) portal. This connection shall be used to securely download firmware and software updates.
- Both the CEM and the ESA shall communicate with a remote manufacturer, or service provider portal, using a logical interface defined by the manufacturer/ service provider.
- As a minimum, this interface shall be used to supply the CEM and ESA with firmware updates, certificate management information (new certificates, certificate revocation etc.), during the CEM and ESA mutual authentication phase described in 5.3.2 and to indicate that the CEM or ESA is to de-register.
- Any software, firmware or security credential updates shall be performed securely, using TLS v1.3 or later.
- The CEM shall check with its manufacturer or service provider portal for manufacturer approved firmware/software updates and perform a secure update if a more recent version is available
- The ESA shall check with its manufacturer or service provider portal for manufacturer approved firmware/software updates and perform a secure update if a more recent version is available.

Registration (network)

PAS 1878 registration refers to:

- Consumer registration with DSRSP
- Device registration of the CEM and the ESA with the DSRSP
- De-registration.

The capability for CEM and ESA registration on the network is a requirement.

Communications security

AS4755.2 requires that communications shall be cryptographically protected. If public key infrastructure is utilized in the EP communication, it shall conform to the requirements of IEC 62351-9.

PAS 1878 has significant security requirements but IEC 62351-9 is not referenced.

Authentication

There is a requirement that the secure communications link shall be set up using mutual authentication and shall allow messages to be encrypted and failures to be logged. The specific authentication and registration requirements are provided in section 6.14.2

Documentation, Certification and Testing

As PAS 1878 is not an actual standard, it does not appear to have requirements for documentation, certification or testing.

Provisions for documenting/reporting compliance

There does not appear to be any documentation or reporting requirements.

Provisions for testing compliance

The scope clearly states that the PAS specifies how compliance can be verified. However, there does not appear to be any testing compliance requirements (other than those that would apply to protocols such as OpenADR implementations).

Availability of testing and certification facilities

There do not appear to be any requirements for testing and certification facilities.

Annex B. Consultations

AEMO

Steve Humphries

AGL

Rob Colson
Rohan Cannon

Elaad (NL)

Stan Janssen
Lonneke Driessen

JetCharge

Tim Washington (also Chair, EV Council of Australia)

NHP

Ross de Rango
Anthony Middleton

OpenADR Alliance (USA)

Rolf Bienert

Open Charge Alliance (NL)

Marc van Dijk

SA Power Networks

Travis Kauschke
Bryn Williams

Tesla Australia

Joseph Tadich
Lexy McArdle

Department of Business, Energy and Industrial Infrastructure (UK)

Laura Schade

Annex C. AREMA Projects

There are several AREMA-supported projects currently under way that bear on home EV charging. The following information is based on the progress reports published in May 2021. The main aspects of the projects are summarised in Table 16. Notably, the EVSE and charging software supplier Jet Charge is involved in all four trials.

Table 16 Summary of ARENA-supported EV charging trials

Project & timeline	Res - Smart charge (a)	Res API	Res V2G	Bus-iness, Fleet	EVSE partners	EV Partners	Charge, fleet services	DNSPs involved	Standards referenced
AGL 2020-2023	100 (82)	50 (25)	50 (0)	NA	Schneider, Wallbox, Quasar V2G (Jet Charge)	Tesla (API) Nissan (V2G)	Flexcharging Chargefox	United E AusNet Jemena SAPN Ausgrid Endeavour Energex Ergon	OCPP2.0 AS/NZS 4777.2 (for future V2G part)
Origin 2020-2022	75 (70)	NA	NA	75 (33)	Schneider (4G, wifi, ethernet)	Nissan Hyundai	Greenflux CustomFleet	United E Ausgrid +SA, Qld	OCPP1.1 OCPP1.6
Jemena	176	NA	NA	NA	Jet Charge customers	Tesla Nissan Hyundai	Jet Charge	Jemena United E AusNet Evo E TasNetworks	IEEE2030.5
ActewAGL Realising V2G Services (REVS) 2020-2022	NA	NA	NA	51	Bidirectional EVSEs still being sourced	Nissan	Jet Charge SG Fleet ActewAGL ACTGovt ANU	Evo E	

(a) Target participant numbers (recruited by May 2021)