D23/27

Smart Metering Infrastructure integration assessment

Combined report;

D23 SMETS Integration – Lab Testing

D27 SMETS Integration – Analysis Report

Moixa Technology Ltd, 29-31 Saffron Hill, London, EC1N 8SW | info@moixa.com | 020 7734 1511 | moixa.com

1.0 Definitions

ESS - Energy Storage System

ESA - Energy Smart Device

PAS 1878/1879

SAPC - Standalone Auxiliary Proportional Controller

HCALC - HAN connected auxiliary load control switch

HAN - Home Area Network

DER - Distributed Energy Resource

OEM - Original Equipment manufacturer

DCC - Data Communications Company

DUIS - DCC User Interface Specification

CPO - Charge Point Operator

OCPP - Open Charge Point Protocol

OVGIP - Open Vehicle Grid Interface Platform

VPP - Virtual Power Plant

HEMS - Home Energy Management System

BOM - Build of Materials

2.0 Executive Summary

At the start of the Home Response project the intention had been to utilize the smart metering network as an alternative to Moixa's, or a partners, existing communication gateways as a means of managing devices, initially via HCALC. This would offset the capital cost required to install control systems and limit home visits for installation and maintenance to end customers.

As the project has evolved and Moixa understood more of the challenges of the original approach, the aim has changed to mapping and understanding how smaller, innovative companies can leverage the smarter metering network most effectively. Additionally, the project looks to understand how the smart metering network could potentially be used to secure domestic devices.

This document summarizes how for several use cases common amongst UK aggregators for the control of DER the opportunities and challenges of interactions with the smart metering network.

2.1 Key findings

Below are summarized the key findings from the project;

- Some use cases could potentially allow for control via the smart metering network, this would be well suited to a DSO/Utility level top down control of smart but unmanaged assets with simple load profiles (such as EVs or Hot Water Tanks)

- It is difficult to see how this could be applied to more complex system or those with active management (such as offered by Moixa) without a separate telemetry channel

- In nearly every scenario considered, a separate communication channel would be required in order to allow at least telemetry data to be returned from the device to an asset management system. This is particularly important if the systems are being deployed in a VPP

- There is potential for use of the smart metering network in the securing of the use of DER from cyber attacks, this needs to be developed in a way that provides a

credible integration path for product manufacturers. Two proposals are made in this report.

- Access to the DCC UI for 3rd parties and the market structure that will be supported need immediate attention as having device level interactions from smart metering equipment cannot scale without this being clarified

- Internationally evolving standards must be utilized to avoid placing too high an entry barrier to the UK market for smart technology providers

2.2 Original Scope and project plan

The original plan for the project was to investigate the potential for integrating Moixa's GridShare with the DCC platform and through this allow us to control smart devices.

Throughout the project Moixa has been talking to DCC about integration options for dispatching assets via the smart metering network. This was initially focused on using the HCALCS technology, but this was soon found to be unworkable within the time frames of the project. Therefore the aim was shifted to be rather than completing a physical integration and running some tests to mapping how this can be completed in future projects.

This has been targeted at two areas of the integration;

- Within the home looking at data availability and system performance, and concerned with the physical systems and their characteristics
- Between Moixa and the cloud infrastructure which operates the network centrally

During the project the integration target for the local system has shifted as well from being the use of HCALCS, to looking at the more recently developed SAPC,. This has been conducted with SLS, the only manufacturer currently of SAPC devices.

Additionally the aim of the original project had been to trigger some lab tests demonstrating an end to end control of a device, via the smart metering network, from Moixa's cloud. This was originally scaled back to simply some lab tests triggered locally, but even this has proved problematic to set up.

2.3 Alternate approaches

Since it became clear the project could not be delivered at the targeted scale using this approach, Connected Response were engaged to fill the role of tech provider on the hot water tank use case. This has required installing an additional communications channel to facilitate this.

Alongside this we have continued to engage with the DCC and other bodies to try and understand the timelines and requirements for making this possible with the intention of proving out some part of the model with a test.

During this discovery work two other key points emerged;

- The production of the SAPC device for load control which has some communication capabilities and can be sited locally with a smart device
- A further workstream to look at the use of the smart meter network in the securing of residential flexibility assets from cyber attacks

Alongside both of these is the continued definition of PAS 1878/1879 and it's role in the coordination of residential flexibility and how that would be incorporated into any proposal.

Moixa also works across several countries and so is aware of the emergence of different international standards being used around the world. Therefore some time is taken to review the use cases being analyzed here in the context of that context.

3.0 Smart Metering Integration Options

This section details the work conducted to map the integration options that exist for interacting with the smart metering network to improve the potential products and services offered by DER.

This is considered for 6 use cases, one core use case into which considerable detail has been added and 5 additional ones to act as checks to the conclusions developed. These use cases are;

- Moixa Residential battery and solar panels; Core Use Case
- 3rd party battery and solar panels, Use Case 1
- Residential battery, electric vehicle charger and solar panels, Use Case 2
- Residential electric vehicle charger, control via the charger, Use Case 3
- Residential electric vehicle charger, control via vehicle telematics, Use Case 4
- Mesh network with gateway, Use Case 5

Core Use Case

A number of use cases will be considered when conducting this analysis in order to assess the limitations of the suggested methodology.

The most detailed analysis will be conducted against the core use case of an ESS and PV installed in a domestic residence. This is Moixa's core product and is the example where the deepest insights into how an integration would be conducted.

Figure 1 shows the functional pieces that take place in the operation of a Moixa battery, and the external connections that are maintained between Moixa and the various energy system actors to enable this.

Figure 2 shows a communications diagram to explain architecturally how these connections are maintained.

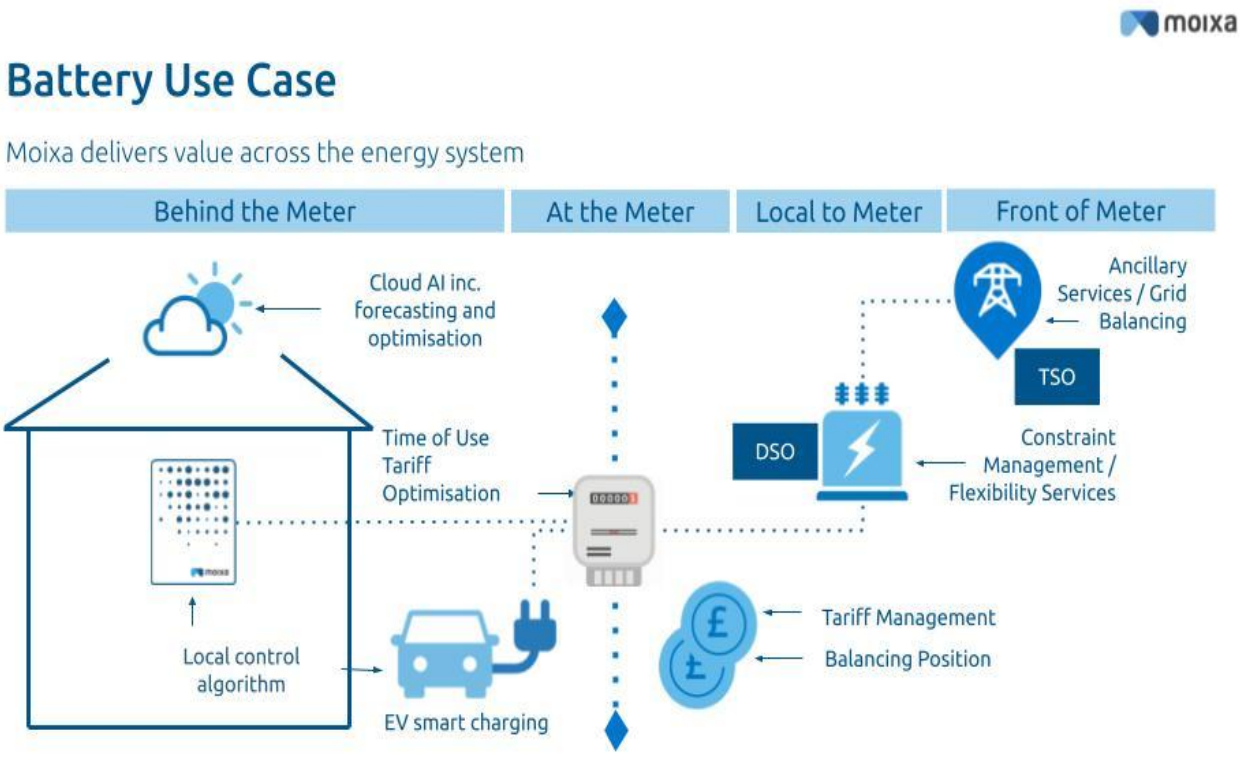

Figure 1 - System diagram explain battery relative to wider system

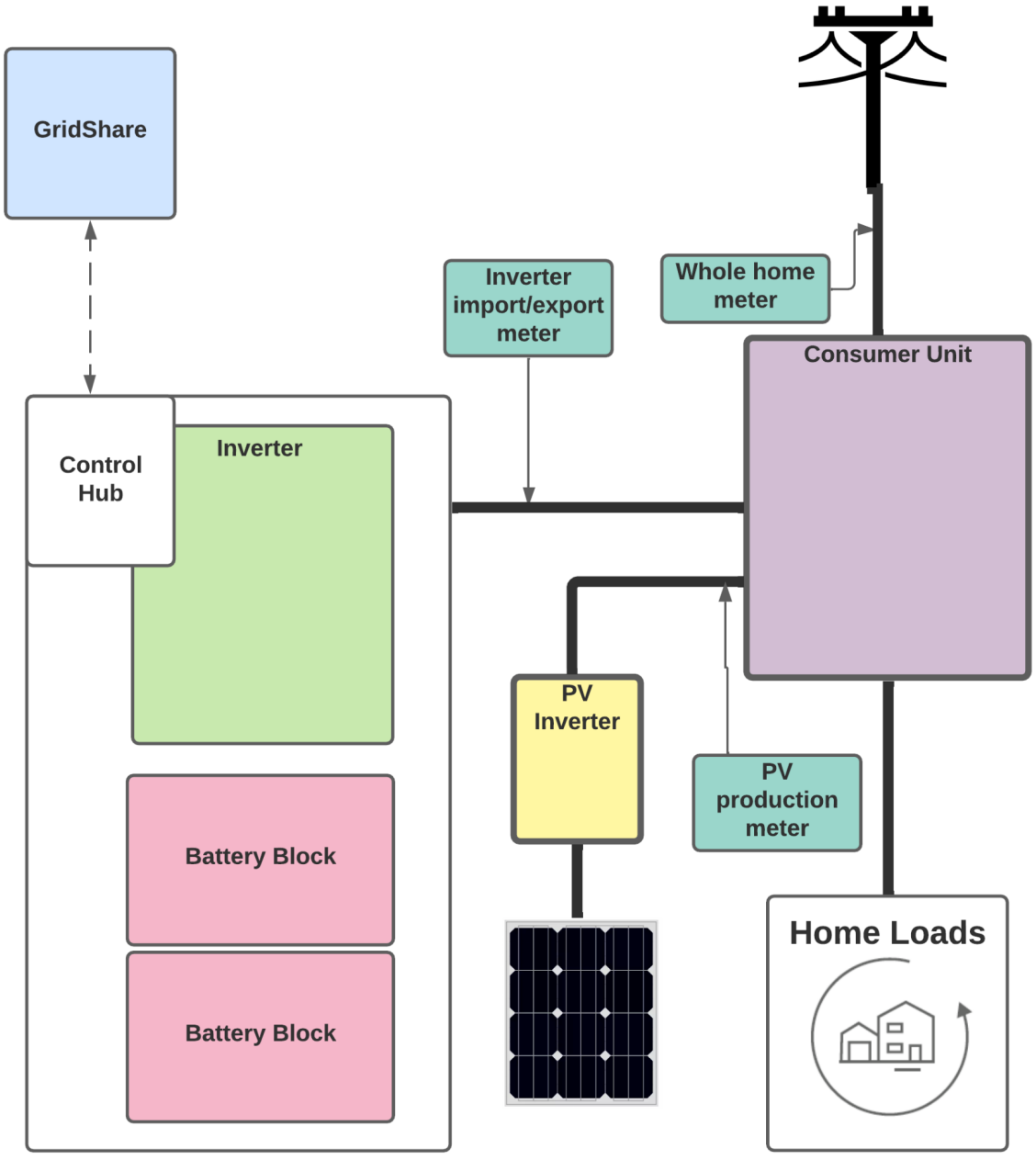

Figure 2

One important point to note here is that the battery will often be installed physically close to the consumer unit and boundary meter, and will nearly always have some cable runs to it to allow for inline meters or clamps to be installed. This is often not the case for some of the other use cases described.

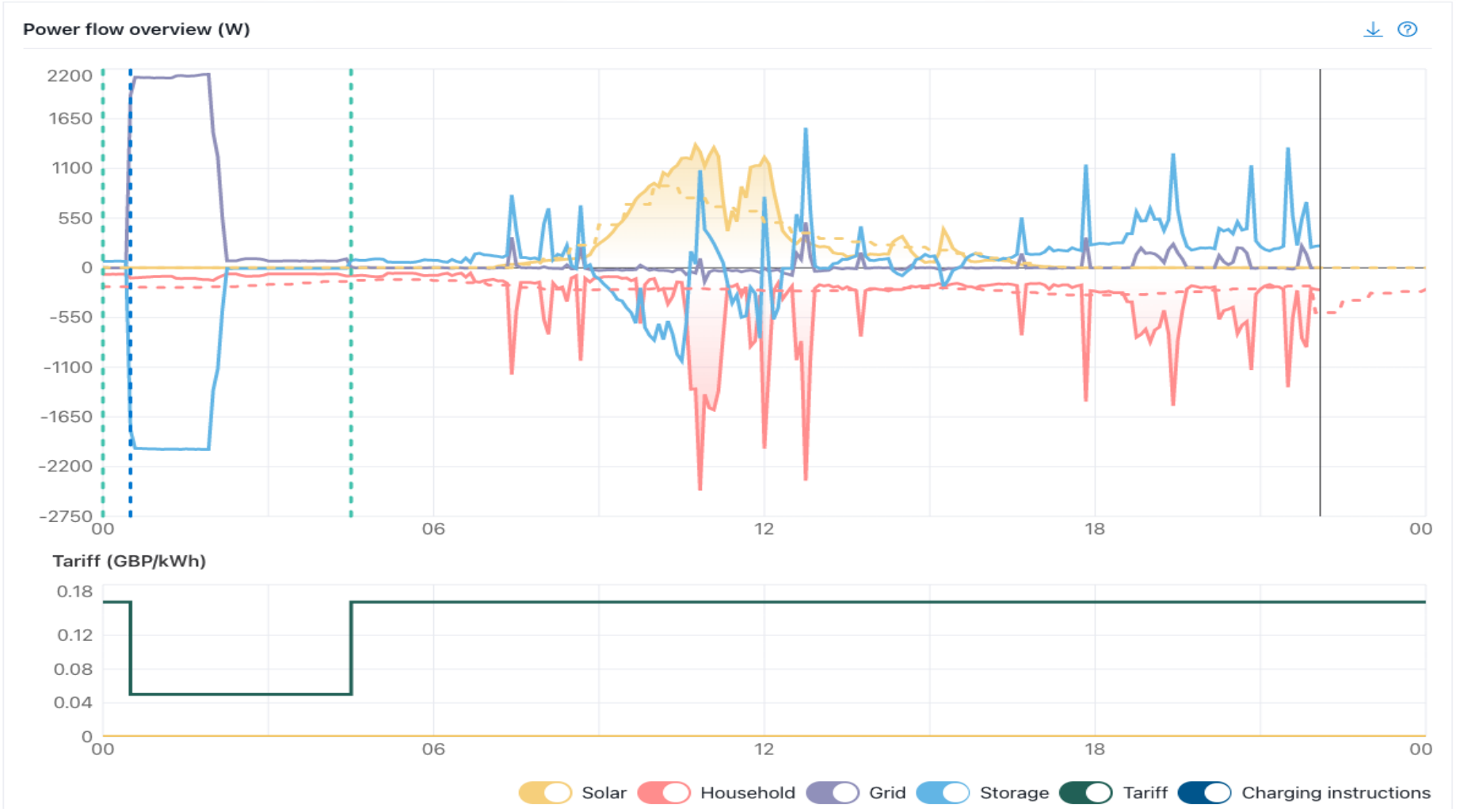

Figure 3 - Example day of operation for battery system

Figure 3 shows the standard operation on a battery on a typical day. The aim here is to highlight the communications that are happening between both the control hub and the inverter and the cloud platform and the control hub, and the actions they allow for.

The battery has the concept of a “plan” which is comprised of a set of operational modes which can be set with specific configurations. These can either be permanent and stored locally on the device, or time limited (usually up to 48 hours) and pushed from the cloud to the device to override the local plan temporarily. For most batteries with PV and a time of use tariff a new plan is pushed each day to incorporate the latest solar and load forecast in an updated set of commands. The control hub is capable of exercising decision making locally, based on data such as metering, to operate the battery. It does so within the bounds set by the plan it has been given.

In figure 3 several operational modes can be observed;

- 0030-0200 - the battery has received a charge instruction to coincide with the start of a low tariff period
- Approx 0900 - 1230 - the battery received a balance instruction at 0430. This means it will charge from “spare” solar generation that would otherwise be exported
- 1530-2200 - the battery still has a balance instruction, however now it is discharging to cover load that would otherwise be imported from the grid

The specific set of operational modes laid out in the plan are generated in the cloud by an algorithm designed to minimize cost across the day. One of the key inputs to the algorithm are the forecasts for PV generation and site consumption (shown in dotted lines in figure 2). Forecasting however is not an exact science and so monitoring is used to check observed data that does not deviate from the forecast by more than a particular margin. In the event of a deviation the algorithm is rerun and a new plan transmitted to the device.

To allow this high resolution data is being transmitted from the local meters and inverter to the control hub and from there to the cloud.

This mode of operation would mean 1-2 plans being pushed to a device each day, each with a lifespan of around 48 hours.

However there are several other use cases that require plans to be pushed to systems;

- Proactive asset management - Moixa monitors all connected devices on our system and this requires data being pushed from devices. This includes often a large amount of operational logs etc and can often need an operator to modify settings on the device
- System resets or fault finding - A customer service representative or technical operative may need to remotely access a battery to attempt to correct an issue without a site visit

- User control - Moixa exposes several user configuration options through our customer apps allowing for users to set their own battery schedules for instance. These are pushed to the battery as plans from the cloud, in the same way as those generated by the AI
- Grid Services - increasingly more batteries are enrolled in grid service programs and as such may need to receive instructions from the cloud with only seconds latency allowable in some cases
- Grid service management - All aggregators will monitor the dispatch of devices for grid services live and will bring additional systems on if required by failures to others. This requires rapid and responsive plans to be pushed, potentially every 5 minutes for the dispatch window

These additional uses could mean that there are considerably more plans being pushed, with potentially dozens on a given day.

VPP READINESS

For devices being included in grid services Moixa firmly believes that the only way to deliver residential flexibility effectively is to ensure that the customer gets best service through it. This requires that the needs of the grid service are optimized simultaneously in conjunction with the optimization of any smart device. Any smart device will have a day job or regular operational mode, be that providing economic benefit, heating a home or offsetting carbon, this must be respected when adding another use (grid flexibility) to the system.

The architecture described above allows for this, but is generally ahead of what standards currently easily allow for. It is therefore key that this use case is not suppressed through a desire to implement reform based on current industry practice which could result in a more top down, command and control approach to grid services.

Therefore when considering these additional use cases then the number of cloud to device instructions per day could be considerably higher.

Additional Use Cases

Below is described the additional use cases that will be covered in the report, along with some key points that could impact some of the integration options described.

Battery + PV (UC1)

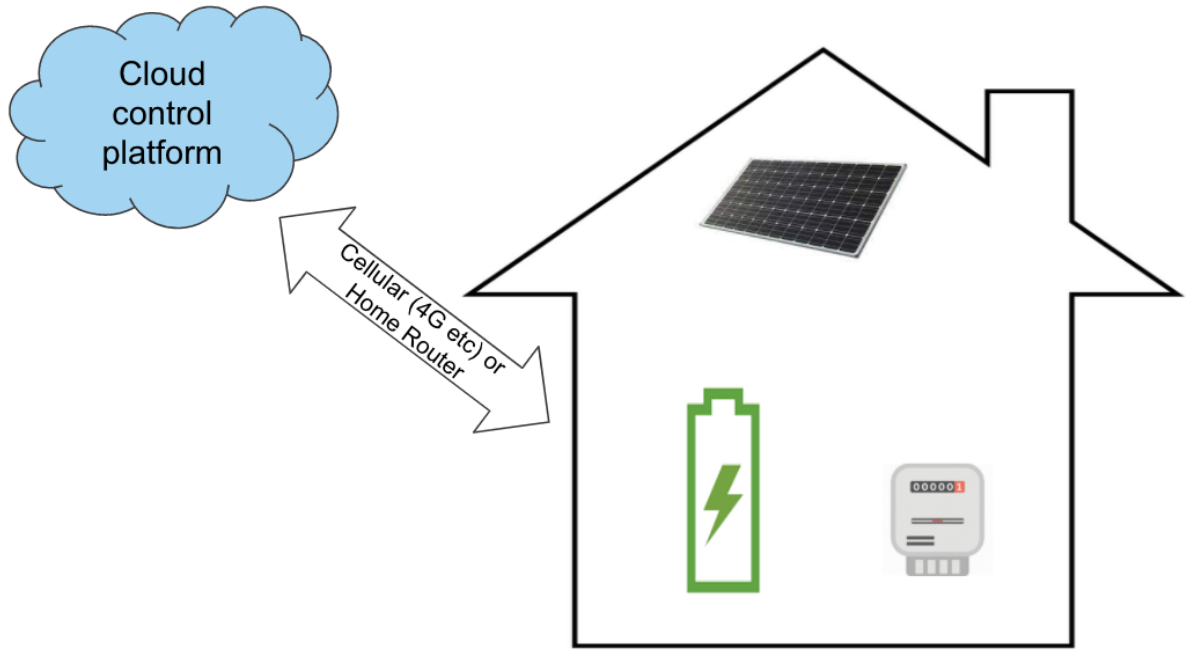

Figure 4: Control architecture for remote ESS control

Figure 4 shows the simple system diagram for this use case. There is no Moixa hardware onsite with the ESS, and control and telemetry go through a 3rd party server in the cloud.

Key points - Moixa has integration experience with a number of ESS systems and whilst some support the model described in core use case, others do not.

One of the most significant variations is that the way any OEM has defined their local control modes has a major impact on how it is made conformant with the Moixa data model. For instance if no locally supported variant of balance mode is possible then it will be necessary for the cloud to push far more regular commands to the device. Or it may not be possible for the device to accept time limited plans, and as such each individual operational change must be pushed to the device, one by one.

This will result in many more plans being generated and received by the device, considerably increasing the network traffic required.

Assuming a control scheme can be found whereby the system is conformant with the Moixa data model then the system will be operated as described in the core use case, in terms of how control is executed.

Telemetry data is typically routed to the crowd and then on to Moixa via API, and will be of similar volumes to that seen for Moixa devices, or 30 second to 5 minute data.

ESS+EVSE (UC2)

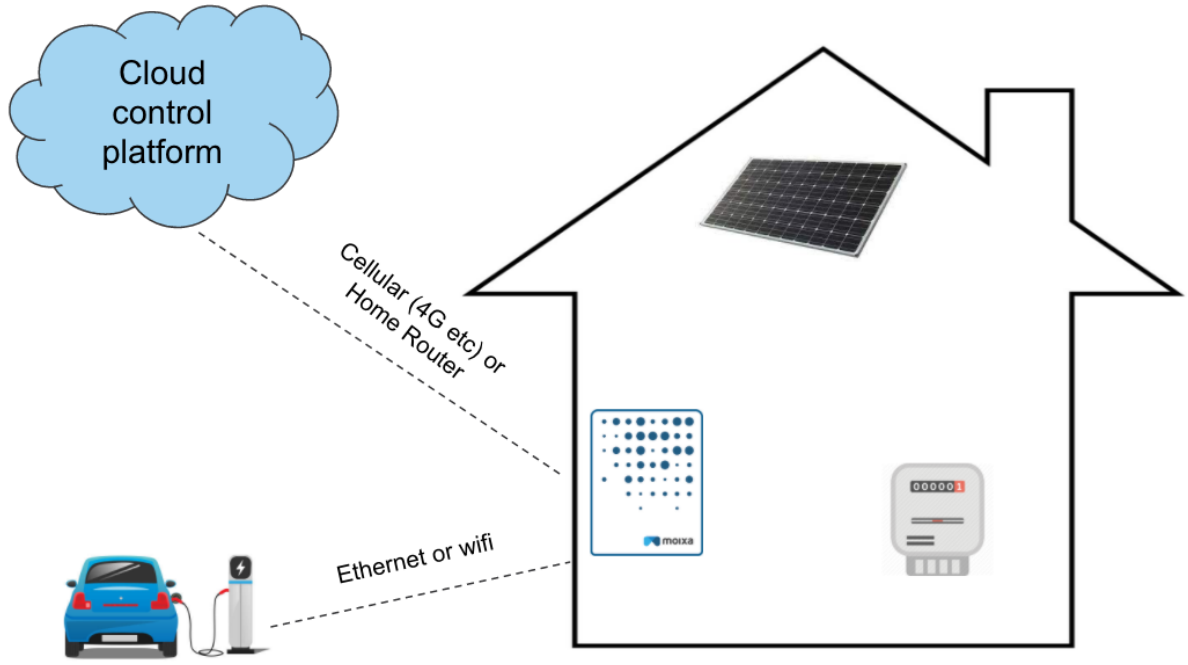

Figure 5: Control architecture for battery and electric vehicle charger

Figure 5 shows the simple system diagram for this use case. There is Moixa hardware onsite.

This use case is operated identically to the core use case with the exception that the control hub in the battery is orchestrating both the battery inverter and the EV charger at the same time. Each device will have a separate control plan, based on the appropriate predictive models, however there will be coordination between the two.

EV CONTROL VIA SMART EVSE (UC3)

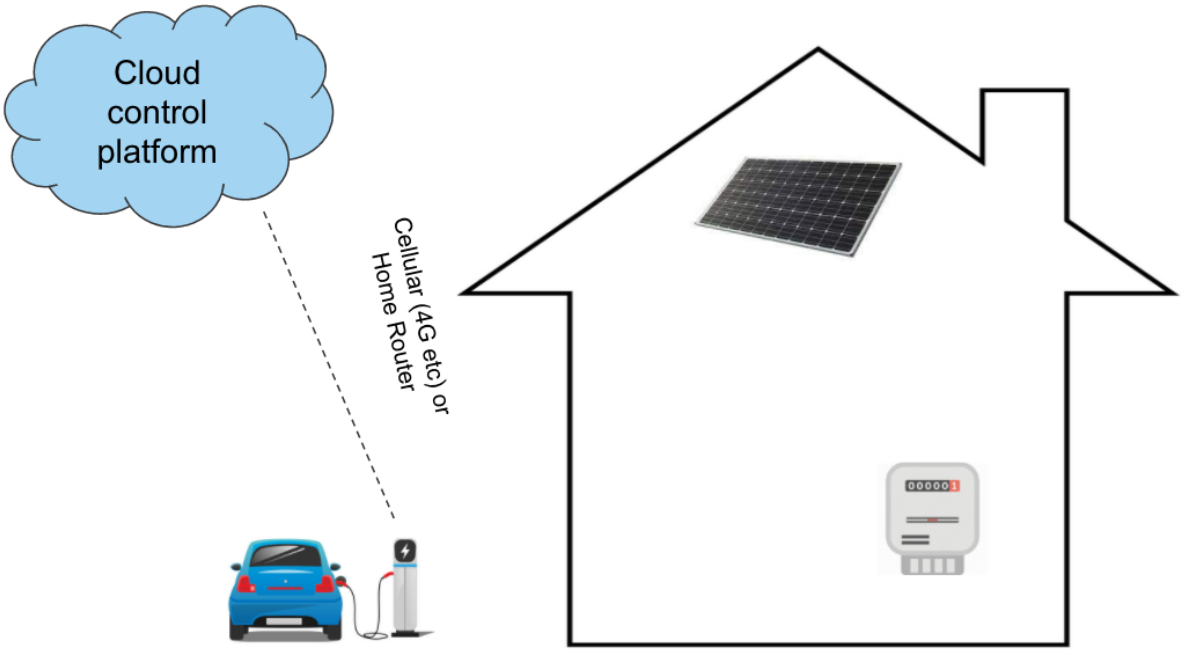

Figure 6: Control architecture for remote (CPO type) electric vehicle charger control

Figure 6 shows the simple system diagram for this use case. There is no Moixa hardware onsite, and all communication is via CPO-EVSE link. This is a typical setup for one of the core control options for managed EV charging, most likely a cellular connection to the cloud for reporting telemetry.

As EV charging events are limited in number and telemetry is less verbose, this data channel does not require as high bandwidth as more complex systems. It is assumed that the charger is being communicated with via OCPP, and the standard control set is available. This limits the type of controls to essentially proportional load control of the charger.

It should be noted that the EVSE is not in control of the charging here, and can be overridden by the vehicle telematics, i.e. if a charging session is terminated. Until more standardization, particularly ISO 15118, are rolled out across auto OEMs and EVSE OEMs, this behavior will make the control scheme something that cannot be relied on comfortably.

EV CONTROL VIA TELEMATICS (UC4)

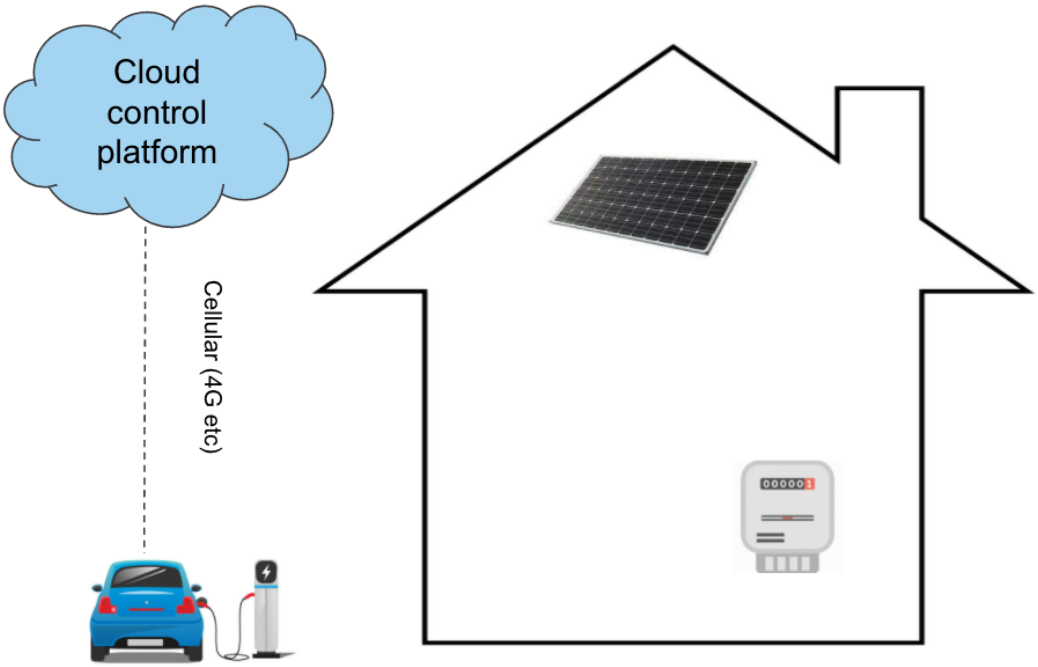

Figure 7: Control architecture for remote EV control

Figure 7 shows the simple system diagram for this use case. There is no Moixa hardware onsite, and all communication is via the EVs telematics system.

In this use case control of the EV charging is handled via the cars online telematics system. This could be linking back to the auto OEM directly, or an appointed 3rd party who has integrated with the telematics or is appointed to do aggregation, such as in the case of OVGIP in the United States. Alternatively it could be the customer app setting schedules (or being spoofed by a 3rd party), and thus allowing smart control. The EVSE attached would obviously need to conform to smart metering standards but given current vehicle-EVSE communications would be unable to manage charging if the vehicle were set to a differing schedule.

MESH NETWORK (UC5)

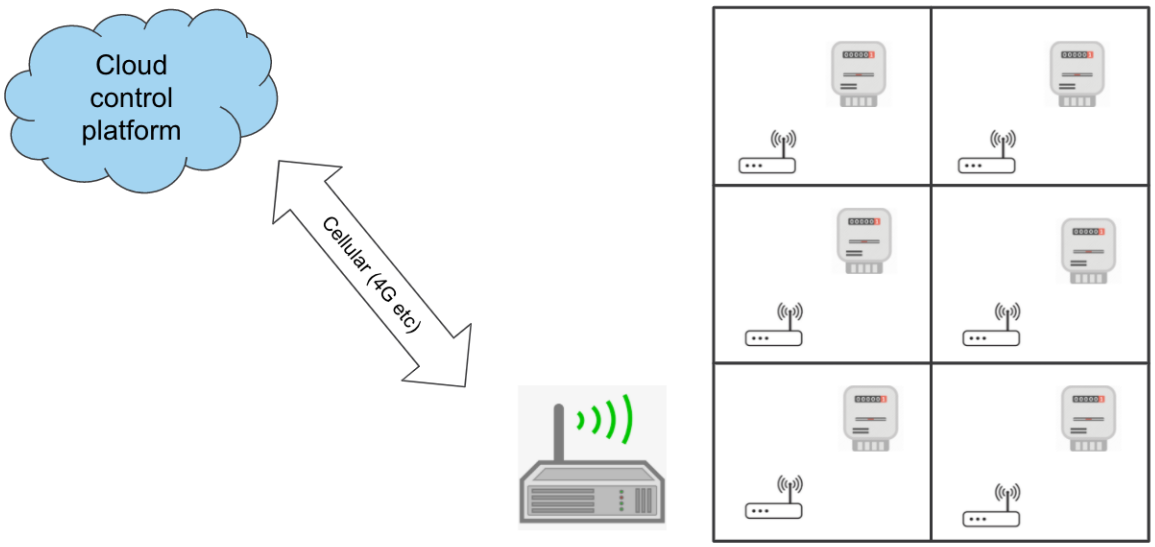

Figure 8: Control scheme for a Mesh Network

Figure 8 shows the simple system diagram for this use case. There is no Moixa hardware onsite.

In this use case a zigbee (or alternative) mesh network is deployed across a set of geographically close properties, such as a tower block or a village. A single gateway provides connection for all systems back to the cloud, and relays commands and telemetry. It is assumed that in the majority of cases the individual devices are installed behind separate boundary meters, and therefore separate smart meters.

Telemetry is at considerably lower data volumes than for the battery use cases, and command will only be issued, in most cases, if the event of a change of tariff plan and usually much less than once a day.

Each piece of switching equipment is relatively low cost compared with an ESS or EVSE however there is perhaps more opportunity to conform with existing technology such as HCALCS.

4.0 SAPC integration Options

Referring back to figure 1 which shows the system architecture for the smart metering network a control provider such as Moixa would need to map and understand how messages are are managed at both ends of the network

During the project Moixa reviewed the potential of integration with a SAPC device with their manufacturer SLS.

The functionality, from a smart control perspective, that would be possible is reasonably equivalent to that provided by an HCALC with several notable differences;

- The unit is stand alone allowing the possibility for it, or some future derivative of it, to be included physically alongside a smart device
- There exists alongside the possibility to use a proportional load control value (0-100%) the ability to use some additional characters in the messaging format. These could theoretically be used to convey more complex information

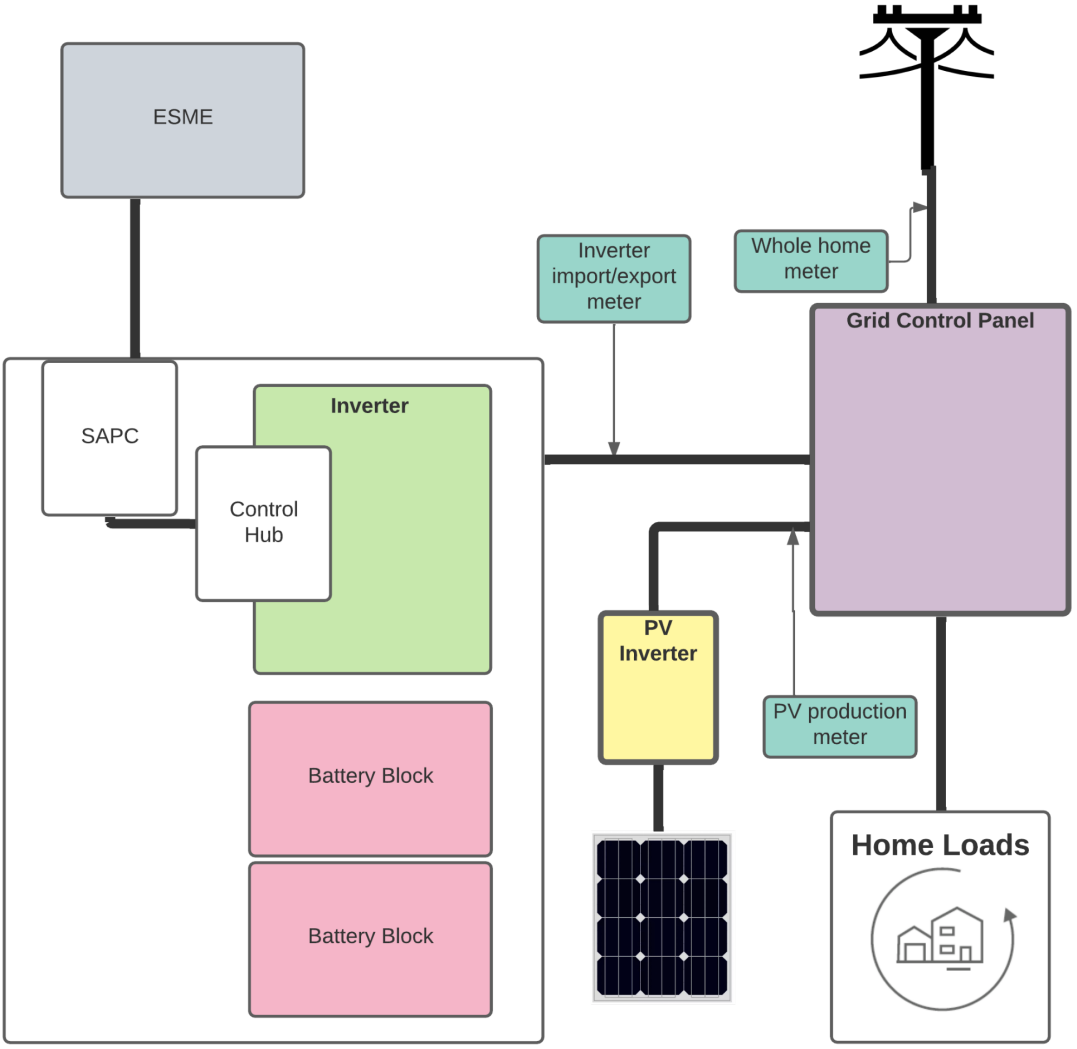

Figure 9 describing the integration of a SAPC device

SUPPLIER SIDE INTEGRATION

If the challenges of passing a message from the physical smart meter to the DER can be met then the other end of his loop must be addressed. On this front the examination done in the project has been less fruitful.

The platform control end of the system still remains a complex problem, the solution to which will require cross industry agreement on a standard approach. Currently companies such as Moixa are faced with a high barrier to entry in terms of cost to integrate and complexity of contractual frameworks required if they wish to serve their whole customer base and remain supplier agnostic.

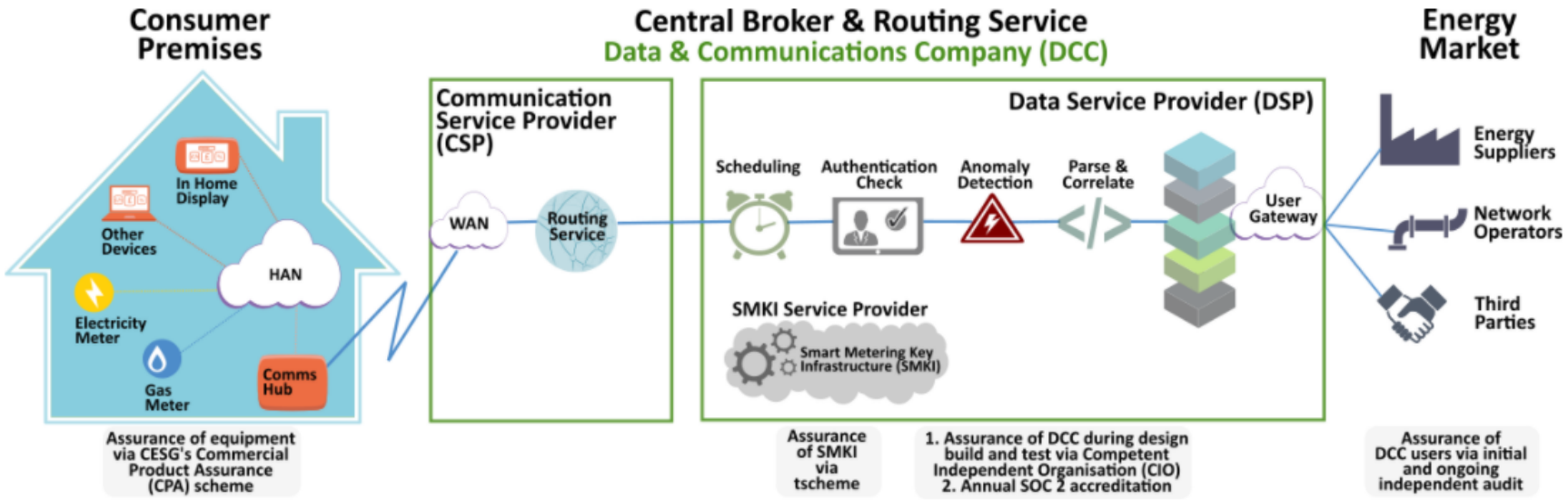

figure 10: DCC communication system schematic from ref;

The requirements for connecting as a third party to the DCC DUIS are onerous especially for small businesses, with difficult or expensive to implement technical specifications and high bars for cyber security needing to be met.

Once these are met the actual functionality that is available to a third party is unclear and seems primarily limited to trials at present. As what the project is trying to achieve essentially replaces one part of any given organization's key infrastructure with the DCC platform it is hard to commit to that without confidently being able to fully map all functionality.

Additionally, for a non-supplier the requirements for being able to consistently access devices connected via the smart metering network involves considerable interaction with an end users supplier. Some of this interaction needs to be triggered by the end user themselves. An example of this would be switching customers to be half hourly settled where many suppliers simply would not support it, and for those that do the process is bureaucratic and slow.

5.0 Use Case Analysis

When looking across the use cases and mapping this to the options for integration a number of key factors have been considered which are outlined below;

Physical integration constraints

The fact that the SAPC device is stand alone allows for more options and seems the most appropriate for integration with a 3rd party system. It also paves the way for a perhaps longer term approach where OEMs can be supplied with a set of standard components to include in a BOM. In the core use case UC1 we have the most obvious strategy whereby a SAPC, or future device, is physically integrated into the design of the system at manufacture.

The current understanding of how this would be achieved is that the SAPC would need to be fully incorporated into the physical form of the smart device such that it could be deemed the tamper protection boundary was not compromised. The SAPC would then be connected to a serial port on the device, to allow communication, and facilitate communication back to the DCC.

When compared to the integration path that was considered when using an HCALC then there are notable advantages but from an OEM perspective there still remains the need to allow provision for a 3rd party device to be securely fitted into your product. This has implications for form factors that would likely have major design implications if the UK requirement were notably different from those seen internationally and require the inclusion of significant additional electronics. This raises the need for standardization on how such components are designed and manufactured.

Below are some observations regarding the other use cases;

UC2 - The integration strategy would be the same as for the ESS, however there is an open question as to whether a single coordinating node could control multiple systems without the need to secure each individually. As noted the control scheme here works by setting separate plans for each device and coordinating this at the grid edge. Therefore having parallel communication channels from separate SAPC devices would be challenging.

UC3 - The same challenge would be faced as for the battery with the cost of integration needing to be borne by the OEM, and the lower the total BOM cost the higher the proportional cost of securing the equipment. Additionally there is a question of SAPC to ESME communication as many EVSEs are installed at some distance from the main consumer unit and IoT connectivity is always a challenge over longer distances.

UC4 - The challenge here again seems to be that any device would need to be fully integrated with the vehicle, and again standardization will help. Additionally the parking location of the vehicle would be a problem, as it would be difficult to guarantee good

communication back to the ESME. The other workable solution here seems to be that the EVSE is enabled and can overwrite any EV enabled commands.

UC5 -The main question arising here is cost, if you are installing relatively cheap control switches as part of a Zigbee mesh across a block of flat connecting each one to a SAPC (or equivalent) will be a major challenge. Therefore again a clear set of standards and integration options for OEMs will be key.

Cloud Infrastructure

The access route for the Third Parties as described in figure 10 is complex and expensive currently and there is no clear path for a company such as Moixa to enable any of the functionality or architectures described above. This would be common across all of the use cases considered to a greater or lesser extent.

Considerable effort needs to be made to agree and then implement a centralized infrastructure and market model that would allow access to smart meter enabled DER for organizations with different business models.

As much as possible evolving standards such as OADR should be leveraged to lower barriers to entry. Minimizing the number of connections that a flexibility participant needs to maintain to participate should also be a key consideration.

This feedback will be common to all use cases considered as in all cases a central aggregator cloud platform collates the data.

Bandwidth, data volumes and messaging complexity

As discussed above the data transfer requirements alone are orders of magnitude different between the requirements of how DER aggregators typically monitor their systems and what is possible using the smart metering network. Even a very simple switch use case, such as a hot water tank, would require more bandwidth and with far lower latency to understand and manage the amount of flexible capacity that was available and online for any given flexibility service. Without this you are reliant on another service to provide this data.

Therefore it will, in nearly all cases, be necessary for an aggregator to maintain a parallel channel to extract telemetry from devices at required data rates, and that this cannot be

supported using the smart metering network. This would be common for all use cases considered in this document.

Far fewer control signals are sent on any given day so there is more scope here for using the network. For simple use cases, such as an “charge now” or simply scheduled EV charger then the use of SAPC messaging seems more plausible, i.e. for Use Case 3. A flexibility request could be made to simply dial up or dial down the charging by a percentage, visibility of the response is still in the blind however the command could be sent.

However, once the complexity of both the device, such as an ESS in Use Case 1, or the complexity of the energy system in the home, such as in Use Case 2, increases the requirement for regular and often complex command signals increases. Typical command sets, or “plans”, as outlined above will run forward for several days and will contain a structured set of conditional commands for the local system to interpret. This makes the use of the network less and less viable as an option for sending commands.

Beyond this is the key ability for OEMs to be able to push firmware updates to IoT devices, these are often large packets of data and there seems no solution but to maintain a separate communication channel.

Other applications

Through the project several other possibilities to interact with the smart metering network have come up. These are either realizable now, or if they could be made possible would greatly improve the reusability of the network.

- Tariff extraction - being able to read a customers tariff from their smart meter, or from a CAD supplier integration would improve the amount of administration required for end customers or a subject they are often not particularly informed on. Additionally a centrally maintained register of tariffs to compare against.

- Data Extraction via CAD - Being able to extract finer resolution meter data from an integration with a CAD supplier. This would allow an aggregator or smart device provider to calibrate their meter data with that recorded on the fiscal bill. This would remove issues with verification of savings based on two separate sets of metering reporting on the same thing. For this example and for the tariff example above any improvements to how a customer can set this up, and allow Moixa or equivalent, to extract this data without undue administrative effort would again greatly improve engagement.

- Standardized metering - The smart meter system was installed with a standardized set of meters, potentially just CT clamps, of fixed accuracy. These would be used to monitor home consumption, local renewable generation and any installed devices (if not supplied on their own). This would mean that all smart devices in the home had a single reference point for optimizing energy behavior without installing multiple meter sets. It would also mean that all flexibility actions taken by the site would have metering data on which the grid actors (DSO, TSO, utilities) could agree on the standardization of.

Alternate Business models

It should be noted that this report has not considered in detail the potential for other business models than those supportable by Moixa. However it should be noted that if the intended structure was more top down in it's approach to domestic DSR then the smart metering network could offer potential for allowing this.

An example of this would be a DSO level organization having connection into sets of devices that have simpler on/off operational modes such as;

- electric vehicle chargers
- hot water tanks
- storage heaters

Triggering turn down events to ease network congestion would be a viable option here. They would then be able to monitor this with substation metering. The challenge of compensating customers for the use of their systems would still require some mechanism to complete however there are alternatives to metering data that could be used for this.

Other options for business models based on the use of the smart metering network will likely exist but would fall outside Moixa's current capabilities and so have not been explored in depth.

Integration Options Summary

To summarize the review of the considered use cases against potential integration with the smart metering network the prospects of a deep integration where large parts of the existing aggregator IoT infrastructures can be replaced seems highly unlikely without a major upgrade to the capabilities of the network.

Some lighter data requirement use cases, with simpler technology can likely be supported however they have not been explored in depth during the project.

The peripheral use cases described above all seem like plausible options to improve product offerings and service to end customers but they do not address the core aim intended at the start of the project.

The next section deals with a more specific use case of using the smart metering network to add additional cyber security to the service.

6.0 Cyber Security Implications

The most pressing topic to emerge during the project is the suggestion of using the smart metering network as a method for securing distributed energy resources being used for DSR.

This becomes particularly critical when a level of scale up is reached and the volume of power under control reaches what would be considered Critical National Infrastructure, CNI.

Various options have been discussed across the industry for use of the smart metering network to allow DER aggregators to meet the cyber security requirements of the future gri. These all involved leveraging the smart metering network, to a greater or less extent, to help secure these devices.

These proposals range from complete centralisation of all control to a set of standards to which all aggregators should comply, a more decentralized approach.

This document will not address the decentralized approach other than to note that the suggestions laid out in the documents seen by Moixa of attempting to base this on standards such as PAS 1878/9 and OADR would make access for aggregators more straightforward. It should also be noted that this decentralized approach is Moixa's preferred course of action and will have the least disruptive impact on businesses like Moixa.

Below is presented two alternatives for how the smart metering network could be utilized if it were deemed not possible to find a set of standards that would be both acceptable to NCSC and possible for aggregators to achieve operationally and in a cost effective manner.

Both are long term developments however and would require additional projects to prove them out before serious work could start,

As has been established in the above section looking at the more general full integration use case it is suggested that with most solutions a parallel communication channel will need to be maintained alongside any smart metering implementation. Therefore the two proposals outlined below are focussed on how the smart metering network could potentially be used as a security strengthening measure.

The National Cyber Security Centre, NCSC, has started a Smart Energy Information Exchange, which Moixa will be a member of, enabling future discussion of this. This will commence later in 2022 and Moixa intends to continue the discussions laid out in this document through this forum.

Proposal 1 - Control Override

This proposal assumes that the primary DER communication channel from the aggregator to the device will be used for sending all commands, as has been outlined in the use case descriptions above.

However it will propose that all DER being installed in the UK that are capable of a certain level of functionality are required to be connected to a SAPC, or other stand alone device. The criteria for what qualifies as a device under these terms should be reviewed carefully, as it may not require every smart appliance to need it, potentially only a central coordinating node device would.

Using an agreed standard, a centralized body would have the option to disable or take control of the device in the event of an emergency, extreme event or behavior that triggers an alert in something akin to the "anomaly detection" functionality coordinated by the DCC.

This requires integrations at two places, one at the device level to allow communication which would take place as described above in section 4.0 and one in the cloud as is discussed below.

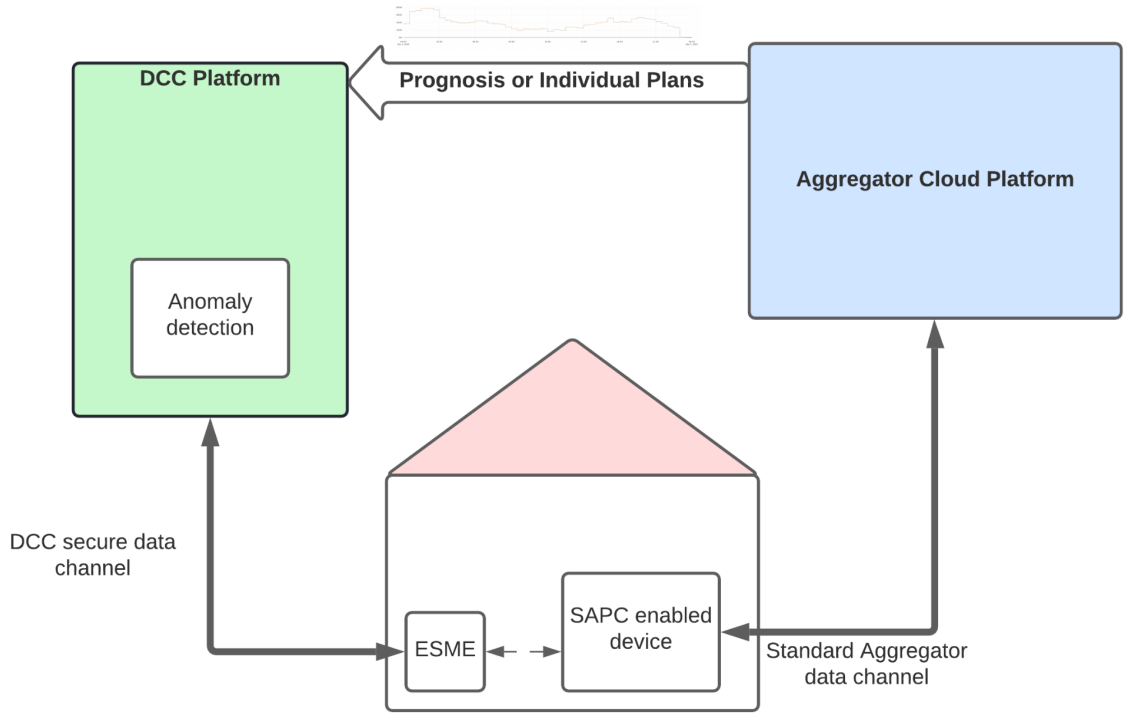

Figure 11: Simple diagram of architecture for proposal 1

The response taken by the central body could then be informed by what the devices are expected to be doing. Some typical operational modes are described below;

- Flexibility services - all devices enrolled in TSO/DSO services or being operated on behalf of a supplier could be registered and their expected and allowed behaviors understood by the central body
- Tariff optimisation - even the most extreme tariffs on the market, such as Octopus Agile, do not vary that wildly in the timings of their behavior. Therefore overnight plunge pricing or evening peaks could again be understood by the central body
- User control - If end users are coordinating their own device behavior it is unlikely to cause large scale correlated effects, unless driven by tariff. In which case this can be seen as a subset of the above case
- Major firmware releases - Major software releases to the edge are generally staged and tested carefully however at some point a whole fleet release is required and if an unknown bug is detected then this could cause anomalous behavior across a group of devices

Cloud side integration approach

One of the key questions to answer if all device control communications are not being routed through the smart metering network is how threat detection is being handled; who is monitoring and how?

There is an open question as to whether it would be possible to build a system that could monitor and manage device commands across all DER installed in the UK even if they were all routed through the same channel. Would this need regionality, or would it need to be UK wide? Clearly the bandwidth and processing power of such a system would be considerably larger than what is supported by the smart metering network currently.

However given we have established this seems impractical there is then the question of how any Central Monitoring Body, CMB, could review the device commands being sent by aggregators. Moixa employs the principle of a “prognosis” which is a concept defined in the USEF, Universal Smart Energy Framework, standard for the forward prediction of a group of sites including the actions being taken by any DER and PV and consumption predictions for instance. This typically runs ahead for around 48 hours and would give a baseline from which unexpected departures could be monitored. This however incorporates predictions of site load and local generation which are not 100% accurate.

This could be published to a centralized body for whichever groups were of interest to allow for monitoring to take place. Groups could be based on assets known to be taking part in grid service programs, for instance, or those enrolled with particular assuming a centralized registration process for these could be established.

This connection would also require securing, and guidance would need to be given to aggregators on how this could be achieved. However as this would strictly be a one way publishing service this is a likely easier thing to achieve.

IEEE 2030.5

Taking this approach would also imply that all devices conform to a specific standard for device level communications with the SAPC device. When assessing the choice for this it would make sense to look at standards that are gaining international traction and provide the needed functionality.

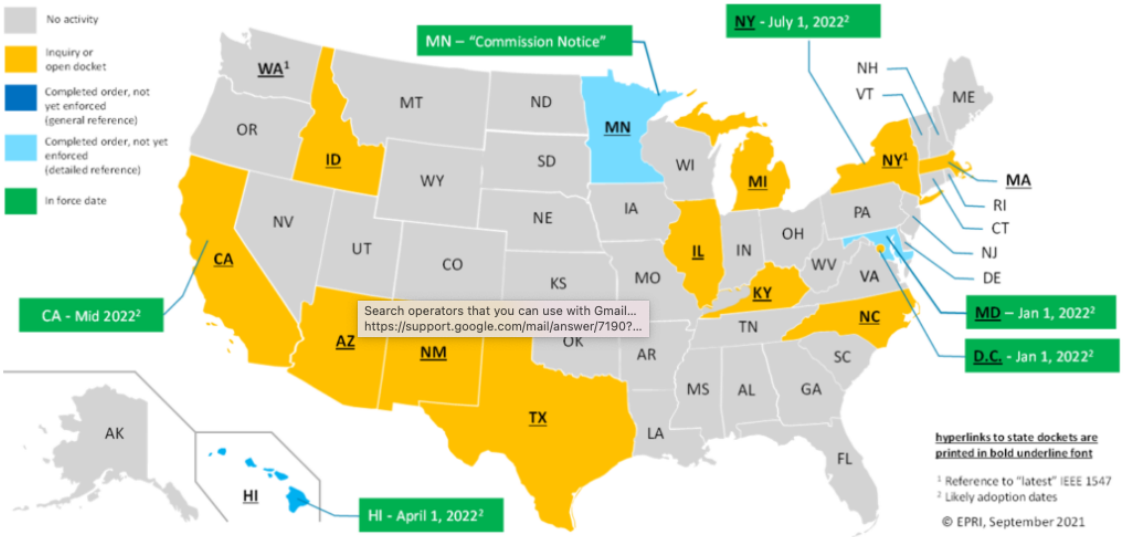

Figure 12, Rule 21 (IEEE 2030.5) usage across the US

IEEE 2030.5 (and IEEE 1547.1) fits the bill here in that it is now widespread across the United States, see figure 12, and is in active use for all new DER planned to be deployed in California. It is also gaining international traction with Australia recently adopting it for grid connected inverters.

IEEE 2030.5 provides a number of functionalities in it's full implementation, including telemetry and device statuses. However in California it provides a way for the Utility level actors to set response curves on devices under which they will behave in the event of a grid instability, i.e. frequency instability.

The use case being suggested here is in fact not one of the core use cases being used at the moment however having reviewed the standard with expert partners it seems there are possibilities for how this could be implemented. The standard contains (in section 10) the DER Control Function Set, and one of these commands "Cease to Energize" would effectively shut the DER down and prevent whatever plan.

2030.5 commands have attached to the a primacy allowing the device to interpret which should be followed first, and so a command could be issued to supersede all other commands the device was currently responding to.

Proposal 2 - Plan Validation

Proposal 2 acts in a similar fashion to Proposal 1 but the level of scrutiny being applied is extended down to device level commands. The integration pathways described in proposal one would still need completing in that;

- the device would physically be connected to the smart metering network
- The aggregator would be integrated with the CMB

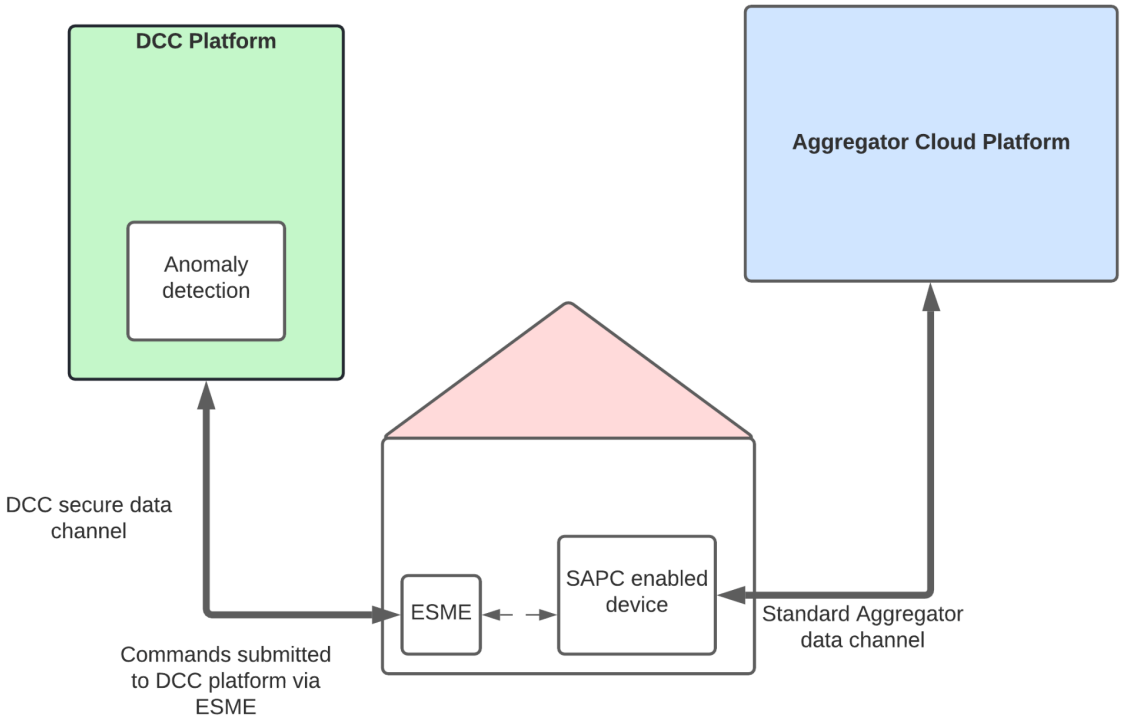

Figure 13: Simplified architecture for proposal 2

Plan submission

Every time a new plan was generated and pushed to a device then it would simultaneously be transmitted to the CMB.

This could be achieved in one of two ways. Either the secure channel described in proposal 1 could be used to submit device by device level plans to CMB for them to run through the anomaly detection. Alternatively plans can be transmitted back to the DCC via the SAPC-ESME link. This would require modification of the currently used messaging format to allow for this additional data transmission.

The monitoring body can then run all the received plans through it's anomaly detection algorithms. If anything resembling a threat is identified then the same methodology as described in proposal one could be used to deactivate the affected systems. Ideally this would again be achieved using a standard such as 2030.5 to avoid OEMs needing to maintain multiple territory bespoke firmware versions.

Key questions to answer

There are considerable questions to answer here around the processing capabilities and bandwidth needed to achieve this as a functioning system, as it would be a large undertaking. Whether the DCC could support such infrastructure without incurring significant costs is to be seen, but it would require careful testing before being mandated.

One key factor that requires answering is the latency between a plan being submitted to the CMB and that plan being deemed safe. For daily tariff plans then some latency would be of little consequence as they are often submitted ahead of any actions being required. However for live management of a grid service then any additional latency is likely to be a serious problem. This begs the question could some devices be exempted under these grounds and plans be allowed to be transmitted directly from the aggregator without review.

Additionally it would be suggested that the same information around tariffs and grid service program enrollment could be used to understand what an expected behavior and baseline looked like.

7.0 Smart Home/Smart Grid architectures

The final area this report will review is how the proposals laid out in this document fit with both the PAS 1878 and 1879 as well as smart energy frameworks being developed internationally.

PAS 1878 and 1879

The proposed UK standards PAS 1878 and 1879 deal with the interactions of Energy Smart Appliances (ESAs), with each other and the grid. This report has referred to ESAs as DER as the term is more common internationally, however then can be considered interchangeable for this analysis. This section is a brief summary of how these standards fit with both the proposals above and the wider aim of leveraging the Smart Metering system.

Figure 14 shows the simple logical diagram for the two standards, and as can be noted interactions with the Smart Metering system are envisioned at similar places.

The home/grid boundary line can either occur between the DSRSP-CEM or between the CEM-ESA. For instance in the core use case the CEM is likely to be the control hub of the battery, whereas for an telematics controlled car it would be in the cloud.

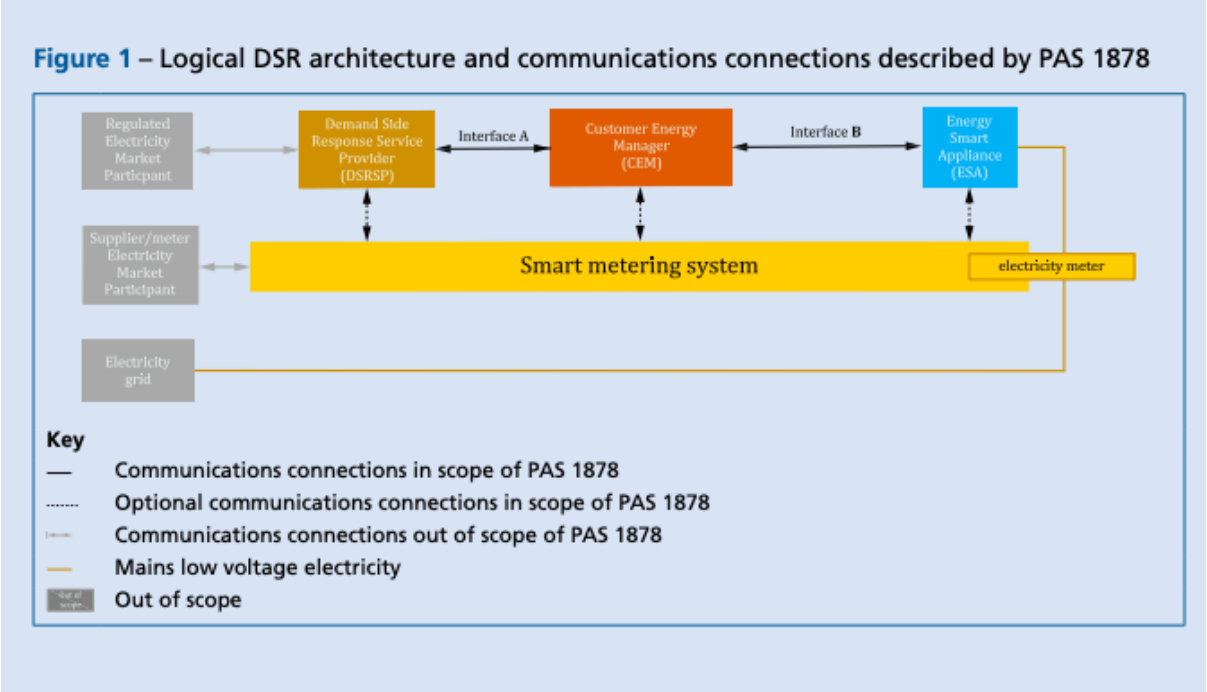

Figure 14 (figure 1) from PAS 1878

Figure B.1 – Single DSRSP controlling multiple ESAs via multiple CEMs for on-premises and in-cloud CEM configurations

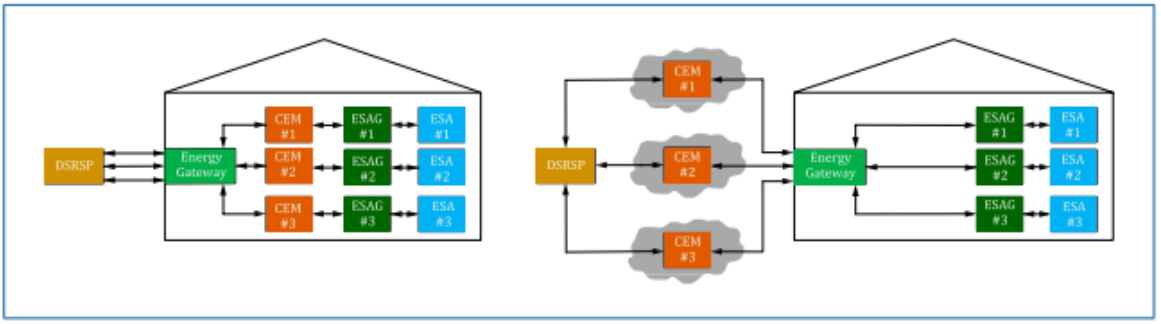

Figure B.2 – Multiple DSRSPs each controlling their own set of ESAs in a premises

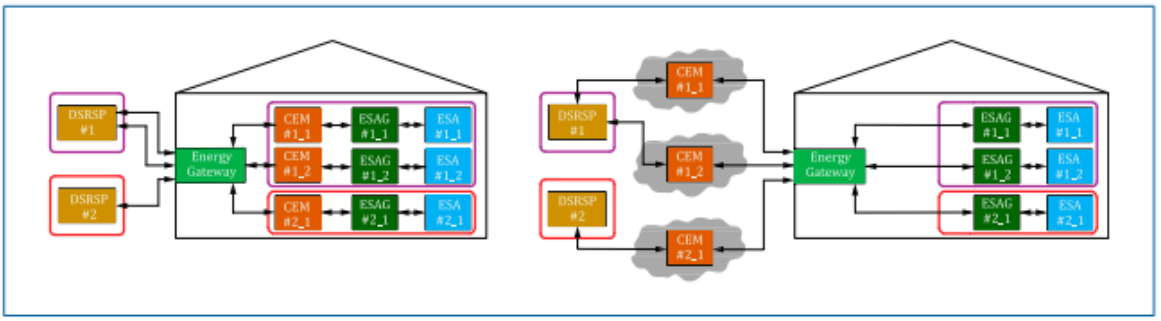

Figure 15 (figure B.1 and figure B.2) from PAS 1878

Figure B.5 – Multiple and/or premises level energy management using "single ESA" CEMs and a HEMS

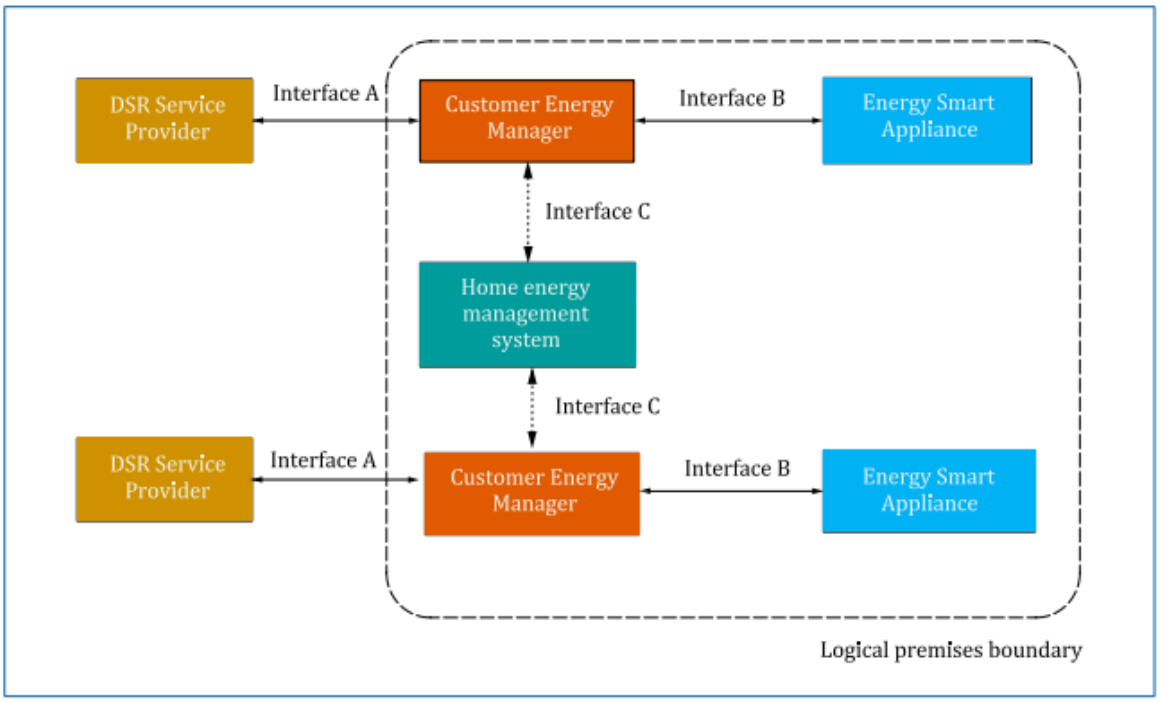

Figure 16 (figure B.5) from PAS 1878

Figures 15 and 16 show different potential configurations which PAS 1878 envisages ESAs interaction with each other and the grid. In every location where we have intersection of lines from ESAs, either a Home Energy Management System (HEMS), or Energy Gateway there is the potential for ESA level instructions to be updated, or a new plan generated, and as such a need to interact with the Smart Metering network if any kinds of device security was being employed.

As discussed above the key limiting factor of the smart metering network is it's bandwidth and ability to complete many processing actions quickly. It therefore seems a challenge to marry these two concepts.

On a more general level the concepts outlined in these standards align well with the architecture deployed in Home Response and the use cases described above can be mapped into these schemas without undue modification required.

Moixa has experience working across Japan and also the US and as such is aware of the emerging standards in these markets. Some notes are added below, and have been split between those governing devices operating in the home and connection to the grid and then those governing the grid infrastructure and market actors.

USA

The US market is generally led by the innovation that takes place in California and most of the early regulation and policy changes are tested here before being propagated to the rest of the county.

Smart Home

IEEE 2030.5 and IEEE 1547.1 are both becoming standard to allow Utility - DER communication and control, as noted in the above section on IEEE 2030.5. However whilst it is a requirement for all new grid connected DER to have a IEEE 2030.5 client and to produce the data mandated by IEEE 1547.1 in every case known to Moixa the OEM maintains a secondary connection for telemetry and control.

Moixa's analysis of the control points available over IEEE 2030.5 indicate that while some smart control could be offered then the full range of functionality described for the core battery use case cannot be mapped completely. Therefore either a secondary channel would need to be maintained or a more limited, but potentially still valuable, set of control options could be offered.

A second set of standards that are gaining traction here are published by the Connectivity Standards Alliance, namely Matter and Smart Energy.

These do not try to specify the unit specific actions, but instead act as a transport and certification layer between all devices conforming to a specific standard. This would work well with some of the concepts laid out in PAS 1878, and could govern the communication between ESA.

Smart Grid

There are a number of emerging standards across the US governing the communication between the utilities and the various grid actors.

Open ADR 2.0b is being explored by many utilities as the mechanism for communication of grid service signals with aggregators. It's a well known standard and it is noted that PAS 1879 references it as a potential route.

IEEE 2030.5 also includes a standard for cloud to cloud communication between servers, hosted by the utility and an aggregator. This is not in common use in the US, with only communication to assets individually larger than 1MW mandated to happen in this way. It is unclear at present whether this will see further roll out as the backbone infrastructure standard, or whether it will remain only to be used for top level device control when required.

DNP3 is also gaining traction as it is commonly in use with Utilities already for the management of large C&I scale sites run by SCADA. As these units have typically been the first to access grid service markets, some for decades, then this path represents a lower cost option for utilities without the resources to enact a major digital transformation of their business processes. It's usefulness in applications involving many thousands of residential sites is as yet unproven.

Japan

Japan is in the process of opening it's grid service markets to residential scale assets with the first trials happening in recent years. However they have reasonably well accepted HEMS standard called ECHONET Lite which allows operability between batteries, HVAC, EVSE etc.

Smart Home

ECHONET Lite is an advanced and mature mesh network that allows devices that participate in it to interact with each other using common interfaces. This enables the implementation of concepts such as the HEMS (Home energy management system) for the whole household. For instance a device control unit with an ECHONET communication layer installed in a home with multiple devices on an ECHONET domain and with the appropriate software it would be able to optimize for all of them at the same time (batteries, EVSE, HVAC etc). The devices can communicate wirelessly or via ethernet and after the initial configuration to join the subnet has been done everything else (finding other devices in the network, configuring oneself, etc.) happens automatically.

The full potential of this standard is only starting to be explored as more complex use case interplay (BTM optimisation, grid service, natural disaster resilience), but it is a promising potential backbone.

Smart Grid

Open ADR 2.0b is also looking likely to be the standard for communication between grid side actors and has been commonly used by all the participants in the trials conducted so far.

Additionally Japan has launched a wide ranging initiative called Society 5.0 which seeks to define a set of standards and frameworks for governing life in a distributed world. Moixa is

already starting to see the first impacts of this in the cyber security frameworks that have been suggested to govern the upcoming grid service trials.

8.0 References

https://sagroups.ieee.org/scc21/standards/1547rev/

https://www.ncsc.gov.uk/files/CPA-SC-SAPC-v1-3.pdf

https://www.ncsc.gov.uk/information/the-smart-security-behind-the-gb-smart-metering-system

https://www.bsigroup.com/globalassets/localfiles/en-gb/energy-smart-appliances-programme/pas1878.pdf

https://www.bsigroup.com/globalassets/localfiles/en-gb/energy-smart-appliances-programme/pas1879.pdf

https://csa-iot.org/all-solutions/matter/

https://www8.cao.go.jp/cstp/english/society5_0/index.html