energy
taskforce

Work Package Three:

Smart Charging Technical Requirements

allocated bay
the charge point or enter the
point reference number into your app.
3. Follow the on-screen instructions to charge
your vehicle

Office for
Low Emission
Vehicles

CATAPULT
Energy Systems

LowCVP
Low Carbon Vehicle Partnership

Contents

1 Introduction

Introduction

The Electric Vehicle Energy Taskforce [1] was set up to address a range of questions related to meeting the demands of the wide scale adoption of Electric vehicles (EV) on the electrical networks. The Electric Vehicle Energy Taskforce established four Work Packages to consider the following issues:

- Work Package 1 - A common strategic understanding of the requirements of the energy system to support mass EV uptake.
- Work Package 2 - Engaging EV Users in Smart Charging and Energy Services
- Work Package 3 - Smart Charging Technical Requirements
- Work Package 4 - Accessible Data for Decision Making

Work Package 3 was asked to focus on the technical requirements for smart charging, all forms of charging were in scope. In the Section: Response to Specific Questions you will find the specific questions set for Work Package 3 and it's answers in summary. The key objective for Work Package 3 was to ensure that Distribution System Operators (DSOs) and possible Electricity System Operators (ESOs) can send signals to market participants that will reliably result in modifications to EV charging patterns, allowing them to minimise the need for costly network reinforcement. Work Package 3 recognised that this should also consider support of load management in response to energy availability. The question of whether there are sufficient incentives for consumers to respond to the signals was considered outside of the scope of Work Package 3; the group simply focused on ensuring that there were the technical foundations to support this service.

Work Package 3 identified four key themes during its work, these were:

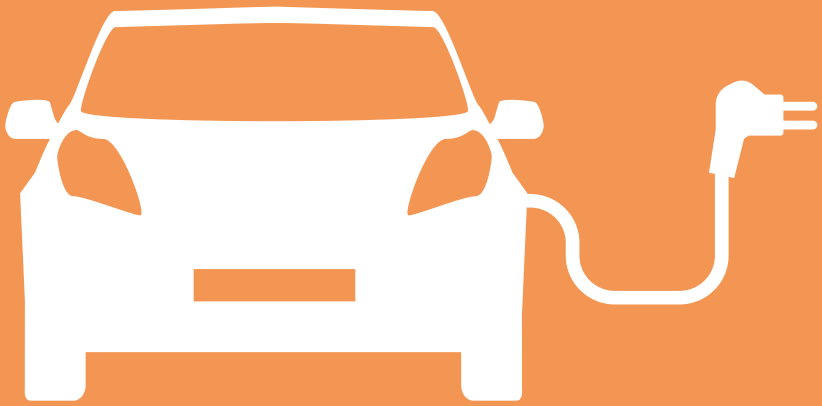
- Minimum technical requirements for smart chargers.
- Cyber security and data privacy.
- Interoperability.
- Flexibility.

Work Package 3 has managed to address many of the questions set for us. There are some exceptions to this:

There was insufficient time or suitable governance in place to carry out a detailed technical analysis, so our recommendations are limited to government and industry setting up the necessary governance and technical groups to agree detailed requirements.

We could not find consensus on the issue of chargepoint operator (CPO) interoperability; that is the freedom of a customer to switch the operation of their chargepoint (CP) from one CPO to another without having to replace the CP or for a technician to visit the site. There were strong arguments for and against this capability while the market and technology are immature, and about whether interoperability would reduce the value of the CPO market. The Work Package 3 proposal is to defer mandating CPO interoperability at this time but to begin developing suitable standards and certification regimes that would support CPO interoperability.

2 Context of Work Package 3



Context of Work Package 3

Aims and objectives of Work Package 3

The aim of Work Package 3 has been to gain a common strategic understanding of the functional requirements of smart chargers to support mass EV uptake and market and technical innovation.

Scope of work, what is in/out of scope

It is important to note that from the beginning of this work the minimum requirements have been developed as a response to the provisions included in the Automated and Electric Vehicles (AEV) Act 2018. The Act only has powers to set requirements for CPs, and this has limited the scope of the requirements set out here. It later became clear that setting the technical requirements more widely, for instance to include the vehicle, might deliver better results for the user. To examine how this might be developed the SMMT circulated a questionnaire to its members to understand the position of stakeholders on industry agreements outside the scope of the AEV Act. Elements of the responses of

Description of methodology used and references to previous work

This section sets out the process that WP3 followed to develop its recommendations. Work Package 3 has been led by the BEAMA Limited with sponsorship by the SMMT and the Automotive Council. At the commencement of the project, two groups were established; a Core Team of experts who worked together to draft the WP3 content and an Expert Group, of expert stakeholders, who reviewed and challenged the work of the Core Team. WP3 was led by John Parsons of BEAMA with support from David Wong and Greg Sanchez of the SMMT and Richard Parry Jones and Neville Jackson from the Automotive Council. Throughout the programme, Work Package 3 has engaged with a wide range of stakeholders including:

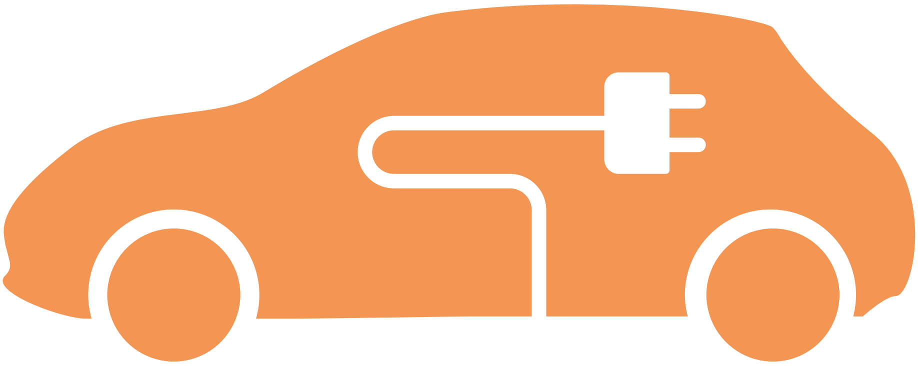
- Chargepoint manufacturers and operators.
- EV Manufacturers.
- Flexibility providers.
- DNOs.
- Smart Metering manufacturers.
- Cyber security experts.
- Academics.

Including input from organisations including:

Core Team:
BEIS, BP Chargemaster, Cenex, ECA, GE, GEO, InnovateUK, L+G, Octopus Energy, Ofgem, NCSC, Newcastle University, The Alan Turing Institute, NPG, Nuvve, Siemens, Shell, TechUK, Thales Security, UKEVSE, UKPN, Warwick University.

Expert Group:
ABB, BEIS, BMW, BP Chargemaster, ChargePoint, Cornwall Insight, Drive Energy, EDMI, Eaton, ENA, Ford, Gemserve, HSBC, IET, Intel, NG, Nissan, Octopus EV, Ofgem, Ovo Energy, PodPoint, RAC Foundation, Siemens, Smart Energy GB, Tesla, TfL, Trilliant, VW, WHP Telecoms, SSE.

Work Package 3 held a series of meetings to understand and plan the programme of work and identify groups of experts with expertise in particular topics. From these discussions it became clear that there was a need for greater clarity on the scope of our work, specifically which charging scenarios and use cases would the smart chargers' support.



This led to a joint exercise with the other Electric Vehicle Energy Taskforce Work Packages to identify charging scenarios and use cases. Based on this analysis, Work Package 3 identified that the key charging scenarios were the 'duration' charging events:

- Off-street residential.
- On-Street.
- Destination, such as workplace parking.

In each of these situations, the EV would be connected for an extended period (overnight or during working hours such that there would be more time available to recharge the EV than needed. These charging scenarios lend themselves to reducing network congestion or matching energy availability. Housing stock surveys indicates that 70% of GB homes can support off-street parking [2,3], and Work Package 3 chose to focus its attention on off-street parking with the intention of subsequently taking forward its conclusions to on-street and destination charging.

This does not mean that it was decided that other charging should not be smart. Rather it was considered that en-route charging was not appropriate for demand modification; generally, customers would not want to extend these charging scenarios. It should also be stressed that there are many features of charging that could be considered smart, such as capturing journey details and the location of nearby chargepoints. These topics were not covered in Work Package 3 as they did not relate to power network management. It would also be possible to extend energy smart charging requirements to other charging scenarios over time as their relevance became clearer. With the exception of the on-street charging scenario, the focus on these duration charging scenarios is consistent with the OLEV Smart Charging Consultation [4].

Having focused on off-street charging, Work Package 3 next studied the variety of business models that are currently being considered to provide flexibility. These included:

- Distribution System Operator (DSO) direct management.
- Aggregator offering flexibility services to a Distribution System Operator (DSO) or Electricity System Operator (ESO).
- Supplier offering ToU tariffs reflecting variable network or energy charges.
- Home Energy Management (HEM) integrating the operation of multiple smart energy devices in the home.

Examining how each of these business models might remotely operate a chargepoint revealed a very complex situation with multiple possible routes for control signals and business specific requirements that would have to be supported. After discussion with stakeholders, it was concluded that setting chargepoint requirements around providing support for all of these use cases would likely make the CP very complex and expensive. It would also, potentially, introduce barriers to charging models that had not been identified at this time.

It followed that, rather than specify a smart chargepoint that met all possible needs, the requirements should be reduced to the minimum that would meet the needs of all stakeholders. This is consistent with the Minimum Technical Standards [5] approach adopted by OLEV for current regulatory and fiscal policy for CPs. To test this approach, a long list setting out possible requirements was developed. This list was then circulated to the Expert Group and additional stakeholders for review and challenge, with the intention of removing any requirement that could not be justified as essential. Stakeholders submitted their comments and proposals for changes to the list of requirements. This feedback was then reviewed by the Core Team and a further version produced. This was again circulated to stakeholders for further challenge and has formed the basis of this report. The main recommendations of Work Package 3 have been presented to three Electric Vehicle Energy Taskforce stakeholder workshops to with general acceptance. The SMMT also sent the main recommendations to its members for review, and where their response diverges from the report's recommendations this has been indicated.

Not all issues examined have achieved consensus. Specifically, requirements related to the ability to change the CPO remotely have been the subject of strong views on each side of the argument. To attempt to illuminate this discussion, an exercise was undertaken to better understand the arguments and the result of this is set out in the section on interoperability.

Key assumptions used in preparation of this report

Below are set out the principles that were used to guide the preparation of this report.

- It has been assumed that the CP can be remotely operated by an authorised party. This party may fulfil a variety of commercial relationships with the user but, in this document, we refer to this party as the ChargePoint Operator (CPO). The intention of this principle is to provide clarity over the responsibilities of the party that has remote control of the smart charger, regardless of the business model that they adopt. Ensuring the robustness of this recommendation is important, and further mapping of different business models to the CP will inform this work. There should be no more than one party acting as the CPO; there should not be more than one party able to communicate with the CP. An exception to this might be necessary if there were a separate connection to the chargepoint as part of an emergency load limitation function. In this case it would be important to inform the CP user which party had modified the chargepoint's operation.
- In order to support maximum business flexibility, only the minimum requirements necessary should be mandated. These requirements should be specified to ensure cyber security, data privacy, security of supply and a basic level of interoperability such that consumers have confidence that smart chargers are fit for purpose and to ensure safe and secure delivery of charge to electric vehicles. These requirements represent the minimum physical, minimum functional, minimum interface, minimum data and minimum testing and certification requirements of Electric Vehicle Supply Equipment (smart charger) that a CPP must comply with in order to install and operate a smart charger. The view of the Work Package 3 Core Team is that these requirements avoid defining 'smart functionality' within the CP but allow 'smart' control to be implemented separately (including within the CP) and to be as defined by any CPO definition. These requirements ensure that the CP will respond appropriately to the smart control.
- To avoid burdening all chargepoints with unnecessary or inappropriate requirements, only those smart charging scenarios that are relevant to network management or system balancing should have minimum requirements set for them. These are considered to be off-street residential, on-street overnight and destination charging where EVs are routinely connected to a smart charger for sufficient time to engage in flexibility services. Existing commercial arrangements exist to manage most other applications, although these may require examination and amending.
- Minimum technical requirements to support smart charging should be appropriate to the charging scenario. As only the minimum requirements should be mandated and these will differ by charging scenario, it follows that the minimum requirements should be specific and different for each application. In other words, the smart charger minimum requirements must not attempt to cover all applications. This will create a need for ensuring that correct smart charger equipment is provided for each application. CP manufacturers would be at liberty to include additional features and functionality requirements to produce multi-purpose CPs, but this would be based on their assessment of manufacturing costs and market volumes.

3 Current position

Current position

At present, provision of chargepoints varies depending on the application. For off-street residential, they are generally either provided with an EV by the OEM or obtained by the customer from a CP provider, or independent electrician, at the time of purchasing an EV. If the chargepoint is attracting a grant from OLEV, it must comply with the OLEV minimum technical requirements applicable at the time of purchase.

- For public chargepoints, the company offering the service will either purchase them from a CP manufacturer or manufacture their own.
- In general, for off-street residential, the chargepoints are commonly allowed to supply the EV without constraint or according to a Time of Use (ToU) tariff. Aside from a number of technology and consumer acceptance trials there has been limited active control of off-street residential chargepoints for the purposes of managing network constraints. EV users are able to manage the time of day the EV is charged via functionality offered by the EV supplier, whether from the dashboard or via an App.
- Technology trials have demonstrated the potential for chargepoints to provide 'managed charging' that allows either the time charging takes place to be shifted or the power transfer to be moderated. These trials have also investigated the active control of chargepoints for the purposes of managing network constraints. This functionality is commonly referred to as 'smart charging'. The use of 'smart charging' is more advanced for off-street public parking and for fleet depot operations. Although on-street or public chargepoints might not necessarily be 'smart', owners or operators may choose to install a demand management system that manages the demand across a number of chargepoints and distributes it accordingly.
- There are a variety of ways in which the customer is charged for electricity: for a residential customer this will be captured by the meter supplying the house and reconciled with their supplier. On route and destination charging can be offered for free but is commonly charged for either through a membership subscription, via charges for access and use, or both.

Desired outcome

Work Package 3 considered the questions set within the scope of Electric Vehicle Energy Taskforce and decided that there were three primary objectives that should be considered by Work Package 3:

1. What technical requirements should be specified for chargepoints that would allow them to be reliably operated in smart mode, responding to signals from the local DSO reflecting network constraints or from an Energy Supplier sending signals, possibly via intermediaries, indicating energy availability or the opportunity to charge on lower cost tariffs.
2. What technical requirements should be recommended to increase consumer acceptance; for instance, the ability of the consumer to override the smart operation of a CP if required or to be rewarded financially for accepting flexible charging regimes.
3. Consideration of how government and industry should support the longer-term development of smart integrated operation of electrical assets, linking V2G and other residential smart appliances and generators.

Work Package 3 expects these recommendations to contribute to OLEV's considerations when it sets out secondary legislation regarding smart charging under the AEV Act. It is also recognised that there might be proposals for short-term and longer-term activities beyond the immediate constraints of the AEV Act.

Issues identified which need to be addressed

Work Package 3 was not able to engage in detailed technical analysis and has deferred the definition and development of current and emerging approaches to communication and control, including technical standards, to follow-up activity. Such an analysis would need the close involvement of technical experts from a full range of industry participants and Work Package 3 did not have this level or depth of engagement. This will require a joined-up approach to ensure vehicle manufacturers and CP suppliers can develop and certify products for more markets than just the UK.

Work Package 3 agreed to make a key assumption in order to avoid speculation about future market development and their respective merits. Work Package 3 has considered only the technical functionalities that are considered necessary to achieve the Government's expectation of network and energy constraint management. Work Package 3 has made no comments about the regulatory, commercial and market conditions under which these capabilities would be used.

4 Key Themes

Minimum requirements of smart chargers

A high-level task for Work Package 3 was to produce a set of technical requirements for smart chargers. Work Package 3 was also asked to consider how to mitigate the risk of bad network consequences if a single operator were to stop and if CPs were to go dumb at the same time.

As described in the section on Methodology, applying the above key assumptions and taking the work from the LowCVP Use Case Report[6], it was identified that multiple different commercial models could be developed to reward customers for shifting their demand from periods of high network loading or high energy costs. These included Supplier ToU tariff offerings, aggregators passing on balancing contracts from TSOs or DSOs, and Energy Service Offerings. It was concluded that supporting all of the smartness needed for these different offerings in the chargepoint would make it very complex and that the better option would be to reduce the requirements for the chargepoint to the minimum needed to support these offerings and allow the companies to add on their 'smartness' either locally on the chargepoint, within the building as part of a smart home energy management system, in the EV, or in the Cloud.

Work Package 3 consulted widely with stakeholders to identify the minimum set of technical requirements that would be consistent with these applications. These included DNOs, CP manufacturers and EV OEMs.

Charging scenarios considered

Work Package 3 further took account of the objective of the Electric Vehicle Energy Taskforce, which was to avoid the take-up of EVs being delayed by levels of available electrical infrastructure. Specifically, it seemed to Work Package 3 that key to this would be allowing the DSOs to influence the loads on their networks. It was clear that the charging scenarios of most relevance would be those where EVs are left connected to the network for longer than they normally require to fully charge, such that there is an opportunity to shift the charging period. The highest priority scenarios that we considered were off-street residential, on-street residential and destination charging. This does not mean that other scenarios could not provide flexibility, but they were seen as being a lower priority.

Minimum requirements were considered against the known smart charger business models. The minimum requirements are intended to allow ready adoption of a smart chargepoint with these functions whilst allowing providers to offer additional functionality at their discretion.

Key recommendations regarding minimum requirements by Work Package 3

The AEV Act provides government with powers to legislate the minimum technical requirements for smart chargepoints. This was taken as the starting point for Work Package 3, and we identified a number of specific recommendations related to technical requirements for smart charging. These have been developed specifically for off-street residential applications, but they should be extended to other 'duration' charging situations, applying the same principles. Work Package 3 used the SMETS requirements as a template as these have been subject to extensive industry development.

The minimum requirements proposed by Work Package 3 are set out below.
Minimum functional components of the chargepoint

Recommendation 1: In order for the smart charger to support a wide variety of different smart applications, Work Package 3 identified the minimum functional components that should be included in all smart chargepoints listed below and further expanded in Annex 1.

- Clock.
- Data store.
- An electricity meter to meet the needs of the application. For off-street residential charging, fiscal metering would be provided by the supply meter and the chargepoint would only need to provide information. On-street and destination chargepoints might require a fiscal meter.
- A remote network interface capable of supporting communications as required.
- A proportional load control calendar [This would store the daily load programme for the chargepoint and could be altered either continuously (to revert to 'dumb' mode) or less frequently. The provision of the proportional load control calendar allows the chargepoint to continue to operate according to its programme in the event of a loss of communications with the CPO and for the chargepoint to be pre-programmed prior to supply to the customer if desired.].
- A proportional controller to allow the chargepoint to control the current as defined in the proportional load control calendar; [The smart charger should be capable of performing proportional import load control for between 0% (zero import) and 100% (full import) in steps of 10% or less].

With a load control calendar in the CP, if the CPO lost communication with the CP, the CP would be able to continue operating as per its last programme. Generally, it might be expected that the previous day's programme would be appropriate, but there would be cases where the previous day's mileage was very different and, consequently, re-using the previous programme would not be adequate.
An alternative option in the case of lost communications would be for the CP to monitor for lost communication and, in the event of detecting that communications have been lost, begin operating in a default mode.

Recommendation 2: smart charger should be capable of operation under supply limitation conditions as signalled by the local DSO
DSOs require the capability to curtail the load of smart chargers connected to their network briefly at times of excessive network demand to maintain continuity of essential customer supplies. It is envisaged that such functionality would only be used on rare occasions when the local demand management or commercial arrangements provided by a supplier, aggregator or home management system were insufficient or ineffective. Transparency is important to demonstrate to customers and the market that this functionality will only be used as a last resort to prevent fuse operation or damage to plant. This can be achieved via a new requirement to report when such functionality is deployed. The signal could be local (automatic), remote, direct (DSO) or indirect (DSO via a third party) and should only limit the load for a small number of half-hour periods on rare occasions to prevent network faults and/or system outages. Further thought needs to be given to the DSO remote supply limitation to refine this requirement. For example, to be able to do so, static (e.g. location, import/export rating, connectivity etc.) and close to real-time information on chargepoint status (active, rate of charge/discharge) may be required to determine whether an emergency signal will deliver the intended results. Without this information, a signal may be sent to limit the charging/discharging of a chargepoint that in fact is not in use, and that will deliver no benefit.

In the view of the SMMT, 'Where load limitation is required, the DSO should send a signal to the chargepoint operator, who would then execute a supply intervention. There should not be a separate communication path for DSOs. A separate communication path will only increase complexity and add additional cost. Furthermore, in the context of future HEMS, the DSO's demand can be addressed by the HEMS based on consumer presets that will temporarily limit the power to certain appliances.' Accepting this approach would depend on ensuring that the speed of response was sufficient to meet the network protection needs of the DSO.

Note: Low voltage networks already have a protection mechanism (e.g. a fuse) which ensures that network assets are not overloaded. Operation of a fuse would result in the loss of supplies to all customers on the circuits supplied via the fuse. The intent of the above functionality is to provide a means of avoiding loss of supply arising from the operation of a fuse by reducing the load from EVs (or any other smart appliance of significant load), hence maintain supply to customers.

Recommendation 3: The operation of the smart charger during and after fault conditions should be agreed and specified.
Smart charging use cases identify a number of fault conditions (such as loss of mains supply during a charging operation) and it should be required that CPOs and smart charger providers equip the smart charger to operate in an agreed manner during these conditions.

Recommendation 4: When controlling import or export, the smart charger shall be capable of applying a randomised offset to change of load events.
A randomised offset will ensure that there are no step changes of load on the network as a result of synchronised switching of significant customer load in response to a single event (e.g. ToU tariff or implementation of DSR or even a cyber attack). A randomised offset could also apply when load is restored following a network outage to mitigate the effects of cold-load pick-up. However, where a supply limitation has been issued (point 3 above), this should not be time delayed, ensuring it delivers any load reduction instantly as intended.

Recommendation 5: Local control.
To ensure that the chargepoint retains some smartness in the event that it is no longer actively managed by the CPO, there should be a local interface that the user can access and use to set the CP time programme.
This would also be used to allow users to override the programme if they choose to opt out of a particular flexibility response. In the case that the CPO were still in communication with the CP, the customer programme would be overwritten; if there were no communications, the programme would continue until changed by the customer.

Recommendation 6: Reuse.
There should be consideration of the processes required around the re-use of the working but redundant CPs, especially if CPO interoperability is not mandated, meaning that customers may have to swap CPs more frequently.
To support re-use, there should be agreement on factory re-set functions. In all cases, the user data should be securely deleted. Consideration should be given to the options for re-setting operational settings, such as cyber security credentials, that, under the correct circumstances, could be transferred by the CPO to a new site.

Cyber security

Connected infrastructure is a potential target for cyber-security attacks, with motives including information theft, cyber-warfare (e.g. the attack against a Smart Grid in Ukraine, during which 250,000 homes were cut off power), or organised crime (e.g. WannaCry ransomware attack that paralysed critical infrastructure, such as the UK NHS). The UK government recently published eight key principles of vehicle cyber security for connected and automated vehicles [7], emphasising that the automotive industry is not immune from those threats.

When charging an EV, the vehicle is connected to a smart charge point, which means there is an exchange of information between the EV, chargepoint and the national and regional grid. Electric Vehicle Energy Taskforce Work Package 4 sets out the exchanges more fully. In the case of a compromised EV, an attacker can impact EVs in the network or disturb the electricity utility system since, in the case of Vehicle-to-Grid (V2G) technology, the data flow is bidirectional. In order to prevent this, the technical cyber security requirements must consider all entities that are involved in this process, starting from the customer, EV, chargepoint, CPO and DSO.

To establish technical requirements, it is necessary to first identify all potential attack vectors and attack surfaces. Following this, threat modelling [8] needs to be undertaken for every attack to emulate the various potential scenarios, followed by analysis of the impact of each threat. The key challenges facing this complex ecosystem include:

- Physical limitations of devices and communications.
- Heterogeneity, scale, and ad-hoc nature of threats.
- Authentication and identity management.
- Authorisation and access control.
- Implementation, updating, responsibility, and accountability [9].

Any cyber security analysis of the smart charging system and measures to secure it should consider all the accepted cybersecurity functions: 'Identify; Protect; Detect; Respond; Recover and Manage' [10,11,12]. Identify and Protect focus on product assets and information, hardware and software from all cyber threats, including the cyber protection for the Embedded Controller Unit (ECU), secure design of the architecture (segmentation, boundaries protection) and secure information like payment information and vehicle identification. Detect includes monitoring of all anomalous behaviours and vulnerabilities in the system. Respond and Recover cover the functions and actions relating to any detected threat or vulnerability to minimise the impact and restore the system to normal operations. Manage covers system security operations such as risk management, incident handling, vulnerability updates, reporting, security awareness, policies and procedures.

Also, cyber security technical requirements should cover the supply chain. For example, establishment of guidelines for cyber security during procurement phase, to guide the customer through the security measures of the purchased EV or chargepoint. The cyber security requirements for third parties involved in the smart charging process such as building an energy management system charging station should also be defined.

Physical security is also considered to be a concern in the smart charging process as the chargepoints are necessarily available in public spaces, or often easily accessible when off-street and currently, with little or no extensive physical security measures applied.

Although in the work undertaken by Work Package 3 we have focused on the technical requirements of the chargepoint, this does not mean that the responsible party would only need to consider the chargepoint: their analysis and response would need to cover all the elements outlined above. Currently, a reference architecture is proposed by European Network for Cyber Security (ENCS), commissioned by ElaadNL [13].

The ENCS documents describes security requirements for the EV charging systems including requirements to ensure the security of the chargepoint and the security of the communication between the chargepoint and a charge point operator. It is recommended that a UK government and industry stakeholder group review the ENCS document to assess whether it is suitable to be adopted in the UK. This reference architecture lays the foundation for further research and development but is not the only such work. It is expected that the BSI PAS 1498 will set out such a framework [14].

There is currently further activity addressing smart charging cyber security, for instance within IEC SyC Smart Energy and its recent work on the IEC 62351 Cyber Security Series for the Smart Grid. Industry should work with government and international partners to decide which options best promote cyber security and which would leave the UK aligned with international markets. As should be clear, ensuring that an EV charging system is cyber secure requires measures and standards at multiple levels from the CP and EV through the system to the back office. Relevant players need to understand their roles and responsibilities in terms of the NIS Regulations [15]. The Security of Network & Information Systems Regulations (NIS Regulations) provide legal measures aimed at boosting the overall level of security (both cyber and physical resilience) of network and information systems for the provision of essential services and digital services.

The publication of the European Cyber Security Act has also triggered the development of Network Code for Cyber Security related to European Transmission Systems. It is clear from the preparatory study carried out by the Smart Grid Expert Group 2 [16] that the cyber security impact of smart charging will be a significant part of this work. Network Codes have legal status within the European Union and the UK has implemented previous codes. Whether this will be the case in the future will depend on the UK leaving the European Union and how the UK Government chooses to align with European Legislation in future, and with these requirements in particular. However, a large part of the European market adopting common standards and frameworks for smart charging cyber security would mean that adopting different approaches could potentially make the UK market less attractive to manufacturers and operators.

Trust and privacy of users

Sharing users’ data by default without obtaining their consent is risky as they might resist participating in smart charging initiatives. This is specifically relevant given there are some users who do not always trust “smart” systems and could resist a transition to smart systems. To draw a comparison to previous smart meter rollouts, it was learnt that overlooking non-technical factors such as social and ethical considerations would have a considerable impact on the success of the smart meter roll-out and a future smart energy system [17,18]. In GB there is a robust data access privacy framework in place that could mitigate similar issues [19].

In addition to gaining users’ trust, new government regulation and guidance emphasises the importance of data privacy requirements, which should be applied to connected smart charging systems. Regulation and guidance include the GDPR regulation, the guidance on the Internet of Things (IoT) and the guidance on principles of cyber security for connected and automated vehicles. Moreover, a consultation on setting standards for smart appliances concluded that Government intends to take powers to set regulatory requirements for smart appliances based on principles that include data privacy and consumer protection [20]. Consequently, it is expected that any consultation on smart EV charging and subsequent regulations would also include requirements for data privacy and consumer protection.

First, GDPR (General Data Protection Regulation) was enforced May 2018, with stronger rights for end-users with respect to their personal data [21]. Specifically, the users have:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights related to automated decision making and profiling.

These end-user rights detailed in GDPR are emphasised in a recent government publication on the Internet of Things (IoT) [22]. The document highlights the requirement to ensure that personal data is processed and protected in accordance with data protection law (GDPR). The document indicates that device manufacturers and IoT service providers must provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. Moreover, users should be provided by means to preserve their privacy by configuring device and service functionality appropriately. In more detail, where personal data is processed on the basis of consumers’ consent, this must be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time. Consumers should also be provided with guidance on how to securely set up their device, as well as how they may eventually securely dispose of it [23].

While the document does not specify electric vehicles, smart charging would fit the definition of a connected IoT device, and the actors involved in smart charging should adhere to this government's code of practice for consumer Internet of Things. In particular and when applicable, EV ecosystem actors would need to be mindful of:

- "Providing clear and transparent information to consumers about what personal data devices and services process, the organisations that process this data, and the lawful basis on which the processing takes place."
- "Building privacy and security into the product lifecycle from the design phase and ensure these are continued throughout."
- "Ensuring that appropriate technical and organisational measures are in place to protect any personal data, including processes to ensure the confidentiality, integrity, availability and resilience of processing systems and services, and regular testing to ensure the effectiveness of such measures".

The Information Commissioner's Office (ICO) is the UK's data protection regulator, providing advice and guidance to organisations and consumers and, where necessary, undertaking appropriate and proportionate enforcement action, which can be significant. For example, ICO fined BA £183m under the GDPR for an attack in which user traffic to the British Airways website was diverted to a fraudulent site [24].

More specifically to the automotive sector, DfT in partnership with the Centre for the Protection of National Infrastructure (CPNI) and the Centre for Connected and Autonomous Vehicles published eight principles for obtaining good cyber security within the automotive sector. Principle 7 relates to data privacy and provides guidance on the key principles of vehicle cyber security for connected and automated vehicles and is aligned with the text of GDPR and the guidance on IoT. Principle 7 states that "the storage and transmission of data is secure and can be controlled".

In detail:

- Principle 7.1: "Data must be sufficiently secure (confidentiality and integrity) when stored and transmitted so that only the intended recipient or system functions are able to receive and / or access it. Incoming communications are treated as unsecure until validated."
- Principle 7.2: "Personally identifiable data must be managed appropriately. This includes:
  - What is stored (both on and off the ITS / CAV system).
  - What is transmitted.
  - How it is used.
  - The control the data owner has over these processes.
  - Where possible, data that is sent to other systems is "sanitised."
- Principle 7.3: "Users are able to delete sensitive data held on systems and connected systems."

It is recommended that, under existing regulations, relevant actors in the EV ecosystem are made aware of their obligation to be mindful of data privacy issues [25,26]. The ICO or data regulator could provide guidance and when necessary enforce fines for failure to comply with data protection laws.

Work Package 3 recommendations for cyber security and data privacy

Recommendation 7: As smart charging enables the remote operation of significant levels of electrical power load, it is assumed that the CPO will be subject to cyber security obligations and will have a duty to carry out a risk assessment of its system to demonstrate that it is cyber secure and then to implement all necessary measures identified in this assessment.

Recommendation 8: OLEV (and any agency established to oversee cyber security for smart charging) should conduct a review based around international standards and identify a 'preferred' option that receives support. Compliance with this approach would provide an assumption of conformity. This would relieve the CPO of the need to justify its choice of standard and encourage a common approach while allowing innovators to find their own approaches.

Recommendation 9: An expert group should develop organisational requirements of cyber security that are proportionate to the amount of load under control" for smart charging including ISO 15118 and recommend a preferred UK implementation.

Recommendation 10: Relevant actors in the EV ecosystem need to be mindful of data privacy issues, with the UK data regulator, the ICO providing guidance and when necessary enforcing fines for failure to comply for with data protection laws.

Interoperability

A key element of the work carried out by Work Package 3 addressed the issue of interoperability. Interoperability in general refers to the ability of a system to continue working correctly when a change is made to it. For instance, if a device that forms part of a network is swapped for a device from a different manufacturer, it would be considered interoperable if the system continued to work as before providing the same core services and functionalities. It would not be guaranteed that all functionality would be retained, as some manufacturers could offer devices that provided functions beyond the minimum functions governed by the interoperability requirement. Consumers would be familiar with various elements of their home IT systems meeting interoperability criteria. A Freeview box would be expected to work in any home AV system but different boxes might offer enhanced features, such as support for BBC's iPlayer, that might not be found in a replacement device.

Interoperability generally involves a degree of engineering design to ensure that the systems in question have compatible interfaces, communications protocols and data formats. However, systems often experience change to their functionality in-life. Security threats can also change. Therefore, a key aspect of interoperability is the activity required for systems to remain interoperable through life.

Therefore interoperability, at the highest level, refers to:

- Compatibility of interfaces, data formats and functionality: This refers to the engineering design and intellectual property that defines the systems required to interoperate and the ways in which they will interoperate when in use.
- Standardisation: Particularly when systems are to be designed by different organisations, standardisation of the interfaces, data formats and minimum functionality is often vital to interoperability.
- Test and assurance: The means by which products are deemed to meet common standards. This is important to manage the commercial risk associated with a device's failure to interoperate as designed. Test tools, conformance tools and assurance schemes may be required.
- Industry and community governance: The set of rules and responsibilities that the various parties involved in an interoperable system agree to abide by. Without this governance, change can become difficult to manage and proprietary interests can undermine the consumer benefits.

Smart charging interoperability

There are multiple types of interoperability relevant to smart charging and each of these will create a need for requirements, such as common devices, common core functions and protocols. Interoperability may also create a need for component testing to ensure that devices from different manufacturers can all operate in the same way within a given system. Work Package 3 has identified three relevant forms of interoperability, listed below:

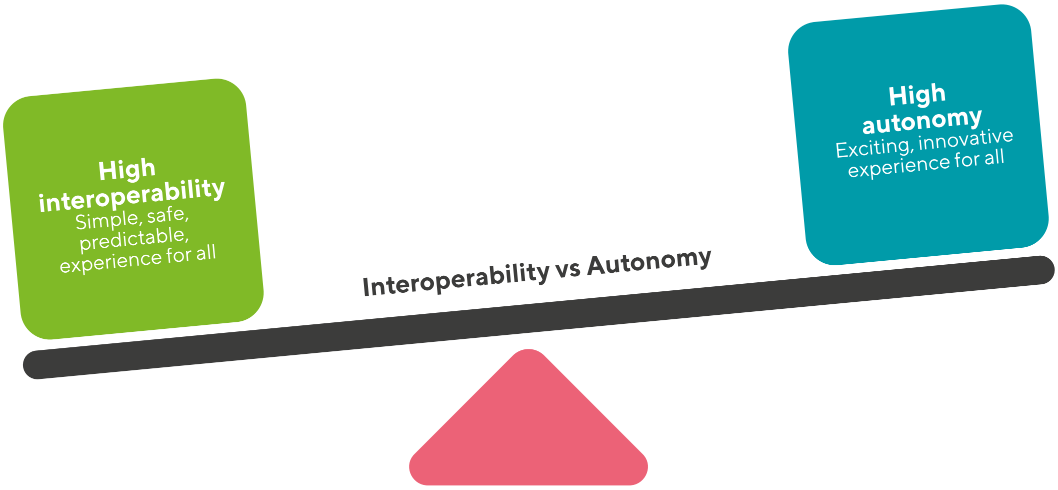
- 'Chargepoint Operator interoperability' which "refers to a consumer being able to switch chargepoint operator without the chargepoint losing its smart charging functions and without a visit to the premises to restore it."[4]
- Demand response interoperability, which refers to the ability of a smart charger to respond to a remote command from any DSO to change the load being presented to the grid in a predictable manner.
- EV interoperability, which refers to the ability of a chargepoint to charge a variety of different EV makes and models.

Implications of interoperability

Demand response interoperability has been a key focus of the work of WP3 and would be met by adopting the minimum requirements set out above. Chargepoint Operator interoperability is more complex and was the subject of extensive discussion and research by WP3.

CPO interoperability can be thought of in terms of consumer experience. The 'interoperability vs proprietary seesaw' (fig 1) shows how interoperability can be a balance between a uniform service and a more variable offering, depending on the priorities for consumer experience. High levels of interoperability are associated with high levels of simplicity and predictability for consumers. However, tip the balance in favour of autonomy (i.e. freedom for system designers to design the system however they wish) and many (but perhaps not all) consumers can expect much more innovative solutions to emerge from a liberalised market. Although they may not think of it in these terms, some consumers may want high levels of interoperability resulting in a safe, reliable, predictable service that they can purchase from any energy supplier or CPO and obtain the same basic experience. On the other hand, some consumers may prefer more exciting, innovative services which they can perhaps only buy from a handful of suppliers and for which they are willing to pay a premium and accept the inability to transfer these equipment, data and other assets to a different system.

The interoperability vs proprietary seesaw (fig. 1)


High interoperability
Simple, safe, predictable, experience for all
High autonomy
Exciting, innovative experience for all
Interoperability vs Autonomy

Implications of smart charging interoperability

The potential benefits of smart interoperability can be broken down further from the high-level requirements in section a. The table below lists the major consumer benefits that interoperability might deliver alongside some implications for smart chargers themselves. Note that nothing in the table implies any kind of restriction on the smart charger capability. Rather it refers to features and capabilities that might be included while not restricting or precluding any other innovative features.

Consumer benefit	Implications for Interoperability
Consumers want to be pleased with new mobility-related services that the advent of EVs and smart chargers can offer. They want to benefit from technological and commercial innovation.	Interoperability may put constraints on the degree to which companies can innovate and provide consumers with experiences they want. Therefore, interoperability should be restricted to the absolute minimum required to achieve the key regulatory requirements.
Consumers may wish to be able to change their smart charger independently of their CPO. Equally they may wish to change their CPO independently of their smart charger. They don't want to be 'locked in' to particular smart charger / CPO combinations.	May require some form of standardised communications protocol which all CPOs and all smart chargers implement to allow change of CPO and related functions to take place securely.
Consumers may want confidence that their EV electricity bill is easy to understand and directly comparable with their domestic electricity bill and bills from other EV energy suppliers.	To achieve a common billing format which customers can easily understand may require a common data model for recording consumption that all smart chargers and CPOs can implement. For example, time of use tariffs are a standardised way to record electricity consumption in half-hourly intervals.
Consumers may be concerned that installation of smart chargers could be inconvenient (for example requiring the consumer to be present for the installation and potentially disruptive to the electricity supply within the property). Consumers may also be concerned that the installation may affect the fabric or appearance of their property. It could therefore be beneficial for smart chargers to be manageable remotely without the need for frequent replacement, home visits or supply interruption (for the lifetime of the equipment.)	May require some form of standardised communications protocol which all CPOs and all smart chargers implement to allow change of CPO and related functions to take place securely.
Consumers may want to be able to take advantage of smart tariffs, for example those which are based on time of use. They may wish these EV-specific tariffs to be independent of their domestic electricity tariffs (for the lighting, home appliances etc.) Also, government may wish to be able to charge a different rate of VAT for EV electricity and for that cost to be apparent to the consumer in real-time.	May require a common data model for recording consumption that all smart chargers and CPOs can implement. For example, time of use tariffs are a standardised way to record electricity consumption in half-hourly intervals.
Consumers may wish to be able to provide their EV energy consumption data to third parties in a standard format for the purpose of receiving comparison advice on their energy services.	May require a common data model for recording consumption that all smart chargers and CPOs can implement. For example, time of use tariffs are a standardised way to record electricity consumption in half-hourly intervals.

Consumer benefit	Implications for Interoperability
Consumers may want their smart chargers to be kept up to date with the latest developments in technology, security standards and consumer preference.	It is possible that smart charger interoperability functions will need to be updated. A governance framework involving all relevant stakeholders may be required to oversee the continued operation and development of the smart charger interoperability in the best interests of consumers and government policy implementation. Open standards may be required in order to provide confidence to the market, accelerate adoption of EVs and provide a competitive marketplace which operates in the best interests of the consumer. However, it must be possible for industry to offer innovative products and services in addition to any smart charger interoperability requirements. Clearly once agreement has been reached on any change to the smart charger interoperability features, these changes may need to be applied to the smart charger devices through over-the-air firmware upgrades.
In order to protect low voltage networks in extreme circumstances, the DSOs should have the ability to control smart charger loads.	As an emergency measure only, the DSO may wish to take control of the smart charger and ensure that the power drawn by the charger is reduced. A control command to reduce power could be sent, followed by a metrology check to verify that the command has been successful. If the command had not been successful, the supply could be completely disabled as a last resort. This supply disablement could be achieved in various ways but would be disruptive to the customer and therefore for grid and local networks protection and safety purposes only.
Consumers want to be confident that their electricity supply is secure in the face of cyber attack.	Cyber security is dealt with elsewhere in this report. However, interoperability generally implies a much greater attack surface than would be present in a non-interoperable system. Therefore, the security requirements must be developed in the context of the interoperability capability.
Consumers want to be confident that their personal private data will not be stolen or shared without their consent.	Cyber security is dealt with elsewhere in this report. However, interoperability generally implies a much greater attack surface than would be present in a non-interoperable system. Therefore, the security requirements must be developed in the context of the interoperability capability.

Use cases for interoperability

Demand response refers to the ability of a smart charger to respond to a remote command to change the load level being presented to the grid.

This has been considered the absolute minimum level of interoperability to meet the needs of network load management. DSOs will need confidence that when they identify a network constraint they can send a signal to various commercial entities, for example aggregators or suppliers, and that the charge points will respond in an appropriate way. The DSO may see relatively predictable constraints, for instance: a peak demand around 5pm for which a time of use tariff will suffice, shorter term situations such as local renewable generation output creating constraints, or very short-term situations arising from network plant failure. In each case the DSO will identify the constraint and signal to an appropriate party the need to modify the charging programme of relevant chargepoints. The objective of Work Package 3 was to ensure that the chargepoints would respond reliably. Work Package 3 refrained from investigating options for signalling between the DNO and aggregators as these protocols could be specified in the contracts between the parties and appropriate standards already exist (such as OpenADR or EEBus with other options in development).

Having received a signal from the DNO, the aggregator or similar would send appropriate instructions to the customer chargepoint either directly or via an intermediary CPO. The minimum requirement is that all smart chargepoints will behave consistently, and this requirement is met if it is possible to remotely change the charging pattern of the chargepoint.

This level of interoperability can be achieved without specifying communication paths and protocols because there is a one-to-one relationship between the CP and the CPO: the CPO would simply need to enable reliable and secure communications. The situation when the ability to switch CPO for any given CP is significantly different; this is discussed below.

For the purpose of responding to network constraint signals, what is essential is that the smart chargepoint is able to perform a minimum level of functions that meet the needs of network or energy management. Proposals for these requirements are set out in the Minimum Requirements section.

Work Package 3 also considered support for the ability of the DSO to modify the output of the CP via an emergency load limitation signal that might follow a different communications path with respect to the 'normal' programme modification signal. It will be important that the operation of this function is defined in a consistent way so that it is interoperable between different DSOs. Stakeholders were also very clear that the market for CPs is an international one, and that requiring different CPs to respond to different load limitation signals from DSOs would introduce a high degree of product and system variation that would be undesirable.

The user switches electricity supplier

The principle of providing the ability for consumers to switch between energy suppliers is a fundamental tenet of how UK electricity markets are regulated. However, in some cases consumers with smart meters have found that the SMETS1 smart meter is not supported by their new electricity provider. This issue has influenced the Electric Vehicle Energy Taskforce to investigate the implications of switching electricity supplier where smart chargers have been deployed.

There are existing mechanisms to support two import suppliers in a property (e.g. one supplier for heating and another for the rest of the load). The property would be allocated two Meter Point Administration Numbers (MPANs) with separate bills from each supplier. This would be the existing arrangement for residential customers wishing to have separate supply contracts for their EV charging and for the remainder of their house supply. The consumer rights with regards to supplier switching would be the same for both suppliers.

With regard to smart metering, SMETS2 metering equipment will support switching.so that a new supplier would be able to use the existing meter when they took on the new contract, There will be a small number of situations in which a SMETS meter cannot be installed in a property and, because it should not depend on a customer having a SMETS meter if they want to charge their EV at home, Work Package 3 has aimed to produce requirements that can be implemented with SMETs metering but also with other non-SMETS implementations.

The following text from the AFID was also noted: '12. Member States shall ensure that the legal framework permits the electricity supply for a recharging point to be the subject of a contract with a supplier other than the entity supplying electricity to the household or premises where such a recharging point is located [27]. This would be satisfied by the measures set out above.

Work is currently underway for larger electricity consumers for providing settlement metering 'behind the meter' [28,29,30]. At present, settlement is normally carried out at the site boundary. However, there may be assets within a property that can offer balancing services whose response would be difficult or impossible to detect at the boundary meter. It may also be desirable to allow customers to contract with different suppliers for different assets in their property, for instance EV chargers within residential premises. Again, this cannot be accommodated with a single supply meter. If the supplier remotely managed the chargepoint as well as providing the electricity supply, then the customer would be able to switch the electricity supply contract but switching the CPO contract would depend on the commercial arrangements agreed between the supplier and the customer. It might be possible for the supplier to encourage their customer to retain their electricity supply contract if it was necessary to retain the CPO service and this was not interoperable. That is to say, the customer would need to install a new CP in order to contract with a new CPO. Allowing CPO interoperability, so that the customer could contract with a new CPO who would take control of the existing customer's CP is discussed below under the heading 'Mitigate risk of involuntary...'

The user switches to another EV brand and/or model

Work Package 3 focused on addressing the powers of the AEV Act, which restricted the scope to the CP and excluded the EV from our proposed requirements. For these reasons, the requirements have not related in any way to the EV. This means that they are neutral to the choice of EV or to any change of EV. The requirements would thus meet this level of interoperability. Should the EV itself become involved in the smart charging process, this conclusion would need to be re-examined.

Mitigate risk of involuntary lock in as a consequence of hardware purchase

As discussed above, smart charger, functionality, communications and protocols could be defined to a level that would allow a customer to choose to switch their electricity provider and CPO without the need to change their smart charger and without requiring a site visit. This would imply that CPOs were able to communicate with any CP, transfer cyber security credentials for the previous to the new CPO and be sure that, at least for the minimum level of functionality, the CP will respond as they expect. The stakeholders who Work Package 3 discussed this issue with had strong views for and against this level of interoperability. Some felt strongly that this was an important requirement to prevent customers from being locked into their CPO contracts, such that, if they wanted to contract with a new CPO, they would need to pay for and install a new CP.

Against this view, there was a strong view that mandating this capability would strongly limit market and technical innovation at this time. There was also a view that standards and cyber security requirements are currently insufficient to define CPO interoperability fully, Thus, although we are aware of the conflict with some consumer (and industry) stakeholders who have recommended allowing this interoperability, Work Package 3 was not persuaded that this is a suitable time for other than recommending support for open standards. In the absence of consensus, Work Package 3 chose not to propose the mandating of CPO interoperability at this time. However, it should be allowed as an option for market participants to choose whether they offer this capability, where different parties jointly choose to define it and offer such a service.

Whilst Work Package 3 did not propose requiring CPO interoperability in the short term, it is noted that there are on-going market developments and emerging open standards to support home energy management with much higher levels of interoperability. This is discussed in more depth in the Flexibility Section.

One recent development that may bear upon this consideration is the proposal by OLEV to include in the Building Regulations a requirement for new homes to be fitted with a smart chargepoint [31] The installation of large numbers of CPs with no CPO linked to them might create a need for a 'standard' CP that CPOs could adopt once a customer has an EV and a need for home charging and seeks to use their CP services. OLEV has not announced its decision on the consultation so this can only be a possibility at the time this report was written but it does illustrate the possibility for a market need to stimulate the development of an interoperable CP.

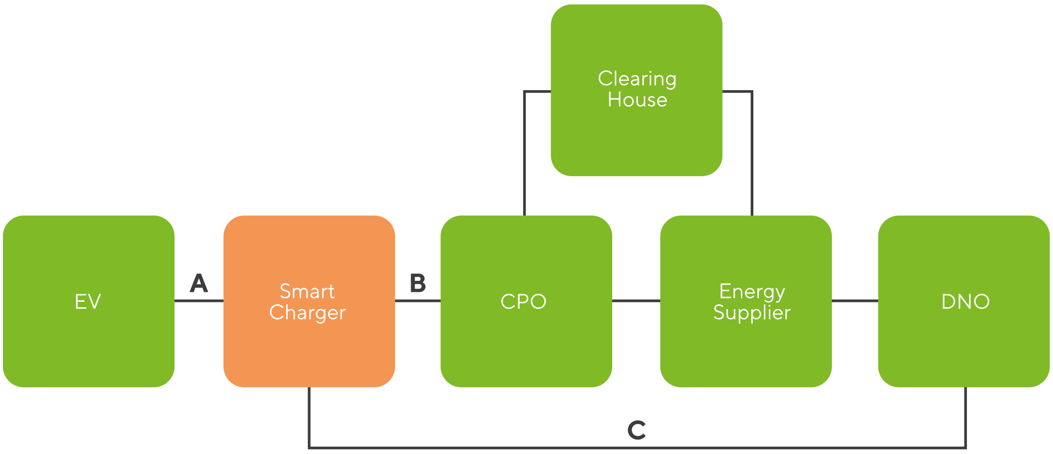
Labelling and customer understanding

A consequence of allowing CPOs a choice as to whether they offer CPO interoperability is that consumers may be offered different levels of interoperability when they choose a CP. To allow consumers to make an informed decision it must be clear which forms of interoperability the smart charger equipment they are being offered is capable of providing.

Protocols for smart interoperability

This section discusses some options available for achieving smart interoperability based on existing standards. This section draws partly on the ELAAD-NL EV related protocol study [32].
We refer to Fig. 2 in discussing the various protocols available for smart charger interoperability. This diagram shows a number of actors operating within an EV charger system, connected by various interfaces. Additional actors and interfaces may be possible, but this diagram focuses on the smart charger and the interfaces that are likely to be required for successful market adoption.

The protocols available for smart charger interoperability (fig. 2)



The letters 'A', 'B' and 'C' in the diagram denote the main interfaces that the smart charger is likely to require.

Interface A – between Smart Charger and EV

Two options are discussed for interface A in Fig 2. Table 1 below lists these options and discusses the pros and cons of each.

Interface designation	Pros	Cons
IEC61851-1	Well established, official and open IEC standard for interoperability between the chargepoint and the EV. Includes communications protocol for agreeing the charging level to be demanded by the EV / provided by the chargepoint. The most widespread EV charging standard throughout Europe and therefore well understood.	Limited ability to establish EV state of charge or to operate in vehicle to grid configuration.
ISO/IEC15118	Official and open ISO standard for interoperability between the charge point and the EV. Superior capabilities compared to IEC 61851, for example supports state of charge and vehicle to grid. High level of definition in the standard at multiple layers in the OSI model likely to encourage adoption in the future. Significantly more interoperable than IEC61851.	Not yet widely adopted.

Table 1

The advantages of both protocols could be achieved by deploying both in smart chargers, although over time the more advanced ISO/IEC 15118 protocol is expected to replace IEC 61851-1.

Interface B – between Smart Charger and CPO

Two options are discussed for interface B in Fig 2. Table 2 below lists these options and discusses the pros and cons of each.

Interface designation	Pros	Cons
OCPP	Provides many functions for managing and operating chargepoints including maintenance, transactions and scheduling. The protocol is well established, open and defined to a high level of detail.	Limited support for metering and billing functions such as time of use tariffs and consumption history may limit support for smart tariffs, common billing format, consumption profiles. Limited security features.
DUIS	Secure and well-established open protocol for monitoring and controlling smart devices. Includes extensive features for switching energy supplier, secure commissioning, over-the-air firmware upgrade, smart tariffs and energy consumption profiles. Detailed and mature specification. Mandated and already adopted by many energy suppliers and DNOs. Based on the international DLMS standard for electricity metering. 'Minimum standard' nature of specification allows for innovation if security requirements are maintained.	Requires a connection to the Data Communications Company (although this can be achieved using DCC service-provider). Requires dedicated HAN/WAN communications (Zigbee/2G/3G/Long range radio).

Table 2

While the two options presented for interface B, OCPP and GBCS, are very different, they appear to be complementary. OCPP provides the device and session management functions, while GBCS provides many of the security, energy supplier / CPO switching and metrology functions required to protect consumer interests and exploit the benefits of smart tariffs, smart switching services and other future energy-related services.

GBCS was conceived as a protocol for transmission over dedicated Zigbee HAN and 2G/3G/long range radio WAN, covering 99.3% of the GB. This feature provides much of the security associated with the protocol, being physically separate from the internet However the dedicated communications modules and DCC connectivity adds cost to the overall solution (although other communications solutions will also add cost).

Interface C - between Smart Charger and DSO

Three options are discussed for interface C in Fig 2. Table 3 below lists these options and discusses the pros and cons of each. The primary function of interface C is to ensure grid protection, by enabling the DSO to send a curtailment signal to the smart charger, instructing it to cause the EV to reduce its load, or in an emergency situation where the EV did not cooperate with that instruction, to cause the smart charger to unilaterally disconnect the EV from supply. As use of interface C could allow multiple parties to modify the CP charging pattern, this could cause confusion to the customer and they should always be informed as to the source of a load modification.

Interface designation	Pros	Cons
OpenADR	Enables automated demand response communication, commanding the smart charger to change power consumption including through emergency signals for grid protection. Well established and supported protocol with interoperability tools, test labs, test events and certification available. Detailed open specification. High level of market adoption [Ref ELAAD-NL study.	Limited security features.
IEEE2030.5	Enables automated demand response / load control communication, commanding the smart charger to change power consumption including through emergency signals for grid protection. Also supports metrology. Mature and open protocol, having been derived from Zigbee Smart Energy profile and now standardised within IEEE.	Generic definitions would require effort to define specific smart charging implementation. UK support for testing / conformance would need to be established. Few examples of market adoption.
DUIS	Secure and well-established open protocol for monitoring and controlling smart devices. Capable of supply enablement / disablement, proportional control for fine-grained control of demand response, and direct metrological verification of demand response command having been successfully enacted (instantaneous consumption read). Detailed and mature specification. 'Minimum standard' nature of specification allows for innovation if security requirements are maintained.	Generic definitions would require effort to define specific smart charging implementation. UK support for testing / conformance would need to be established. Few examples of market adoption.

Table 3

All three protocols would appear to be capable of achieving a level of emergency response capability. OpenADR is possibly the least secure, operating over the internet and providing a limited number of security features. DCC User Interface Specification (DUIS), in conjunction with Great Britain Companion Specifications (GBCS), offers significant security features including end-to-end encryption and a security certification scheme. It is difficult to assess the costs associated with the different solutions. However, the fact that DNOs are already mandated to connect to the DCC and implement the DUIS interface would imply that it is also low-cost.

Note that other, indirect means for achieving emergency load control may be available, whereby the DSO curtailment signal is passed through energy supplier or CPO systems en-route to the smart charger. These indirect routes, while potentially feasible, are not considered here but may be worth consideration if the latency and security implications can be established.

Work Package 3 interoperability recommendations

Recommendation 11: **In the absence of consensus, Work Package 3 chose not to propose the mandating of CPO interoperability at this time. It should be allowed as an option for market participants to choose whether they offer this capability, where different parties jointly choose to define it and offer such a service.**

Recommendation 12: **Government should encourage the development of interoperability by supporting 'preferred' interpretations of supporting standards and necessary product certification.**

Recommendation 13: **Establish a testing and certification regime. To address interoperability and aid consumer uptake of DSR-enabled smart appliances, a standardized testing and certification regime needs to be developed and adopted. Test houses and certification bodies should be involved in the development of this regime to ensure they are providing input to the standards and capability as it is being developed. This testing and certification regime would be derived from the foundation standards suggested above.**

Recommendation 14: **It must be clear to customers from Point of Sale information and package labelling and other product material, what forms of interoperability the smart charger equipment they are being offered are capable of providing.**

Flexibility

As de-carbonisation measures encourage increased use of electricity for transport, heat and other applications, there will be a need to minimise the costs of reinforcing the power networks. Primarily, flexibility is seen as the best way to do this. This involves providing encouragement to consumers to shift their power demands from periods of high network load to periods of lower load. As the UK shifts towards higher levels of renewable generation, which is less predictable than conventional fossil fuel plant, the same principle can be applied to shift demand to periods when there is high renewables output and away from periods with low supply. Customers may similarly want to purchase low carbon electricity and may be willing to modify their demand pattern to minimise their carbon footprint.

Work Package 3 noted the following text in the AFID

'In the long term, this may also enable electric vehicles to feed power from the batteries back into the grid at times of high general electricity demand. Intelligent metering systems as defined in Directive 2012/27/EU of the European Parliament and of the Council enable real-time data to be produced which is needed to ensure the stability of the grid and to encourage rational use of recharging services. Intelligent metering systems provide accurate and transparent information on the cost and availability of recharging services, thereby encouraging recharging at 'off-peak' periods, which means times of low general electricity demand and low energy prices. The use of intelligent metering systems optimises recharging, with benefits for the electricity system and for consumers.'

Additionally, Work Package 3 was challenged to seek means to mitigate the risk of smart charger and other smart appliances, being excluded from smart home energy ecosystem.

Both BEIS and OLEV are developing policies to support the implementation of smart appliances and EVs. In July 2018 BEIS completed a consultation on the need to set regulatory requirements for smart appliances, highlighting the principles of interoperability, data privacy, grid security and cyber security. The Department for Transport and OLEV also announced their Road to Zero Strategy in July 2018 which aims to reduce emissions from vehicles and promote uptake of ultra-low emission vehicles on UK roads.

In the context of Recommendations 15 and 16, to enable interoperability in a common Demand Side Response (DSR) context for smart appliances and EV chargepoints, further research is needed to understand the synergies and dependencies. Such additional research should inform any future iteration or internationalization of both the proposed UK-wide DSR framework standard, and the smart appliances classification standards. This in turn would enable the wide adoption of common DSR functionality across both smart appliances and EV chargepoints globally. Such functionality should define, in terms that can be understood by consumers, which modes of operation are available to respond to DSR signals and how the responses impact on the use or operation of the smart appliance or EV chargepoint.

There is considerable international standardisation activity underway developing standards for home energy management systems, including management of flexibility services for EV charging and V2G. OCCP does not currently have any protocols for communicating with an off-street residential chargepoint and routinely references OpenADR[33] for the connection between the residential CP and network management signals. OpenADR 2.0b Profile Specification has recently been published as IEC 62746-10-1 ED1 [34].

In Europe, Cenelec TC 205 WG 18 has been developing a similar set of concepts following on from the European Commission's Smart Grid Mandate M/490. BEIS and OLEV are supporting the development of two PASs for DSR framework and energy smart appliances. This work will take account of IEC SyC Smart Energy work and take account of the HEMS model being developed by Cenelec TC205/WG18.

These architectures aim to provide a pathway for network control signals from the DSO to pass through to residential smart loads, such as a smart charger, alongside signals from an Energy Service Company supporting a commercial offering, based on variable time of use tariffs (driven by network constraint costs, energy costs or other, such as carbon factor).

A key feature of these, is the ability of the ESCO and DSO to send control signals into the home without needing to know the precise details of the customers' smart devices. These are effectively abstracted as various types of load and local software translates between the remote and local signal. The HEMS is able to interrogate the smart loads to find out what flexibility they can offer. The documents referenced are useful sources covering this activity [35,36,37,38].

It is known that some European EV manufacturers are developing smart chargers based on EEBus[39] smart home technology, that is intended to integrate into such a system, as one of the Networks shown in the diagram below.

It is important to note that these systems will offer greater levels of interoperability. An EV included in such a HEM scheme will be visible to the system and will be required to indicate its flexibility in providing and drawing current. The EV appears as just another smart appliance. Thus, in principle, concerns over CPO interoperability would recede.

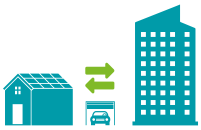
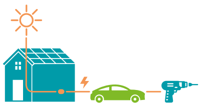
From the perspective of EV OEMs, CP manufacturers and customers, it is highly desirable that UK product requirements are based on international standards so that manufacturers can benefit from the economies of scale. UK industry should join international initiatives to ensure that consequent products and services are available for the UK market and that their definition has included consideration of the UK energy market.

EVs are one of the largest residential loads and there is an inherent flexibility in their charging demand requirements which could facilitate demand management strategies for optimal power system integration [40,41,42,43,44]. Several on-going trials are testing grid services that EVs can provide.

In the UK, several on-going trials are testing flexibility services from EVs. Some trials are funded by the Network Innovation funds such as CarConnect [45] (WPD) which is building a monitoring algorithm that could detect EV charging by monitoring LV substations. Other projects are examining the potential to procure flexibility from EVs to support the operation of LV networks and reduce the need for reinforcement. For example, Smart Charging Architecture Roadmap (SmartCAR) [46] (UKPN) have already produced designs to test market-led smart charging solutions at distribution level. Shift [47] (UKPN) is building on the results of smartCAR by demonstrating these designs and the relevance of flexibility markets at distribution levels. While SmartCAR and Shift are carrying out detailed analysis for EVs, Customer led distribution system [48] (NPg) is taking a holistic view and investigating market designs at distribution network level for DER energy products including EVs. Moreover, a £30 million government programme on V2G, a technology allowing bi-directional charging, would see over 2,000 chargepoints rolled out in the UK with private and fleet customers [49]. The flexibility services on these V2G trials span from providing frequency regulation to the transmission system operator to benefiting from half-hourly tariffs to reduce the energy bills to customers. Additional projects in the UK include trialling the smart metering infrastructure to control EV chargers [50].

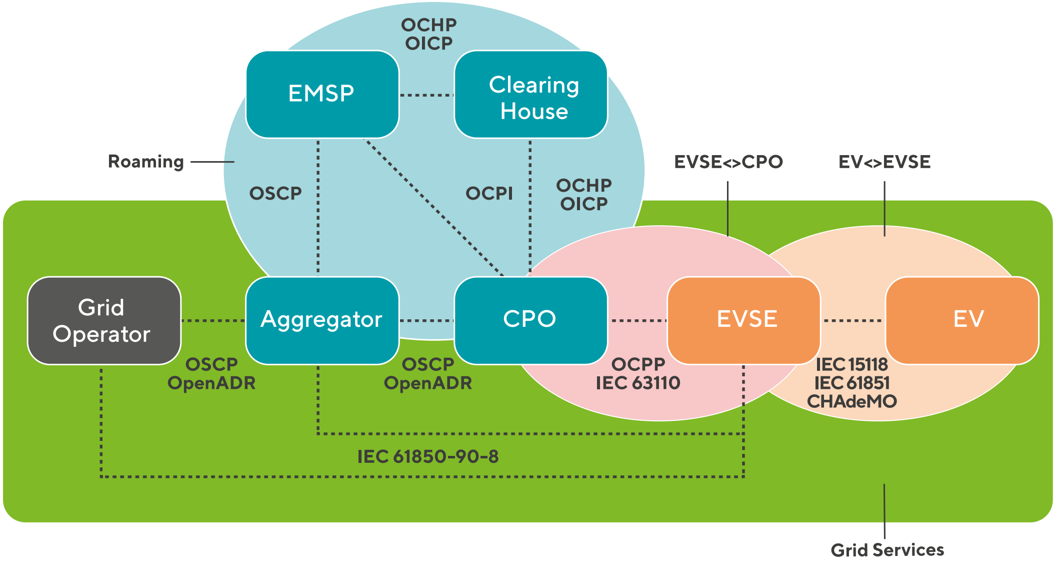
Similar activities are on-going internationally, for example, INVADE is a Horizon2020 project demonstrating flexibility from EVs across 5 sites in Europe [51]. A demonstration in Eindhoven in the Netherlands looks at how a DSO can use flexibility to maintain power quality in the grid economically. In Amsterdam, flexible charging is currently being tested as part of the Flexpower project [52]. The Parker project in Denmark tested an extensive list of flexibility services that EVs could provide to support grid operation [53] (Fig 4).

Potential flexibility services from electric vehicles (fig. 4). Source: Parker Project, DK, 2019

Domain	Categories	Service examples	Short description	EV and EVSE Technical requirements	USER Incentives
Region (Transmission)	**Power balancing**	Synthetic inertia	Mimic inertia of rotating machines	• Fast activation •Controllable ramping rate • Bidirectional (V2G)	Availability payment
		Frequency containment	Keep the frequency within a required interval		
	Energy balancing	Wholesale energy	Responsiveness to varying energy prices	(no special performance requirements)	Savings on energy costs / Renewable-based charging
		Regulation	Balancing energy schedules/portfolios		
		Marginal emission	Defer charging based on CO2 cost of marginal consumption		
Neighbourhood (Distribution)	**Grid contingencies**	Loading issues	Mitigate overloading of transformers and cables in LV network. May also include phase load balancing	- 4Q / Reactive power capabilities	Savings on connection costs / compensation from utility
		Voltage issues	Mitigate overvoltage and voltage drops in distribution systems		
	**Energy autonomy**	Bilateral trading	Local peer-to-peer trading of energy	- Bidirectional (V2B)	Savings/ independence/ renewable support
		Self consumption maximisation	Ensure the highest possible utility of locally produced energy		
Building (Behind the meter)	**Islanded operation**	Back-up power	Sustain a small power system temporarily disconnected form the grid	- Bidirectional (V2B) -Islanding capability	Security of supply/ independence
		Fully off-grid	Sustain a small power system permanently disconnected form the grid		
	**Mobile load serving**	Vehicle-to-tool	Provide a mobile power-source for equipment during in-field use	- Bidirectional (V2L)	Access to mobile power source
		Vehicle-to-vehicle	Provide energy directly from one vehicle to another		

Various mobility and energy entities need to collaborate and coordinate their charging management strategies to ensure that the flexibility from electric vehicles can support the power system. To facilitate the collaboration between various mobility and energy entities, communication protocols provide guidelines for information exchange. For example, the number of kWhs that the battery could offer into flexibility and would require to bring it to the state of charge expected by the user needs to be communicated to relevant parties to ensure a charging control strategy is taking into account the users' needs while supporting the operation of the power system. Figure 5 lists some of the main communication protocols currently available linking EVs and various entities in the EV ecosystem. The green box in Figure 5 lists relevant communication protocols relevant for flexibility service provision from electric vehicles.

EV ecosystem energy and mobility entities and open communication protocols (fig. 5) [54].



Some of these protocols are mature, while others are being developed. It is important to note here that these protocols (except CHAdeMO) are universal, open standards which facilitate interoperability and integration of EVs into the power system.

In addition to open communication protocols ensuring that flexibility from EVs is maximised, forecasting and prediction of EV charge demand will also be key. Properly estimating demand requirements, by using advanced forecasting and prediction techniques, would help EV ecosystem entities such as DSOs to roll out cost effective plans to maintain reliable operation of their networks. Access to data from the EV charging infrastructure and electricity networks is key to develop fit for purpose forecasting and prediction tools to support decarbonisation of transport and electricity systems [55,56,57] and it is recommended that data access is facilitated, while respecting the privacy of users.

Flexibility recommendations

Recommendation 15: **Develop a framework standard for DSR definition, operation and management and a standards classification for smart appliances in a DSR context.**

Recommendation 16: **Research opportunities for convergence of EV chargepoints and smart appliances in standards, currently being considered under PAS 1788 and 1789.**

5 Response to specific questions

Questions asked of Work Package 3

In order to fulfil its aims and objectives Work Package 3 was asked to address the following questions. The table provides answers to some of the questions and indicates where a fuller response to these questions can be found in the report.

Main question	
What are the technical requirements for cyber security, grid stability and data privacy?	Cyber security is dealt with in the Cyber Security Section. We have not commented directly on grid stability but have identified minimum technical requirements for smart chargers that should enable them to respond to grid stability management functions. Data privacy has been addressed. It is largely covered by current legal requirements such as the GDPR, but a number of additional needs have been identified, such as the need to ensure that a factory reset for a smart charger clears all consumer data.
Can internet connections be secure enough for smart charging? What are the viable alternatives?	We have not addressed this question directly, partly because it is an area of active development. However, we have proposed that there is a clear responsibility on the chargepoint operator to carry out a risk assessment of their entire system to ensure that it is secure. This will require a holistic view of the solution with the threats and risks mapped and a risk treatment plan to identify how the risks can be / are mitigated to an appropriate level followed by appropriate independent testing / auditing.
Randomised time delays for responses from smart chargepoints might be needed for grid stability. How can this be done whilst mitigating the impact this would have on the ability of the chargepoints to be involved in frequency response services?	Work Package 3 has set out proposed minimum technical requirements for an off-street smart charger that includes the ability to randomise their response. It is also proposed that the control protocol should allow a signal that disables this randomised response.
What level of testing (e.g. for cyber security) should chargepoints have?	Under European Legislation, smart chargepoints are likely to be identified as a high level of cyber security assurance. This would imply that chargepoints would require third party certification by a National Accreditation Body or an approved organisation. It has been proposed that the government, working with industry, includes smart chargepoints in the CPA process.
What requirements are needed for these in relation to the disposal or re-selling of chargepoints?	It is proposed that the chargepoints are provided with a factory reset function. This should have different levels depending on the change of use. In all cases, consumer data should be deleted. In some cases, where it is intended to re-use the chargepoint with the same CPO, but a different location, it may be desirable to retain the cyber security credentials. If it being disposed of, it should be completely cleared of all operating data.

Subsidiary questions	
What are the technical requirements for interoperability	See Section on Interoperability
OCPP is very widely used as a comms protocol. Is this the starting point for interoperability or does it have barriers that can't be overcome?	OCPP protocol is increasingly becoming a de-facto standard for the management of chargepoints. However, it was found that they have no standards covering the communications to a residential off-street smart chargepoint. For this OCPP refers to OpenADR communications standards. This is an alternative to the work currently being developed by BSI on Energy Smart Appliances sponsored by BEIS and OLEV. This is discussed in the Flexibility Section.
Beyond a common communications protocol or appropriate interface between protocols, is anything else required to achieve interoperability?	It was found that there are a number of different interoperability capabilities. One of these is the ability for a CPO to take ownership of another CPOs CP without visiting the site. There was a strong view from some stakeholders that this would require a common functional capability of the CP and extensive interoperability testing. This issue is discussed in the Interoperability Section.
What are the technical barriers to getting the full benefits from smart chargepoints, including how they work together with smart meters (and smart cars)?	Currently the availability of suitable standards is the main barrier and the availability of data from the EV. IEC 15118 Part 2, which will soon be published will support a greater degree of communication between the EV and the CP. There is also much work being done on extending smart metering to support smart charging and developing Home Energy Management standards that will facilitate this capability and a number of EV manufacturers are working to include smart charging in these standards. This is discussed further in the Flexibility Section.
What are the potential technical opportunities or limitations of using the smart meter infrastructure as the communications system for smart chargers?	Work Package 3 considered the use of smart metering infrastructure and concluded that it could provide the basis of smart charging, subject to confirmation of the service level for speed of messages. However, it was concluded that it should not be the only solution available. Our recommendations have been developed so that they are compatible with smart metering infrastructure and also other possible implementations. All implementations will need to meet cyber security requirements and grid stability.

Subsidiary questions	
Are EU and international standards developing quickly enough to be useful at this stage? Will there be exceptions where the UK should deviate from them (e.g. for cyber security reasons or in order to be more closely integrated with UK smart meters)?	It was noted that, especially for cyber security, smart charging is subject to considerable development at the European level following the publication of the European Cyber Security Act. Specifically, this allows ENISA to develop European Certifications Schemes for products, such as smart chargers. The publication of the Cyber Security Act also triggers the development of the Network Code for Cyber Security and this will almost certainly address smart charging. The relevance of this will depend on UK Government decisions post BREXIT. However, there was strong representation to Work Package 3 that the UK must avoid introducing requirements that create a unique UK market for smart chargers and EVs as these are international products.
What are the remaining technical barriers to innovation such as V2G and how can they be overcome?	There are a number of technical challenges that prevent V2G and the wider involvement of EVs in home energy services. These include EV-CP communication and lack of interoperable standards. These are being developed and this is described further in the Flexibility Section.
Can a single or small number of technical frameworks or architectures for smart charging be agreed at this point in time? If so, is this helpful/ necessary or does it limit innovation?	Work Package 3 has proposed that the lack of published standards and the high level of innovation around smart charging mean that government should not mandate any specific architecture or framework at this time. However, industry should commence work with government to begin development of suitable frameworks as this will be essential when the sale of EVs accelerates.
What are the product safety issues relating to smart charging?	Chargepoints are currently subject to a variety of safety requirements, including the IET Electric Vehicle Charging Equipment Installation - Code of Practice (currently being revised). One specific safety related question is the behaviour of the chargepoint following an interruption of supply. It would be very useful if protocols could resume operation automatically in a safe manner.

6 Conclusions

Conclusions

Work Package 3 has engaged extensively with stakeholders from a wide variety of sectors and sought to find consensus responses to the questions set. What has been clear is that the development of smart charging (where the smartness intended to allow best use of power networks and available electricity) is in its infancy with many trials in progress and supporting standards and innovations only now emerging. How to meet consumer expectations of market freedom whilst respecting the needs of industry to continue to innovate was a major concern of Work Package 3. Related to this concern was the need to respect the international nature of the EV and Chargepoint (CP) industries. The view of EV OEMs and CP manufacturers were agreed on the undesirability of creating requirements that were unique to the UK as this was expected to reduce the attractiveness of investment in UK smart charging, increase costs for consumers and create barriers for UK export businesses.

Finally, WP3 identified three charging scenarios that were considered relevant to network load management; off-street residential, on-street and destination (such as workplace parking). These are the charging scenarios that generally involve EVs being connected for longer than they need to recharge and hence are able to offer flexibility. Work Package 3 has focused on off-street charging, as this represents the largest fleet of EVs. WP3 did not have time to develop requirements for on-street and destination. It is our view that the basic principles set out for off-street would equally apply for the other two scenarios; indeed as in those cases there would likely be multiple CPs connected to a central controller, the implementation might be considerably simpler than for the one-to-one relationship between off-street CPs and their CPO.

7 Recommendations and actions proposed

Recommendations and actions proposed

Recommendation 1: In order for the smart charger to support a wide variety of different smart applications, WP3 identified the minimum functional components that should be included in all smart chargepoints listed below and further expanded in Annex 1.

Recommendation 2: smart charger should be capable of operation under supply limitation conditions as signaled by the local DSO.

Recommendation 3: The operation of the smart charger during and after fault conditions should be agreed and specified.

Recommendation 4: When controlling import or export, the smart charger shall be capable of applying a randomised offset to change of load events.

Recommendation 5: Local control
To ensure that the chargepoint retains some smartness in the event that it is no longer actively managed by the CPO, there should be a local interface that the user can access and use to set the CP time programme.

Recommendation 6: Reuse
There should be consideration of the processes required around the re-use of working but redundant CPs, especially if CPO interoperability is not mandated, meaning that customers may have to swap CPs more frequently.

Recommendation 7: As smart charging enables the remote operation of significant levels of electrical power load, it is assumed that the CPO will be subject to cyber security obligations and will have a duty to carry out a risk assessment of its system to demonstrate that it is cyber secure and then to implement all necessary measures identified in this assessment.

Recommendation 8: OLEV (and any agency established to oversee cyber security for smart charging) should conduct a review based around international standards and identify a 'preferred' option that receives support. Compliance with this approach would provide an assumption of conformity. This would relieve the CPO of the need to justify its choice of standard and encourage a common approach while allowing innovators to find their own approaches.

Recommendation 9: An expert group should develop organizational requirements of CS that are proportionate to the amount of load under control" for smart charging including ISO 15118 and recommend a preferred UK implementation.

Recommendation 10: Relevant actors in the EV ecosystem need to be mindful of data privacy issues, with the UK data regulator, the ICO providing guidance and when necessary enforcing fines for failure to comply for with data protection laws.

Recommendation 11: In the absence of consensus, WP3 chose not to propose the mandating of CPO interoperability at this time. It should be allowed as an option for market participants to choose whether they offer this capability, where different parties jointly choose to define it and offer such a service.

Recommendation 12: Government should encourage the development of interoperability by supporting 'preferred' interpretations of supporting standards and necessary product certification.

Recommendation 13: Establish a testing and certification regime. To address interoperability and aid consumer uptake of DSR-enabled smart appliances, a standardized testing and certification regime needs to be developed and adopted. Test houses and certification bodies should be involved in the development of this regime to ensure they are providing input to the standards and capability as it is being developed. This testing and certification regime would be derived from the foundation standards suggested above.

Recommendation 14: It must be clear to customers from Point of Sale information and package labelling and other product material, what forms of interoperability the smart charger equipment they are being offered are capable of providing.

Recommendation 15: Develop a framework standard for DSR definition, operation and management and a standards classification for smart appliances in a DSR context.

Recommendation 16: Research opportunities for convergence of EV charge points and smart appliances in standards, currently being considered under PAS 1788 and 1789.

6 Appendices

Data or evidence not possible to include in the main body of text

Work Package 3 examined the implications of mandating greater or lesser degrees of chargepoint interoperability with a view to elucidating further discussions on the topic and to explore if a partial implementation might meet the objectives of those who are calling for interoperability and avoid the negative impacts seen by those opposing this. There was insufficient engagement with stakeholders to fully develop this work so it has not been included in the main body of the report but it was considered that there was useful material that could be included in this section for future reference.

Smart charger capabilities for interoperability

Interoperability can notionally be achieved to a high degree, or to a low degree and anywhere in between. Furthermore, the degree of interoperability to be adopted will have implications with respect to the different smart charger functionalities that exist in the product. For example, the degree of interoperability will have implications for:

- Provisioning: The process of installing and commissioning a smart charger onto the CPO system including physical and logical connection, identification, registration, configuration and putting into operation.
- Security: The mechanisms for ensuring confidentiality, integrity, availability and non-repudiation of the smart charger in a whole-system context. Examples include mechanisms such as tamper-detection, key distribution, encryption, role-based access control, integrity checking, multi-factor authentication.
- HAN/WAN communications: in the case of smart chargers, most likely to involve standardised wireless data communications but wired data communications also possible.
- Transactions / Meter values: To enable correct billing and innovative tariffs which help to achieve whole-system benefits such as demand response through time-of-use tariffs.
- Smart charging: The ability to change the charging level according to external signals, such as DSO emergency control or dynamic pricing.
- CPO switching service: The ability of a consumer to switch CPO without having to change the smart charger.
- User interface: The way in which the consumer interacts with the smart charger system, e.g. through a smartphone app or displays / indicators on the smart charger itself.

This section explores the implications that different notional levels of interoperability (high, medium and none) might have for these aspects of smart charger capability. Firstly, we describe a scenario in which there might be considered to be a high level of interoperability, mandated by government. Secondly, a medium level of interoperability is considered and thirdly the implications of a zero interoperability are considered.

High level of interoperability

Firstly, consider the case where the smart charger is assumed to be highly interoperable. In this scenario, the interoperability requirements are extensive and substantial industry and government work is required to agree and maintain the interoperability standard. The implications for the various capability aspects are considered together with pros and cons for each.

Implications for	Description	Pros	Cons
Provisioning	Any smart charger device model can be provisioned by any CPO. A set of minimum requirements for smart charger provisioning must be defined including features such as device data and messaging interface, modes, communications bearers, security characteristics, configuration parameters, configuration etc.	Provides consumer benefits of consistent experience, less frequent device replacement and disruption. Potential safety benefits arising from reduced frequency of device replacement.	Constrains industry to use common standards e.g. OCPP, SEC
Security	CPOs must implement technology and processes according to open common standardised security requirements. CPOs must gain assurance that their service conforms to the common security requirements as determined by a recognised certification authority.	Most secure, assuming that non-mandated solutions would optimise for other factors such as consumer experience, convenience and cost	Possibly complex to implement, depending on mandated security requirements and architecture
HAN/WAN communications	Smart chargers are able to connect to a range of available HAN/WAN e.g. Wi-Fi, Zigbee, 3G/4G/5G, Long range radio.	Ensures maximum geographic availability and bandwidth-related functionality of smart charger services for all premises in GB.	May require multiple communications technologies to be supported by smart charger - increased device cost
Transactions / Meter values	All smart charger device models employ the same minimum requirements for transactions and metering formats based on open standards. Full set of meter metrics defined including active and reactive consumption registers, credit/prepay, debt management, instantaneous registers, time of use. Common metering accuracy standard required for all smart charger device models.	Facilitates common format for consumer bills, aligned to domestic bill formats. Facilitates smart tariffs. Facilitates pay-as-you-go. Facilitates accurate and comparable bills and consumption data from different CPOs. Facilitates 3rd party energy management services e.g. uSwitch	Constrains industry to use common standards e.g. DLMS, EDL, OCPP, MID

Implications for	Description	Pros	Cons
Smart charging	All network operators employ a common means of interfacing directly with smart chargers to prevent a distribution network overload.	Most direct and potentially reliable control method	Requires network operators to manage control signals at smart charger level. Requires agreement to use common standards e.g. OpenADR, SEC, IEC61850-90-8
Switch CPO	If CPO interoperability were similar to supplier switching, any smart charger device model would have to be switched from one CPO to any other CPO remotely within 31 days and, ideally, without the need for a premises visit. All transaction / metering data is stored on the smart charger and is preserved throughout the transition.	Avoids barrier to competition in the CPO market. Minimises cost and disruption to consumer. Preserves consumer's historical data	Requires agreement to common standards for provisioning, security, transaction and metering data
User Interface (on smart charger or Smart phone app)	All smart charger user interface and physical marking requirements standardised.	Ensures consumers have a common experience of all smart charger functionality. Simplified consumer experience	Requires agreement of user interface requirements. Will may limit market innovation.

Medium level of interoperability

Secondly, we consider the case where the smart charger is assumed to be somewhat interoperable. In this scenario, the interoperability requirements are moderate, and some industry and government work is required to agree and maintain the interoperability standard. The implications for the various capability aspects are considered together with pros and cons for each.

Implications for	Description	Pros	Cons
Provisioning	Each smart charger device model implements core requirements related to security including device authentication and key management, DSO disconnection (grid management) controls, FW update etc. These core requirements are supported by any CPO. Device data and messaging interface, communications bearers and configuration parameters are vendor specific.	Allows for secure product offering while enabling market to innovate in data-driven services	Risk of 'post facto' standardisation and loss of market coherence / adoption rate. Potential for market confusion and delay to EV adoption. Risk of market dominance by small number of vendors.
Security	CPOs must gain certification from a recognised certification authority that their service presents an acceptable risk to UK security of supply and consumer data privacy. Requires an agreed set of risks from which would be derived agreed security requirements for a 'certification body (which would need to be created and assessed as adequate to assess against these requirements) to assess CPOs.	Allows more freedom for industry to define permissible solutions	Risk to investors of sinking costs into 'uncertifiable' solutions Higher workload for certification authority
HAN/WAN communications	A subset of communications technologies is selected as standard requirements for smart charger, providing a balance of availability, data rate and cost.	Allows for 'standard' product offering achieving 'reasonable' GB geographic availability and functionality while enabling market to define innovative offerings and control product cost.	Unclear whether 'standard' product would achieve availability and functionality goals. Requires agreement to use standard HAN/WAN technologies. Possible security implications e.g. Wi-Fi-only communications may be considered low-resilience.

Implications for	Description	Pros	Cons
Transactions / Meter values	Each smart charger supports an agreed subset of transaction / metering data which is defined and standardised. Core functionality TBD. Common metering accuracy standard required for all smart charger device models.	Facilitates common format for consumer bills, aligned to domestic bill formats. Facilitates accurate bills	Requires agreement to use parts of common standards e.g. DLMS, EDL, OCPP, MID
Smart charging	Network operators and CPOs employ an indirect common means of conveying disconnect signals to smart charger.	Allows network operators to delegate grid management to CPOs. Enables CPOs to offer innovative grid management services	Indirect control method implies more difficult to quantify effectiveness (availability) of service. Requires agreement to a common standard e.g. `OSCP
Switch CPO	A range of defined smart charger device models can be switched from one CPO to any other CPO remotely within 31 days. Any stored transaction / metering data is erased as part of the switching process.	Allows for 'standard' product offering while enabling market to define innovative offerings Erasure of smart charger data makes switching process simpler	Requires agreement to common standards for provisioning, security, transaction and metering data Unclear whether market would develop 'standard' offer. Risk of 'post facto' standardisation and loss of market coherence / adoption rate Erasure of smart charger data limits benefits of smart tariffs that use consumption history.
User Interface (on smart charger or Smart phone app)	Common minimum features for all users: e.g. Current price Charge rate (H, M, L) Reason for charge rate limitation (ToU price optimisation, DSO protection limit etc.) Markings (e.g. import only or import/export, unique ID, meter accuracy, device model)	Offers simple basic functionality for consumers, helping them to understand core functionality. Allows market innovation over and above minimum requirements.	Requires agreement to use common standard for user interface.

No interoperability

Thirdly, we consider the case where the smart charger is assumed to be minimally interoperable. In this scenario, the interoperability requirements are low and little industry and government work is required to agree and maintain the interoperability standard. The implications for the various capability aspects are considered together with pros and cons for each.

Implications for	Description	Pros	Cons
Provisioning	CPO to define which smart charger device models they support. All functions, communications and data are vendor specific.	Simple to implement. Minimum constraints on market innovation.	Risk of 'post facto' standardisation and loss of market coherence / adoption rate. Potential for market confusion and delay to EV adoption. Risk of market dominance by small number of vendors. Security solution unclear.
Security	Security measures determined by CPO. No certification required.	Maximum freedom for industry to determine optimum trade-off of security versus cost and other factors.	Potentially insecure, depending on industry design choices
HAN/WAN communications	HAN/WAN communications bearers determined by CPO.	Simple to implement. Minimum constraints on market innovation.	Possibility of limited geographic availability Possible security implications e.g. Wi-Fi-only communications may be considered low-resilience.
Transactions / Meter values	CPO to define transaction and metering data formats. CPO to define meter accuracy standard.	Simple to implement. Minimum constraints on market innovation.	Lack of common data format may limit consumer and economic benefits of data-driven smart tariffs and services. Risk of 'post facto' standardisation and loss of market coherence / adoption rate. Potential for market confusion and delay to EV adoption. Risk of market dominance by small number of vendors. Risks uncertainty over billing accuracy and clarity. Not clear how to implement smart tariffs / PAYG.

Implications for	Description	Pros	Cons
Smart charging	Network operators and CPOs make bilateral arrangements for conveying indirect disconnect signals to smart chargers.	Allows network operators to delegate grid management to CPOs. Enables CPOs to offer innovative grid management services	Indirect control method implies more difficult to quantify effectiveness (availability) of service. Requires agreement to a common standard e.g. `OSCP
Switch CPO	If a consumer wishes to change CPO, then the smart charger must be physically replaced.	Simple to implement. Minimum constraints on market innovation.	Extra cost and disruption to consumer Safety risks associated with device exchange, but risks should be mitigated if carried out by qualified electrician and in accordance with the existing/prevailing IET Wiring regulations and EV Infrastructure Code of Practice. Loss of smart charger data limits benefits of smart tariffs that use consumption history. Environmental costs of device replacement.
User Interface (on smart charger or Smart phone app)	All smart charger user interface and physical marking requirements defined by CPO	Simple to implement. Minimum constraints on market innovation.	May confuse customers and limit market adoption.

Acronyms

AEV	Autonomous and Electric Vehicles
AFID	Alternative Fuels Infrastructure Directive
AV	Audio Visual
BSI	British Standards Institute
CAV	Connected Autonomous Vehicle
CP	Chargepoint
CPO	Chargepoint Operator
CPP	Chargepoint Provider
CPNI	Centre for the Protection of National Infrastructure
DCC	The Data Communications Company
DLMS	Device Language Message Specification
DNO	Distribution Network Operator
DSR	Demand side response
DSO	Distribution System Operator
DUIS	DCC User Interface Specification
ECU	Embedded Controller Unit
EDL	EnergieDienst-Leistung (Energy Service)
ENCS	European Network for Cyber Security
ESCO	Energy Services Company
ESO	Electricity System Operator
EV	Electric Vehicle
GB	Great Britain
GBCS	Great Britain Companion Specification
GDPR	General Data Protection Regulation
HAN	Home Area Network
HEM	Home Energy Management
HEMS	Home Energy Management System
ICO	Information Commissioner's Office
ID	Identity
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
ITS	Intelligent Transport System
MID	Measuring Instruments Directive
MPAN	Meter Point Administration Numbers
NHS	National Health Service
NIS	Network and Information Systems
OCPP	Open Charge Point Protocol
OEM	Original Equipment Manufacturer
OLEV	Office for Low Emission Vehicles
OSCP	Open Smart Charging Protocol
PAYG	Pay As You Go
SEC	Smart Energy Code
SMETS2	Smart Metering Equipment Technical Specification 2
SMMT	Society of Motor Manufacturers and Traders
SyC	Systems Committee Systems Committee
ToU	Time of Use
TSO	Transmission System Operator
V2G	Vehicle to Grid
WAN	Wide Area Network

References

1 Electric Vehicle Energy Taskforce. [Online]. Available: http://www.evenergytaskforce.com/.

2 Ministry of Housing, Communities & Local Government, English Housing Survey 2010. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/6748/2173483.pdf

3. Cenex, Next Greencar, Systra: "Plugging the Gap: An Assessment of Future Demand for Britain's Electric Vehicle Public Charging Network", Reference number 105852, 11/01/2018,

4 OLEV, Electric Vehicle Smart Charging, July 2019. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/817107/electric-vehicle-smart-charging.pdf

5 OLEV, Minimum technical specification – Electric Vehicle Homecharge Scheme (EVHS), (installations after 1 July 2019)

6 LowCVP: Report on Use Case Workshop, Ian Alexander, 15 January 2018

7 UK Government (2017). "The key principles of vehicle cyber security for connected and automated vehicles". [Online]. Available: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles

8 SAE (2016). J3061: "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems". [Online]. Available: http://standards.sae.org/j3061_201601/ [Online].

9 Journal of Cyber Policy: "Security and privacy in the internet of things" [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1366536

10 NIST: "Cybersecurity Framework". [Online]. Available: https://www.nist.gov/cyberframework

11 CPNI: "Passport to Good Security". [Online]. Available: https://www.cpni.gov.uk/system/files/documents/b0/69/CPNI_Passport_to_Good_Security.pdf

12 Centre for Internet Security: "Cybersecurity Tools". [Online]. Available: https://www.cisecurity.org/cybersecurity-tools/

13 ENCS: "EV Charging Systems Security Requirements". [Online]. Available: https://encs.eu/encs-document/ev-charging-systems-security-requirements/

14 BSI: "The Energy Smart Appliances Programme An Overview, A programme implementing recommendations from the Standards Landscape Report on smart appliances and electric vehicle chargepoints."

15 GOV.UK: "The NIS Regulations 2018". [Online]. Available: https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

16 SMART GRIDS TASK FORCE -EXPERT GROUP 2 -CYBERSECURITY, September 2019: "Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management."

17 Sovacool, B.K., Kivimaa, P., Hielscher, S., Jenkins, K., 2019. Further reflections on vulnerability and resistance in the United Kingdom's smart meter transition. Energy Policy 124, 411–417. [Online]. Available: https://doi.org/10.1016/j.enpol.2018.08.038

18 Véliz, C., Grunewald, P., 2018. Protecting data privacy is key to a smart energy future. Nat. Energy 3, 702. [Online]. Available: https://doi.org/10.1038/s41560-018-0203-3

19 DECC, 2012: Smart Metering Implementation Programme Data access and privacy [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf

20 BEIS, 2018. Proposals regarding setting standards for smart appliances [Online]. Available: https://www.gov.uk/government/consultations/proposals-regarding-setting-standards-for-smart-appliances (accessed 11.1.18).

21 ICO, 2018. Guide to the General Data Protection Regulation (GDPR) [Online]. Available: https://icoumbraco.azurewebsites.net/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (accessed 11.26.18).

22 Department for Digital, Culture, Media & Sport, 2018. Secure by Design [Online]. Available: https://www.gov.uk/government/publications/secure-by-design (accessed 11.26.18).

23 Department for Digital, Culture, Media & Sport, 2018. Secure by Design [Online]. Available: https://www.gov.uk/government/publications/secure-by-design (accessed 11.26.18).

24 ICO: "Intention to fine British Airways £183.39m under GDPR for data breach." [Online]. Available: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

25 Alan Turing Institute: "A personal issue: How can we enable personal data to be shared without compromising our privacy?" [Online]. Available: https://www.turing.ac.uk/research/research-programmes/defence-and-security/programme-articles/personal-issue-how-can-we-enable-personal-data-be-shared-without-compromising-our-privacy

26 Mace, John C., Charles Morisset, and Luke Smith. "A Socio-Technical Ethical Process for Managing Access to Smart Building Data." (2019): 10-6.

27 DIRECTIVE 2014/94/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 October 2014 on the "deployment of alternative fuels infrastructure".

28 Elexon, P375. "Settlement of Secondary BM Units using metering behind the site Boundary Point."

29 Elexon, P376. "Utilising a Baselining Methodology to set Physical Notifications for Settlement of Applicable Balancing Services."

30 Elexon, P379. "Enabling consumers to buy and sell electricity from/to multiple providers through Meter Splitting".

31 OLEV, July 2019: "Electric Vehicle Charging in Residential and Non-Residential Buildings".

32 ELAAD-NL, v1.1, January 2017. "EV related protocol study".

33 OpenADR: [Online]. Available: https://www.openadr.org/

34 IEC: "IEC 62746-10-1:2018". [Online]. Available: https://webstore.iec.ch/publication/26267

35 EN 50491-12-1:2018 General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS). Smart grid. Application specification. Interface and framework for customer. Interface between the CEM and Home/Building Resource manager. General Requirements and Architecture (from CLC/TC205)

36 IEC TS 62746-3:2015 Systems interface between customer energy management system and the power management system - Part 3: Architecture (IEC TC57)

37 IEC SRD 62913-2-3:2019 Generic smart grid requirements - Part 2-3: Resources connected to the grid domains (from IEC Syc SE)

38 A report from CGSEG: SG-CG/M490/L_ Flexibility Management Overview of the main concepts of flexibility management

39 SMA: EEBus for the Smart Home. [Online]. Available: https://www.sma.de/en/eebus-uniform-communication-standard.html

40 Neaimeh, M., Salisbury, S.D., Hill, G.A., Blythe, P.T., Scoffield, D.R., Francfort, J.E., 2017. Analysing the usage and evidencing the importance of fast chargers for the adoption of battery electric vehicles. Energy Policy 108, 474–486. [Online]. Available: https://doi.org/10.1016/j.enpol.2017.06.033

41 Andersen, P.B., Toghroljerdi, S.H., Sørensen, T.M., Christensen, B.E., Morell Lodberg Høj, J.C., Zecchino, A., 2019. Parker Project Final Report. [Online]. Available: https://parker-project.com/wp-content/uploads/2019/03/Parker_Final-report_v1.1_2019.pdf

42 California Energy Commission, 2018. California Vehicle-Grid Integration Roadmap Update [Online]. Available: https://www.energy.ca.gov/transportation/vehicle-grid-integration/

43 Idaho National Lab, 2016. AVTA: The EV Project | Department of Energy [Online]. Available: https://www.energy.gov/eere/vehicles/avta-ev-project (accessed 3.5.18).

44 Quiros-Tortos, J., Ochoa, L.F., Butler, T., 2018. How Electric Vehicles and the Grid Work Together: Lessons Learned from One of the Largest Electric Vehicle Trials in the World. IEEE Power Energy Mag. 16, 64–76. [Online]. Available: https://doi.org/10.1109/MPE.2018.2863060

45 Smarter Networks Portal: "CarConnect". [Online]. Available: http://www.smarternetworks.org/project/nia_wpd_013

46 Smarter Networks Portal: "Smart Charging Architecture Roadmap". [Online]. Available: http://www.smarternetworks.org/project/nia_ukpn0034/documents

47 Smarter Networks Portal: "Shift". [Online]. Available: http://www.smarternetworks.org/project/nia_ukpn0045

48 Smarter Networks Portal: "Customer-Led Distribution System". [Online]. Available: http://www.smarternetworks.org/project/nia_npg_019

49 GOV.UK: "£30 million investment in revolutionary V2G technologies". [Online]. Available: https://www.gov.uk/government/news/30-million-investment-in-revolutionary-v2g-technologies

50 GOV.UK: "Electric vehicle smart charging: smart meter demonstration project". [Online]. Available: https://www.gov.uk/guidance/electric-vehicle-smart-charging-smart-meter-demonstration-project

51 INVADE Horizon 2020: "Integrated electric vehicles and batteries to empower distributed and centralised storage in distribution grids." [Online]. Available: https://h2020invade.eu/

52 Amsterdam Smart City: "Mass-charging electric vehicles by using flexible charging speeds". [Online]. Available: https://amsterdamsmartcity.com/projects/flexpower-amsterdam

53 Andersen, P.B., Toghroljerdi, S.H., Sørensen, T.M., Christensen, B.E., Morell Lodberg Høj, J.C., Zecchino, A., 2019. Parker Project Final Report.

54 Martinenas S. 2017. "Implementation of E-mobility architecture for providing".

55 Alan Turing Institute: [Online]. Available: https://www.turing.ac.uk/research/research-projects/vehicle-grid-integration

56 Alan Turing Institute: "Vehicle grid integration". [Online]. Available: https://www.turing.ac.uk/research/impact-stories/towards-greener-grid

57 Newcastle University, Supergen Energy Networks Hub [Online]. Available: https://www.ncl.ac.uk/supergenenhub/research/

energy
taskforce

Low Carbon Vehicle Partnership
3 Birdcage Walk,
Westminster,
London SW1H 9JJ