A Smart, Flexible Energy System

Department for Business, Energy and Industrial Strategy
Call for Evidence response

National Centre for Energy Systems Integration

Introduction

This document is a response to the joint call for evidence on A Smart, Flexible Energy System from BEIS and Ofgem from Newcastle University, which leads the EPSRC National Centre for Energy Systems Integration (CESI). The authors of this response work on a number of interdisciplinary projects on power and energy systems, encompassing electrical and mechanical engineering, computer science, and social science; findings these projects have formed the basis of our response. We have responded selectively, answering only questions where we felt we could make strong points, backed up by tangible evidence. Taking this approach has highlighted to us that, in many areas, the evidence that exists is not conclusive, and has not been demonstrated at sufficient scale to give confidence that the same results would be produced in a large-scale or national roll out.

About CESI

CESI brings together a wide spectrum of industrial and academic energy experts from around the world in an innovative collaborative five year research program. The Centre aims to investigate the challenges of the energy trilemma of security of supply, sustainability and affordability.

CESI draws on the expertise of leading academics from the universities of Newcastle, Heriot-Watt, Sussex, Edinburgh and Durham. The Centre is actively steered by both an industrial innovation and an international advisory board comprised of representatives of local and national government, international researchers, industrial partners and consumer stakeholders, such as the USA's National Renewable Energy Laboratory (NREL), Siemens, National Grid, housing associations and the gas and electricity distribution organisations.

Response

1. **Have we identified and correctly assessed the main policy and regulatory barriers to the development of storage? Are there any additional barriers faced by industry?**

We broadly feel that the correct policy and regulatory barriers have been identified. We feel that more emphasis should be placed on how a DSO could procure services from an ESS developer, how this could affect potential connection agreements, how flexibility can be exploited in the distribution network, and how the potential monopoly for providing a given service can be resolved. A detailed overview is given in a report by UK Power Networks [1].

Please provide evidence to support your views.

[1] UK Power Networks, “SNS4.13 – Interim Report on the Regulatory and Legal Framework”, (2014)

2. **Have we identified and correctly assessed the issues regarding network connections for storage?**

We believe that the correct priorities have been set out, and agree that standardisation between DNOs is critical for storage to compete on a level playing field against other providers of flexibility. We believe that the ability to free up underutilised capacity is something that should be exploited, but would go further and say that emerging technologies which provide flexible (real-time or dynamic asset ratings) [1] or intermittent (storage or distributed generation) [2] capacity should be accounted for within connection agreements. Research suggests that these technologies can offer significant capacity increases at low cost, if their intermittency can be mitigated by a dispatchable asset such as energy storage. Furthermore, emerging flexible technologies should be covered by the prevailing security of supply standards (which are currently undergoing a fundamental review.

EPSRC Engineering and Physical Sciences Research Council
Newcastle University

Have we identified the correct areas where more progress is required?

Flexible connections, as discussed in Table 3, will enhance how storage, and other flexibility providers, can deliver changes in power when required. However, if the flexible connection agreement contains fixed terms, it could preclude the flexibility providers from changing which services they are offering. Given that the business case for energy storage is often predicated on provision of multiple services [3,4], it is essential that connection agreements enable this; longer term flexibility could also be unlocked if storage assets are free to alter which services they are providing based on demand.

Please provide evidence to support your views.

[1] D. M. Greenwood, N. S. Wade, P. C. Taylor, P. Papadopoulos and N. Heyward, "A Probabilistic Method Combining Electrical Energy Storage and Real-Time Thermal Ratings to Defer Network Reinforcement," in IEEE Transactions on Sustainable Energy, vol. 8, no. 1, pp. 374-384, Jan. 2017. doi: 10.1109/TSTE.2016.2600320

[2] J. Yi et al., "Distribution network voltage control using energy storage and demand side response," 2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), Berlin, 2012, doi: 10.1109/ISGTEurope.2012.6465666

[3] R. Moreno, R. Moreira, and G. Strbac, "A MILP model for optimising multi-service portfolios of distributed energy storage," Applied Energy, vol. 137, pp. 554-566, 1/1/ 2015.

[4] D. Greenwood, N. Wade, P. Papadopoulos, N. Heyward, P. Mehtah, and P. Taylor, "Scheduling Power and Energy Resources on the Smarter Network Storage Project," presented at the 23rd Int. Conf. and exhibition on Electricity Distribution, Lyon, France, 2015.

3. Have we identified and correctly assessed the issues regarding storage and network charging?

Do you agree that flexible connection agreements could help to address issues regarding storage and network charging?

Yes. Flexible connection agreements could also be used to incentivise storage systems to provide services to the local network. While storage is intermittent, it is also dispatchable, so doesn't necessarily present the same network issues as renewable generation. However, the extent to which this is true depends on its network applications – storage fulfilling EFR for example, could well operate in a similar fashion to an intermittent generator. Examples of the output of storage fulfilling a variety of services can be found in [1].

Please provide evidence to support your views, in particular on the impact of network charging on the competitiveness of storage compared to other providers of flexibility.

[1] Dr Panagiotis Papadopoulos, Ms Adriana Laguna-Estopier and Mr Ian Cooper, "Smarter Network Storage SDRC 9.7 Successful Demonstrations of Storage Value Streams." (2016)

4. Do you agree with our assessment that network operators could use storage to support their networks?

We agree that network operators could use storage to support their networks. We have evidence that DNOs can use storage to provide voltage support and power flow constraint management, and that storage can be operated alongside demand side response or real-time thermal ratings to provide additional flexibility [1-3]. However, in all cases the storage was operated directly by the network operator, which would not be permissible under the proposed definitions for energy storage.

Are there sufficient existing safeguards to enable the development of a competitive market for storage?

There are existing competitive markets in which storage can compete (Capacity Market), or in which *only* storage can compete (EFR). There are not sufficient safeguards for a competitive DSO service market, or for storage to compete within the conventional balancing service markets (STOR, FFR).

Are there any circumstances in which network companies should own storage?

This question is inherently linked with some later questions related to the transition from a DNO to a DSO. If a network function is best fulfilled by storage, then there should be a mechanism to allow storage to fulfil it – this could be in the form of a DSO service market, or a license exemption to allow the network company to own and operate the asset for this function. The majority of evidence for the benefits of storage in distribution networks came from demonstration projects in which the storage was owned and operated by network companies. Therefore, while there is no technical reason that this support could not be offered via a third party storage operator, there is a lack of evidence to support such an arrangement.

Gas network companies inherently own storage, since the linepack within the system represents a physical store of energy. This storage could be exploited by the electricity network through Power to Gas (P2G); in these cases, the network company would own the storage, but would not necessarily own the P2G assets, such as electrolysers and fuel cells, which are the generation aspects that present difficulties for regulatory purposes.

Please provide evidence to support your views.

[1] Jiang, Tainxiang, et al. "Electrical Energy Storage 2 (100kVA/200kWh) Powerflow Management CLNR Trial Analysis." (2014).

[2] Lyons, Pádraig, Tianxiang Jiang Pengfei Wang, and Jialiang Yi. "Analysis of collaborative voltage control on HV and LV networks CLNR Trial Analysis." (2014).

[3] Dr Panagiotis Papadopoulos, Ms Adriana Laguna-Estopier and Mr Ian Cooper, “Smarter Network Storage SDRC 9.7 Successful Demonstrations of Storage Value Streams.” (2016)

5. Do you agree with our assessment of the regulatory approaches available to provide greater clarity for storage?

We believe that the assessment is generally correct, and that clarity is essential for the large scale uptake of storage. However, we believe that not all storage should fall under the same classification, since the technology, application, and scale of storage will vary, and this should be reflected in the regulation.

Please provide evidence to support your views, including any alternative regulatory approaches that you believe we should consider, and your views on how the capacity of a storage installation should be assessed for planning purposes.

In the existing regulations, energy storage is explicitly defined as a generation asset – this is fine for existing storage, which is primarily pumped hydro, but is not well suited to the distributed storage installations that are anticipated to play a key role in future networks. Consequently, we propose creating a new class of Distributed Energy Storage (DES), and leaving existing Energy Storage, renamed Bulk Energy Storage (BES) classed as generation. For planning purposes, DES could be considered by local planning authorities, and BES under national planning, though there could be exceptions if the scale dictated it.

This proposed classification could allow a gradual transition based on the proposed methods for regulating ES, starting with issuing guidance, declaring that DES does not fit with other licensed activities, and ending with legislation formally defining and regulating DES. We propose differentiating between BES and DES using 3 metrics: Scale, purpose and voltage level.

Scale

BES can typically provide GWs or hundreds of MWs of electrical power, while DES is in the range of hundreds of kWs to 10s of MWs.

Purpose

BES exists to perform energy arbitrage and operating reserve on a large scale. DES is more focussed on local network services, and fast-acting, lower energy system wide services such as primary frequency response. Some services could be fulfilled by either BES or DES, as shown in figure 1.

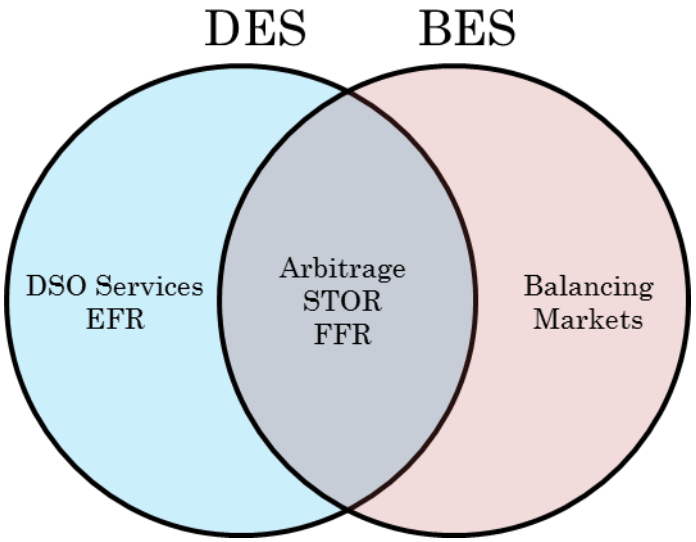

Figure 1: Different service types as used by distributed and bulk energy storage

Voltage Level

We envisage BES connecting to transmission networks, at voltages higher than 132kV, while DES will connect at distribution voltages, 132kV and below.

6. Do you agree with any of the proposed definitions of storage?

The ESN and capacity market definitions broadly identify the same 3 functions for a storage system: importing electrical energy and converting it to a storable form; storage of the energy; and reconversion of the energy to electrical energy.

If applicable, how would you amend any of these definitions?

These definitions seem to preclude the use of a storage medium in which the energy could be moved between storage facilities via a vector other than electricity - the most mature example of which is Power to Gas (P2G) [1,2].

P2G involves the conversion of electricity into either hydrogen or synthetic natural gas, which can then be stored *within the gas network* as linepack. The stored energy can be moved via the gas network, and reconverted to electricity via a fuel cell or gas turbine. This activity meets the definitions, but the regeneration may not take place at the same electricity storage facility as the P2G. The research in this area has primarily considered the linepack available in the gas transmission network, but large volumes of energy could also be stored within the gas distribution network.

Therefore, we recommend the definition be expanded to include facilities from which the energy could be removed via an alternative vector.

Please provide evidence to support your views.

[1] Clegg, Stephen, and Pierluigi Mancarella, "Integrated Modeling and Assessment of the Operational Impact of Power-to-Gas (P2G) on Electrical and Gas Transmission Networks," in IEEE Transactions on Sustainable Energy, vol. 6, no. 4, pp. 1234-1244, Oct. 2015. doi: 10.1109/TSTE.2015.2424885

[2] Clegg, Stephen, and Pierluigi Mancarella, "Storing renewables in the gas network: modelling of power-to-gas seasonal storage flexibility in low-carbon power systems." *IET Generation, Transmission & Distribution* 10.3 (2016): 566-575.

15. To what extent do you believe Government and Ofgem should play a role in promoting smart tariffs or enabling new business models in this area?

As outlined in the call for evidence, the ability to introduce half hourly settlement (HHS) for domestic and small non-domestic consumers will be of considerable value in the transition to a smart, flexible system. We believe that the work currently undertaken by the Regulator in relation to enabling HHS for all consumers is a key area for continued influence. As also noted in the call, we believe a key area for Government / Ofgem involvement is in consumer engagement and education with regards to smart tariffs.

It has been noted that many consumers, in particular at the domestic level are mistrusting of energy suppliers [1] and there is the potential for smart tariffs to alienate some consumers due to a perceived lack of control or a necessity to purchase smart equipment to allow for automation. Ensuring competition, fairness and non-discrimination against consumers will be crucial to the uptake of smart tariffs.

Tariffs are not the only means of engaging customers in demand response and flexibility, as has been demonstrated through projects such as Activating Customer Engagement (ACE) [2]. ACE used a gaming based system to recruit domestic customers and community groups, and to reward participation in DSR – Ofgem and Government should incentivise novel approaches, which have the potential to engage customer who would otherwise be unlikely to participate.

[1] Kathryn Buchanan, Nick Banks, Ian Preston, Riccardo Russo, The British public's perception of the UK smart metering initiative: Threats and opportunities, Energy Policy, Volume 91, April 2016, Pages 87-97, ISSN 0301-4215, http://dx.doi.org/10.1016/j.enpol.2016.01.003.

[2] Davison, P.; Blake, S.; Spencer, A.; Burton, E.; Lee-Favier, S.: 'Activating residential demand side response to relieve network congestion', IET Conference Proceedings, 2016, p. 163 (4 .)-163 (4 .), DOI: 10.1049/cp.2016.0763

17. What relevant evidence is there from other countries that we should take into account when considering how to encourage the development of smart tariffs?

A useful resource providing much information as to the results of multiple smart tariff intervention projects can be found in the documentation of the S3C project. A useful summary can be found in Deliverable 3.4 [1] of this project.

[1] http://www.s3c-project.eu/Down.asp?Name={HYADKPEKMW-630201493832-FBPRIFTPZK}.pdf

36. Can you provide any evidence demonstrating how large non-domestic consumers currently find out about and provide DSR services?

There are a number of potential routes by which large non-domestic consumers are informed or directly contacted with regards to the provision of DSR. A number of fora / organisations exist whereby such consumers could be provided with information on DSR such as National Grid's Power Responsive programme or through bodies such as a the Energy Intensive Users Group (EIUG). As noted in Ofgem's survey responses, where consumers are directly contacted regarding service provision, those surveyed were typically through energy suppliers, independent service aggregators, National Grid, DNOs and additional trade organisations.

Large non-domestic consumers presently provide a number of forms of DSR, with each contact point for DSR often resulting in differing end-user DSR services [1]. Services have been provided for a number of potential markets, although the dominating factor in each of these service provisions is that to date it has typically been the result of the use of on-site generation as opposed to pure load-reduction.

[1] https://www.ofgem.gov.uk/publications-and-updates/industrial-commercial-demand-side-response-gb-barriers-and-potential

37. Do you recognise the barriers we have identified to large non-domestic customers providing DSR? Can you provide evidence of additional barriers that we have not identified?

We recognise the barriers outlined in the call for evidence and make one additional point as to interaction with such consumers. A review of DNO interactions with I&C consumers carried out as part of the LCNF CLNR project found that, when contacting large non-domestic consumers, accessing a suitable initial point of contact within the organisation was key to prevent stalling of further discussions.

This was found to be particularly the case when discussing DSR with consumers who did not already provide some form of DSR. For those who provide some form of service presently and are being contacted with regards to enhancing or varying the nature of their service, this is potentially less of an issue.

[1] http://www.networkrevolution.co.uk/wp-content/uploads/2015/04/IC-Final.pdf

38. Do you think that existing initiatives are the best way to engage large non-domestic consumers with DSR? If not what else do you think we should be doing?

Commonly occurring feedback with regards to the engagement of large non-domestic consumers is in the apparent complexity of the available options perhaps limiting the perception of available revenue streams. Suppliers, aggregators and DNOs have been shown to be successful in procuring DSR services, though such services have perhaps not been exploited to their full potential.

Schemes such as Power Responsive (http://powerresponsive.com/) appear to display positive feedback as to the benefits of DSR provision for large organisations it would appear that Government / Ofgem are perhaps best suited to educating, streamlining and overall reducing the perceived complexity of engagement with DSR provision.

One example of such streamlining could be increasing consumer empowerment across the marketplace, reducing the number of individual contracts for singular services between two parties and engaging across a wider range of potential services. This may help to alleviate some of the perceived complexity which has been commented upon previously

39. When does engaging/informing domestic and smaller non-domestic consumers about the transition to a smarter energy system become a top priority and why (i.e. in terms of trigger points)?

Smaller consumers, by default, have a smaller effect within electrical networks. However, with the proliferation of embedded low carbon technologies at reduced network voltage levels, there is a need to embolden such consumers with an ability to value their potential contributions to the network. A significant increase in acceptance of domestic smart appliances is perhaps an indication of a suitable 'trigger point'. Increasing penetration of domestic EV chargers, or similar 'behind the meter' storage could also serve as suitable trigger points to begin increased engagement with such consumers.

40. Please provide views on what interventions might be necessary to ensure consumer protection in the following areas:

Data and privacy

The security of smart meters is critical to preserve the consumer's data privacy and integrity because it provides a two-way communication and acts as a gateway between the consumer, utility providers and third parties. The assumption is utilities can access data from household appliances through smart meters and smart meters can feed data (appliance/ renewable generation) to the grid. Thus, there is a requirement to consider security mechanisms for such sensitive assets to protect the privacy of data and have better access control.

In order to avoid cyber-attacks on smart meters, the International Electro-technical Council (IEC) has proposed a set of appropriate interventions techniques. From technical angle, solutions are [1]: encryption, access control, anti-virus, firewall, Virtual Private Networks, intrusion detection systems (IDS), etc. While, from a security management perspective, solutions are [1]: key management, risk assessment of assets during-attack coping and post-attack recovery, security policy exchange, security incident and vulnerability reporting, etc.

The following discussion provides view on other intervention techniques that exist to mitigate cyber-attacks on Smart Meters to ensure consumer protection against three main cyber-security requirements outlined by NIST which are: availability, integrity, and confidentiality.

Availability: A possible intervention mechanism to mitigate availability attacks on overall Smart Grid system is to use Self-organising architecture [2]. On the lower level of the Smart grid potential intervention scheme to ensure consumer protection is to [1]: Replace compromised or tampered smart meters, change the channel frequency for message transmission, update the secret keys, and enable the security mode of the ZigBee standard.

Integrity: A possible intervention mechanism to mitigate the effect of smart meter integrity attacks is to generate and maintain secret keys of reasonable length between the sender and receiver of the electricity usage data. Another countermeasure approach to mitigate a bad data injection attack which compromises data integrity is to consider cyber-physical fusion strategies [3].

Confidentiality: The confidentiality and privacy of consumer data is critical because the electricity usage patterns can disclose sensitive parameters which can be used by competitors of the service providers or to fool the billing systems, manipulate the market, or other incentives such as breaking into a house. A number of intervention schemes have been proposed to diminish the effect of data confidentiality breach within a smart meter. These include [1]: replacing secret keys that the smart meter shares with a data concentrator unit in a neighbourhood area network, device reconfiguration/resetting to remove the traits of the malicious attacks, including secret key resetting, and replacing the actual device. Differential privacy techniques, which aim to introduce some

controlled noise in the data to limit the identification of individuals in case of data leakage, should also be considered [4].

[1] Z.A. Baig and A.R. Amoudi, "An Analysis of Smart Grid Attacks and Countermeasures." 2013.
[2] C. Cameron, C. Patsios, P. Taylor, Z. Pourmirza, "Using Self-Organising Architectures to Mitigate the Impacts of Denial-of-Service Attacks on Voltage Control Schemes", *IEEE Transactions on Smart Grid,* 2017 (submitted)
[3] D. Wang, X. Guan, T. Liu, Y. Gu, Y. Sun and Y. Liu, "A survey on bad data injection attack in smart grid," *2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, Kowloon, 2013, pp. 1-6.
[4] J. Zhao, T. Jung, Y. Wang and X. Li, "Achieving differential privacy of data disclosure in the smart grid," *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, Toronto, ON, 2014, pp. 504-512.

41. Can you provide evidence demonstrating how smart technologies (domestic or industrial/commercial) could compromise the energy system and how likely this is?

Traditional energy systems are already exposed to a range of cyber threats. Although smart technologies are not yet embedded in a large scale in energy systems their deployment can increase the risk of vulnerabilities and introduce new ones. This is more likely to be associated with increased connectivity between various assets and with the internet.
Currently there seems to be a lack of evidence in the form of particular incidents suggesting smart technologies can be held exclusively responsible for compromising the operation of energy systems. However, over past few years a number of incidents have been reported in which legacy energy systems have been compromised due to their partial dependence on smart technologies (eg; For instance, in November 2016 the heating system of two residential blocks in Finland were hacked using DDoS attack to disable the computers controlling heating and warm water, leaving the residents in sub-zero temperature for number of days [1]). Based on these recent incidents it is envisaged that similar types of attacks could increase in numbers as smart technology deployment increases introducing additional access points (cyber and physical) for infiltrators. Potential attacks in equipment could lead to financial loss and disruption of services for buildings and households and possible safety concerns both for the owners/occupants and the broader network depending on the power ratings and role of the asset attacked. A number of cyber-attack incidents that have occurred on legacy energy systems are reported below. Although smart technologies have not directly compromised the security of the system incidents:

2003: Computers infected by the slammer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic, it shut down safety display systems at the power plant in Ohio [2].
2010: Stuxnet, targeting Industrial Control System (ICS) of Iranian nuclear program [3]
2012: Aramco, computer virus, able to infect the network and enable the attackers to delete data from the Aramco employees remotely [4]
2013: Journalist reported gaining access to Insteon which is a networking technology for the connected home, showing its vulnerabilities [5].
2013: Journalist reported hacking into Philips Hue automated lighting system [6].
2014: The smart thermostat Nest provided by Google was shown to be vulnerable to a physical attack, potentially allowing attackers to take full control of the device [7]
2014: A bug called Heartbleed has been identified, potentially threatening encrypted data in OpenSSl, potentially affecting buildings and other organisations [8].

2015: The attack on a workstation in Ukrainian utility company was the first cyber-attack on the energy sector infecting SCADA controls and remotely switching off the substations [9].
2016: Nissan reported hackers can switch on the header to drain the battery, as the consequence Nissan disabled leaf electric app [10].
Israel and Turkey reported hack attacks. Finland reported hack attack on two apartments, by disabling computers controlling heating and warm water [1]. Another evidence reported on 31st December 2016 that Russian operation hacked into a utility company in U.S, showing risks and vulnerabilities of U.S electrical grid security [11].

[1] Lee Mathews (2016) Hackers Use DDoS Attack To Cut Heat To Apartments, Available at: http://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/#3580ef2b7472 (Accessed: 8/1/2017).
[2] Brent Kesler (2011) 'The vulnerability of nuclear facilities to cyber attack', *Strategic Insights,* (), pp. 15-25.
[3] Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." White paper, Symantec Corp., Security Response 5 (2011): 6.
[4] Bronk, Christopher, and Eneken Tikk-Ringas. "The cyber attack on Saudi Aramco." Survival 55.2 (2013): 81-96.
[5] Gary Marshall (2016) How hackers are making your smart home safer, Available at: http://www.techradar.com/news/world-of-tech/how-hackers-are-making-your-smart-home-safer-1320500 (Accessed: 7/1/2017).
[6] Sal Cangeloso (2013) *Philips Hue LED smart lights hacked, home blacked out by security researcher,* Available at: *https://www.extremetech.com/electronics/163972-philips-hue-led-smart-lights-hacked-whole-homes-blacked-out-by-security-researcher* (Accessed: 7/1/2017).
[7] Hernandez, Grant, et al. "Smart nest thermostat: A smart spy in your home." *Black Hat USA* (2014).
[8] Michael Rundle (2014) *Heartbleed' Bug: OpenSSL Flaw Rips Open The Encrypted Internet,* Available at: *http://www.huffingtonpost.co.uk/2014/04/08/heartbleed-bug-openssl_n_5109087.html* (Accessed: 7/1/2017).
[9] Kim Zetter (2016) *EVERYTHING WE KNOW ABOUT UKRAIN'S POWER PLANT HACK,* Available at: *https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/* (Accessed: 5/1/2017).
[10] Leo Kelion (2016) *Nissan Leaf electric cars hack vulnerability disclosed,* Available at: *http://www.bbc.co.uk/news/technology-35642749* (Accessed: 5/1/2017).
[11] Juliet Eilperin, Adam Entous (2016) *Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say,* Available at: *https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html?utm_term=.2cb769eaa38b* (Accessed: 4/1/2017).

42. What risks would you highlight in the context of securing the energy system? Please provide evidence on the current likelihood and impact.

Risks:
Modern energy systems are becoming increasingly decentralised, with a greater degree of observability provided through a network of sensors and local controllers in addition to existing centralised SCADA platforms. The addition of these elements raises concerns among various players such as consumers, utilities, and regulators; due to the coupling the communication networks to the transmission and distribution grids. While dependability against relatively rare physical failures can be argued on a “one out of n” basis, cyber-attacks have the potential to damage “n out of n” systems simultaneously because security vulnerabilities can be exploited in parallel. This is particularly worrying as the physical dimension of energy systems is prone to cause a cascading effect in case of targeted failures, due to the required reorganisation of the system to cope with failure.

Some of the critical risks and vulnerabilities of smart energy system have been identified as: physical vulnerabilities, platform vulnerabilities [1], policy vulnerabilities [1], interdependency vulnerabilities [2] and, Information and Communication Technology (ICT) network vulnerabilities [3].

Impact:
Any attack on the ICT of the energy system will therefore have negative impacts of varying severity on energy system operation. There is a wide range of possible attacks against the ICT of the energy systems, including, according to the US National Institute of Standards and Technology (NIST), those targeting the availability, integrity, and confidentiality of the ICT. Those attacks are usually undertaken to: mislead the operation and control of the utility provider [4], manipulate market and misguide the billing systems [5], compete with other utility service providers, disturb the balance between demand and supply [6], carry out terrorist activities to damage local and national power infrastructure [5] and convey distrust between people and government, increase or decrease the cost of energy consumption and energy distribution [7], etc.

In order to address the diverse cyber-security issues related to the smart energy systems there is an increasing need for experts in multidisciplinary fields to work jointly in the identification and treatment of these. Newcastle University has recently launched a multi-disciplinary team comprising cyber security and smart grid experts co-funded by EPSRC and working with other stakeholders from industry and academia offering a powerful collaboration of electrical power systems, ICT architecture and cyber-systems expertise to tackle this pressing problem.

[1] I. Ghansa, "Smart grid cyber security potential threats, vulnerabilities, and risks," 2012.
[2] R. Ebrahimy, Z. Pourmirza, "Cyber-Interdependency in Smart Energy Systems.", International Conference on Information Systems Security and Privacy, 2017.
[3]L.Mathews, Hackers Use DDoS Attack To Cut Heat To Apartments, Available at: http://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/#3580ef2b7472 (Accessed: 8/1/2017).
[4] D. Wang et al, "A survey on bad data injection attack in smart grid," 2013
[5] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," 2009
[6] T. Liu, Y. Gu, D. Wang, X. Guan and Y. Gui, "A Novel Method to Detect Bad Data Injection Attack in Smart Grid," 2013.
[7] J. Lin, W. Yu, X. Yang, G. Xu and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," 2012.

Conclusion

The views that we have presented are based on evidence, but the evidence which exists arises from a limited number of demonstration projects (in the case of storage and DSR), and incidents and theory (in the case of cyber security). We believe that a future energy system will need to have the smart, flexible capabilities this call for evidence is seeking, but we also believe there is a need for more evidence, based on larger scale demonstration and pilot schemes. Much of the evidence available also comes from testing and demonstrating schemes or technologies in isolation – a whole systems approach is needed to ensure that the emerging methods can operate in synergy with one another.

It is essential that stakeholders across the industry, from the TSO, to flexibility providers, to consumers, have confidence in the methods which will be used to deliver affordable, reliable, low carbon energy; the current evidence base has merit, but we do not believe that it delivers that confidence.