JRC Response to the consultation

A SMART, FLEXIBLE, ENERGY SYSTEM
A call for evidence

JRC Ltd
Dean Bradley House
52 Horseferry Road
London SW1P 2AF

☎ +44 (0)20 7706 5199
🖷 +44 (0)20 7222 0100
info@JRC.co.uk
www.JRC.co.uk/about

KEY POINTS

- JRC welcomes the opportunity to respond to this consultation.
- JRC highlights that almost all products and services that are offered to the UK's citizens, consumers, and businesses rely directly or indirectly on the stable provision of electricity and / or gas (gas is used to generate typically 50%[1] of the UK's electricity) by the UK's Critical Infrastructure Utility Operations.
- The stable supply of electricity relies increasingly on the systems that control the electricity grid. This includes resilient private radio systems such as the 9.6 kbit/s in 12.5 kHz narrow band[2] channels used for the UK-wide supervision, control, and data acquisition (SCADA) systems.
  - Whilst these systems may be included under the general heading of Machine to Machine (M2M), they are more appropriately referred to as Resilient M2M (RM2M) Standard public M2M solutions are unlikely to provide adequate resilience (Up to 96 hours mains independence.)
  - Many SCADA / RM2M systems operate to the remote parts of the UK beyond the economic coverage areas of public mobile systems.
- The current 2 x 1 MHz of 400MHz UHF Band spectrum that was allocated by Ofcom's predecessor in 1985 for critical infrastructure utility operations is now only just enough spectrum to control the existing SCADA grid systems.
- The ever increasing roll-out of distributed generation, e.g. wind turbines, is putting an increasing strain on keeping the existing grid stable. The critical infrastructure utility operations therefore need to move to Smart Grid systems.
- The move to Smart Grids will require a significant increase in data rates, e.g. from the current 9.6 kbit/s to 64 / 100 kbit/s, and increased spectrum access. The European Utility Telecom Council (EUTC) forecast that the spectrum requirement will increase to 2 x 3 MHz of 400 MHz Band private spectrum.
  - It should be noted that the average future private spectrum requirements for critical infrastructure utility operations networks, including Smart Grids, is equivalent to ~1.5 percent of the 1,200 MHz of spectrum identified for public mobile / IMT systems in the European Radio Spectrum Policy Programme.
- Monitoring and control of critical network functions does not require the high data transfer rates being considered for business and consumer markets. For network monitoring and control, parameters such as resilience, latency and availability are more important than bandwidth. A need for on-site private broadband networks may emerge to meet security requirements on sensitive sites.

[1] Source: Grid Carbon

[2] Narrow band: 6.25 / 12.5 / 25 kHz bandwidth channels. (Not to be confused with 200 kHz, LTE 'narrow band' public mobile systems.)

CONSULTATION QUESTIONS

Aggregators

10. Do you agree with our assessment of the risks to system stability if aggregators' systems are not robust and secure?

Answer 10: Demand side management does create a number of scenarios under which it might prejudice the stability of the electrical network. As communications specialists, JRC's focus is that it is likely that demand side management will be dependent on telecommunications signals to trigger those responses, and these may be subject to 'common mode' failure situations (for example when all public telecommunications networks fail simultaneously due to a wide-area mains power supply incident).

Common mode failure of the telecoms required to implement demand response could be potentially catastrophic where the cause of the failure – or disruption – of the telecoms networks correlates with stresses to the energy networks. Conceivable scenarios might include:

- New Year's Eve, when telecoms networks, especially elements such as the short message text service, become overloaded just before and after midnight and congestion management mechanisms are implemented, but at the same time the load on the electrical power networks can be unpredictable, requiring demand side management for mitigation of unexpected peaks.
- Flooding incidents where telecoms, electricity and gas networks can be degraded, but in unpredictable ways, thereby requiring demand side management of the power network at the same time as telecoms are disrupted.
- Storm conditions when electrical networks are disrupted which could be mitigated by demand side management, but the telecoms networks which would facilitate these measures are also disrupted.

If this is recognised as a potential vulnerability, JRC would be interested in working with the industry to develop options for mitigation of the vulnerability.

Other Government policies

25. Can you provide evidence to show how existing Government policies can help or hinder the transition to a smart energy future?

Answer 25: The Department of Business, Energy & Industrial Strategy (BEIS), the Office of Gas and Electricity Markets (Ofgem), and the Office of Communications (Ofcom) have differing interpretations of policies and responsibilities with regards to businesses, citizens, and consumers. Under the Communications Act, Ofcom interpret the obligation to serve the interest of 'consumer/citizens' as according higher priority to direct consumer-facing services – mobile data and broadcasting – than communications directly related to delivering cost effective and reliable essential services for the consumer/citizen.

Almost all products and services offered to UK's businesses, citizens, and consumers rely directly or indirectly on a reliable, affordable and sustainable energy supply. It would be helpful if the dependence of 21st Century energy networks on telecommunications was recognised, and that consumers and citizens benefit directly from utilities having access to resilient radio communications systems to supervise and control the critical infrastructure electricity and gas grid networks.

Once agreed, it is hoped that the three organisations will recognise that the move to Smart Grids is only likely to require a modest increase in the existing typical data rates, e.g. from 9.6 kbit/s to 64 / 100 kbit/s, and therefore only a correspondingly modest increase in spectrum access. Indeed, only 2 x 2 MHz of additional 400 MHz Band private spectrum is predicted to be required in addition to the currently allocated 2 x 1 MHz of 400 MHz spectrum.

- Whilst this may be seen as a 200% increase, it should be noted that the average additional future private spectrum requirements for Critical Infrastructure Utility Operations Networks is likely to be equivalent to only ~1.5% of the 1,200 MHz of spectrum identified for public mobile / IMT systems.

Ultra Low emission vehicles

34. What barriers are there for vehicle and electricity system participants (e.g. vehicle manufacturers, aggregators, energy suppliers, network and system operators) to develop consumer propositions for the:
a) control or shift of electricity consumption during vehicle charging; or
b) utilisation of an electric vehicle battery for putting electricity back into homes, businesses or the network?

Answer 34a: the distribution network operators (DNOs) are already aware of the regular peaks and troughs of power demand throughout the average days and, for example, special event days so they can prepare for them well in advance.

The use of 30-minutes time-slot pricing mechanisms may help to control the times that vehicle charging is typically undertaken. It may be, however, that some users are prepared to pay whatever price in order to have the flexibility to connect to the network whenever and wherever they want to. If the power to these areas is uncontrolled, this may cause an issue if enough devices are connected unexpectedly in an area that is already operating close to capacity.

It should be noted, however, that, assuming there is sufficient radio spectrum access, the SCADA systems, etc, should detect these unexpected increases and report them back to the control centre so that additional power may be provided to those areas automatically.

Answer 34b: The batteries in electric vehicles have a limited number of discharge / re-charge cycles before they need to be replaced. It is understood that the cost of replacing the batteries is very high. Once aware, owners may be reluctant to allow their batteries to be used for putting electricity back into homes, businesses, or the network for fear of the high cost of replacing the batteries. Where vehicles batteries are leased rather than bought outright, presumably the leasing company will determine whether they can be used in vehicle-to-grid mode or not as it will potentially degrade the service life.

Consumer protection and cyber security

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

Answer 41: Electricity and gas networks have traditionally protected their control systems from cyber-attack by the inclusion of an air gap between their resilient telecommunications networks and publically accessible networks, especially the Internet.

In the future, there is concern that the regulatory regime for the energy sector will make the separation of operational and commercial networks financially unattractive, or effectively impossible. Public telecommunications networks generally give indicative service levels, and provide a 'best endeavours' service. This is not suitable for monitoring and control of critical infrastructure.

At present, smart meters are less sensitive elements of network control, and can therefore be connected with less resilient public mobile networks and licence-exempt radio services, although this may change in the future if they become critical elements in energy network management, as is being considered in some countries.

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

Answer 42: This consultation is not the place for a detailed analysis of the security vulnerability of 'smart networks', but thinking which assumes that all monitoring and control will conducted through the public internet needs to be challenged. Although monitoring and control is generally migrating to 'Internet Protocol', this does not mean that the equipment has to be connected via the public internet. Separate and private communications networks are easier to secure than the public internet. In an environment where hostile 'actors', some backed with government resources, see action against energy networks as a way to undermine an economy, separating critical monitoring and control networks from public networks may be a useful countermeasure. [Separacy of itself is not adequate as was illustrated by the 'Stuxnet' attack on Iranian nuclear facilities, but interconnection of 'operational telecoms' with the public internet creates more opportunities for compromise as was demonstrated by the attack on the Ukrainian power network.]

Even where data security has not be compromised, dependency on the public internet has demonstrated at least two vulnerabilities which can be mitigated by separate secure 'operational telecoms' networks:

- Denial of service attacks where the public internet get so overloaded than all traffic becomes congested and delayed, even if the contents of the secure messages are not compromised. This is not critical for most services which can tolerate delays, but can be fatal for real-time control where responses are required within defined time periods, in some case sub-second.
- Lack of identification of separate redundant telecoms routing, such that a single physical failure – the destruction of a bridge carrying telecoms cables or a fire in a cable tunnel results in interruption to both main and back-up telecoms circuits.

Roles and responsibilities

43. Do you agree with the emerging system requirements we have identified (set out in Figure 1)? Are any missing?

Answer 43a: Efficient use of system resources (including flexible resources and innovative solutions) for local network and system-wide operations:

Currently, the efficient use of system resources includes the incorporation of resilient private radio SCADA systems to monitor ~10,000 of the UK's electricity sub-stations. Efficiently will increase significantly because this is expected to rise to ~100,000 as the grid becomes increasingly smart. The number of monitored locations increases further when the distributed generation sources, etc, that require resilient communications are added to this total.

Caution should be observed before assuming that any new 'innovative' solutions will always be better than existing solutions. For example, the upload data rate (144 kbit/s) of the new innovative 200 kHz, 'narrow band' LTE (NB-LTE) systems is lower than the upload data rate (153 kbit/s) of a standard 50 kHz private digital system. So, in this case, the narrower channel system is ~4 times more efficient than the 200 kHz wide-band channel system.

Communications technologies installed by the critical infrastructure utilities need to use long-life technologies rather than technologies that have a limited lifetime, e.g. public mobile GSM systems. Indeed, in 1985, Ofcom allocated 2 x 1 MHz of 400 MHz spectrum for the use of SCADA systems within the UK. During these past 30 years, the primary innovative solution that has been introduced into those systems is their changing from 12.5 kHz narrow band analogue systems to 12.5 kHz narrow band digital systems. This change enabled an increase in typical data rates from 2.4 kbit/s to 9.6 kbit/s. NB: these SCADA systems now need to be updated to include the ability to operate 64 / 100 kbit/s in 25 kHz channels and, perhaps, 154 kbit/s in 50 kHz channels. The critical infrastructure utilities are therefore seeking 2 x 2 MHz of additional 400 MHz spectrum so that as to have the flexibility to introduce these two options and other wide-band channel options.

It should also be noted that the current narrow band private radio systems, as well as being resilient, operate to the remotest parts of the UK. This is beyond the economic coverage areas of most public mobile systems. Further, the communications infrastructure is in place already so, providing it remains within the current 400 MHz frequency band the cost of the expansion to cover ~10 times more remote sites should be relatively low when compared with changing to a higher frequency band(s).

Answer 43b: Resilient and secure system with efficient emergency and system recovery procedures:

Whilst the existing and Smart Grid systems may be included under the general heading of Machine to Machine (M2M), they are more appropriately referred to as Resilient M2M (RM2M). This highlights that standard communications systems, including public mobile based M2M, LTE, and IoT solutions, are unlikely to be suitable for critical infrastructure systems. Electricity and gas grid networks are cautious to ensure that their control systems are resilient by, among other measures, the inclusion of an air gap between their networks and publically accessible networks, especially the public internet.

It should be noted that the base stations of critical infrastructure utilities typically have up to 96-hour power backup resilience. This is to enable efficient emergency and system recovery during the most extreme weather, etc, conditions. The cost of this power resilience is high and is therefore not typically included in standard communications systems. It is particularly important that there is resilient wide-area communications to remote rural areas because this is often where damage to the power network is likely to occur during heavy storms.

System resilience is also part of the health & safety aspect of the wide-area instant-access voice communications networks used for day-to-day maintenance and emergency repairs.

Whilst they may not recognise the importance of system resilience, the public are acutely aware of their dependence on affordable, reliable and sustainable energy supplies.

Answer 43c: Responsiveness to and readiness for rapid / unpredictable change:

The responsiveness to, and readiness for rapid / unpredictable change, is typically managed by the critical infrastructure utilities' supervision, control, and data acquisition (SCADA) networks. Any changes are reported to a communications hub that addresses the issue automatically. This can be as simple as detecting the loss of power from a faulty sub-station and re-supplying power to that area via an alternative sub-station / route. In this context, it is important to note that radio technology is of particular importance as it can be deployed more quickly than wired networks, often at lower cost as well.

45. With regard to the need for immediate action:

a) Do you agree with the proposed roles of DSOs and the need for increased co-ordination between DSOs, the SO and TOs in delivering efficient network planning and local/system-wide use of resources?

Answer a: Transmission companies already remotely monitor their sub-stations using resilient private SCADA communications networks. This remote monitoring is expected to increase to ~100,000 sub-stations. The data acquired from the DNO's sub-stations, some of which are in the remote rural locations, should be communicated to the transmission companies so that they may plan and control the transmission supplies more efficiently.

- Whilst this increase in communications requirements may be onerous, the UK's critical infrastructure utility operations have more than 30 years' experience of designing, installing, operating, and maintaining their own private SCADA / private resilient machine to machine (RM2M) systems so they are well qualified to establish the appropriate communications systems to use for smart grids.

Answer b: How could industry best carry these activities forward? Do you agree the further progress we describe is both necessary and possible over the coming year?

The DNOs, etc, would very much like to manage their networks more efficiently. Unfortunately, the lack of suitable radio spectrum is a major contributing factor that is preventing them from achieving this. As highlighted elsewhere in this response, the DNOs are seeking an additional 2 x 2 MHz of 400 MHz Band spectrum. This spectrum will enable them to remotely supervise and control most of their infrastructure. This will enable them to sweat their power assets and quickly identify, and rectify, any faults on the system.

46. With regard to further future changes to arrangements:

a) Do you consider that further changes to roles and arrangements are likely to be necessary? Please provide reasons. If so, when do you consider they would be needed? Why?

Answer 46a: on the communications side, the transmission and distribution operators appear to work very effectively together. They understand that different areas of the country require different communications solutions. For example, there are plenty of opportunities for private fibre communications in Central London whereas this may not be available in other areas. (If mandated, however, the very high cost of fibre, when compared with private radio solutions, would ultimately be passed on to the consumers.)

There is still also an on-going debate about whether the way in which the UK has implemented smart meter communications will deliver the connectivity required for real-time control. In most other countries, distribution companies are responsible for smart meter communications and back-haul data through the local substations, facilitating real-time control and distributed intelligence. It is not clear at this stage whether the UK's chosen architectural model will allow this model of distributed control to be adopted.

Innovation

48. Do you think these are the right areas for innovation funding support? Please state reasons, or if possible, provide evidence to support your answer.

In following the outcome of LCNF/LCNI projects, most have a telecommunications requirement as an essential element of the project. Frequently this is identified as a weakness, and although the chosen telecoms solution is adequate for the purposes of proving the project concept, it would be inadequate as a long term solution if the project were rolled out into 'business as usual' on a wider scale.

In JRC's view, there is a need to identify the telecoms element of projects more clearly, and trial telecoms solutions being adopted in other countries – mainly radio solutions, but currently not being deployed in the UK. The reason often relates to access to suitable radio spectrum, and the likelihood that if a wireless technology is adopted, whether adequate radio spectrum at suitable cost would be released by the UK radiocommunications regulatory authorities.

At present, there is an initiative to investigate release or sharing of radio spectrum held by government bodies which is either unused or not fully used. It is felt that closer co-ordination between the relevant government departments and regulators – BEIS, DCMS, Ofcom, Ofgem and the Central Management Unit could unlock progress to progress trials in this area with the potential for world-class innovation to the ultimate benefit of UK electricity and gas consumers through more affordable, sustainable and secure energy supplies.

Joint Radio Company Ltd (JRC):

JRC Ltd is a wholly owned joint venture between the UK electricity and gas transmission and distribution companies specifically created to manage the radio spectrum allocations for these industries used to support operational, safety, and emergency communications. JRC also represents gas and electricity interests to government on radio issues.

JRC manages blocks of VHF and UHF spectrum for Private Business Radio applications, telemetry & tele-control services and network operations. JRC created and manages a national cellular plan for co-ordinating frequency assignments for a number of large radio networks in the UK. JRC also manages a significant number of microwave links

The VHF and UHF frequency allocations managed by JRC support telecommunications networks to keep the electricity and gas industries in touch with their network assets and field engineers throughout the country. The networks provide comprehensive geographical coverage to support the operation, installation, maintenance and repair of plant in all weather conditions on a 24 hour/365 days per year basis.

JRC’s Scanning Telemetry Service is used by radio-based Supervision, Control, and Data Acquisition (SCADA) networks which control and monitor safety critical gas and electricity industry plant and equipment throughout the country. These networks provide resilient and reliable communications at all times to unmanned sites and plant in remote locations to maintain the integrity of the UK’s energy generation, transmission and distribution.

JRC works with the Energy Networks Association’s Future Energy Networks Groups assessing the ICT implications of Smart Networks, Smart Grids, and Smart Meters. JRC is also active in Utility Telecoms Councils in Europe, USA, Canada, Latin America and Africa.

www.jrc.co.uk