JRC Response to the consultation RSPG Draft Opinion on the Spectrum Aspects of the Internet-of-things (IoT) including M2M

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

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

Responses

- JRC welcomes the opportunity to respond to this consultation.
- JRC asks that the following responses be considered when finalising the text of the Spectrum Roadmap for IoT document.
- JRC highlights that almost all products and services that are offered to Europe'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 critical infrastructure utility operations.
    - It is believed, therefore, that the stable supply of electricity should be very high on the list of essential requirements for most citizens, consumers, and businesses.
- The stable supply of electricity relies increasingly on the systems that control the electricity grids.
    - Please note that whilst these fixed point-to-point (PtP) and Point-to-Multipoint (PtMP) data control systems may be included under the general heading of Machine to Machine (M2M), they are more appropriately referred to as Resilient M2M (RM2M).
- Noting the definition: *'IoT refers to the interconnection **via the Internet** of computing devices embedded in everyday objects, enabling them to send and receive data'.*
    - It is recommended that the term IoT is therefore not used when referring to critical infrastructure utility operations networks. This is because one of the easiest methods included to maximise network resilience is for the network control systems to not be connected to the Internet, or any other publicly accessible networks.
    - The broad terms of IoT and M2M are considered suitable for non-critical utility operations systems, e.g. Smart Meters.
- Noting the examples of Critical Communications systems in Table 2:
    - Not everything within a national infrastructure sector is judged to be 'critical'. The UK government's official definition of critical national infrastructure (CNI):
        - *'Those critical elements of national infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life.'*

[1] Source: Grid Carbon

- To avoid ambiguity, it is suggested that the table be sub-divided to, perhaps, include the headings of Critical Infrastructure Communications, Safety Critical Communications, Mission Critical Communications, and Business Critical Communications.
    - This is because the level of criticality of a system will dictate the level of resilience required.
    - Best Practice Resilience ('measures that can be taken to guarantee resilience, irrespective of cost'[2]) is likely to be used for Critical Infrastructure Utility Communications, Safety Critical Communications, and, perhaps, Mission Critical Communications.
    - Good Practice Resilience ('measures which can be taken to provide a degree of resilience commensurate with the Corporate risk strategy'[2]) is likely to be used for Business Critical Communications.
- It is recommended that the IoT document highlight the difference between Best Practice Resilience and Good Practice Resilience so as to prevent potential suppliers from believing that they need to deliver resilience far beyond that which may be required:
    - For example, the controlling of systems managing power lines carrying up to 400,000 volts are very likely to require Best Practice Resilience whereas public mobile systems are only likely to require Good Practice Resilience.
- Critical infrastructure utility communications Best Practice Resilience typically includes:
    - 100 % coverage of the utility service area, including remote and unpopulated areas (e.g. 30 km+ wide-area coverage);
    - Resilient Machine to Machine (RM2M) operation;
    - designed to meet exacting technical requirements, rather than for economic gain;
    - instant and guaranteed channel access;
    - ability for very low end-to-end latency, e.g. 10 ms for protection circuits;
    - up to 99.99 % link availability (e.g. for power line protection and SCADA);
    - link diversity:
        - when the primary route is interrupted, it is essential that the diversity route works immediately and correctly;
    - system and transmitted data have high levels of network security and integrity, including:
        - no connection to the Internet or other publicly accessible systems;
        - hardened to ensure reliable operation in severe environmental conditions, including electromagnetic disturbances such a lightning strikes;

[2] Source: http://www.cpni.gov.uk/documents/publications/undated_pubs/1001002-guide_to_telecomms_resilience_v4.pdf

            - up to 96 hours power backup;
        - Very closely controlled co-ordination of all systems within the band(s) of operation, e.g. using private / single-licensee licensed spectrum;
        - access to sufficient licensed spectrum, in bands with different propagation characteristics:
            - the bands may be used for redundant / diversity routing, e.g. using two or more wireless links from different sources to a remote station;
        - low jitter and synchronous requirements; and
        - longevity of equipment life and support, e.g. 10 to 20 years.
    - Please note that table 2 in the draft Spectrum Roadmap for IoT document may include items that do not require critical communications.
- Further requirements for Smart Grid Systems and Other Radio Systems suitable for Utility Operations may be found within ETSI TR 103 401. This will be followed by an SRDoc.
- The ever increasing roll-out of distributed generation, e.g. wind turbines, is putting an increasing strain on keeping the existing grids 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. For example, and as noted in the IoT document, from the UK's current 9.6 kbit/s to 64 / 100 kbit/s (see EN 300 113), and increased spectrum access. An increase to 2 x 3 MHz of 400 MHz Band private spectrum is predicted for the UK.
    - This, typical, 2 x 3 MHz of 400 MHz Band spectrum requirement for many Member States was highlighted by the European Utilities Council (EUTC).
    - The continued use of the 400 MHz band is required because of the low environmental impact of the infrastructure ("We thought it was a TV aerial!") and the propagation characteristics of the band.
    - It is understood that several Member States, e.g. The Netherlands, have already licensed systems in the 450 MHz band for critical infrastructure use.
    - It should be noted that the average future private spectrum requirements for critical infrastructure utility operations networks, including Smart Grids, is only likely to be equivalent to approximately 1.5 percent of the 1,200 MHz of spectrum identified for public mobile / IMT systems.
    - It is hoped that, when sought, this approximately 1.5% of alternative spectrum will not be seen as an excessive resource to keep the lights on, the Sunday Dinners cooked, and next door's children quietly occupied.
- Noting the comment under Section 6.b. Private Mobile Radio (PMR) networks:
    - *"PMR networks (from 30 MHz up to 942 MHz, including the 80 MHz, 150 MHz and 400 MHz bands) have provided solutions for M2M applications for many years."*
    - It should be noted that Critical Infrastructure Utility Operations have up to 50 years of experience in designing, installing, operating, and maintaining resilient machine to machine (RM2M) systems such as those used to supervise and control electricity and gas grids. It is therefore suggested that each Utility Operation may be best placed to decide which solution(s) should

be used for its own Smart Grid(s).

- Also noting the comment:
    - '*Challenges could be related to the introduction of new technology (e.g. NB-IoT) with different channel bandwidth (e.g. 200 kHz instead of 25 kHz) or to capacity shortage':*
    - It should be noted that the upload data rate (144 kbit/s) of a 200 kHz, so called, narrow band LTE system is less than the upload data rate (155 kbit/s) of a 50 kHz data system operating to EN 302 561. In this case, the 50 kHz systems are therefore approximately 4 times more spectrally efficient than the wider bandwidth 200 kHz systems.
    - Also, the 50 kHz systems have a much narrower out-of-band (OOB) impact than the OOB impact of 200 kHz systems. Broadband systems have an even greater OOB impact on adjacent spectrum.
- Noting the comment under Section 6.c. Fixed service frequencies:
    - *'ECC Report 215 (Assessment of the technical feasibility of introducing very narrow channel spacing in some existing plans, in guard bands and centre gaps of FWS channel arrangement at 6 GHz and 10 GHz) identifies additional, licensable, spectrum that may be suitable for low and medium data rate M2M systems.'*
    - It should be noted that the definition of '*narrow channel spacings for FS (25 kHz to 2 MHz)*' within ECC Report 215 does not reflect the ITU-R's definition of narrow band as being '*less than 40 kHz of necessary bandwidth*'.
    - The repeated inclusion of wide band and broadband channel spacings under the narrow band heading within international documents and meetings can be confusing. This frequently requires presenters to clarify the channel widths when referring to, so called, narrow band systems.
- Considering the availability of frequencies for IoT:
- Noting the '*challenge to make IoT stakeholders aware of their options for accessing spectrum*':
    - It may be best to limit the introduction of IoT devices to existing licence exempt devices spectrum and to operators supplying IoT services.
    - Careful consideration should be given as to how much additional spectrum may be made available for further licence exempt use. This is especially the case for IoT technologies whose radio path may not be included within the definition of a short-range device (SRD).
- Finally, there is some concern that senior decision makers could misunderstand data transfer requirements and mistakenly believe that only broadband system solutions will be acceptable for controlling critical infrastructure smart grids. Whilst it may be helpful to have the option of having private broadband radio (PBR) systems, e.g. for use within major sub-station sites, it is hoped that this response will convince decision makers and potential solution providers that 12.5 / 25 kHz narrow band and 150 kHz wide-band systems, including within the 400 MHz Private Mobile Radio (PMR) Band, are also very much a part of the long-term solution.

Joint Radio Company (JRC):

JRC Ltd is a wholly owned joint venture between the UK electricity and gas industries 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 1.4 GHz links and is keen for their protection and the on-going access to this band.

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.

Website: www.jrc.co.uk