Cover sheet for response to an Ofcom consultation

BASIC DETAILS

Consultation title:

To (Ofcom contact):

Name of respondent: Ivan Reede

Representing (self or organisation/s): AmeriSys Inc.

Address (if not received by email):

CONFIDENTIALITY

Please tick below what part of your response you consider is confidential, giving your reasons why

Nothing ☒

Name/contact details/job title □

Whole response □

Organisation □

Part of the response □

If there is no separate annex, which parts?

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

DECLARATION

I confirm that the correspondence supplied with this cover sheet is a formal consultation response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom seeks to publish responses on receipt. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here. □

Name Ivan Reede for AmeriSys Inc.

Signed (if hard copy)

Executive summary

Question 1. The executive summary sets out our proposals for licence-exempting cognitive devices using interleaved spectrum. Do you agree with these proposals?

The executive summary in section 1.5 states "The device must be able to determine with sufficiently certainty that the spectrum is not in use in the vicinity. Depending on how this is achieved, parameters such as sensing levels need to be set." Furthermore, in table 1, section 1.9, proposes the sensitivity thresholds to be "-114 dBm in 8 MHz channel (DTT) and -126 dBm in 200 kHz channel (wireless microphones)". We believe these level to non technically achievable unless modulation formats are pre-set and determined. Without such determination, it may very well be impossible for a device to discrimintate between a "signal" and spurious, man made or background noise. We don't know of any way to design toady a sensor with such discriminatory abilities for a signal format which may not exist today but may appear on the air some time in the future.

Another problem sensing brings is the possibility of sensing while in the shadow of an obstacle, such as a mountain or a hill, thereby transmitting in good faith while causing interference to other receivers that are beyond the shadow area and interfering with their normal reception.

At a minimum, all license-exempt transmitters may need to quiet down for a periodically, in a synchronous fashion and for a sufficient time period to ensure their propagated emission die out to a level significantly below the sensing threshold and thereafter for a sufficient time to allow the sensors to do the actual sensing in this quiet period.

We also question the feasibility of such a sensing scheme, at these sensitivities, as other devices, acting as non-intentional radiators, may produce spurious signals which are well within the current general EMI requirements but may mask such low level signal by causing energy to be received tens of decibels higher than the signal which the sensor intends to detect (negative D/U causing D/U sensitivity limitation rather than SNR sensitivity limitation).

For all these reasons, we believe that the sensing parameter and requirements set forth in section 1.5 will invariably lead to some level of interference, if it works at all. Moreover, if these devices are mobile, tracking them down, identifying the culprit device and silencing it may be close to impossible, with time, effectively converting this precious spectrum resource into a "junk" band, aka a tragedy of the commons. Such a situation in our view not only does not protect the consumer but places them at a serious after-sales disadvantage over time, where manufacturers and merchants are encouraged to "dump" anything on the market as long as it produces sales, with no regard for the long-term good of the people.

As an operator, we have had to confront similar problems and have concluded that the only viable solution is a database oriented approach which we have created and successfully put into operation.

In section 1.6, a database polling approach seem to be assumed. With technology readily available today, data does not need to be pulled by the device from the database. Rather, the device or the device network operator may register with a network of databases informing it of an area of interest and the network of databases may push any changes affecting said area to the device or to the device network operator.

Geo-located databases also have the advantage that they closely conform to the current regulatory models, where transmitters and coverage area are protected. Databases with the ability to push changes however may allow for dynamic changes, on a second by second basis. We have been working on such a database, starting from the well know, reliable a scalable internet domain naming system (DNS) model and transforming it into a full fledged Geo-located Electromagnetic Radiation Domain Control System (GERDCS) which has been presented to some regualtors as well as to the IEEE802. It is well received, broadcasters, manufacturers and operators alike as a very viable approach. It has the marked advantage of allowing the regulator to remotely shut down an offending device or network of devices, a class of devices found to have manufacturing defects (such as a specific model form a specific manufacturer), etc.

The geo-located database approach also allows the regulator to dynamically allocate and de-allocate spectrum over specific areas as well as across a whole country with a few keystrokes. It also relieves the constraint of “relatively low power”, as power is an output parameter set in the device by a cognitive engine we call a resolver (after the resolver in the DNS model) which, after due consideration of the terrain topology, time of day, weather, ionospheric conditions, etc... and area coexistence information, including update notices on an area of adjacent and co-channel incumbent and other license-exempt operations. A prime example of such dynamic parameters may be the current inclusion of taboo channels and out of band performance to protect existing receivers with a published gradual phase out of such protections as receiver performance improves. This could lead to a much more efficient use of this scarce and valuable spectrum resource.

Detection

In section 2.4, it is stated that low power and high power devices, if they use the same spectrum, would interfere. We would like to introduce an alternative perspective, that with properly time-synchronised resolvers, not only both may coexist, but they may time-share the channel allowing the consumer to reap the benefits of both types of networks with the same device. Cell phone industry evolution clearly demonstrates the customer's desire to be able to access multiple services from a single device rather than having to carry multiple devices, each for a specific service.

Another advantage of the geo-located database approach is that the resolver in our model is a program that can be corrected, improved and updated as technology advances. This provides more future proofing than any other technology. Therefore, the geolocated database network approach can be designed to alleviate all of the concerns raised in section 2.11

The geo-located database approach also allows from economies of scale. Thus, a regualtor may enfoce it's rules on the cognitive device on it's own terms and the same or similar device may follwe different rules as ti crosses a boundary into a different regulator's domain. Moreover, the resolver can take into account border conditions where the regulations of more than one regulator may limit the transmission levels and frequencies whithout having a “custom” unit designed for each regulatory domain.

In sections 2.13, valuable questions are proposed. In section 2.14, most answer appear to have come from the broadcast industry already using the band. We claim that a new industry is rising, with equal if not superior value to the people, that of the wireless regional area networks (WRAN) such as the up coming IEEE802.22 standard providing both traditional and interactive content over the internet. In sparsely populated areas where wired networks can no reach viable and economically sustainable operation, this may be the only way to economically bring this type of service to the people at par with what is enjoyed by people living in more densely populated areas. Here again, we believe it to be more readily testable and the results to be more positively concluding as to whether a cognitive engine like a resolver and a device complies to the conditions contained in a database versus the unsure effect of a future modulation scheme on a sensing engine.

Question 2. Do you agree that the sensitivity level for DTT should be -72 dBm?

No numerical answer as to this value, as we do not believe sensing is a viable approach to protecting the incumbents, especially in the light the future incumbents may not be modulating their signal in a method known or widespread today (we consider a 20 year horizon as reasonable and the recent advent of OFDMA and possibly new modulations, such as UWB may become more prevalent).

Question 3. Do you agree with an additional margin of 35 dB resulting in a sensitivity requirement for cognitive devices of -114 dBm?

No numerical answer as to this value, as we do not believe sensing is a viable approach to protecting the incumbents. Table 3 further illustrates the regional discrepancy, whereby applying urban and suburban parameters to rural areas would significantly, artificially and uselessly hinder usability and would probably prove to be detrimental to the good of the people. Moreover, given the typical residential separation between dwellings in rural settings, emission from one dwelling has much lower impact on the next dwelling than if they were adjacent. We believe sensing should not be considered as a viable approach to protecting the incumbents.

Question 4. Do you agree with a maximum transmit power level of 13 dBm EIRP on adjacent channels and 20 dBm on non-adjacent channels?

We agree with these values for personal portable devices, however, in the case of fixed Wireless Regional Area Network (WRAN) professional installations, as in those proposed by 802.22 which require a professional installation, many of these considerations would be addressed by the professional installer. We believe this should provide additional protection and suggest the limit for professionally installed, fixed devices be +36 dBm EIRP in non-adjacent channels. We view this as a prime example of values that should reside in a database network and could be altered region by region and over time to benefit the people by allowing services which would otherwise be precluded. This is in part why we propose the use of a geo-located, pro-active database network such as GERDCS, which has been proposed to 802 committees and is gaining momentum and acceptance.

Question 5. Would it be appropriate to expect DTT equipment manufacturers to improve their receiver specifications over time? If so, what is the best mechanism to influence this?

Yes, we believe that DTT equipment manufacturers should see protection needed to allow deficient designs will gradually fade away, according to a published public schedule. This would allow both manufacturers to improve their products and customers to gradually do away with the worst performing receivers.

Question 6. Do you agree that the reference receive level for wireless microphones should be -67 dBm?

No answer

Question 7. Do you agree with an additional margin of 59 dB for wireless microphones?

No answer

Question 8. Do you agree with a sensitivity requirement for -126 dB (in a 200 kHz channel) for wireless microphones?

No answer

Question 9. Do you agree with a maximum transmit power level in line with that for DTT? Are there likely to be any issues associated with front end overload?

No numerical answer as to this value, as we do not believe sensing is a viable approach to protecting the incumbents. Our interest is towards professionally installed fixed devices to serve customer premise equipment. Here again, applying such requirements to professionally installed, fixed equipment would significantly, artificially and uselessly hinder usability and would probably prove to be detrimental to the people. We believe that fixed, professionally installed devices could easily operate up to a +30dBm conducted transmit level for customer premise equipment (CPE) and +56dBm for base stations (BS) using a database network to protect such venues. Moreover, the database could then prohibit transmission on channels immediately adjacent to the channels used by the microphones yet provide permission to use such channels when the microphones are not in use (for example, from 3AM to 6AM). The database could be used to specify the maximum power (conducted as well as EIRP) rather than regulating power a priori.

Question 10. Do you agree that the sensitivity level for mobile television receivers *should be -86.5 dBm?*

No answer

Question 11. Do you agree with an additional margin of 20 dB for mobile television?

No answer

Question 12. Is it likely that mobile television will be deployed in the interleaved spectrum? If so, would it be proportionate to provide full protection from cognitive access?

Given that there are fully protected, clear channels, we believe television should be disallowed in the interleaved spectrum. We believe it disproportionate that the interleaved spectrum should hinder provision of wireless internet to the people. Although we do appreciate the value of broadcasting, we also believe in the undeniable value to the people of ubiquitous low-cost internet delivery via air waves (where it is also possible to deliver the same television content in a spectrally more efficient, streaming IP format).

Question 13. Should we take cooperative detection into account now, or await further developments and consult further as the means for its deployment become clearer?

No, over and above high complexity and risk, we believe there are too many problems associated with this, including mechanisms allow denial of service attacks.

Geolocation databases

Question 14. How could the database approach accommodate ENG and other similar applications?

ENG is an activity generally made by a collective of people. From the managed decision of actually gathering news to the time news are gathered, one could foresee that a few seconds may occur. The management could simply inform the database that it wishes to use some frequencies for ENG in a given area. The GERDCS system allows for this, whereby an authorised person defines on a graphical interface the frequency range to be provided protection, the geographical area over which the protection is to be offered and the time period at which it applies. Within a fraction of a second, GERDCS pushes forward this information to all affected devices, thereby offering protection much faster than any database polling system. Moreover, it is totally conceivable that the news crew itself could make such a request over the internet or could (using a device such as an autheticated cell phone) make such a request, providing an instantaneous temporary “bubble” of protection around it, including the possibility of a “mobile” bubble if the ENG event is mobile.

Question 15. What positional accuracy should be specified?

The approach we take with GERDCS makes away with such a requirement. GERDCS places the onus and responsibility where is traditionally resides, with the network operator. Any transmitter under its control is not to cause harmful interference. GERDCS proposes a two tiered system of database servers and a resolver in each network. We use a two tiered system in GERDCS to allow protection of privacy for substribers. We also use a two tiered system of database servers and a resolver in each network, thereby preserving the network operator's responsibility to provide a bubble of sufficient diameter to protect PMSE ENG activities. With this database network approach, there are no possible evasion as to responsibility that sensing may provide given it's uncertainty. In our view, the cognitive device operator has to provide protection, without excuse, as all other radio operators must.

The ENG crews simply states the reasonable area to be covered by the protection bubble. It is up to the network operator to increase the size of the protection bubble by the transmitter's positional uncertainty or take any other action to provide protection, no questions asked, no side-stepping or evasion being possible as to his responsibility.

We believe such a regulation is more readily enforceable, simpler for the regulator and allows for remedial action against the network operator, thereby ensuring such operator will err toward caution rather than unacceptable risk.

For this reason, GERDCS keeps a log of all changes made to it by the PMSE (with date, time and authenticated, authorised author)

Question 16. How rapidly should the database be updated? What should its minimum availability be? What protocols should be used for database enquiries?

Section 6.9 states that there must be a single “master” database. We believe this to be one of many possible paradigms. The internet DNS system clearly demonstrates a scalable, distributed database network of information sources. IEEE 802 has come to accept this paradigm of the database-resolver approach. GERDCS follows this approach, being formed of a collective of databases. Each database operator is responsible and accountable for the completeness and correctness of the information his database contains. Moreover, he assumes full liability for any damage his database content may do to third parties, whomever they are. Licensed PMSE and DTT operators could be responsible for losses that excessive and unwarranted protection claims may cause to cognitive device network operators in exactly the same way that cognitive device network operators would be responsible for any damage they may cause to DTT and PMSE ENG activities if they do not provide them reasonable protection from interference. Using this approach, we believe responsibility and liability can be clearly delineated and the traditional court system may deal with any infringement claims within the industry rather than needing continuous oversight by OFCOM.

Moreover, we believe that in this model, there is no question as to the probability the network will be “put up”. It will be to each one's advantage to put up their own database server or to obtain access or gain protection. Updates in the GERDCS approach are virtually instantaneous as information is pushed rather than polled. Incumbents should be able to count on the existing OFCOM database for protection. They could, like PMSE ENG activities, also provide their own database servers in the network. Database availability would be the concern of the incumbents and the network operators and therefore would not need to be regulated. Incumbent protection for sporadic events would simply be offered while the database is available. Cognitive network operators could be required to only transmit while they are connected and “on-line” with the database network.

GERDCS uses standard ssh connections, using open, time proven and well known authentication and access control mechanisms. It logs and journals all instructions it receives, all queries it receives, all responses it provides and the acknowledgements it gets.

Question 17. Is funding likely to be needed to enable the database approach to work? If so, where should this funding come from?

We believe long term funding will not be needed as it will be to the advantage of each operator (incumbents as well as cognitive network device operators) to have their servers and resolvers up and running. The long term cost structure we see should be similar to that now seen for URL registration on the internet. Much as in the DNS system, the regulator (or his delegated authority) would only need to operate a “root” domain database for a given country. We do not see such minuscule costs of doing business as an impairment to the day to day operation of DTT, PMSE or cognitive network device operators.

Question 18. Should the capability to use the database for spectrum management purposes be retained? Under what circumstances might its use be appropriate?

Section 6.13 appears to be based on the premise of a central database. In the distributed model GERDCS proposes (although a central database could be supported), there is protection for confidentiality of information via resolvers, as required in certain countries of the commonwealth. GERDCS does not cause a database inquiry for each end device. Rather, the operator runs a resolver service (a cognitive, network “better connected device”) that informs the database of his area of interest (normally a superset of his coverage area and frequency ranges). The resolver periodically performs a standard “rsync” (for added security) and thereafter, the database network only sends change notices when they occur to the resolver. If connectivity between the resolver and the database network is lost, the operator has to cease all transmissions within a given period of time. The resolver controls all the network's transmitters. It does not need to bother the database with all the individual queries for each individual transmitter, queries which may indeed be very frequent if the devices are mobile. More importantly, it does not need to relinquish any information about any subscriber to the network, this being un-neccessary and which may violate privacy of information laws in some jurisdictions. To provide traceabliity in case of interference, network devices need only broadcast the network ID to which they are tethered and a unique network device ID. Resolver keep a live registration in the system as to all the domains they control via network Ids.

We believe the retention of the use of the database for spectrum management is of value. It allows a definite ability to audit incumbent protection claims and for database network operators to validate incumbent database contents. It also assures some redundancy in the network of databases, being the ultimate authoritative means for the protection of incumbents.

Question 19. Should any special measures be taken to facilitate the deployment of cognitive base stations?

In the GERDCS system, the database network describes protection contours rather than signal levels and the resolver, taking into account base station antenna pattern, height, etc, computes and decides on the actual permissible radiated power in any given direction. This decoupling simplifies and provides for scalability of the database network, as the database does not concern itself with transmitter specific parameters, it concerns itself with describing the protection to be given. In the GERDCS model, since a network operator is responsible for any damage he may cause to others, will have to operate or obtain the services of a resolver before any network device can effectively transmit. Special measures are therefore not required.

Beacon reception

Question 20. Where might the funding come from to cover the cost of provision of a beacon frequency?

In our model, we use a similar approach to that is offered by the upcoming 802.22 standard. We believe the devices are in communication with a resolver. Base stations wanting to allow devices to associate with them will periodically transmit in their medium access control headers information thereby removing the need for beacons on a separate beacon frequency. Any mobile device or client device will refrain from transmitting until it hears a service provision announcement from a master or base station.

Question 21. Is a reliability of 99.99% in any one location appropriate? Does *reliability need to be specified in any further detail?*

In our model, there is no need for a beacon network. If the base station or master station signal is not received, the devices are out of range and need not and shall not transmit. Clients and the market forces they generate will impose reliability, people moving away from unreliable networks in favour of the more reliable networks.

Comparing the different options

Question 22. Do you agree with our proposal to enable both detection and geolocation as alternative approaches to cognitive access?

No. We believe detection to be unworkable in the real world at this time. Allowed EMI, caused by unintentional radiators far exceeds the levels sensing requires and the signals to be detected may be masked by the unintentional radiators. The bus example used fairly illustrates such eventuality. It is not uncommon in a crowded bus to find quite a few personal electronic devices operating and they all have the potential of causing some form of EMI, making sensing fail and rendering it useless to protect incumbents and PMSE. In our view, the sensing proposal also has a major flaw in that it allows easy and simple denial of service attacks, attacks which the internet has already shown are not only possible by highly probable. There are financial concerns which may fear the advent of the competitive capabilities and have reason to legally exploit such an easy denial of service mechanism. Operators, being uselessly denied service (due to DOS attacks of simply sensing detecting false positives), may be tempted to circumvent the failing mechanism, thereby denying incumbents the protection to which they are entitled, by license. We believe sensing, although interesting, is not technically feasible as the sensitivity required to protect low power microphones is so high that man-made noise will make it fail in real-life environments. Moreover, the use of such a technology will impose un-necessary and excessively restrictive limitations on base station or master station power. Such restrictions are not compatible with the good of the people.

Other important parameters

Question 23. Should we restrict cognitive use of the interleaved spectrum at the edge of these bands? If so, what form should these restrictions take?

Not directly. We believe protection requirements can and should be described in a database network (like GERDCS) and cognitive network operators should be allowed to exploit this spectrum if there is incentive for them to do so. Candidly, we believe that such incentive will be low as long as alternative, easier to use spectrum is available. When spectrum usage becomes crowded, this situation may change. We expect usage will vary by region, following population density, market demand and penetration and types of services provided.

Question 24. Do you agree that there should be no limits on bandwidth?

Yes, provided total power and power spectral density is limited such as to prevent a narrowband transmitter to gain dominance over others by concentrating all the admissible power over a very narrow bandwidth is made and provisions are made to allow wide band and narrow band devices to communicate together for coexistence and band sharing. We do believe spectral power density may need to be controlled to avoid a few narrowband devices from gaining dominance by using high power densities and denying access to the band by a plurality of wideband devices which may otherwise be delivering valuable service to the people.

Question 25. Do you agree that a maximum time between checks for channel availability should be 1s?

We believe channel checks should be made via the database. Under those circumstances, updates should be practically immediate. We propose that the resolver contact the databases every 60 seconds to establish and maintain live virtual connections. Furthermore, we propose that the entire network of cognitive devices cease to transmit if database access cannot be confirmed within a 2 minute period. Such database would allow for sudden microphone appearance (as in the example given) be reserved for a few hours, covering the entire show and allowing show staff to confirm protection exists a-priori rather than risk mis-detection and the quite distasteful and embarrassing consequences.

Question 26. Do you agree that the out-of-band performance should be -44 dBm?

We believe this is a database network parameter. We believe that sensing is not viable, neither technically or reliably.

Question 27. Is a maximum transmission time of 400ms and a minimum silence time of 100ms appropriate?

We believe this can be managed by the database. We do not believe in sensing is workable in real life at this time. Moreover, if silent periods are implemented for sensing, in view of the weak signals to be detected, they must all be synchronised, no matter what the device is. Such a requirement is very constraining, especially when there is no proof that such a constraint is necessary as applied to a non-existant sensing technology. One such example constraint is the barring of all video and audio quasi-real-time traffic. We propose that if such silent periods are provided for sensing incumbents, that they be synchronous to the upcomming IEEE802.22 and IEEE802.22-TG1 PMSE protection beacon standard now in sponsor level approval. This group of industry professionals, including equipment manufacturers, network operators and broadcast incumbents has taken many years, studying and determining how to balance quality of service allowing both audio and video quasi real-time streaming as well as network access fairness. We believe OFCOM should pay close attention to the work done in this group of experts as it combines the joint interests and expertise of Broadcasters, Manufacturers and Operators from the entire planet.

Question 28. Is it appropriate to allow “slave” operation where a “master” device has used a geolocation database to verify spectrum availability?

Yes, we believe this to be correct, provided that the master device has access to a device such as a resolver and that the bubble of protection used in the resolver takes into account the range of the master station. In the case where the range of the master station may be large, the operator may have an incentive to geo-locate the slave devices in order to allow operation in some areas by some slaves while banning transmission by other slaves in other areas (although broadcast stream, such as video may still be allowable).