SMETS 2 Comments

REDACTED REDACTED REDACTED REDACTED

REDACTED REDACTED

General Comments

SMETS2 is very prescriptive in a number of areas describing the solution rather than the interface requirements. This will have the effect of restricting innovation and cost reduction going forward, limiting the solutions to 2012 technology. Bearing in mind the life of a meter is 20 years and the programme will take a number of years to complete, it is likely technology will have moved on in that time frame. SMETS should be concerned only with interfaces and required functionalities with reference to European Standards, not the detail of how these are to be implemented, this should be left to the manufacturers innovate and the market to decide.

There are a number of European standards and other documents relating to smart metering that DECC should take account of when developing SMETS:

- CEN/CENELEC/ETSI Technical Report TR50572 – Standards for Smart Metering
- IEC 62055 series of standards for payment metering
- IEC 62056 series of standards for communications with meters (DLMS)
- ZigBee Alliance Document 075356r16ZB – Smart Energy Profile
- NIST 7628 – Information Security
- CEN/CENELEC/ETSI Technical Report on Smart Grid Security (M490)

There are a number of features suggested in the document that will add significant cost to the programme. These are highlighted in the relevant sections but to summarise the major ones:

REDACTED

HAN Solution

Do you have any comments on the criteria used in the evaluation of the application layer standards?

There appears to be some confusion throughout the document on what ZigBee Smart Energy Profile and DLMS provide. ZigBee SEP/DLMS is not a protocol and does not exist, neither is it planned to exist.

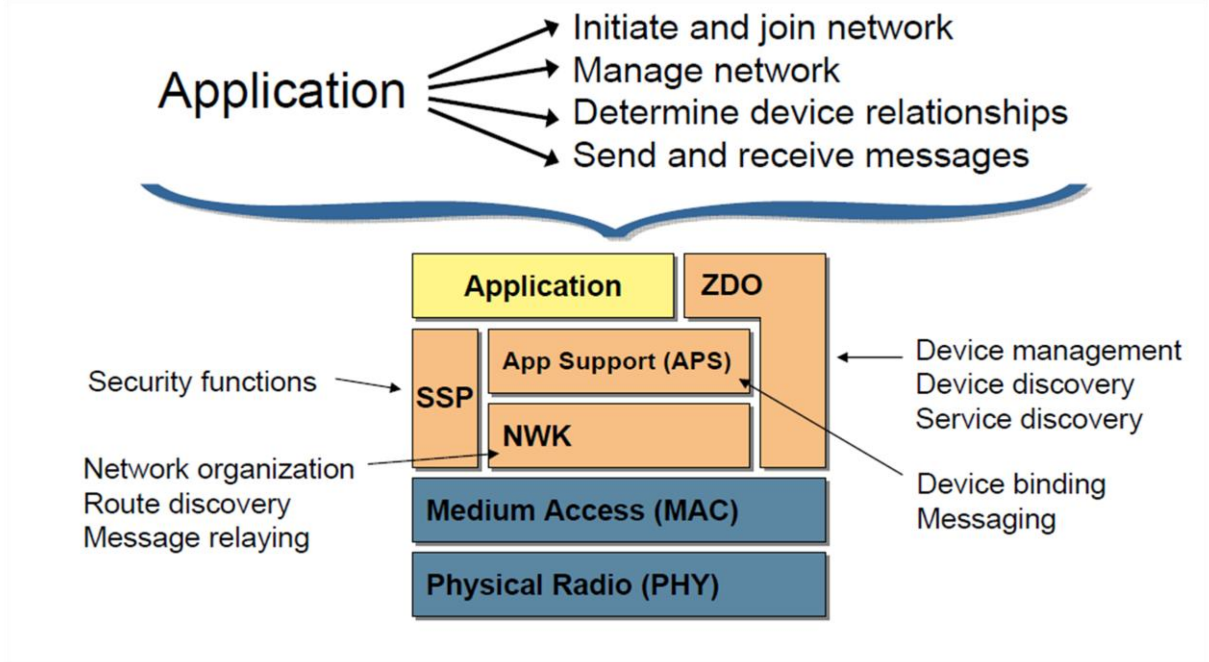

Figure 1 - ZigBee Scope

Figure 1 shows the scope of ZigBee. It comprises three layers:

- The physical/medium access layer (the IEEE 802.15.4 radio).
- The features that control the radio network to support the mesh, the security, service discovery and device management.
- The Application Layer – that specifies a standard set of commands and attributes for a particular application – for example smart energy, home automation, medical, etc.

All three layers must be certified as interoperable in order to gain ZigBee certification.

DLMS is an application layer only. It has features that could be used to control the lower layers of the communication stack. It is not related to ZigBee except through the fact that ZigBee Smart Energy 1.1.1 allows for a tunnel to be created to transport other protocols. ZigBee takes no part in the third party protocol, it simply provides commands and attributes to set up and close the tunnel and a method to allow devices to confirm they can support the third party protocol.

SMETS2 should simply specify ‘ZigBee Smart Energy Profile’ for the HAN.

Do you agree with the proposal to adopt ZigBee SEP / DLMS as the HAN application layer standards for GB?

Firstly, as mentioned earlier, there is no such protocol as ZigBee SEP / DLMS, ZigBee SE and DLMS are completely different.

There are a number of incorrect statements and assumptions in the document when comparing DLMS with ZigBee SE. ZigBee SE is perfectly capable of providing all the functionality required for smart metering and it is already used elsewhere in the world for this purpose (eg Korea).

It is also incorrect to say that DLMS is not suitable for gas as it already supports gas (and heat) meter objects and methods. COSEM objects can be transported over M-Bus as implemented in the Netherlands and Germany. However, it is probably true to say that ZigBee SE is a better solution for gas than DLMS due to the lower power requirements.

DLMS was designed for WAN applications, it is not for the HAN and depending upon the architecture may never appear on the HAN. The electricity meter may or may not support DLMS. If DLMS is used over the WAN then the communications hub must support it.

It is perfectly feasible for ZigBee SE to be used to transport data over the WAN using the ZigBee Gateway Protocol and hence DLMS is not essential for the WAN or the HAN. The latest proposals from STEG recommend the composition of HAN messages at the head end to improve end-to-end security so it therefore seems illogical to consider converting from ZigBee to DLMS at the head end for WAN transportation and then convert back from DLMS to ZigBee for the HAN at the meter end causing extra work for no apparent reason.

The DLMS protocol is only appropriate if the electricity meter communicates directly with the head end through the communications hub over the WAN and HAN. The electricity meter will have to support the ZigBee SE commands and attributes in order to communicate with the IHD. This means the meter will have support two protocols and hence will be increased cost if the recommendations are adopted. The additional cost of hardware to support dual protocols in the electricity meter will amount to approximately REDACTED for the extra memory and processing power. (REDACTED in total for the GB roll out). There will also be a cost associated with handling DLMS in the Communications Hub of similar amount – another REDACTED thereby increasing the total cost for DLMS support to REDACTED.

There will be a cost associated in implementing DLMS and ZigBee messages at the MDMS (head end) – most MDMS systems will have neither at present. The work involved in implanting two new protocols will obviously be higher than one. There should be a cost/benefit analysis in specifying two protocols rather than one – this piece of work appears to have been overlooked by DECC.

There will be an on-going cost associated with supporting two protocols – twice the regression testing every time there is a firmware upgrade and twice the security testing in addition to the extra risk of failure due to software bugs caused as a result of the extra functionality. This extra cost and risk arises simply because one of the devices (the electricity meter) has a perceived requirement to support DLMS in addition to ZigBee. It is difficult to justify why this should be the case in an enduring solution as it will be the root cause of on-going issues throughout the lifetime of the metering fleet. It should be left for the market to decide if DLMS is to be used. It is unlikely given the extra costs and risks involved that a dual solution would be viable, DECC should not therefore be seen to force such a solution on the market.

DLMS GOOO (General Objects Over OBIS)

A new development in the DLMS specification allows users to send other protocol packets over a DLMS network using the GOOO protocol. This allows ZigBee SE (or other protocol) packets to be assigned standard OBIS codes and transported over the WAN.

The advantage with this approach is that the end-to-end system complies with IEC standards and to the ZigBee specification where other systems proposed such as the ZigBee Gateway Protocol do not.

DECC should consider this approach as a viable approach as it reduces the need for protocol conversion at the Hub.

ZigBee SE 2.0

ZigBee SE 2.0 has reached its testing phase and has now caught up with the DECC SMETS2 programme. Maybe it is time to reconsider the decision to adopt ZigBee SE 1.0 and DLMS for the following reasons:

- ZigBee SE 2.0 is IP based with internet standards applying to the transport layers
- ZigBee SE 2.0 objects have been aligned with the IEC 61850 CIM model meaning they are compatible with IEC standard head end systems
- ZigBee SE 2.0 can be transported over any physical layer including 2.4 GHz radio, 868 MHz radio, power line, GPRS, Ethernet or any other IP based PHY.
- End to end security is catered for without any need for translation using standard PKI and symmetric key technologies
- Interoperability is assured through the use of internet protocols.
- Smart Grids are to be IP based, ZigBee SE 2.0 will therefore be compatible.

Do you agree that equipment should be required to comply with SMETS and a GB Companion specification for ZigBee SEP / DLMS?

Companion specifications are essential for both ZigBee SE on the HAN and for DLMS on the WAN. The report from the DECC Application Layer Working Group produced in July 2011 detailed the work required and should be noted.

The ZigBee SE profile specification specifies a set of mandatory commands and attributes that devices must support in order to gain certification. This is a minimal set and will not provide the functionality to meet SMETS. In order to meet SMETS, a specific set of optional commands and attributes must be defined. The ZigBee companion specification has to be in the form of a Protocol Interface Conformance Specification (PICS) and must specify the set of optional commands and attributes required for SMETS. If this specification is to be written by DECC they will most likely require assistance from members of the ZigBee Alliance as it will require specialist knowledge of the Protocol specifications.

DLMS provides a framework to build a set of objects and methods to support the transportation metering data. There is scope for interpretation of how the objects and methods are implemented and this gives rise to interoperability issues. It is therefore essential that DECC provides a definitive companion specification that details exactly how each and every object and method is implemented. Such documents exist in other countries where DLMS has been adopted already. The IDIS organisation has provided such a document for Spain for example. Drafting this document will be a highly specialised and time consuming process and will require the expertise of the DLMS User Association. Typically such a document takes over 1 year to complete.

It should be noted that by specifying both ZigBee SE and DLMS the work involved in producing companion specifications will be doubled as will the conformance testing. A solution based wholly on ZigBee would be much faster to implement and would be lower cost. Use of the GOOO protocol on DLMS will allow ZigBee packets to be used end-to-end.

Do you agree with the overall approach proposed in relation to the HAN physical layer? If not, please provide a rationale and evidence for your position.

The HAG came to the conclusion that ZigBee on 2.4GHz would not provide sufficient reliability based on evidence collected in a small scale evaluation. It did not take evidence from the field where such systems have been depolyed at scale, for example:

- The ~ 1000 EDRP kits installed by REDACTED REDACTED where very few issues were encountered on the 2.4GHz EmberNet HAN (but there were significant GSM based WAN issues).
- REDACTED field experience with 2.4 GHz ZigBee based roll out with ~5000 homes fitted with ZigBee based meters.

- The EDRP kits installed in REDACTED based on Z-Wave 868 based HANs where several issues were encountered in HAN reliability.

Do you have any comments on the criteria used in the evaluation of the physical layer of the HAN?

Propagation theory does indicate that lower frequencies will be more suitable for penetrating walls and this was borne out in the REDACTED tests.

The REDACTED tests failed to take account of the enhancements provided by the full solution such as the error correction, mesh capabilities, routing and retry mechanisms provided by the ZigBee protocol stack and hence did not provide the full picture.

What are your views on the compatibility of the reserved spectrum 870-876 MHz with 868 MHz and the value of considering the use of this band?

No opinion but such a move would allow for greater choice of channels.

Do you consider that additional measures should be taken to encourage the development of an 868 MHz solution?

The ZigBee Alliance has set up a working group to define a suitable 868 MHz solution based on the new IEEE 802.15.4g standard which allows greater payloads and bandwidth than the current sub-Giga Hertz solution. This will be driven by members of the Alliance provided a suitable market exists. There are requirements for sub-Giga Hertz solutions elsewhere in the world (Japan and the USA) that will provide further commercial incentives to add to the UK requirements.

Do you agree with the approach to allow the market to determine the balance between 2.4 GHz and 868 MHz? If not, please provide rationale and evidence.

Use of the two frequencies will cause interoperability issues and add cost if both frequencies have to be supported within the home.

It is likely that the initial use of the 868MHz band will be to reach the gas meter and lead to the need for dual band (and dual radio) solutions which will be higher cost of roughly REDACTED per home or REDACTED REDACTED for the roll out. The market will ultimately decide the best approach however such an architecture will provide the opportunity for alternative solutions such as that detailed in Appendix A. Such an alternative solution will be more versatile, more secure and provide enhanced customer experience.

If 868MHz is considered to be the way forward for reaching gas meters then Wireless M-Bus should be considered. It is already deployed at scale in the Netherlands and Germany and is already an EU standard.

Consider Figure 2. This provides the required functionality for smart metering, uses 868MHz M-Bus for gas communications and ZigBee for the HAN devices and complies with the reference architecture contained in CEN/CENELEC/ETSI technical report TR50572 (Smart Metering architecture to meet Mandate M441). It will also be seen that there is no radio connection between electricity meter and hub in this solution, a cost saving of roughly REDACTED. (REDACTED REDACTED for the programme)

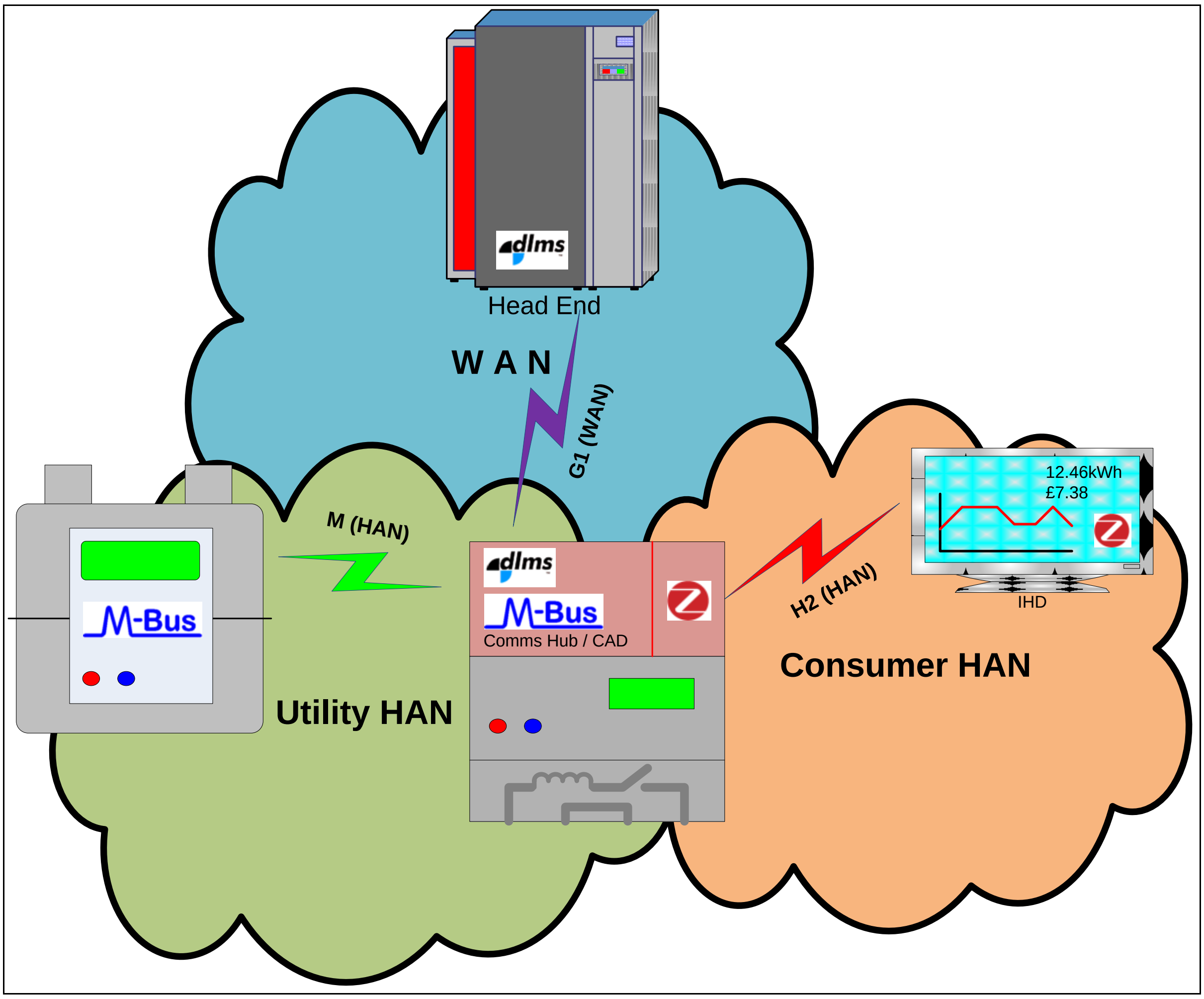

Figure 2 - An architecture using existing EU standards and compliant with TR50572

What are your views on the three options identified for deploying wireless solutions (i.e. 2.4 GHz as the default; dual-band communications hubs; or market led)?

There will be interoperability issues caused by allowing alternative solutions into the market but it will create the opportunity for the best solutions to develop.

Option 1 makes assumptions based on tests that did not take account of the features provided by the communications stack that includes error correction, routing and retry mechanisms. It therefore draws conclusions that may be incorrect. Evidence should be taken from existing real installations.

Option 2 is flawed. The cost of a radio module is REDACTED in volume. The £2.50 assumed cost is only for the silicon chip, additional components such as antenna, ballun, crystal and other peripheral parts have been ignored.

Option 3 makes sense. It would be even better if the architecture shown in Figure 2 were adopted as the consumer HAN would be outside the scope of the utility HAN and therefore most of the issues regarding propagation, installation and security would be outside scope. Repeaters could be used without potential compromise to the metering data – disconnection of a repeater would only affect the IHD and other consumer devices.

Do you agree with the proposal for a ‘fit for purpose’ installation obligation on suppliers?

Such a requirement would be almost impossible to achieve in all types of home. In the extreme it would require a wired solution to be installed in some cases. If the supplier was required only to fit metering equipment in a utility HAN and that had to be ‘fit for purpose’ then this would be more practical and achievable.

Do you have any views on the proposed approach to developing a wired HAN solution?

A wired HAN based on PLC technology would provide a practical alternative but a ‘short hop’ radio link would be needed for gas. It may be possible to devise an ATEX approved wired link to the gas meter.

If a wired link is acceptable, then it may be possible to power the gas module from the electricity meter thereby removing the need for a battery in the gas meter. This approach would work where the two meters are located close to one another as in many modern houses.

Communications Hub

Paragraph 64 outlines the requirement to support a CAD. This will require two HAN radios adding REDACTED per home to the cost or REDACTED REDACTED to the programme. Is there a business case for this?

Do you agree with the proposed scope of functional requirements for a communications hub? Are there any other functions that should be included and what would be your rationale for including those functions (including estimated costs and benefits)?

The communications hub is considered as a stand-alone device. This means it has to be powered from the supply side of the meter if it isn’t to be cut off by the electricity meter’s contactor. It is proposed that the Hub communicates to the electricity meter over the HAN despite the fact there is a wire between the two. This means the electricity meter must be fitted with a HAN radio and the associated functionality to control it and must go through a time consuming commissioning process. All this will add cost to the system of around REDACTED per home or REDACTED REDACTED to the programme cost.

Not only will there be additional cost but there will be issues with security and reliability.

The separate comms hub approach is therefore flawed from a technical and cost point of view.

A Gas Meter Mirror has been specified as a required feature of the Communications Hub which is sensible since the gas meter cannot support full time radio communications. However, the specification for the gas meter states that it must support all ‘smart’ functionality. This functionality can just as well be supported in the Communications Hub since it will be required to support the mirror. In effect DECC is specifying two gas meters per home, one the real meter, the other the mirror. The gas meter electronics can be reduced to a simple pulse counter/data logger with HAN radio and valve control (if required), reducing the cost of the gas meter to between REDACTED and REDACTED depending whether or not a valve is fitted. This represents a saving of around REDACTED per home or REDACTED REDACTED to the programme.

Appendix C outlines a scheme to allow the prepay functionality to be performed in the Communications Hub if required. In the 85% of homes not on prepay, the system would be very much simpler.

SMETS2 does not appear to allow for the gas meter being powered from the Communications Hub in situations where gas and electricity meters are co-located. This option would save the cost of a gas meter battery at REDACTED.

Do you have views on the specification for an 'intimate' interface between electricity meters and communications hubs?

The intimate communications hub would be a sensible approach and this is how other countries have proceeded.

There is a new work item proposal under consideration in CENELEC as part of the M441 standards work that considers how to approach standardisation of the interface (the 'M' interface as described in TR 50572.) This work will consider the mechanical features, electrical requirements and suitable protocols to be adopted. (See Appendix B). The work will take some time to complete, the German authorities have already tried and failed to reach agreement after 18 months of consultation.

Do you agree with the Government's marginal preference for the CSP-led model for communications hub responsibilities, or do you prefer the supplier-led model? Please provide clear rationale for the advantages and risks associated with your preferred option.

The CSP lead approach will require them to not only be responsible for assuring the WAN performs correctly but also that the HAN meets all the necessary requirements – including the operation of the gas mirror. CSPs may not possess such expertise.

The Hub will be the HAN coordinator therefore any issues on HAN connectivity will be the responsibility of the CSP. CSPs may not wish to be responsible for issues on the HAN.

The proposed approach may lead to a monopoly in the supply of hubs similar to the GPO telephone in the days before BT was privatised. There will be little incentive for cost reduction or to provide new features.

A more suitable approach would be for the CSP to license the design of their WAN solution to Hub manufactures to integrate into their products.

Do you agree with the proposal that a CHTS-compliant communications hub should not be mandated for opted out non-domestic sites and that suppliers should be free to use whatever type of communications equipment best supports their processes and WAN service?

This makes perfect sense and allows competition.

Do you agree that the gaining supplier should bear the costs of installing an appropriate communications hub if they decide to switch between opted in and opted out?

Yes – that would provide incentives to ensure standards were adopted within the industry without the need for government intervention.

SMETS Additional Capabilities

Do you agree that the design and implementation of outage reporting functionality should be assigned to CSPs, documented in the communications hub technical specification?

Yes – although the proposals contained (eg report after 3 minutes) will add considerable cost to the power supply in the Hub – anything up to REDACTED per hub (or REDACTED REDACTED to the programme).

Do you agree that it would be inappropriate to require meters operated outside DCC to be required to implement outage reporting? Please provide rationale to support your views.

It would not only be inappropriate for meters outside the DCC to report power outages but it would also be inappropriate for all meters within the DCC to do so. It should only require that a proportion of meters are fitted with this capability to reduce the amount of traffic on the network and to keep costs down. (If one house in a street goes off supply then it would be safe to assume they all go off – it only needs special meters to be place in strategic locations to provide outage alarms.)

Do you agree that maximum demand registers should be included in SMETS? Please provide evidence to support your position and provide evidence on the cost implications of delivering this functionality via back office systems or via the meter.

This functionality is very simple to implement in the meter at little or no cost. It requires a few lines of code and a small amount of memory. Similarly, the cost of implementing the functionality in the back office would be minimal compared with the cost of other functions (such as prepay).

Do you agree with the proposal not to include the capability to generate additional voltage alerts based on counter thresholds in SMETS 2? Do you have any evidence that could justify including this functionality in SMETS 2?

Voltage alerts only need to be added to a proportion of meters. All meters measure voltage, they have to as part of the measuring process so it is a 'no-cost' feature. It only requires a few lines of code to detect a threshold and generate an alert. However if there is an issue in an area then it is not required that every meter reports the problem. The feature should only be enabled in strategically placed meters to prevent overload on the WAN.

If DNOs were permitted to access remote disablement functions, should control logic be built into DCC systems or meters? If the logic should be built into meters, should the logic be specified in SMETS 2? Please provide rationale to support your position including estimates of the cost of delivering this functionality under the different options being considered and any evidence relating to safety issues associated with each option.

Under no circumstances must the switch in the meter be considered a safety device – it is NOT. (See IEC 62055)

The contact gap does not provide for safe isolation and it only disconnects the live feed.

Neither must the switch be reclosed remotely – it will cause a death at some point. The safety features employed in prepay meters must be adhered to whereby the switch is 'armed' such that the consumer can close it by pushing a button.

A 'smart grid' that relies on cutting the supply to a whole house is not a very smart way to control load. A more appropriate method is to control individual loads as the radio teleswitch does today.

Fitting a switch in every meter by definition will reduce the reliability of supply to homes currently not on prepay as the switch will fail in a number of cases and the supply will be cut off. (This has already happened in a number of cases – 100,000 keymeters failed in REDACTED, all radio teleswitches in REDACTED REDACTED failed on two winters nights, mechanical failure in REDACTED meters and numerous others).

The meter will now form part of the critical national infrastructure. It has been estimated in the Netherlands that 45% of the smart meter system costs are associated with security measure to ensure the switch does not open incorrectly.

Meter Variants

Do you agree that variant smart electricity meters should be specified in SMETS 2 and that the cost uplift for variant smart meters is similar to that for variant traditional meters? Please provide evidence of costs to support your views on cost uplifts.

Variants to standard designs will cost more by definition. Some manufacturers will see niche opportunities and supply this market – that is how these meters came into being in the first place. It is up to the market to decide how the functionalities will be provided in SMETS 2.

Randomisation

Do you agree that randomisation offset capability should be included for auxiliary load control switches and registers as described above? Do you have views on the proposed range of the randomisation offset (i.e. 0 – 1799 seconds)? Please provide evidence on the cost of introducing this functionality.

The Radio Teleswitch provides a simple randomisation feature of a few minutes either side of the switching time. To suggest almost 30min of randomisation seems excessive when the electricity pricing is in 30min periods. This could throw a consumer into the next price point for no reason.

I would suggest that the same regime as employed by the RTS that has worked for many years is adopted on the grounds of simplicity.

Consumer Access Device

Do you support Option 1 or Option 2 for ‘pairing’ a CAD to the HAN? Please present the rationale for your choice and your views on the implications that these options have for the technical design of the solution.

It should not be for the government to decide how consumer devices gain access to the HAN – this is a market issue.

If the architecture as shown in Appendix A were adopted then there would be no issues of privacy or issues on how to pair the devices.

The scheme proposed by the government would require suppliers to provide help desks to assist customers with their HAN equipment and would include support when things went wrong – not a prospect that suppliers would like to take on. Also there is no guarantee that equipment added to the HAN will not interfere with the metering. A rogue IHD could easily deny communications to the gas meter for example.

The government need to fully consider the security and privacy implications arising from their proposal and the cost implications on suppliers that may arise.

If Option 2 were adopted, do you agree that obligations should be placed on energy suppliers to support this process by submitting ‘pairing requests’ to the DCC on request from their consumers?

That is up to suppliers to answer but one can imagine the chaos following a special offer at REDACTED where a million ‘Super IHD’s’ were sold over a bank holiday weekend and they proved difficult to pair as the Chinese manufacturer had forgotten to include a minor feature. The option is flawed as it creates the need for call centres with systems in place to handle any issue arising from adding devices to the network and this need will increase with time as more devices become available. This option will commit suppliers to provide a service for an unknown and increasing workload.

Do you consider that other CAD installation options should be pursued? If yes, please explain the approach you favour and your reasons.

Yes – as mentioned earlier, consider Appendix A. A CAD would be included in the hub and the metering HAN would be immune from interference from the consumer HAN (as in the German architecture). The Consumer devices could be added independently of the utility HAN just as WiFi routers are handled today without the support of the supplier.

Prepay Interface Device

Do you agree with the proposal to include in SMETS 2 a specification for a PPMID, connected via the HAN, as described above?

Under SMETS all meters are prepay. This means every meter now has a switch or valve adding roughly REDACTED/meter or REDACTED/house with dual fuel. (REDACTED REDACTED to the programme). Credit customers now have to pay for a more expensive meter, this was partly to level the playing field so prepay customers would not be penalised in the ‘smart world’.

Now the proposal is to supply the prepay customer with a PPMID. Such a device would cost about REDACTED, much the same as a meter, REDACTED more than a standard IHD. Now the situation is back to present day where the cost to serve a prepay customer is more than a credit customer but the difference is that this is on top of the extra cost to serve everyone. This does not make economic sense. (The additional cost of providing 15% of homes that are on prepay with a PPMID would be approximately REDACTED REDACTED.)

Would including the capability to enable gas and electricity supply through a PPMID connected via (a) a wireless HAN or (b) a wired HAN meet GB safety requirements? What impact would including this capability have on the cost of smart metering equipment? Please provide evidence to support your answers.

The cost of including the necessary safety features to control the switch/valve from the PPMID would be low. The technology was developed many years ago at REDACTED for their ‘Libra’ prepay gas meter to allow the prepay module to be remote from the meter whilst incorporating the necessary security and safety features. It was rolled out in small numbers in Ireland and the USA.

Micro Gen Meters

Do you agree with the proposal that the communications hub should be specified such that it can support multiple smart electricity meters? How many smart electricity meters should be supported by each communications hub?

ZigBee SE supports meters for microgeneration. There is no limit on the meters that can be supported by the Hub, it is very simple to implement and the generation meter itself can be very low cost.

Hand Held Terminal

Do you agree that a specification for a HHT interface to the HAN should be defined? If yes, please identify the functions that this interface would need to support and the scenarios in which such functionality could be required.

No – it is not for the government to define how companies are to install the meters. The HHT approach is one of several methods that may be employed. There are already other more cost effective and efficient ways of installing smart meters that do not require HHTs employed.

There may also be security issues in using HHTs as they may provide a back door entry that may compromise the measures to combat fraud.

An HHT that can access an optical port on the meter would provide for a more secure method of access than having it join the HAN.

Security

Do you agree with the proposed approach to the governance of security requirements? If you propose alternative arrangements please provide evidence to support your views.

The issue of security has to date not been taken seriously enough and is woefully inadequate given the fact that meters fitted with switches and valves pose a threat to the critical national infrastructure. Insufficient consideration has been given to the consequences arising from a mass blackout where meters switch off and cannot be switched back on. Such occurrences have happened in the past in prepay meters and there is no assurance it won't happen in the future. (The latest incidents with REDACTED meters were caused through mechanical failure so no amount of software assurances would address this issue.)

The difference between present day meters and smart meters is that it is only a small population (15%) that are fitted with switches and valves whereas for smart meters it is 100% of the population. In a scenario where a large population of smart meters malfunction (accidentally or maliciously) then it would be physically impossible to rectify the situation in less than a few weeks. This would lead to loss of power and therefore heating and in some cases communications on a mass scale leading to riots and deaths.

There appears to be a lack of appreciation of the size of potential issue. Security should be designed into the specification – security by design. It hasn't, rather it has been considered as something to consider later. For example, the data items allow for a huge range of values in the payloads, such as REDACTED credit top up values. Such data should be restricted to sensible amounts to ensure there can never be a situation where the meter can end up with values that are outside the norm. (Such an issue occurred with prepay meters when a large volume of REDACTED top up cards were stolen in REDACTED REDACTED.)

Little thought has been given to how the switch/valve may be controlled in a secure manor. For example there could be a mechanism for the meter to query the head end if it receives a cut off command to assure itself that the command was genuine.

Product assurance would have to take the form of interoperability testing with every combination of every device in the field every time any firmware changes are made no matter how insignificant they may be.

A government panel can deliberate for ever on this issue – the only real assurance that things won't go wrong is through thorough testing. Unfortunately the more complex the product, the variations there are to test (an exponential effect) and the SMETS specification is extremely complex. Meters should be kept as simple as possible in order to reduce risk.

The term 'end to end security' is used in this section but it appears that there is little appreciation of where the 'ends' are. For example it may be assumed that the ends are supplier and meter but in the middle is the DCC so how can the supplier be sure that the DCC carried his wishes correctly and didn't for example switch the wrong meter off?

Do you agree with the proposal to establish independent assurance procedures for DCC and DCC users? Please explain your views and provide evidence, including cost estimates where applicable, to support your position. Comments would also be welcome in relation to the impacts and benefits of the proposed approach with regard to small suppliers.

Independent assurance will go some way to ensuring system integrity. The suggestion that testing need only be carried out when significant changes are made is inadequate. Full regression testing will be required for any change no matter how small.

Do you agree with the proposal that re-testing should occur at least at set intervals and more frequently when significant changes to systems or security requirements are introduced? Please explain your views.

No – any change, no matter how small it may appear must be thoroughly tested. Many examples exist in the industry where the smallest issue gave rise to a huge problem, such as:

100,000 REDACTED keymeters failed a year after a new vending machine was introduced. A very minor bug in each device that would never be detected individually came together to produce a catastrophic failure. The true cause wasn't found until they failed again another year later and the meters had to be replaced again.

The whole population of RTS customers in REDACTED REDACTED were cut off supply when a new message intended for a trial was transmitted and caused the meters to crash. They had been operating without any problems for years. (This situation could easily arise with the DCC who may be asked to send a special message for some reason in the future.)

A missing '@' in one line of code caused a millennium bug in 300,000 keymeters something that was never spotted in testing through 5 generations of meter.

The issue of regression testing grows with time. As more variations are released into the field, the amount of testing required increases exponentially. SMETS appears to have overlooked this issue.

Do you agree with the proposal to establish an independent security certification scheme for smart metering equipment? Do you have any views on the proposed approach to establishing a certification scheme or evidence of the costs or timelines for setting up such a scheme or submitting products for certification?

Yes – there must be an independent security certification scheme along the lines that already exist for standards compliance.

The more complex the metering system, the more testing will be required and the longer it will become over time as more devices are deployed.

A compliance test along the lines of the German model may be the only way to fully assure security.

Do you agree that sanctions for non-compliance with security requirements should be included in the SEC? Do you have views on the nature of the sanctions that might be imposed?

None compliance with security requirements poses a risk to critical national infrastructure which could lead to civil unrest and death. It is as serious as that and must be treated accordingly with the toughest sanctions. Devices found to be non-compliant must be removed and replaced at manufacturer's cost.

Do you agree with the proposal to, in effect, extend the arrangements already proposed for SMETS installations prior to DCC operation, to all installations being operated outside DCC? Please provide evidence of the costs that might be incurred and the impact of this approach on small suppliers.

The answer to the previous question is also relevant here. The same security arrangements must apply equally to those outside the DCC and similar sanctions must apply.

The cost to the country of a major infrastructure failure will be huge compared to the cost of establishing proper security measures.

Assurance of Equipment

Do you agree that interoperability is central to the development of a successful smart metering solution and that activities related to the assurance of SMETS equipment should be governed by SEC? Please provide views on the governance arrangements that would be appropriate for assuring interoperability of smart metering equipment.

Yes – and as stated bodies such as the ZigBee Alliance and DLMS already have testing regimes in place to assure interoperability. These arrangements should be sufficient.

Do you agree with the creation of an 'approved products' list and that requirement on suppliers and CSPs to obtain, retain and provide evidence of appropriate certification should apply regardless of whether they intend to enrol the equipment in DCC

Yes – and as stated above, such arrangements are already in place.

Do you agree that protocol certification (against a GB Companion Specification) should provide adequate assurance that a product will meet interoperability requirements? Please explain your views and identify any additional assurance testing that you consider to be necessary and the rationale for including such testing.

Yes – this is exactly how devices should be tested. Again, such arrangements exist already.

Appendix A:
Alternative SMETS Solution for Hard-to-Read Gas locations

Background

DECC commissioned a study into the propagation of radio signals in UK homes and concluded that in 30% of cases a 2.4GHz low power radio solution may not be reliable to reach between the meters and in-home display.

Alternative solutions have been discussed at the Home Area Networks Advisory Group (HAG). The favoured solution is to use 868MHz based radio technology but at present there is no ZigBee solution based on this technology.

This paper outlines an alternative, already used in the Netherlands and one that conforms to EU standards and the SM-CG architecture proposed to meet EU Mandate 441 detailed in TR50572 published by CEN/CENELC/ETSI.

European Mandate M441 – Smart Metering Technical Report

Figure 3 shows a smart metering configuration example taken from Technical Report TR50572. It shows the 'M' interface between the electricity meter and the communications module (Local Network Access Point). The GB implementation may have the communications housed within the meter or in a separate module. It is likely that the module will have both the HAN and WAN communications and will provide the interface between the two. It may also contain a proxy for the battery powered gas meter.

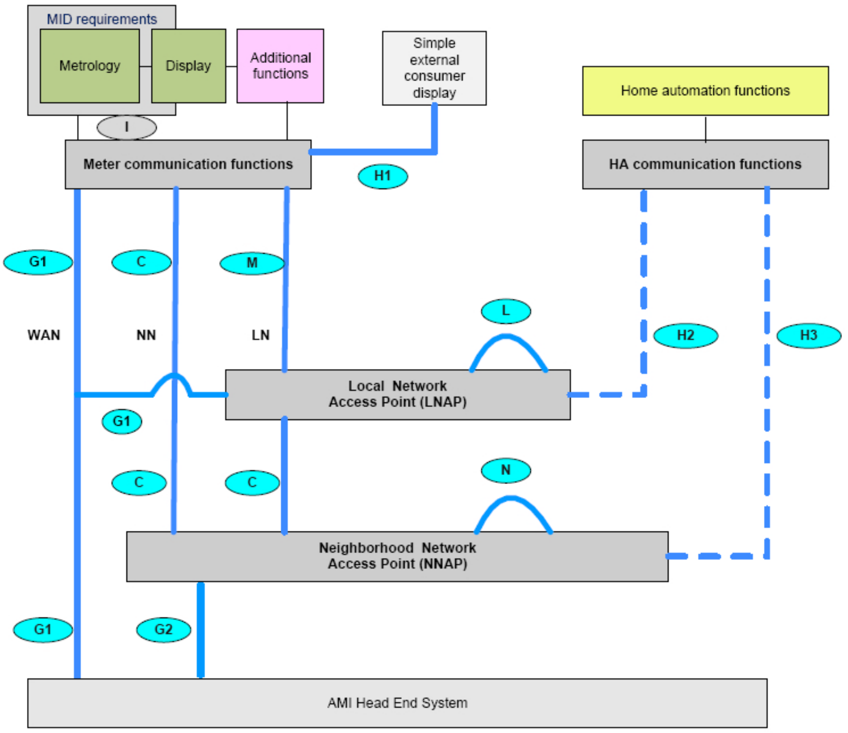
MID requirements
Metrology
Display
Additional functions
Simple external consumer display
Home automation functions
I
Meter communication functions
H1
HA communication functions
G1
C
M
WAN
NN
LN
L
H2
H3
Local Network Access Point (LNAP)
G1
C
C
N
Neighborhood Network Access Point (NNAP)
G1
G2
AMI Head End System

Figure 3 - SMCG Architecture

Smart Metering Solution conforming to TR50572

Figure 4 shows how the SM-CG architecture applies to the GB market, the relevant interfaces and technologies that may be employed. At present, it is assumed that interfaces 'M' and 'H2' are the same but this proposal shows an alternative approach.

The system shown in Figure 4 has the communications hub (LNAP) mounted directly to the electricity meter. The data interface (M) between meter and hub will be optically or electrically connected and hence highly reliable.

The Comms Hub could double as the CAD for the SMETS 2 architecture.

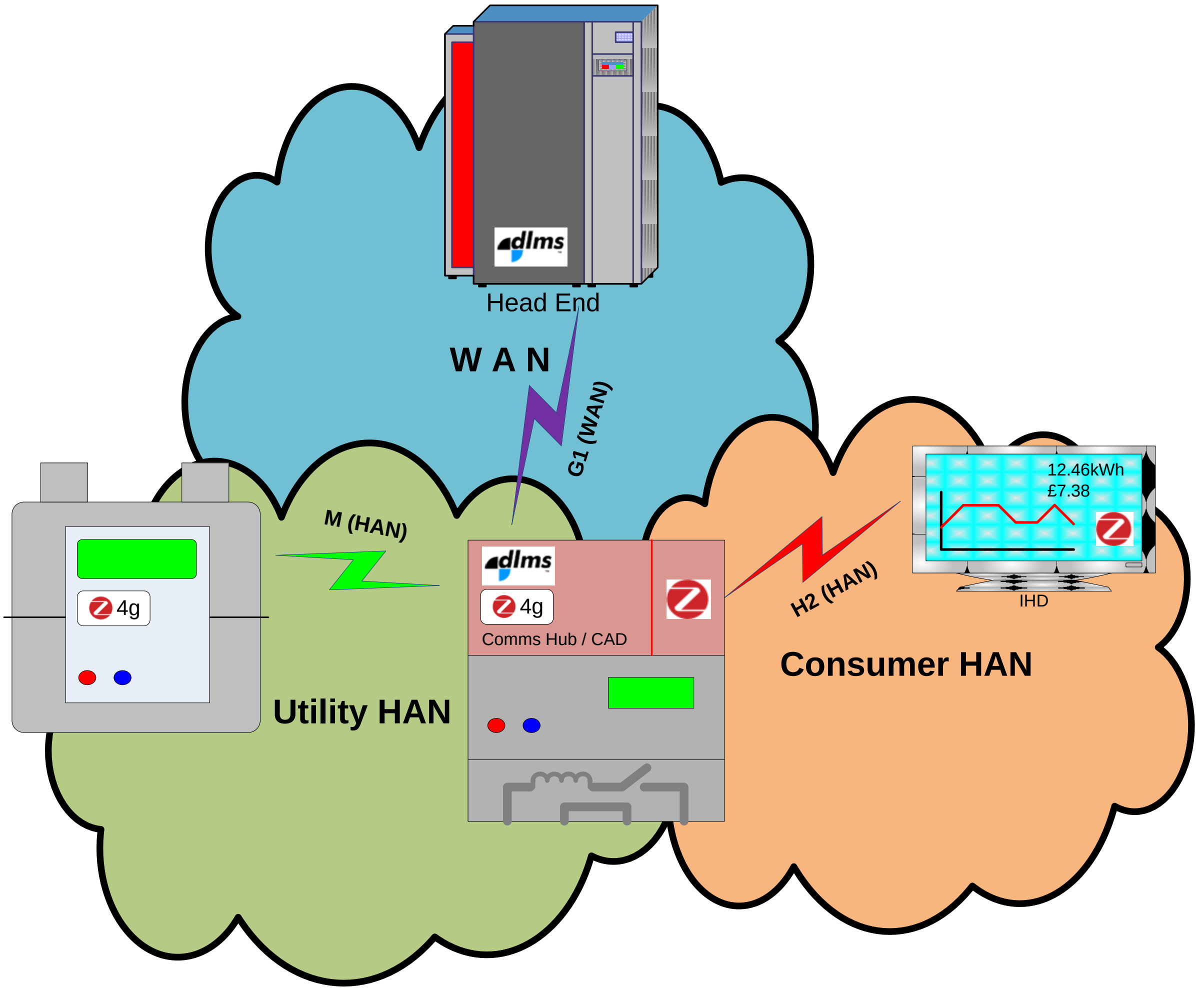

Figure 4: Smart Metering Interfaces

The 'M' interface between gas meter and hub could be via ZigBee over 868MHz running the IEEE 802.15.4g standard. Such a link would use all the features of the 2.4GHz ZigBee Smart Energy stack but running over an 868MHz PHY/MAC. If the DECC report into signal propagation is correct then such a link would be more reliable than a 2.4GHz radio

A separate network could provide the link to the IHD over the 'H2' interface. This interface could also be used for Customer HAN appliances. ZigBee on 868MHz or 2.4GHz could be used, or any other suitable technology could provide this interface, the market could decide. Such an architecture would differ from that already envisaged as the IHD would be outside the utility HAN. This may not be an issue since the IHD is not critical in the operation of the metering equipment. If it were considered an issue, then the link can be secured in the same way as envisaged in the present SMETS 2 architecture.

The major advantage with this approach is that the IHD falls outside the Utility HAN, the consumer would be free to add new IHDs (and other devices) without causing work for the energy supplier and traffic associated with it disrupting the Utility HAN. The security issues associated with data privacy are already covered by ZigBee, others will not be able to snoop (similar to WiFi routers).

This system as proposed would be more reliable and lower cost and simpler to implement compared to that presently envisaged. The requirement for a mesh network no longer exists and the interface link between electricity meter and communications hub is 100% reliable being as it is a physical or optical link.

Appendix B
Modular Interface Standard for Smart Electricity Metering

Background

The SMCG report into smart metering systems highlighted the interfaces within a smart metering system that should be considered for standardisation. The report recommends that existing standards be used where possible to allow for the interchange of communications modules to allow for mid-life upgrades in technology or device swap out without the need to change the meter.
Such a modular approach will require that the interface between meter and communication module should conform to a standard.
This paper makes some proposals that may be considered.

European Mandate M441 – Smart Metering Technical Report

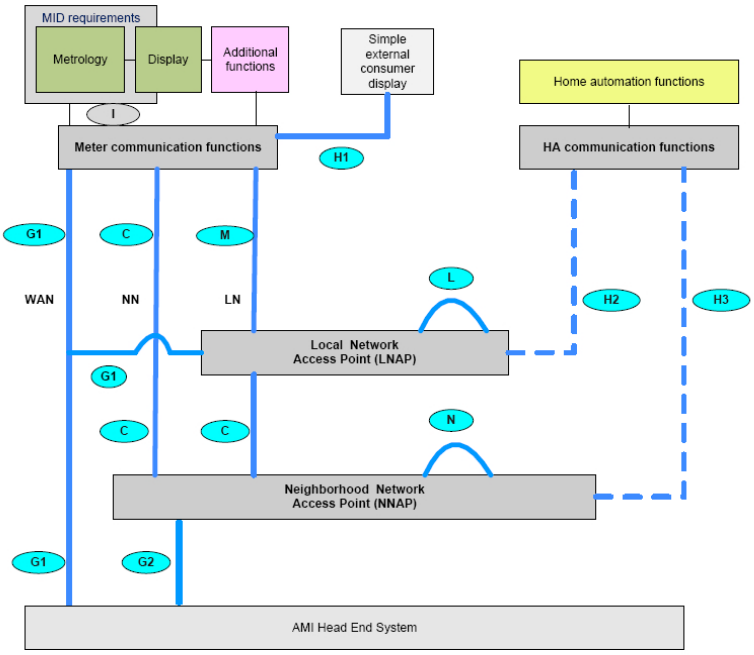
MID requirements
Metrology
Display
Additional functions
Simple external consumer display
Home automation functions
I
Meter communication functions
H1
HA communication functions
G1
C
M
WAN
NN
LN
L
H2
H3
Local Network Access Point (LNAP)
G1
C
C
N
Neighborhood Network Access Point (NNAP)
G1
G2
AMI Head End System

Figure 5: M441 Architecture Diagram

Figure 5 shows a smart metering configuration example taken from the SM-CG Technical Report. It shows the 'M' interface between the electricity meter and the communications module (Local Network Access Point). The GB implementation may have the communications housed within the meter or in a separate module. It is likely that the module will have both the HAN and WAN communications and will provide the interface between the two. It may also contain a proxy for the battery powered gas meter.

British Smart Metering Solution

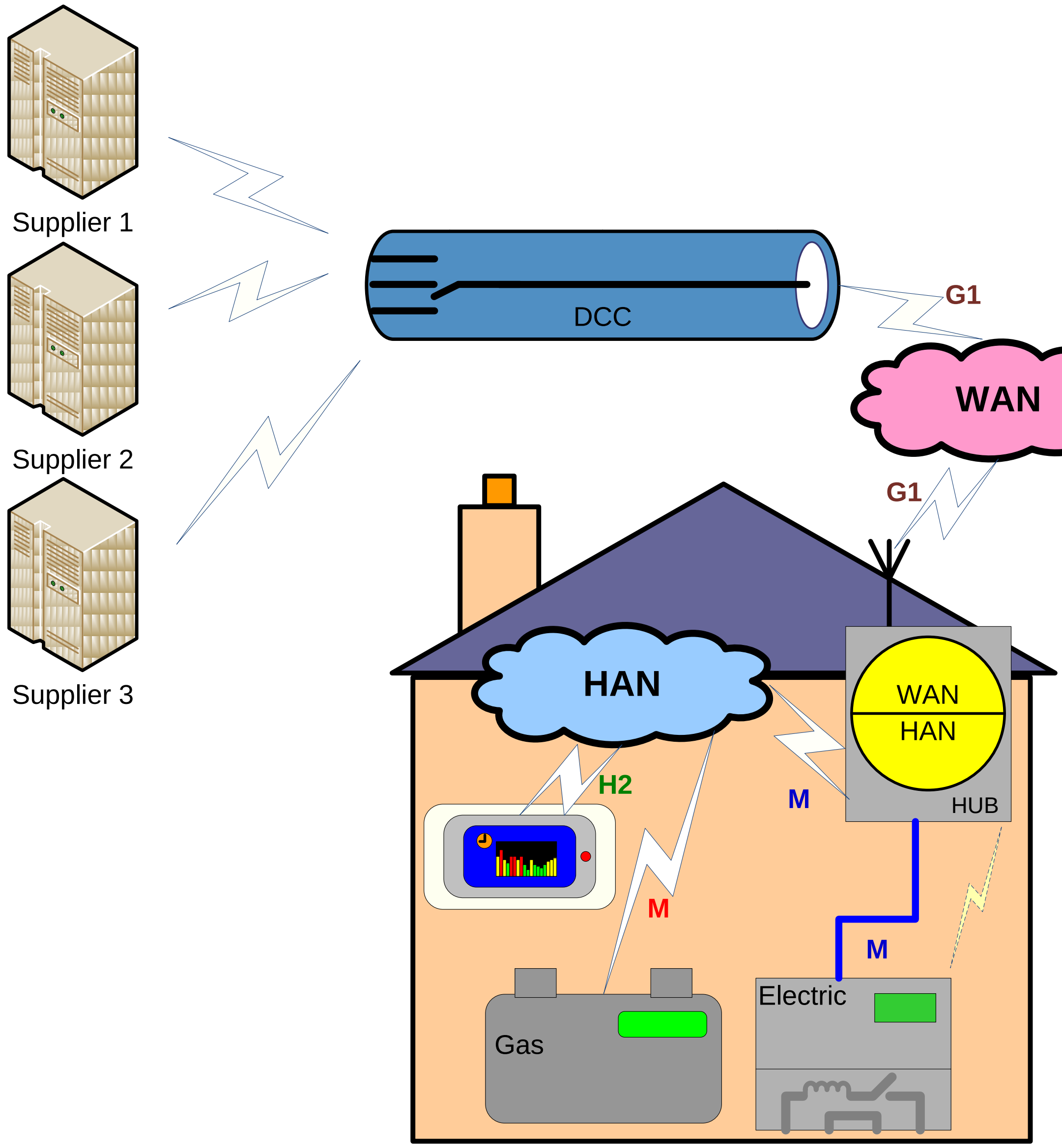

Figure 6: Example of a GB Smart Metering System

Figure 6 shows an example of how a smart metering system may look in Great Britain. The communications module linking the WAN to the HAN is powered from the electricity meter to ensure it remains powered even if the prepay switch is open. The example shows the wired link to the electricity meter carrying DLMS protocol. Communications on the HAN are show as ZigBee in this example.

GB Modular Interface

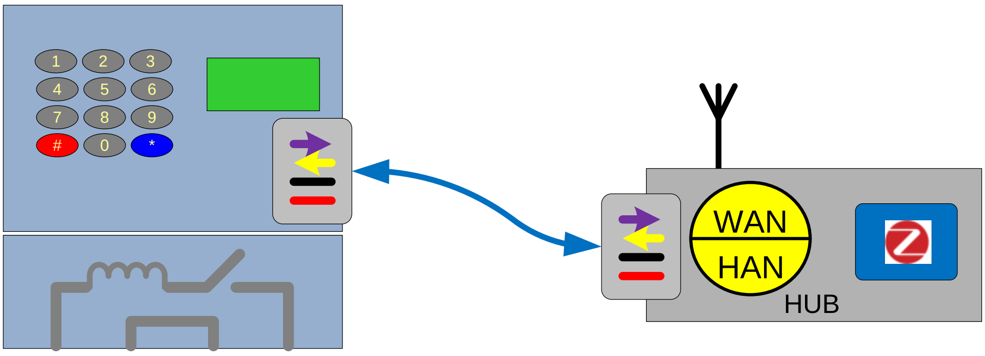

Figure 7: Wired Interface

Figure 7 shows an example of a meter with a wired interface to a communications module. In this example the following features will require standardisation:

- Connector size and physical configuration (eg RJ11)
- Power supply capabilities (voltage and maximum current)
- Maximum cable length supported
- Data protocol (eg DLMS, FLAG)

An integrated approach may also be envisaged as shown in Figure 4 where the same interface exists between meter and module.

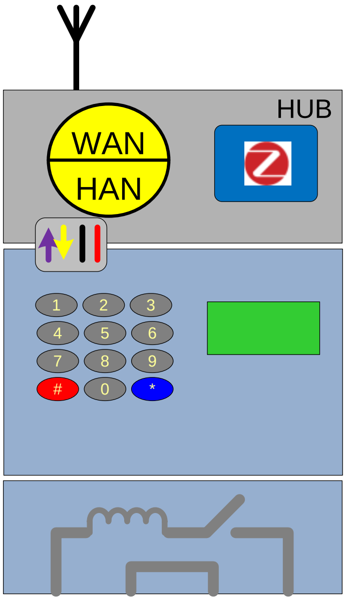

Figure 8: Modular Meter

In this approach, the electrical and data interface is the same as in the wired interface but in this scenario there will be additional features to specify:

- Size and shape of the aperture in the meter to house the module
- Size and shape of the module

Recommendation

The example of the GB smart metering deployment provides a starting point on which to base a CENELEC proposal for a standard metering interface.

The standards that already exist will provide a basis on which to build some proposals, there will have to be a decision on how far the interfaces can be standardised – ranging from the physical size and shape of connectors to the protocols. The recommendation is that it may be better to start with the protocols.

REDACTED REDACTED
23 Nov 2011

Appendix C
Remote Gas Meter Prepay through an Intelligent Hub

This appendix considers how prepay functionality could be performed within an intelligent comms hub running the accounting function and a basic gasmeter fitted with a valve performing only MID related functions.
The architecture shown in Figure 9 below shows the extended functionality of both gas and electricity located within the comms hub. In the case of electricity, the hub will be connected via a wired link either within the meter itself or closely coupled to it. The gas meter is connected only via the HAN and therefore is reliant on communications on the HAN to operate correctly.

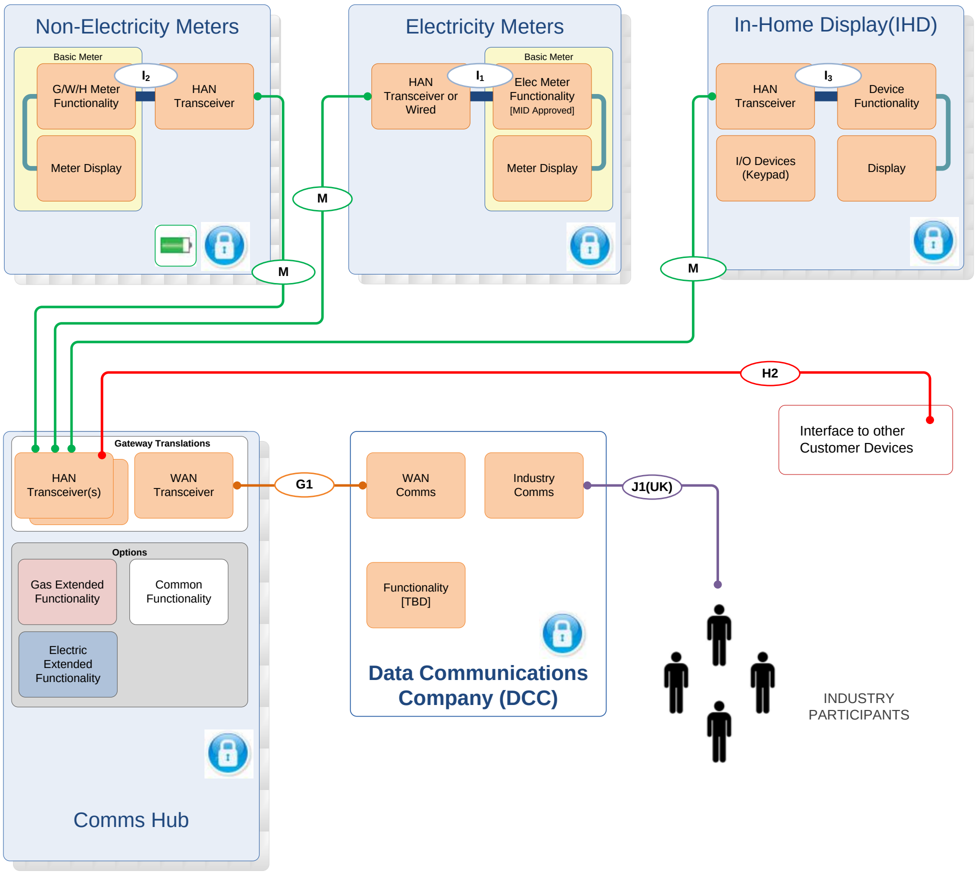

Figure 9 - Intelligent Comms Hub Architecture

Gas Prepay Operation

Meter

The gas meter measures volume of gas, is fitted with a valve and communicates on the HAN. The meter supplies gas consumption data to the comms hub at least every half hour.

The meter has a cut-off volume determined from the credit balance and conversion factors by the accounting function within the Comms Hub and updated every time the meter communicates with the hub. When the value of the total register reaches the cut-off value, the meter will close the valve (assuming friendly credit is not in force). The meter will send warnings to the Comms Hub when the credit is low.

The valve will be opened when the credit has been topped up or emergency credit has been selected.

It is recognised that the communications on the HAN may fail. To reduce disruption to the consumer, the meter will not close the valve if the HAN is down – a delay time, set to a reasonable value, determined by a service level agreement will determine a period of time without communications that will elapse before the valve is closed. This is to enable a site visit to be arranged to diagnose and repair the fault. The delay timer will be reset every time the Comms Hub communicates with the meter provided the account is in credit.

Messages to the gas meter from the comms hub will be limited to:

- Read Total Volume
- Read Cut-off volume
- Read Prepay status (volume, cut off volume, valve state.)
- Write Cut-off volume, cut-off delay
- Open Valve
- Close Valve

Comms Hub

The Comms Hub hosts the gas meter mirror. All devices on the HAN wishing to gain gas metering data will fetch it from the mirror whenever they require it thus allowing the gas meter to sleep for long periods to preserve the battery. It houses the WAN communications, the electricity meter end point on the HAN and the HAN trust centre and coordinator. It provides the Energy Service Interface functionality, supplying pricing data to devices on the HAN and collecting readings from the meters.

Consumption data from the meter is used together with tariff data and credit received over the WAN by the accounting function in the Comms Hub to calculate the cut-off volume to send to the gas meter. In the case that the tariff is multi-rate, the cut-off value will be modified accordingly for each change in rate. Block tariffs could be handled either on the half-hour reporting point. This will not be strictly accurate as there will be a time delay of up to 30 minutes each time the block is changed so it may desirable to implement an alternative based on either data push or on another data item in the meter that specifies the change-over value.

The Comms Hub will feature a display and user interface to show all the enhanced function parameters from the energy meters within the home and allow the prepay encoded number to be entered in the event of a WAN failure.

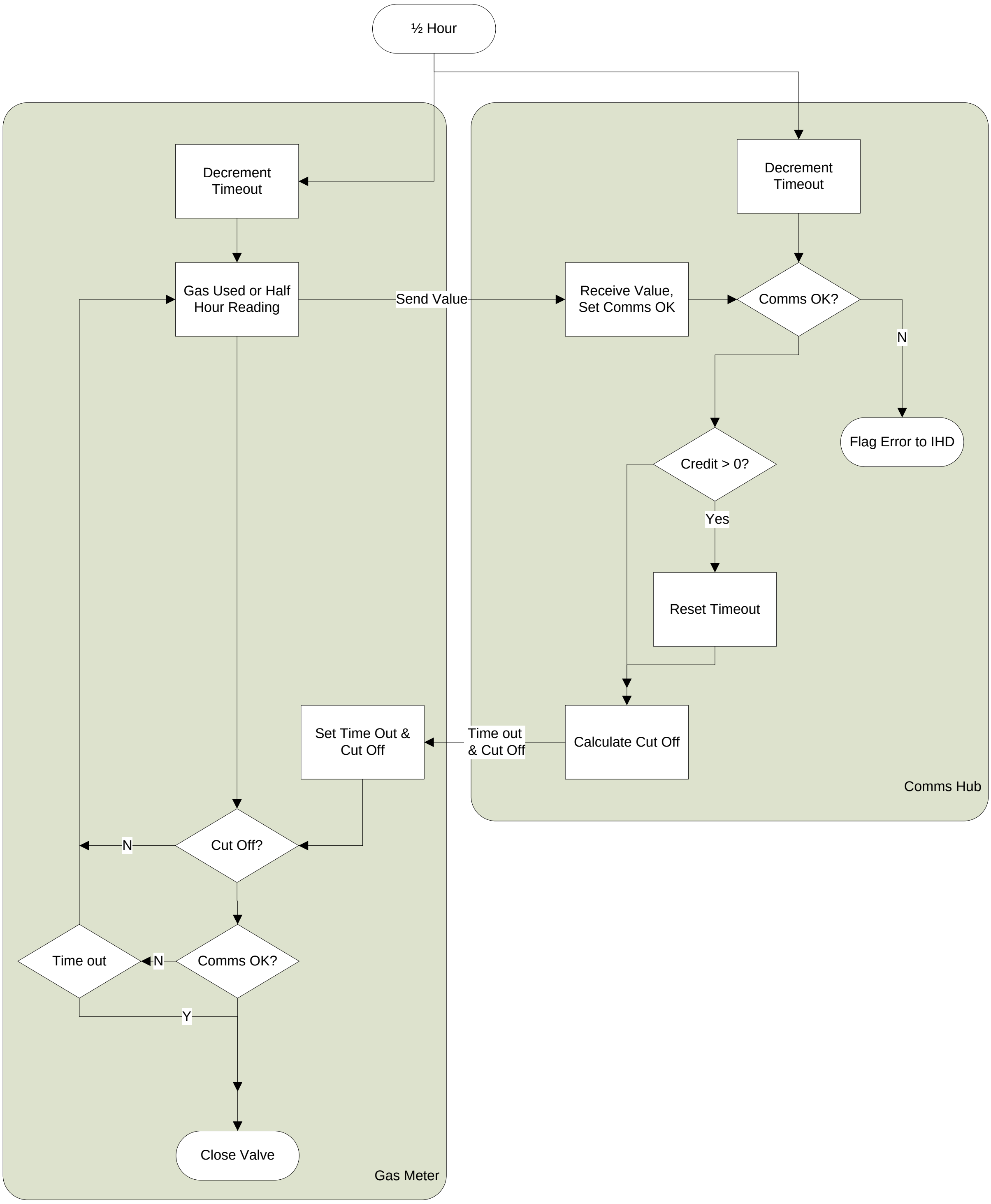

Figure 10 - Gas Prepay processes

Figure 10 shows a schematic of the functions in the gas meter and the Comms Hub. It can be seen that the gas meter will only close the valve if the cut off value is reached, the communications are working and if not, that the predefined time delay is has ended.

The timeout delay is reset every half hour provided the credit balance on the Comms Hub gas account is above zero and there is a valid report received over the HAN from the gas meter. The half hour count is decremented in the meter and the Comms Hub every half hour if no report is successfully sent. Should this occur, a warning message is sent to the IHD.

Operation in case of Communications Failure

WAN Failure

The Comms Hub is fitted with a keypad or push buttons to allow the encoded top up value to be added directly by the consumer should it fail to be downloaded via the WAN.

HAN Failure

The gas meter will not cut off the supply when the HAN is down unless the communications failure timeout has been reached. This timeout can be programmed by the head end and can be in the order of several days to allow support staff to diagnose and clear the fault.
The meter is fitted with an Emergency button which can be used to restore the gas supply in the event of HAN failure after the valve has been closed.
Figure 11 shows how the logic for the operation of the emergency button. The button will only function in the event of the gas valve being in the closed position, the communications is off line and the timeout is non-zero.

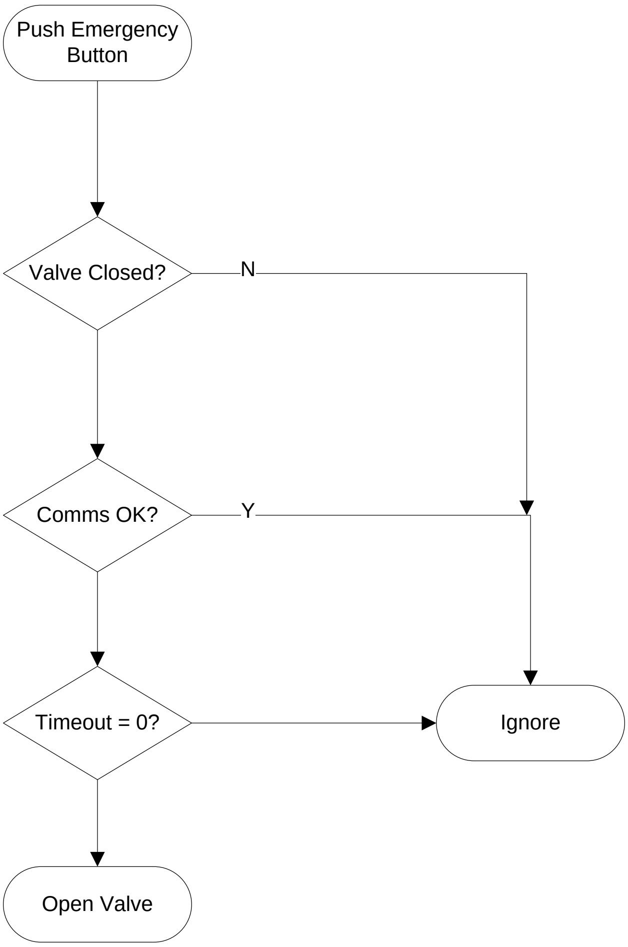

Figure 11 - Emergency Button Operation

There are a number of scenarios to consider:

1. The communications fail permanently

The HAN failure flag will be set the first time that the time out counter is decremented due to the fact that no reading was received from the gas meter on its half-hour reporting period. This can be flagged to both the IHD and Head End. The Head End can tell how long the HAN has been down by reading the value of the timeout.

The HAN failure timeout value will continue to decrement in both the meter and the Comms Hub and as gas is used, the volume cut off value will be reached eventually. If, when the volume cut off is reached, the timeout has also ended, the valve will close. If the volume cut off is reached before the timeout has ended, the valve will remain open until the timeout value reaches zero and then close.

2. The communications fail intermittently

If the communications fails whilst the meter's cut off volume has not been reached and the account on the Comms Hub is in credit, the failure will be detected and reported but if communications are restored before the cut-off volume is reached, there will be no effect on the consumer. If there was a change of tariff rate whilst the HAN was down, the Comms Hub accounting process would recalculate the balance based on the gas consumption data and set a new cu-off volume. This may lead to the supply to be cut off immediately.

The intermittency of the HAN communications would be picked up by the head end through the reports sent over the WAN and investigations could be instigated to determine the cause.

3. The communications fails after the valve has closed

In order for the valve to be closed, the communications must be functioning correctly. The time-out value will only start to decrement once the communications fail. Under these circumstances, the Emergency Button will be enabled and could be used to resort the supply. This will only work if the valve is closed, the HAN is down and the time out timer has not reached zero.

If the communications are restored before the time out ends, the account will be corrected by the Comms Hub, the cut off volume will be adjusted as necessary and the time-out value reset provided the account was in credit.

If the valve closes again and the credit had been below zero when the HAN was restored and it failed again then the balance of the time-out will still remain and the Emergency Button could be used again. This means that it is only possible to use the time-out period once unless or until the credit balance is topped up to take it above zero. It is therefore not possible to repeatedly use the Emergency Button to gain endless free gas by deliberately interfering with the HAN.

Optional Manual Meter Reading

If required, it would be possible to request the consumer to enter the gas meter reading into the Comms Hub via the keypad (if fitted). The reading on the meter could include some check digits to authenticate the value. This would allow the account to be updated on the Comms Hub and to report readings back to the head end. The Comms Hub could generate a simple code to enter on the gas meter to re-open the valve rather than a single button press as proposed earlier. This method may be considered more secure although it would be more complicated to perform and therefore less user friendly.

Credit Top-up Options

The architecture as envisaged by the Prepay working group was the head end would send down to the unique transaction numbers (UTRN) that would contain encrypted credit top-up data. In the case of system failure, the meters could have the code entered manually through push buttons or keypad. This approach limits the choice of technology choices in the future as all the prepay functionality is contained within the meters.

If the prepay functionality resided in the Hub as described in this paper then the same UTRN process could be used and a backup keypad could be provided on the hub. This keypad would serve both electricity and gas. It may also be envisaged that the hub could provide the display function and hence act as a wired in-home display.

The prepay technology would not be limited to UTRN transfer with this architecture, other transfer methods could be introduced without the need to update or replace the energy meters. An example would be a home point of sale terminal such as the Itron remote key update terminal or a home credit/debit card terminal could be introduced in the form of an enhanced IHD to provide prepay top-up functionality. The hub would perform the accounting functions as described earlier and send the cut off values to the meters in just the same way for any top-up method. In this way the prepay system will be future proofed without the need to up-date meter firmware.