Meter Communication in the 868 MHz-Band A proposal for a future standard

A) Physical Layer

I) Frequency Bands

Certain sections of the future European ISM-band 868-870 MHz could be used also for meter communication.
These devices will normally be classified as non-specific short range devices.

This leaves the bands

868.0-868.6 MHz (<1%, 25mW),
868.7-869.2 MHz (<0.1%, 25mW),
869.3-869.4MHz (access protocol),
869.4-869.65 MHz (<10%, 500mW),
869.7-870.0 MHz (<100%, 5mW).

868.0-868.1 MHz is also used by CT2-telephony.

II) Recommendations for band usage

1.) Unidirectional meter readout

This system uses stochastic transmissions of short telegrams (<100ms) in large stochastic time intervals (hours). The band 868.0-868.6 MHz (<1%) is recommended for this application. The reasons are:

a) This application may coexist with CT2-telephony, since channel occupancy of CT2 is < hours and mostly during day time. The short very rare bips of a meter readout might be acceptable for CT2. Due to the CT2 occupancy no other simple and reliable communication service can use this band.

b) The CT2-occupation will diminish during the next years due to the emerging DECT dominance of this market.

c) The parameters <1% and <25mW are acceptable.

d) The band is fairly wide and thus allows easily low cost transmitters with low frequency accuracy and low cost modulation techniques.

e) Leave the other bands to appplications which must rely on their special features

2.) Manual and technical signalling

These applications use short telegrams and rare communication. They include manual remote control devices (often with optical feedback) and simple technical signalling. Both usually require a finite response time (sek to min) and some acknowledgement (often but not always through the wireless channel).

a) These applications should prefer the 868.7-869.2MHz (<0.1%) band. This minimum duty cycle would gives the highest propability of a fast reaction.

b) Other services should not use this band.

3.) Non critical Intersystem-Communication

Several technical subsystems with wireless communication within or between buildings often require occasional communication between these subsystems. This communication might involve larger data volumes (up to kBytes), higher datarates and longer distances. This includes portable readout devices.

a) These applications should prefer the 869.4-869.65MHz (<10%) band with free access techniques. Its allowable higher power (<500mW), higher bandwidth and higher duty cycle make it especially suitable for this type of application.

b) Other services should not use this band.

4.) Controlled intersystem communication

These applications require for a short time period an exclusive access to the communication channel. A universal system wide access protocol is required and must be enforced.

a) These applications should prefer the 869.3-869.4MHz band. They must follow all specifications (including modulation, datarate, bitcoding etc.) of the upcoming European standard.

III) Other HF-Requirements

All other requirements like spurious emission, allowable power and other parameters must follow CEPT recommendations and/or local certification/admission rules.

IV) Channel Occupancy (unidirectional)

Average channel occupancy especially for unidirectional systems:

Each meter should not occupy the said frequency channel longer than a total of 0.5 sec within each day.

Reason: This average daily channel occupancy of <6ppm allows up to 10 000 meters within the reception range of a receiver with a raw collision probability of less than <12 % for 10 000 meters. With multiple stochastic transmissions this propability can be reduced to acceptable levels. At high baudrates and/or short telegrams multiple stochastic transmission within each day would be possible thus allowing a daily readout. The averaging period to 1 day has been chosen to allow such systems with daily readout.

Assuming a maximum distance of 300m between a receiver and a transmitter (with less than 10mW) this corresponds to up to 35 000 meters per square km.

V) Alternate modulation FSK

An alternate modulation is FSK (Frequency Shift Keying) with a modulation index of (0.5..1.5).

Reason: FSK allows a tighter bandwidth control than FSK and is more readily available.
A high transmission rate is required to minimize channel occupancy time and battery efficiency of the transmitters. Such high baudrate require a limited modulation index to limit the bandwidth within the admission bands.

VI) Bitcoding

Each bit is coded according to Biphase Space Rules:
At the beginnung of each bit time there is a level transition.
A space ("0") has an additional level transition in the middle of the bit time. For a mark ("1") the level is constant for the total bit time and changes only at the beginning of the next bit time.
A stationary transmitter off is also treated as a mark state.
Reason: Bit coding allows simpler and safer receiver designs especially for finding the optimum detection level in the AM-receiver section. Bit coding allows also considerable tolerance (+-10%) in the generation of the baud rate thus simplifying the design of low cost transmitters.

VII) Preheader

In front of any telegramm a dataless preheader of a at least 4 bytes all coded as mark i.e. a sequence of transmitter-on-off starting with transmitter on and toggling after each bit time must be transmitted for receiver startup including bit synchronisation and receive level adjustment.

B) Link Layer

I) Standard Baud Rate

The baudrate is 19 200 Baud corresponding to between
19 200 transitions per second (string of marks) and
38 400 transitions per second (string of spaces). This unusually high baudrates limits the channel occupancy and thus saves the scarce bandwith resource.
The bandwidth is often dominantly determined by the frequency tolerance of the devices and less by the baudrate.
The theoretically higher sensitivity of small band devices is often limited by background noise and other ferquency bands.

II) Standard Reference

IEC-870-5-1

III) Allowable Access method for unidirectional communication

Command Field= $44 (Send/No Reply)
Adress Field= $FF (Broadcast/No Reply)

1.) Unidirecional random access
2.) Transmission in allocated timeslots
3.) Transmission in synchronized timeslots

For unidirectional systems with random note the patent situation for details of some of these methods in some countries.

IV) Allowable access method bidirectional communication

In wireless communication without allotted channel occupancy the communication system is better described by a balanced transmission, where no fixed or permanent master-slave relation exists Usually these systems are not capable of true duplex communication.
In balanced systems only send/confirm-type of communication is defined. Note that in a non exclusive wireless channel no fixed communication links may be assigned. Thus a received confirm message of the (temporary) primary station may cannot be asumed to safely originate only from the destination receiver of the preceding send message. Hence each ackowledgement must include at least the senders (primary stations) adress as ist destination adress and single charater acklowledgements are not allowed.

V) Link layer adressing

The adress range must be enlarged to ensure a unique adress in a possible large wireless cell. It is therefore recommended that the (destination) adress field for a bidirectional communication (i.e. C-field #44h) should use the unique (8 Byte) adress, i.e. setting i=8 (Adress field size) in all communication.
In addition all send/confirm dialogs must contain the source adress in their telegrams, to allow the secondary station an adressed acknowledge. A solution could be the inclusion of the source adress directly following the destination adress in each adress field, thus defining a total adress length of 16 bytes in each bidirectional (send-confirm-type) telegram.

VI) Data Protection

Format Class FT3 with variable length and a block length of 16 Bytes. Each 16-Byte block is protected by a 16 Bit (2 Byte) CRC-pattern. No start, -stop- or parity bit is used.
All telegramms must have a length of a multiple of 16 bytes data plus 2 CRC-bytes per block plus a special 2 byte header in front of the telegram. The generator polynomial of the 16-Bit CRC is defined by the standard as:

X^16+X^13+X^12+X^11+X^10+X^8+X^6+X^5+X^2+1.

For the calculation of the CRC the (128) information bits are extended by 16 "0"-Bits and then the total 144 information bits are divided by the generator polynomial. The remainder is then complemented and forms the 2 CRC-Bytes. These two bytes are transmitted high byte first.

.

Reason: FT3 has a hamming distance of 6 as recommend for a noisy channel. For i=16 (16-Byte blocks) it has a high channel efficiency. It is especially suitable for a synchronous channel or a channel with bit coding.

VII) Bit Sequence within each Byte

In accordance to the requirements of IEC870-5-1 for FT3 the bit sequence within each byte is MSB first. This is in contrast to the LSB -first sequence of FT1.2 as used by EN1434 part 3.

Reason: Efficient implementation of the CRC-algorithm dictates such a sequence.

VIII) Telegram structure

The total telegram is thus according to IEC 870-5-1/2:

1.) Preheader: >= 4 Bytes: All Mark-Bits ($FF)

2.) Link layer Header: 2 Bytes: 05h,64h

3.) n*(16+2) Bytes: Data plus CRC.
The first block must contain in its first three bytes:

a) The first byte contains the telegram length not counting the first block and the CRC´s. Due to the fixed 16 byte block length it most be of the form 0x0h with x=$0 to $F.
b) The second byte contains the Control-field ($44 for unidirectional systems)
c) The next 8 bytes contain the destination adress according the first 8 bytes of the “header” of the RSP_UD- telegram of EN1434-3. ($FF for unidirectional systems, C-field=$44)
d) The next 8 bytes contain the source adress, defined as above for the destination adress.

4.) Optional Trailer: Mark Bits
Note that IEC870-5-1 requires at least one mark bit before a transmitter is switched off and a minimum of 54 mark bytes if the transmitter is left on.

C) Application Layer

The application layer is identical to the variable protocol of EN1434 part 3 without the first 8 bytes of the header. It includes a CI-field of $51 (Low byte first), no fixed header and a sequence of data records. Note that the use of the CI-Field $75 (Mode2, High Byte first) or the fixed data structure of EN1434 part 3 is not recommended for wireless data transmission.

D) Optional Data Encryptation

I) Functions

1.) Data privacy for consumption meters values
2.) Detecting simulated meter transmission
3.) Preventing later playback of old meter values

II) Structure of encrypted telegrams

1.) The first 12-byte block containing the ID-number, the manufacturer etc. is always unencrypted. The last word of this block is the signature word. If the following data are unencrypted, this signature word contains a zero.

2.) If the transmission contains encrypted data, the high byte of this signature word contains a code for the encryptation method. The code 0 signals no encryptation. Currently only the encryptation codes 2 or 3 (see below) are defined. The other codes are reserved. The number of encrypted bytes is contained in the low byte of the signature word. The content of this signature word is currently defined as zero, corresponding consistently to no encrypted data.

3.) The encrypted data follow directly after the signature word, thus forming the beginning of the DIF/VIF-structured part of the telegram.

III) Partial Encryption

1.) If the number of encrypted bytes is less than the remaining data of the telegram, unencrypted data may follow after the encrypted data. They must start at a record boundary, i.e. the first byte after the encrypted data will be interpreted as a DIF.

2.) If a partially encrypted telegram must contain encrypted manufacturer specific data a record with a suitable length DIF (possibly a variable length string DIF) and a VIF= $7F (manufacturer specific data record) must be used instead of the usual MDH-DIF=$0F. This is required to enable after decryptation standard DIF/VIF-decoding of a previously partially encrypted telegram containing encrypted manufacturer specific data .

IV) Encryptation methods

1.) Encryptation according to the DES (data encryptation standard) as described in ANSI X3.92-1981

2.) Cipher Block Chaining (CBC)-method as described in ANSI X3.106-1983 with an initial initialization vector of zero: (Encryptation Method Code=2). In this case the data records should contain the current date before the meter reading.
Note that in this case the data after the date record, i.e.especially the encrypted meter reading data change once per day even if their data content itself is constant. This prevents an undetectable later playback of stored encrypted meter readings by a hacker.

3.) The "Initialization Vector IV" with length 64 bits of this standard may alternatively be defined by the the first 6 bytes of the identification header in mode 1 sequence, i.e. identification number in in the lowest 4 bytes followed by the manufacturer ID in the two next higher bytes and finally by the current date coded as in record structure "G" of En1434 part 3 for the two highest bytes. In this case the encryptation method is coded as "3". Note that in this case all encrypted data change once per day even if the data content itself is constant. This prevents an undetectable later playback of any stored encrypted data by a hacker.

4.) To simplify the verification of correct decoding and to prevent an undetected change in the identification of the not encrypted header, the encrypted part of the telegram must contain at least together with the appropriate application layer coding (DIF and VIF) again the same identification number as in the unencrypted header.

5.) Due to the mathematical nature of the DES-algorithm the encrypted length contained in the low byte of the signature word must be an integer multiple of 8 if the high byte signals DES-encryptation.
Unused bytes in the last 8-byte block must be filled with appropriatly structured dummy data records to achieve the required record boundary at the end of the encrypted data. One or several bytes containing the filler DIF=$2F are suggested to fill such gaps.

6.) The application of certain encryptation methods might be prohibited by local laws.

7.) The enclosed example should help in unterstanding and could serve as a first test dataset.