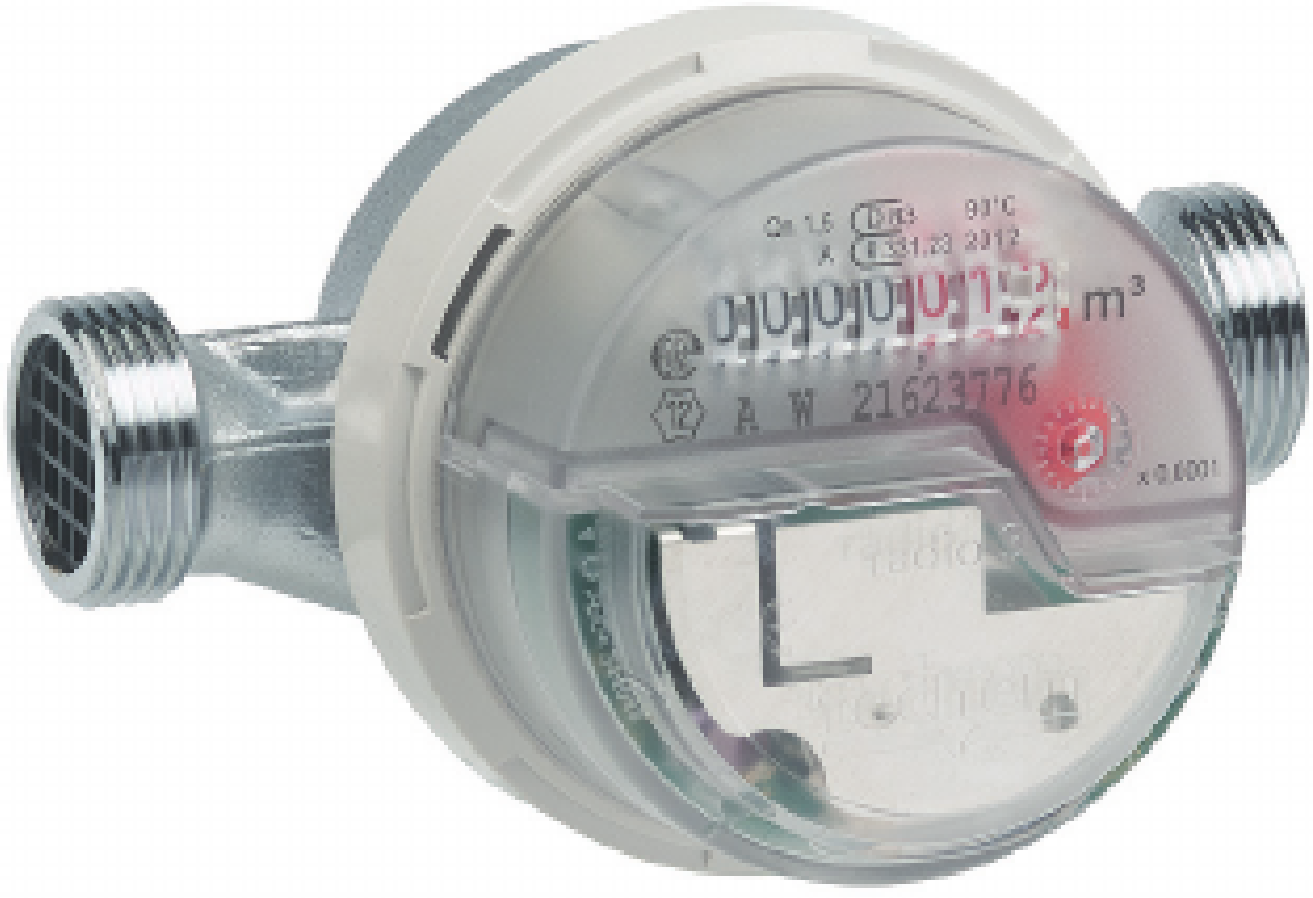
July 11, 2015

boring. . . . then suddenly


m³
21623776

it’s SMART!!!5!

- sign here please
- i can't...


B030


techem

advice

> *Depending on who owns the meter and the box it plugs into and what the contract says... don't remove it, build a faraday cage around it.*

2015/07/06 grarpamp on cypherpunks ml


TERRATEC

Radio system for consumption data acquisition translated from German

DE 10123251 C1

Publication number	DE10123251 C1
Publication type	Grant
Application number	DE2001123251
Publication date	31 Oct 2002
Filing date	12 May 2001
Priority date	12 Mar 2001
Inventors	Martin Hansing, Dirk Matussek
Applicant	Techem Service Ag
Export Citation	BiBTeX, EndNote, RefMan

Patent Citations (3), Referenced by (4), Classifications (9), Legal Events (5)

External Links: DPMA, Espacenet

ABSTRACT translated from German

Radio system for consumption data acquisition from a wireless network with terminals and data collectors (2), a terminal one device for recording consumption values (V) and a radio transmitter for transmitting radio telegrams (1) with the terminal attributable consumption values (V) and a data collector (2) each have a radio receiver for receiving the radio telegrams (1), a CPU with memory (4, 7) for checking and storing the radio telegrams (1, 6) and / or the associated consumption values (V) and a radio transmitter for transmitting radio telegrams (6). In order to create a low-cost wireless system for consumption data acquisition with increased wireless range, the radio station of the terminals and data collectors (2) in the same frequency range to work with the data collector (2) send the received radio telegrams (1) again and the transmission of wireless telegrams (6) is controlled by a wireless telegram management (3) in the data collector (2).

DESCRIPTION translated from German

The invention relates to a radio system for consumption data collection, in particular in buildings of a radio network learning with terminals and Datensamm, with a terminal each worth a device for detecting consumption and a radio transmitter for transmitting radio messages having the the terminal attributable consumption values and a data collector each have a radio receiver for receiving the radio telegrams, a rake factory with memory for checking and storing the radio telegrams and / or the associated consumption and a radio transmitter to send out radio messages has.

There are different concepts of wireless

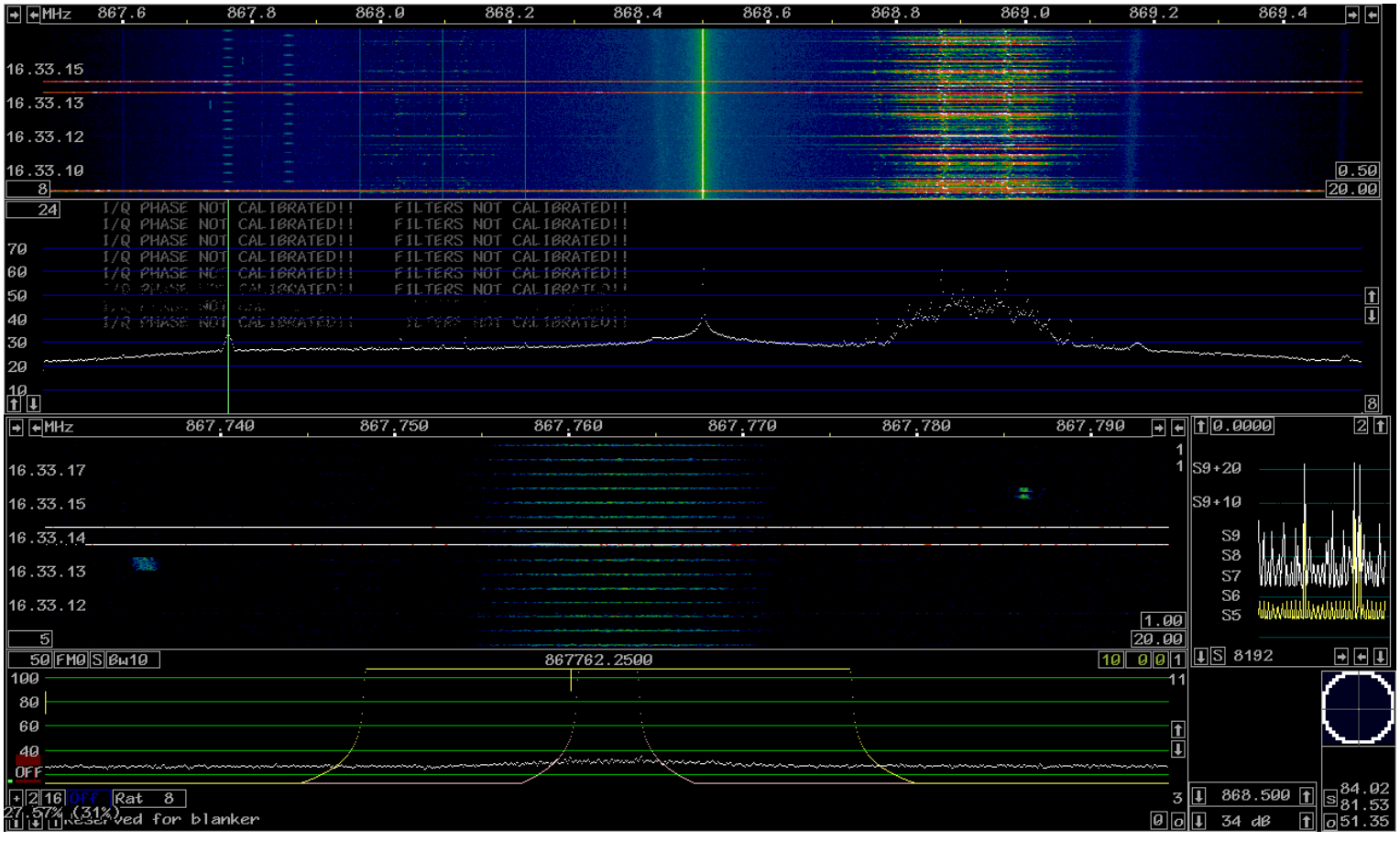
CLAIMS (16) translated from German

1. Radio system for consumption data acquisition from a wireless network with terminals and data collectors **(2),** a terminal one body for a collection of consumption values (V) and a radio transmitter to Off broadcasting of radio telegrams **(1)** with the terminal attributable consumption values (V) and having a data collector **(2)** each have a radio receiver for receiving the radio telegrams **(1),** a CPU with mo ry **(4, 7)** for checking and storing the radio telegrams **(1, 6)** and / or the associated consumption values (V) and a radio transmitter for transmitting radio telegrams **(6), characterized** in that the radio transmitter of the terminal and the data collector **(2)** work rich in the

source:

https://www.google.as/patents/DE10123251C1?cl=en

The frequency range in which the radio system is operating, is at **868 MHz**, *and the* **duty cycle**, *ie the ratio of the transmitter-on time to the transmitter off-time, is* **0.1%**. *In a duty-cycle interval of one hour the transmitter on-time, may still be sent in the wireless telegrams 6, which after 3.6 seconds and the transmitter-off period in which the data collector 2 may send nothing, 3596 , 4 seconds. The maximum continuous transmission time and the maximum continuous interval time are each 720 milliseconds. The* **length of a typical radio telegram is 4.1 milliseconds**, *so that the transmission time slots and the time slots for transmission pause extension with 5 milliseconds can be measured.*


MHz 867.6 867.8 868.0 868.2 868.4 868.6 868.8 869.0 869.2 869.4
16.33.15
16.33.13
16.33.12
16.33.10
0.50
20.00
I/Q PHASE NOT CALIBRATED!! FILTERS NOT CALIBRATED!!
MHz 867.740 867.750 867.760 867.770 867.780 867.790
16.33.17
16.33.15
16.33.14
16.33.13
16.33.12
1.00
20.00
867762.2500
S9+20
S9+10
S9
S8
S7
S6
S5
8192
868.500
34 dB
84.02
81.53
51.35
Rat 8
27.57% (31%)
Reserved for blanker

Basic functions:	FHKV data III: data encoding and radio transfer
	EHKV vario S: prepared for radio use, including a radio module which can be activated
Interface:	Optical for the Techem service device
Radiator performance:	100 W to 15,999 W
Scale:	Product scale
Radio data transmission:	Consumption data from 12 average mid-month figures and month-end figures, reference date figure and status information
Operating frequency:	868.95 MHz
Transmitting power:	3 ... 10 MW
Transmission period:	7.5 ms

it also says:

> *Secure data transfer using the CRC process and data encryption*

weeks of trying to make sense of the radio waves

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 13757-4

June 2003

ICS

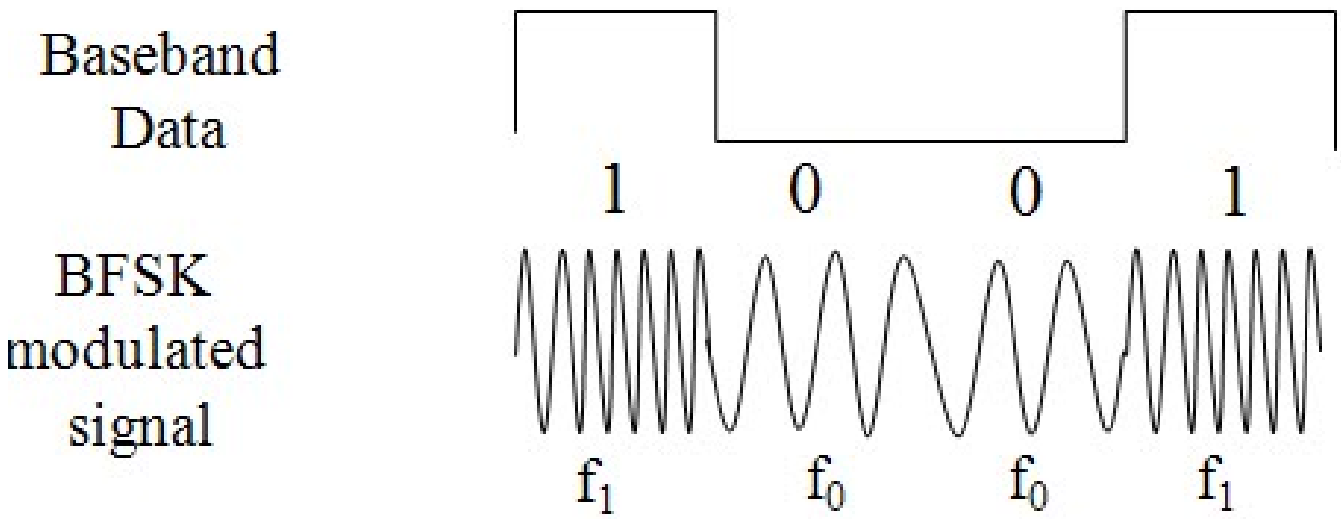
English version

Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio Meter reading for operation in the 868-870 MHz SRD band)

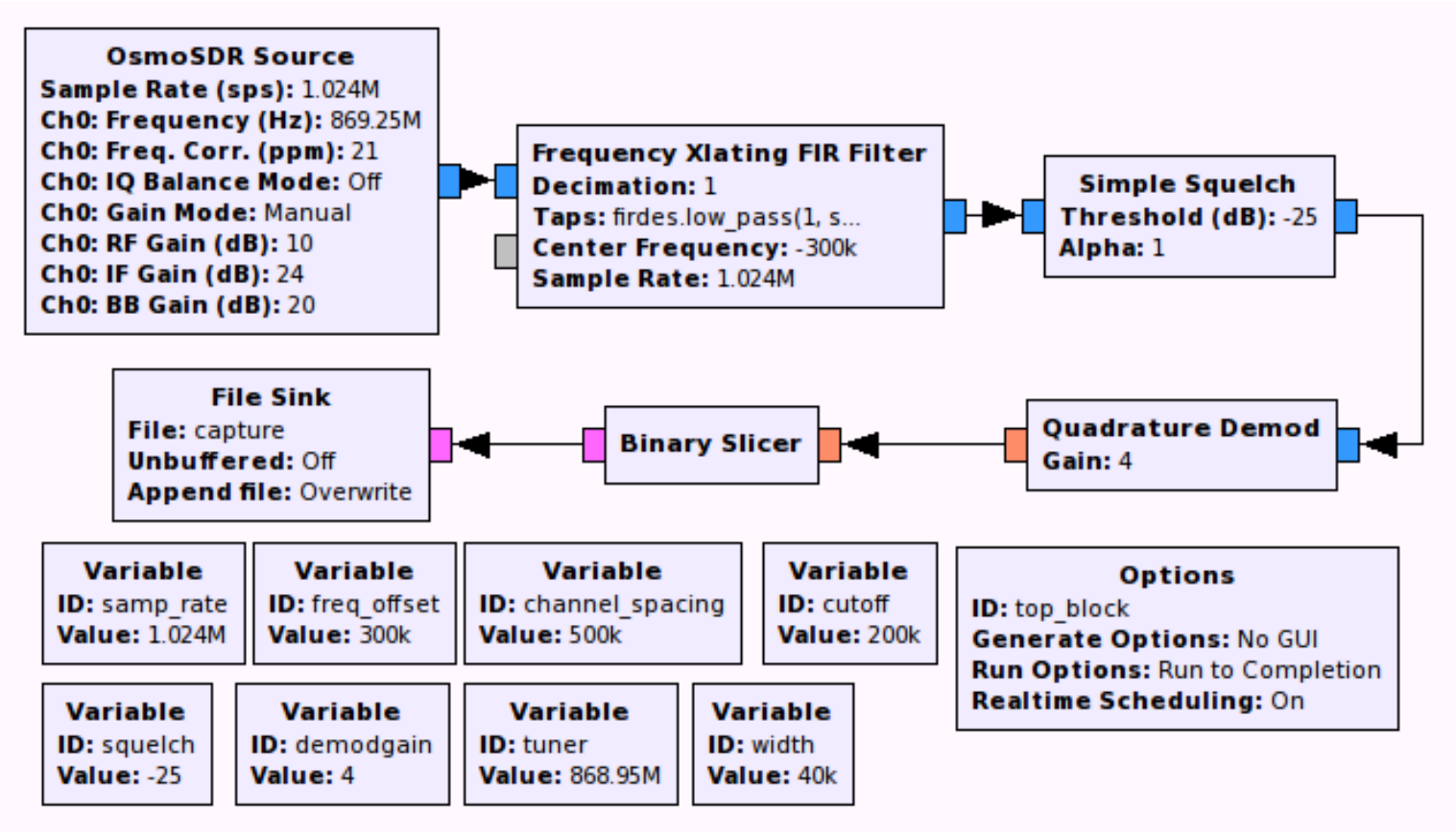
Table 11 — Mode T, transmitter

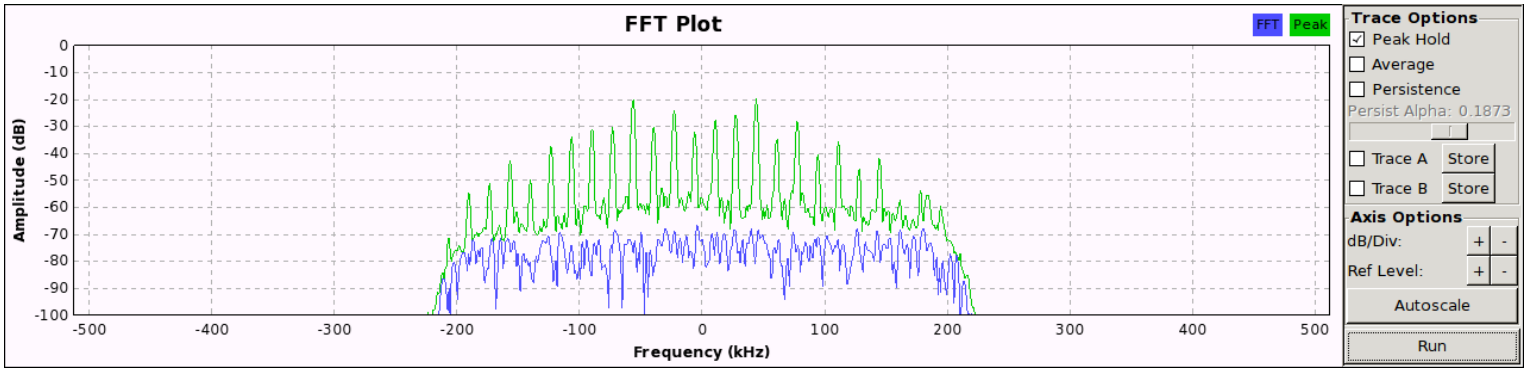
Characteristic	Mode	Sym	Min	Typ	Max.	Unit	Note
Centre frequency : (meter to other)	T1, T2		868,90	868,95	869,00	MHz	~60ppm
Centre frequency : (other to meter)	T2		868,278	868,300	868,322	MHz	~25ppm
FSK Deviation : (meter to other)	T1, T2		+/-40	+/-50	+/-80	kHz	
FSK Deviation : (other to meter)	T2		+/-40	+/-50	+/-80	kHz	
Chip rate transmit : (meter to other)	T1, T2	f_{chip}	90	100	110	kcps	
Rate variation within header + telegram : (meter)	T1, T2	Df_{chip}	-1	0	+1	%	
Data rate : meter to other (3 of 6 encoding)	T1, T2			f_{chip} *2/3		bps	(1)

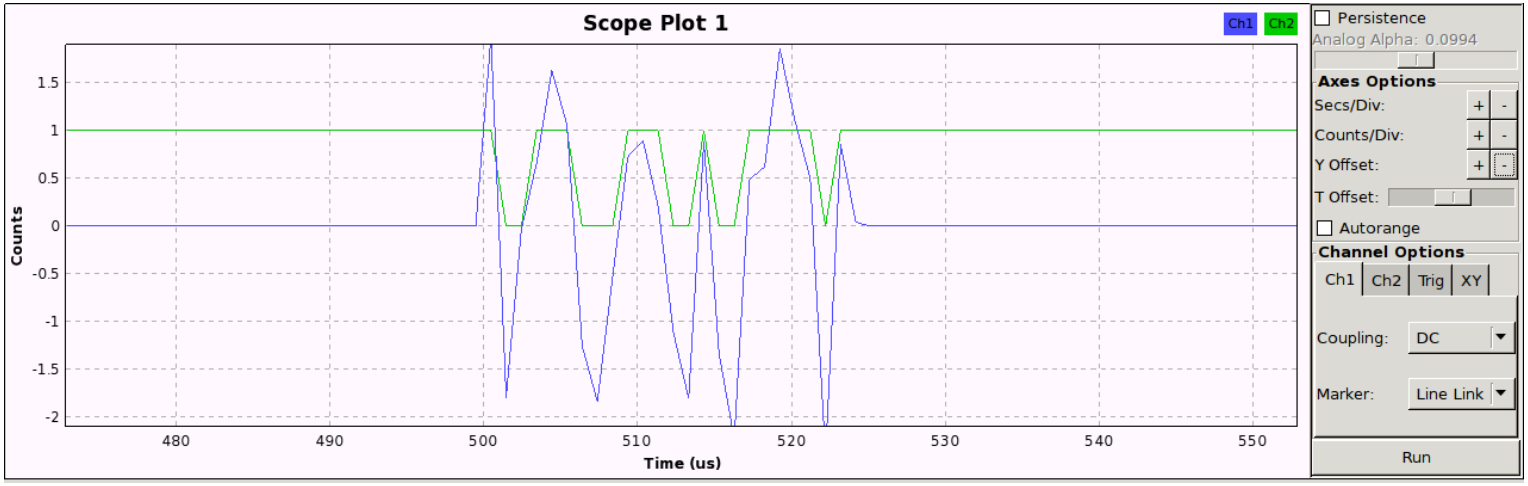
Frequency Shift Keying (FSK)



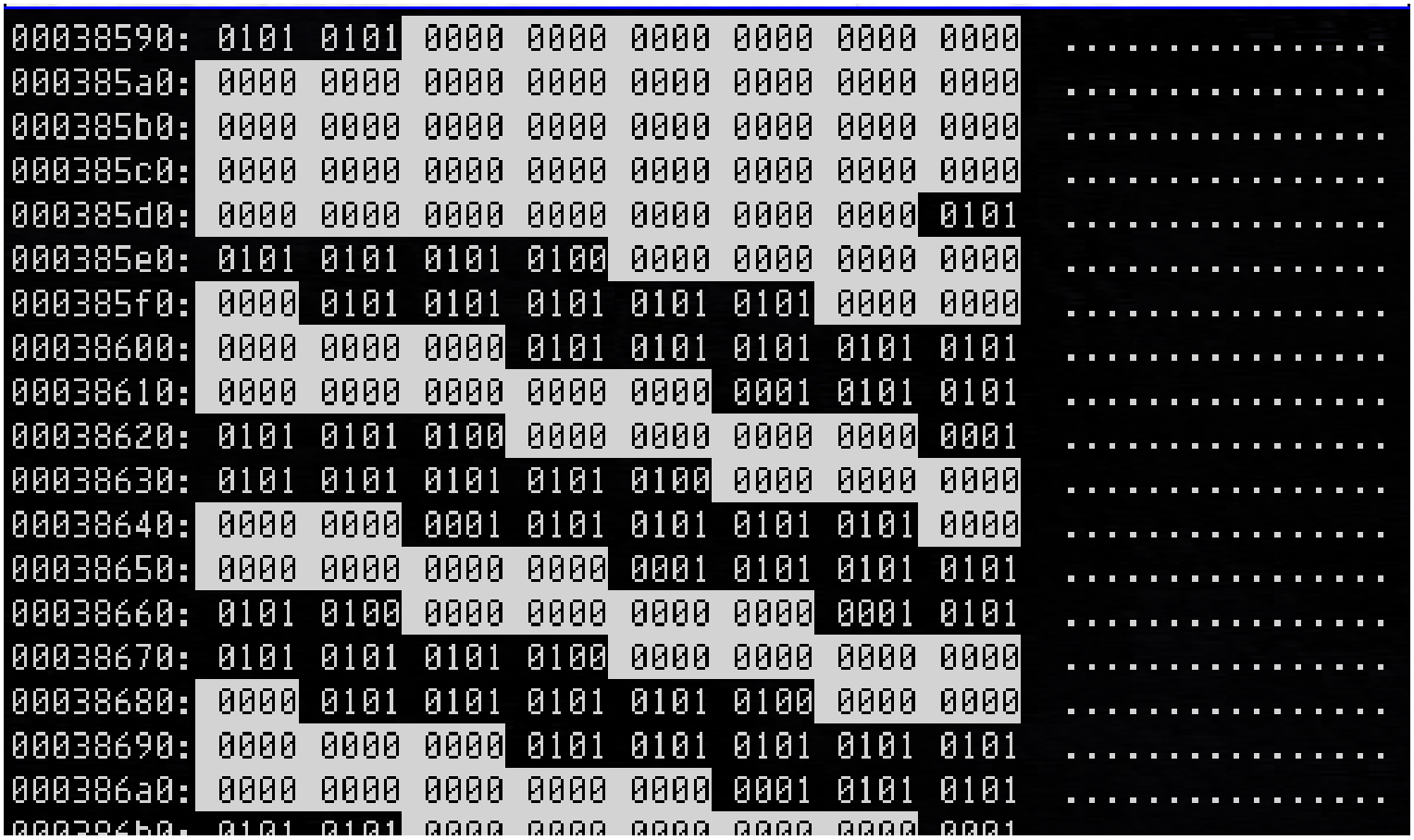
where $f_0 = A\cos(\omega_c - \Delta\omega)t$ and $f_1 = A\cos(\omega_c + \Delta\omega)t$


OsmoSDR Source
Sample Rate (sps): 1.024M
Ch0: Frequency (Hz): 869.25M
Ch0: Freq. Corr. (ppm): 21
Ch0: IQ Balance Mode: Off
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 24
Ch0: BB Gain (dB): 20
Frequency Xlating FIR Filter
Decimation: 1
Taps: firdes.low_pass(1, s...
Center Frequency: -300k
Sample Rate: 1.024M
Simple Squelch
Threshold (dB): -25
Alpha: 1
File Sink
File: capture
Unbuffered: Off
Append file: Overwrite
Binary Slicer
Quadrature Demod
Gain: 4
Variable
ID: samp_rate
Value: 1.024M
Variable
ID: freq_offset
Value: 300k
Variable
ID: channel_spacing
Value: 500k
Variable
ID: cutoff
Value: 200k
Options
ID: top_block
Generate Options: No GUI
Run Options: Run to Completion
Realtime Scheduling: On
Variable
ID: squelch
Value: -25
Variable
ID: demodgain
Value: 4
Variable
ID: tuner
Value: 868.95M
Variable
ID: width
Value: 40k


FFT Plot
FFT
Peak
Amplitude (dB)
0
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-500
-400
-300
-200
-100
0
100
200
300
400
500
Frequency (kHz)
Trace Options
Peak Hold
Average
Persistence
Persist Alpha: 0.1873
Trace A
Store
Trace B
Store
Axis Options
dB/Div:
+
-
Ref Level:
+
-
Autoscale
Run

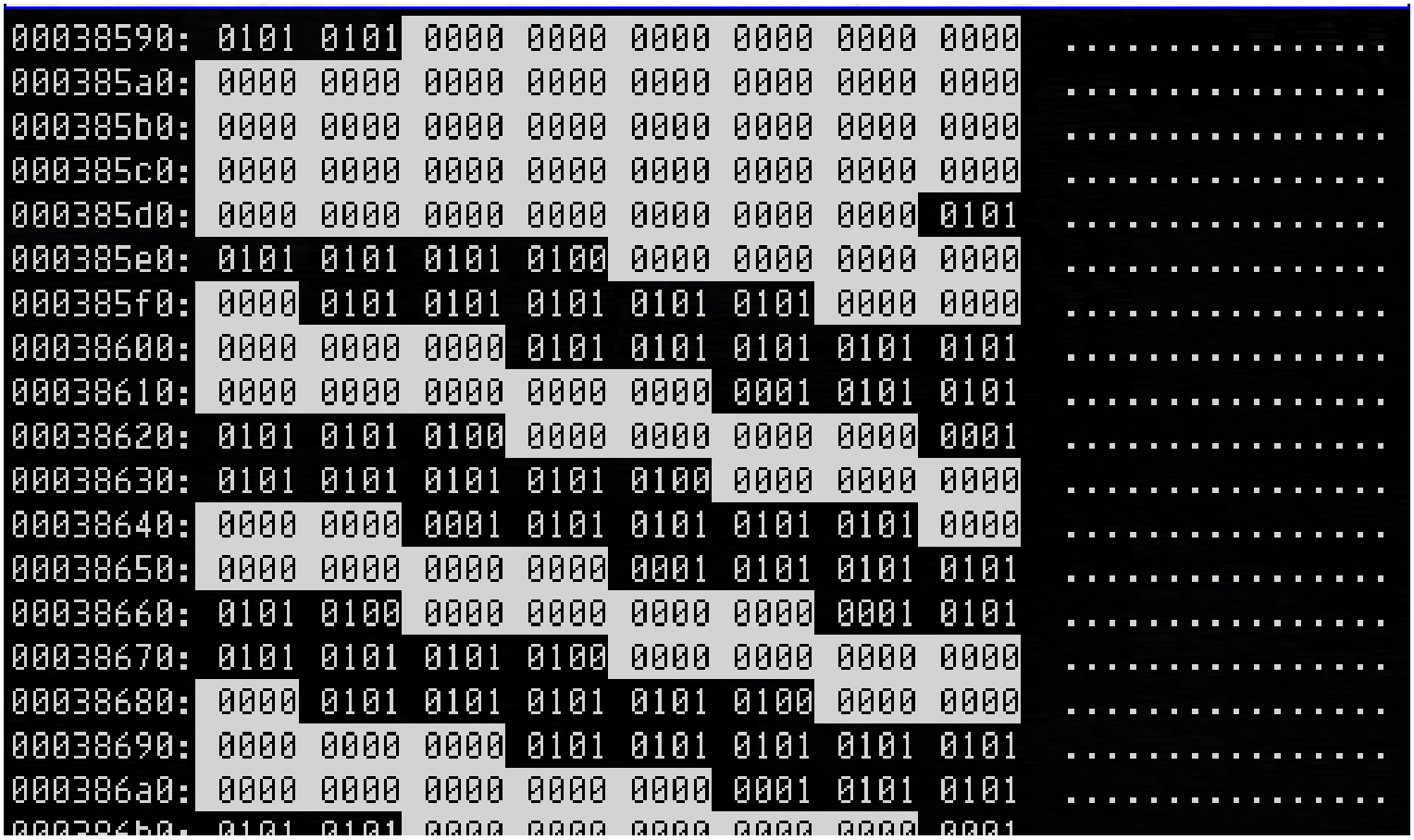

Scope Plot 1
Ch1
Ch2
Counts
1.5
1
0.5
0
-0.5
-1
-1.5
-2
480
490
500
510
520
530
540
550
Time (us)
Persistence
Analog Alpha: 0.0994
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1
Ch2
Trig
XY
Coupling:
DC
Marker:
Line Link
Run


00000000: 0101 0101 0101 0101 0101 0101 0101 0101 ....
00000010: 0101 0101 0101 0101 0101 0101 0101 0101 ....
00000020: 0101 0101 0101 0101 0101 0101 0101 0101 ....
00000030: 0101 0101 0101 0101 0101 0101 0101 0101 ....
00000040: 0101 0101 0101 0101 0101 0101 0101 0101 ....
00000050: 0101 0101 0101 0101 0101 0101 0101 0101 ....
00000060: 0101 0101 0101 0101 0101 0101 0101 0101 ....
00000070: 0101 0101 0101 0101 0101 0101 0101 0101 ....
00000080: 0101 0101 0101 0101 0101 0101 0101 0101 ....
00000090: 0101 0101 0101 0101 0101 0101 0101 0101 ....
000000a0: 0101 0101 0101 0101 0101 0101 0101 0101 ....
000000b0: 0101 0101 0101 0101 0101 0101 0101 0101 ....
000000c0: 0101 0101 0101 0101 0101 0101 0101 0101 ....
000000d0: 0101 0101 0101 0101 0101 0101 0101 0101 ....
000000e0: 0101 0101 0101 0101 0101 0101 0101 0101 ....
000000f0: 0101 0101 0101 0101 0101 0101 0101 0101 ....
00000100: 0101 0101 0101 0101 0101 0101 0101 0101 ....
00000110: 0101 0101 0101 0101 0101 0101 0101 0101 ....
00000120: 0101 0101 0101 0101 0101 0101 0101 0101 ....


00038590: 0101 0101 0000 0000 0000 0000 0000 0000 ....
000385a0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000385b0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000385c0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000385d0: 0000 0000 0000 0000 0000 0000 0000 0101 ....
000385e0: 0101 0101 0101 0100 0000 0000 0000 0000 ....
000385f0: 0000 0101 0101 0101 0101 0101 0000 0000 ....
00038600: 0000 0000 0000 0101 0101 0101 0101 0101 ....
00038610: 0000 0000 0000 0000 0000 0001 0101 0101 ....
00038620: 0101 0101 0100 0000 0000 0000 0000 0001 ....
00038630: 0101 0101 0101 0101 0100 0000 0000 0000 ....
00038640: 0000 0000 0001 0101 0101 0101 0101 0000 ....
00038650: 0000 0000 0000 0000 0001 0101 0101 0101 ....
00038660: 0101 0100 0000 0000 0000 0000 0001 0101 ....
00038670: 0101 0101 0101 0100 0000 0000 0000 0000 ....
00038680: 0000 0101 0101 0101 0101 0100 0000 0000 ....
00038690: 0000 0000 0000 0101 0101 0101 0101 0101 ....
000386a0: 0000 0000 0000 0000 0000 0001 0101 0101 ....

5.4.1.2 Mode T1 and T2 meter transmit : Preamble chip sequences

The total preamble (header + synchronisation) chips sequence for this mode is n(01) 0000111101 with n ¿= 19.*


00038590: 0101 0101 0000 0000 0000 0000 0000 0000 ....
000385a0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000385b0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000385c0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000385d0: 0000 0000 0000 0000 0000 0000 0000 0101 ....
000385e0: 0101 0101 0101 0100 0000 0000 0000 0000 ....
000385f0: 0000 0101 0101 0101 0101 0101 0000 0000 ....
00038600: 0000 0000 0000 0101 0101 0101 0101 0101 ....
00038610: 0000 0000 0000 0000 0000 0001 0101 0101 ....
00038620: 0101 0101 0100 0000 0000 0000 0000 0001 ....
00038630: 0101 0101 0101 0101 0100 0000 0000 0000 ....
00038640: 0000 0000 0001 0101 0101 0101 0101 0000 ....
00038650: 0000 0000 0000 0000 0001 0101 0101 0101 ....
00038660: 0101 0100 0000 0000 0000 0000 0001 0101 ....
00038670: 0101 0101 0101 0100 0000 0000 0000 0000 ....
00038680: 0000 0101 0101 0101 0101 0100 0000 0000 ....
00038690: 0000 0000 0000 0101 0101 0101 0101 0101 ....
000386a0: 0000 0000 0000 0000 0000 0001 0101 0101 ....

5.4.1 Mode T1 and T2 meter transmit : "3 of 6" data encoding (meter to other)

3 of 6 encoding is used for the T mode to give an improved efficiency in comparison with a Manchester encoding. Unique codes are used for specified control functions such as preamble, message start, etc.

Each 4-bit nibble of data is encoded as a 6-bit word and only those words, out of the 64 combinations, with an equal number of zero's and one's, and with a minimum of 2 transitions, have been selected.

Table 13 — Mode T1 and T2 meter transmit, "3 out of 6" data encoding

NRZ-Code	Decimal	6 bit code	Decimal	N° of transitions
0000	0	010110	22	4
0001	1	001101	13	3
0010	2	001110	14	2
0011	3	001011	11	3
0100	4	011100	28	2
0101	5	011001	25	3
0110	6	011010	26	4

3244 6850 3096 8602 6980 d541 a011 9f1d 2029 9a01 8709 2e0a
0023 9a70 0023 1f39 3559 454c 400e 0400 0100 0000 b04f 0000
0000 0000 0001 03

32 44 6850 3096 8602 6980 d541 a011 9f1d . . .

5.5.2.1 Mode T : L : Length field

The first byte of the first block is the length field (L = 0 to 255), which signals the total number of user bytes (excluding the length field and the CRCs). . . .

32 **44** 6850 3096 8602 6980 d541 a011 9f1d 9f01 . . .

5.5.2.2 Mode T : C : Control field

The second byte is the C-field, which signals the telegram type. According to IEC 60870-5-2:

- *for the sub-mode T1 (send-no-Reply) the C-field value C=44h is used ;*

3244 **6850** 3096 8602 6980 d541 a011 9f1d 9f01 . . .

5.5.2.3 Mode T : M : Manufacturer ID

- *Bytes 3 and 4 of the first block contain 2 bytes for a unique user/manufacturer ID of the meter.*

```
manuf = []
vendor = struct.unpack("<H", decoded[2:4])[0]
for i in xrange(3):
    manuf.append(chr(0x40 + (vendor & 0x1f)))
    vendor >>= 5
manuf = ''.join(reversed(manuf))
>>> print manuf
TCH
```

3244 6850 **3096 8602 6980** d541 a011 9f1d 9f01 . . .

5.5.2.4 Mode T : A : Address

This address A must be unique (at least within the maximum transmission range). Each user/manufacturer should guarantee that this ID is unique.

3244 6850 3096 8602 6980 **d541** a011 9f1d 9f01 . . .

5.5.3 Mode T : CRCx : Cyclic Redundancy Check
The CRC polynomial is : x16+x13+x12+x11+x 10+x8+x6+x 5+x2+1. The initial value is : 0. The final CRC is complemented.

3244 6850 3096 8602 6980 d541 **a0** 11 9f1d 9f01 ...

5.5.2.5 Mode T : CI Control Information Field (1 byte)

... A0h-B7h Manufacturer specific Application Layer

and what about the rest?

```
.... .... .... .... .... .... ..11 9f1d
2029 9a01 8709 2e0a 0023 9a70 0023 1f39
3559 454c 400e 0400 0100 0000 b04f 0000
0000 0000 0001 03
```

. . . months of staring at hex dumps

a011 9f1d 9f01 102a 9c01 1108 6108 0002
Probably some kind of TLV indicator, always static

a011 9f1d **9f01** 102a 9c01 1108 6108 0002

mystery, constant for each station.

a011 9f1d 9f01 **102a** 9c01 1108 6108 0002

```
def todate(d):
    d=[ord(c) for c in d]
    return '%02d-%02d-%04d' % (
        ((d[1] & 1) << 4) | (d[0] >> 4),
        ((d[1]>>1) & 0xf),
        (d[1] >> 5) + 2014)
```

a011 9f1d 9f01 102a **9c01** 1108 6108 0002
total consumption

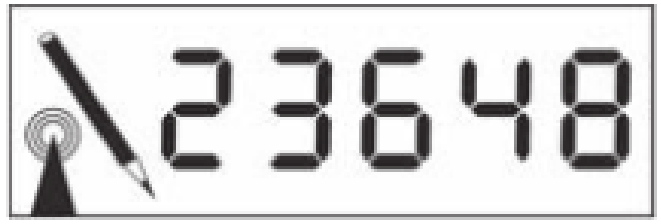
a011 9f1d 9f01 102a 9c01 **1108 6108** 0002
temp1 and temp2

a011 9f1d 9f01 102a 9c01 1108 6108 **00** 02
consumption in current bi-weekly cycle

a011 9f1d 9f01 102a 9c01 1108 6108 00 **02**
consumption in previous bi-weekly cycle

LC displays

Current consumption



Reference date consumption

Serial number of the heating cost distributor

. . . more weeks of collecting samples and staring at hex dumps

the rest:
0002 231f 3935 5945 4c40 0e04 0001 0000 0000 0000 0000 0000
01

- *Radio transfer of the mid-month and month-end figures, making intermediate on-site meter reading superfluous*

water meter packet payload structure

```
<-const-> ????             const
a206 531e 0100 102a 4700 0400 0011
          date ^^^^         cur ^^
              total ^^^^    prev ^^

1113 1310 0000 0000 0000 0000 0000 0000 0000 0000 0000
^------------------last-22-------------------------->
```

conclusion

privacy impact

- the consumption values granularity is not enough to track individuals on a short-term basis. Cannot deduce if someone is at home today.
- In the long-term some demographic values can be deduced, but those I guess were available already to the public utilities.
- Interesting corner-case are the temp1/temp2 values which are updated on each transmission, and could be used to deduce persons short-term presence based on statistical methods.
- lacking a receiver the only way to mess with the meter itself is using the infra port. so this might not be the best target for SCADA-CYBER-APT-IOT fears.
- your neighbours can read this stuff.

reversing

- in retrospect much is already documented, i just messed up the order of finding the docs and fiddling with this device.
- the application specific parts will provide for some further interesting insights with more samples over time.
- would be interesting to also have a look at the collection devices, the receivers.

code

- https://github.com/stef/smeter
- https://github.com/jmichelp/gr-wmbus