Cyble RF 433Mhz installed by my community of municipality

The Actaris radio frequency module for water meters: a reliable, compact and intelligent tool for remote reading, from the distribution network to collective housing. Completely waterproof RADIAN ™ compatible compact radio communication module, Cyble RF can be installed very easily, on site or in the factory, on both a cold and hot water meter. Its installation on site does not require wiring or wall mounting, or removing or unplugging the meter. Specially designed to withstand harsh environments, Cyble RF is suitable for all conditions encountered, from the flooded manhole to the technical shaft. Its many intelligent functions make it possible, in addition to the index reading, to obtain:

- the monthly index history over 13 months,
- detection of backwash, reverse cumulative volume and 13-month monthly history
- leak detection and monthly history over 13 months
- detection of attempted fraud
- end of battery life indication
- various alarms

RADIAN protocol

- impossible to find on the internet, the address http://www.radianprotocol.com/ [http://www.radianprotocol.com/] is no longer active

from web.archive.org

The Radian Protocol

A two-way 433 Mhz Radio Protocol

Radian Protocol is designed for all applications in water, electricity, gas and heat meter reading and data transmitting. Its two way caracteristics allows developed service solutions, including information exchange with final user.

```
reliability

  physical layer: FSK modulation, narrow band
  Logical Link Layer: packet numbering

two ways, half duplex, data transmission
relaying capability

  receive an repeat datagrams
  up to 7 nodes forward

sophisticated wake up mechanism

  standby mode
  wake-up signal => awaken mode
```

my address?

```
 yes => let's communicate!

  no => back to stand by
```

time to get data from a node: 2-3 s

```
both master - slave control and CSMA asynchronous communications
```

from a doc of a survey tool

- FSK process, bidirectional
- Frequency 433.82 MHz
- Asynchronous FSK, NRZ modulation
- Radian Protocol
- 5 KHz modulation offset
- Channel bandwidth 25 KHz
- Transmission rate 2,400 baud
- Central radio transmission emission power + 10 dBm (10 mW)
- Receiving sensitivity - 105 dBm
- Range approx. 50 m

f5943_cyblerfvacatris.pdf does nothing more

other tracks

- standard 13757-4 (DATA \ DOCUMENTATIONS_div) → blah finally the protocol is not really connected
- open-meter_wp2_d2.1_part3_v1.0.pdf -> EverBlu (5.4.11) 10Kbps → false track

- cyble RF technical file [https://www.google.fr/search?q=dossier+technique+cyble+RF&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:fr:official&client=firefox-a&channel=sb&gfe_rd=cr&ei=0wdxVO2GG4TEUNz5gOAK]
    - the carrier is 433.82Mhz
    - they talk about cryptography (apart from the CRC, there's nothing ...)
    - the counter can only be woken up during its “working hours” (indeed, but the hours and days are configurable in the factory)

hacking

In 2011 I released this web page to the wind of the web.

In 2014 julien hooked up, we grouped together some docs that we had on the subject.

He decided to listen to the meters at his residence 24 hours a day with an SDR and a large hard drive.

In February 2016 he managed to capture several meter readings, we started scratching.

But we were missing how to calculate the CRC and how to make the link between what is marked on our meter and the relief frame.

SigmaPic joined the project and he put a lot of things flat (well especially the bits).

There was still this issue of etiquette.

In December 2016 we were all snorting our meters and Julien managed to capture his own meter reading.

1 month later, signacPic was able to read its own meter .

Protocol

Physical Layer

RF Transmission

- FSK process, bidirectional
- Frequency 433.82 MHz
- Asynchronous FSK, NRZ modulation
- Radian Protocol

- 5 KHz modulation offset
- Channel bandwidth 25 KHz
- Transmission rate 2,400 baud

Communication Frame

Any communication frame consists in:

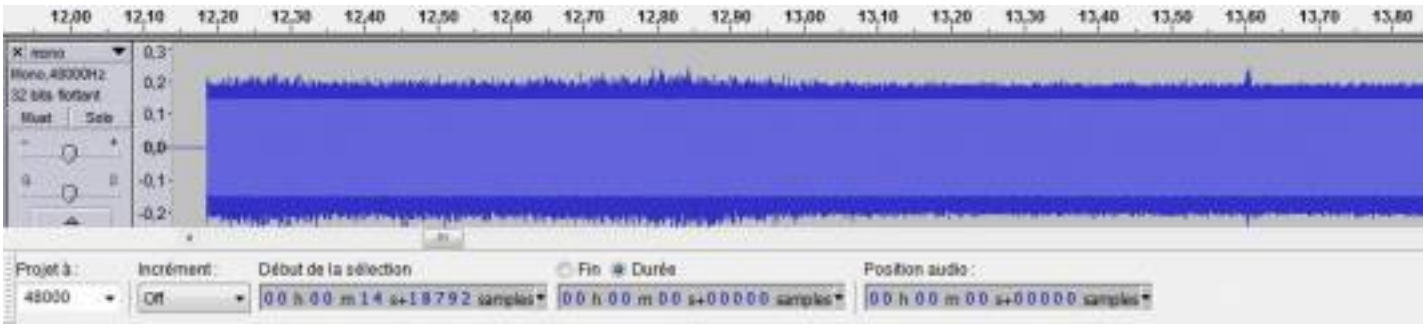
1. A preamble used to notify the receiver that data will be sent
2. A sync word used to notify the receiver that data transmission is starting
3. Some data

Preamble

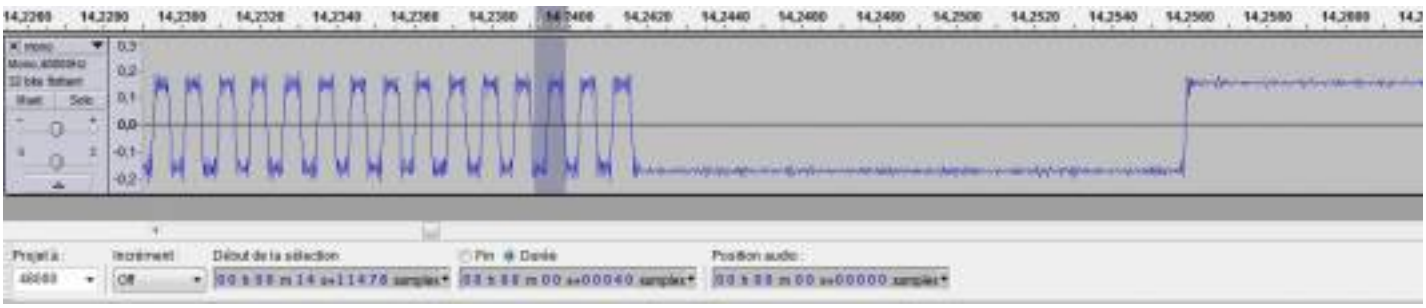
Preamble is a series of 0101…. 0101 at 2400 bits / sec. There are two preamble durations:

- Long preamble for meter wake-up: 4928 bits (2464 x 01)
- Short preamble for other frames: 80 bit (40 x01)

In order to save energy, meter wakes-up every 2 seconds and check if someone is speaking. If nobody is speaking, meter goes back to sleep. This is the reason why long preamble is used when the master send a request.



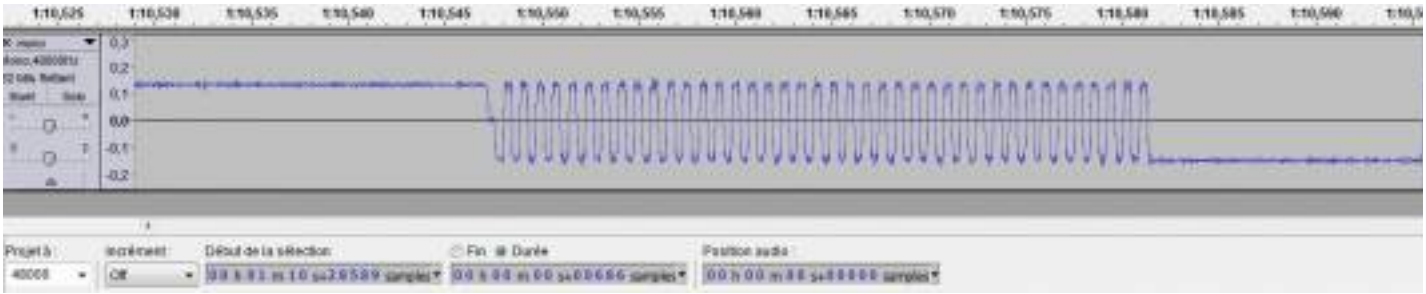
a preamble with a master request



zoom on end of preamble

Sync pattern

Sync pattern starts with low level during 14.3ms followed by a high level during 14.3ms.

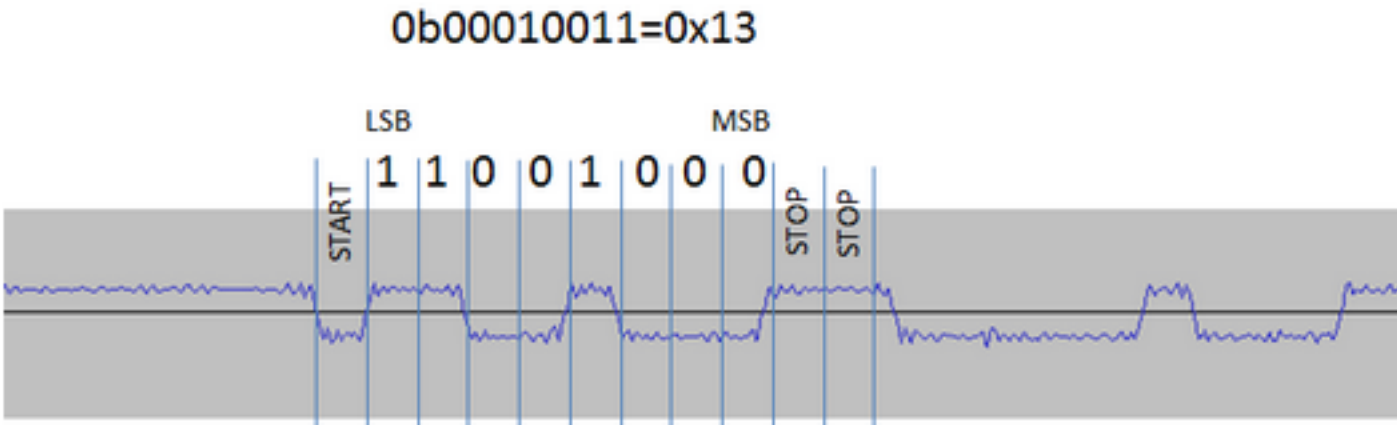


preamble and synch pattern of meter response

Data

Data are sent by UART:

- Baudrate: 2400 bits / sec
- lsb first
- 1 start bit / No parity / 2 or 2.5 stop bits



Frame Structure

L (1)	C (1)	S (1)	Receiver Address (5)	S (1)	Sender Address (5)	S (1)	Data + Checksum (4-240)

- L (Length Byte) Total number of bytes including length byte and checksum
- C (Control Byte)
  - 0x10: Request
  - 0x06: Acknowledge
  - 0x11: Response
- S (Spacer) 0x00
- Receiver Address (5bytes): Meter address when master is speaking and master address when meter is speaking
- S (Spacer) 0x00

- Sender Address (5bytes): Master address when master is speaking and meter address when meter is speaking
- Data Payload (Up to 238 bytes)
- Checksum (2bytes) CRC-CCITT (Kermit [https://www.lammertbies.nl/comm/info/crc-calculation.html])
    - Polynomial: 0x8408
    - Initial Value: 0
    - Bytes are reversed (MSB first)
    - Result is inverted
    - Final XOR: 0
    - Stored in little endian.

Meter Data mapping

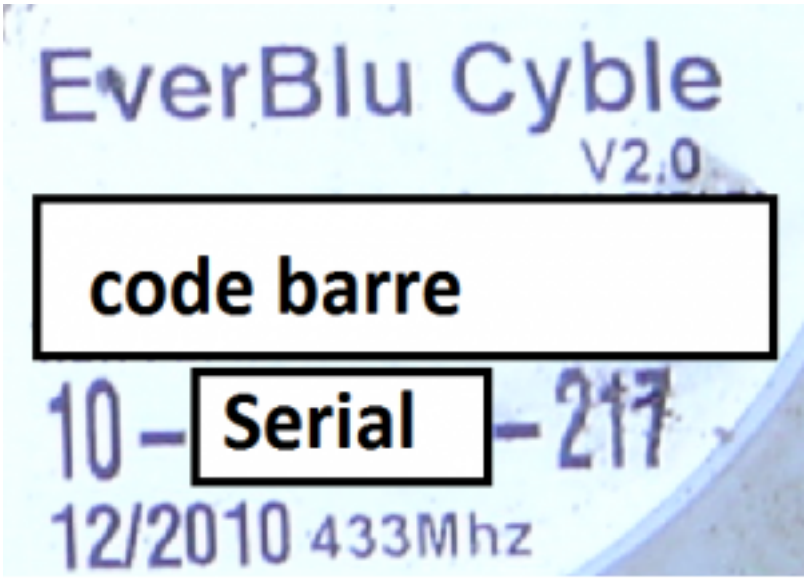
Name	Offset	Size	Description
?	0	1	0x0A if ACK is 0x0A or 0x01 if ACK is 0x06
?	1	1	?
Spacer	2	1	Null byte (0x00)
Current Index	3	4	Current meter index in liter. Unsigned integer in big endian
?	7	1	0x40
?	8	1	0x02 or 0x06
Date	9	3	Date of the request: J/M/Y First byte is J. Second byte is M. Third byte is Y.
Weekday	12	1	Day of the week as an unsigned
Time	13	3	Time of the request: H:M First byte is hours. Second byte is minutes. Third byte is seconds.
Battery Lifetime	16	1	Remaining battery life time in months.
Meter Serial	17	11	Meter Serial Number. Encoded in ASCII and stored in reverse orde character first). String is ended with a null by
Spacer	28	1	Null byte (0x00)
Wakeup Start	29	1	Meter wakeup time. Unsigned integer.
Wakeup Stop	30	1	Meter sleep time. Unsigned integer.
Num. of Reading	33	1	Number of time meter has been read. Uns integer.

M-13 Index	70	4	Index of month -13 in liter. Unsigned integer in big endian
M-12 Index	74	4	Index of month -12 in liter. Unsigned integer in big endian

Index			Unsigned integer in big endian
M-11 Index	78	4	Index of month -11 in liter. Unsigned integer in big endian
M-10 Index	82	4	Index of month -10 in liter. Unsigned integer in big endian
M-9 Index	86	4	Index of month -9 in liter. Unsigned integer in big endian
M-8 Index	90	4	Index of month -8 in liter. Unsigned integer in big endian
M-7 Index	94	4	Index of month -7 in liter. Unsigned integer in big endian
M-6 Index	98	4	Index of month -6 in liter. Unsigned integer in big endian
M-5 Index	102	4	Index of month -5 in liter. Unsigned integer in big endian
M-4 Index	106	4	Index of month -4 in liter. Unsigned integer in big endian
M-3 Index	110	4	Index of month -3 in liter. Unsigned integer in big endian
M-2 Index	114	4	Index of month -2 in liter. Unsigned integer in big endian
M-1 Index	118	4	Index of month -1 in liter. Unsigned integer in big endian

Meter Address Encoding

- Address is encoded over 5 bytes.
- First byte is 0x45 (TBC).
- Four other bytes are deduced from numbers below the bar-code
- format is YY-AAAAAAA-CCC.
    - 2nd byte YY: Years encoded on 8bits
    - 3rd-to 5th Byte AAAAAAA to be converted in from decimal to hex MSB first
    - CCC: Check digits (Not used in address encoding but used to verify YY-AAAAAAA consistency)



example

- Serial number 16 - 0123456 -CCC
- YY = 16d → 10h
- AAAAAAA = 0123456d → 01E240h
- Master request to be predecing by 2s of 2464 * 01 then follow by Sync pattern **and encapsulated in 1 start bit / No parity / 2.5 stop bits (works also with 2bit and 3bit)**
    - 13 10 00 45 10 01 E2 40 00 45 67 89 AB CD 00 0A 40 DA DC (cks) for the calculation of the CKS take the Kermit line and swap the nibbles ⇒ http://crccalc.com/?crc=131000451001E24000456789ABCD000A40&method=crc16&datatype = hex [http://crccalc.com/?crc=131000451001E24000456789ABCD000A40&method=crc16&datatype=hex]

	Length	Control	Spacer	Receiver Address	Spacer	Sender Address	Spacer	Ch
Master request	13	10	00	45 10 01 E2 40	00	45 67 89 AB CD	00	0A DC
Meter Acq	12	06	00	45 67 89 AB CD	00	45 10 01 E2 40	00	0A
Meter response	7C	11	00	45 67 89 AB CD	00	45 10 01 E2 40	00	01 73 40 (48 lite

	Length	Control	Spacer	Receiver Address	Spacer	Sender Address	Spacer	Ch
Master Acq	12	06	00	45 10 01 E2 40	00	45 67 89 AB CD	00	0A

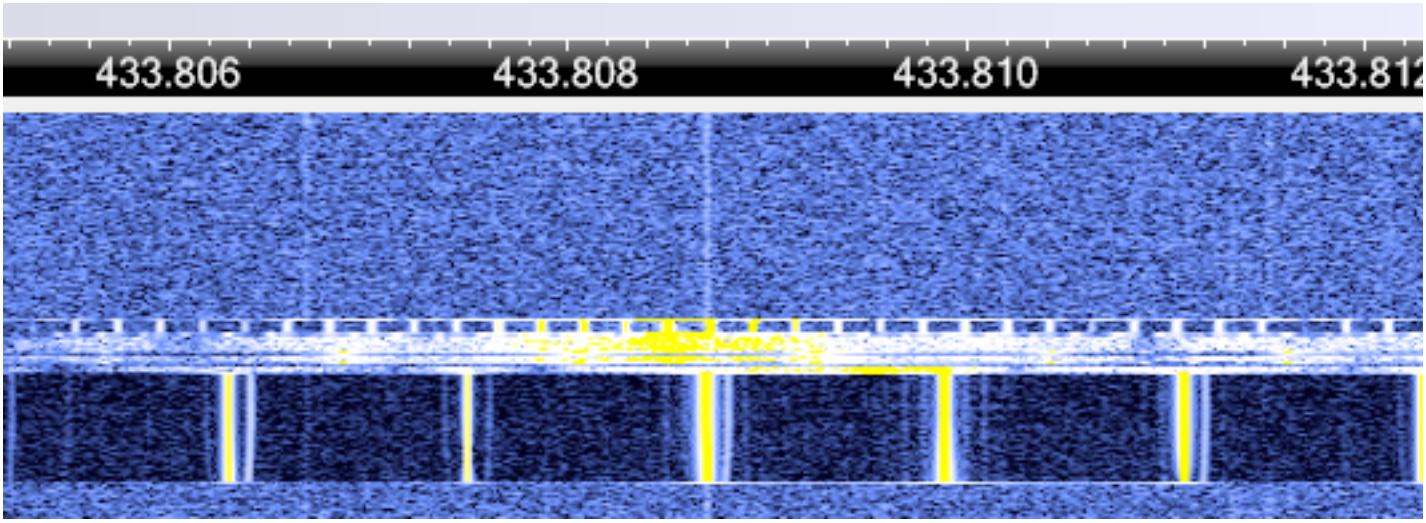
succession solutions

CC1101

the CC1101 is an RF transceiver you can adjust a bunch of parameters, but the actual frequency is not exactly what you are adjusting.

```
// for example I have 2 CC101 cards for the same frequency setting one assembl
halRfWriteReg ( FREQ0 , 0xC1 ) ;  // Frequency Control Word, Low Byte CC1101_N
halRfWriteReg ( FREQ0 , 0xB7 ) ;    // CC1101_N1 810 819.5 OK
my counter also goes F1 :  433808500   F2 :  433819500
```

hence the need to calibrate the FREQ0 register using a TNT key which makes SDR



rpi + CC1101

cable schematics

```
5V , GND ---> RPi HE26 --- . ----- 2 * GND ;  2 * 3.3V , SCLK , MISO , MOSI ,
                           |
                    debug_connector ( HE14 )
```

RPi PIN allocation

WiringPi Pin = WPP

Function	WPP	Name	Header		Name	WPP	Function
		3.3v	1	2	5v		
	8	SDA	3	4	5v		
	9	SCL	5	6	0v		
	7	GPIO7	7	8	TxD	15	
		0v	9	10	RxD	16	
GDO0	0	GPIO0	11	12	GPIO1	1	
GDO2	2	GPIO2	13	14	0v		
LED	3	GPIO3	15	16	GPIO4	4	
		3.3v	17	18	GPIO5	5	
MOSI	12	MOSI	19	20	0v		
MISO	13	MISO	21	22	GPIO6	6	
SCLK	14	SCLK	23	24	CE0	10	Csn
GND		0v	25	26	CE1	11	

```
#define GDO2 2 // header 13
#define GDO1_MISO 13
#define GDO0 0 // header 11
#define MOSI 12
#define cc1101_CSn 10 //// header 24
#define LED 3 // header 15
```

HE10 CC101

Top view

Function	Header		Function
3.3v	1	2	3.3V
MOSI	3	4	SCLK
MISO	5	6	GDO2
CSn	7	8	GDO0
GND	9	10	GND

Flipped view from bottom

Function	Header		Function
3.3v	2	1	3.3V
MOSI	4	3	SCLK
MISO	6	5	GDO2
CSn	8	7	GDO0
GND	10	9	GND

debug_connector (HE14)

SALEAE led (1)

Function	Header		Function
D1	1	2	D2
D3	3	4	D4
D5	5	6	D6
D7	7	8	D8
GND	9	10	GND

```
           DB9 TDA (face
(GND) 5 4 3 2 1 (data)
         9 8 7 6 (5v)
```

HE14

Function	Header		Function
(D1 saleae) DATA TDA	1	2	(D2 saleae) LED
(D3 saleae) SCLK	3	4	(D4 saleae) IF
(D5 saleae) GDO2	5	6	(D6 saleae) SO
(D7 saleae) GDO0	7	8	(D8 saleae) CSn
GND	9	10	GND
3.3	11	12	GND
DATA TDA	13	14	5V

coded

the zip has a mo t d3 pa5se this is the name of the radian_trx.zip zip file

config

the delivered code will not compile (gcc radian_trx.c -o radian_trx -lwiringPi -lpthread -Wall) because there are 2 parameters to adjust + 2 tipo

- frequency to adjust according to your CC1101 CC1101.c: line 229: halRfWriteReg (FREQ0,….)
    - I advise to start with the base frequency then to measure with the TNT dongle to center it on the 433.820 or the response of the counter
    - if there was no response from the counter then you will have to try to shift in steps of 2kHz on each side of 433.820
        - it is necessary to modify FREQ0 by adding / subtracting a few units to shift the main frequency of 2kHz, it is necessary to know that a “SDR key TNT at 20 €” does not give the real frequency in absolute, in relative it is already better
- the serial number of the meter. here is the line of code that goes with the example paragraph
    - CC1101.c: line 664: TS_len_u8 = Make_Radian_Master_req (txbuffer, 16 , 123456);
- in CC1101.c add #define TX_LOOP_OUT 300 at the top
- a “c” character to be deleted on line 5 of radian_trc.c

script

```
sudo crontab -e
55 9 * * * sudo / home / pi / radian_trx / web_tx_releve> / dev / null 2> & 1
55 9 * * * sudo / home / pi / radian_trx / web_tx_releve >> /var/log/crontab.l
```

performance

minepi + CC1101 (2) + lambda / 4 behind bulkhead	shutter open	rssi = 185 lqi = 128 F_est = 255
minepi + CC1101 (2) + lambda / 4 in bulkhead	shutter open	rssi = 185 lqi = 128 F_est = 255
minepi + CC1101 (2) + ant spiral behind partition	shutter open	rssi = 183-4 lqi = 128 F_est = 255

Mbed + CC1101

RTL SDR

- https://www.youtube.com/watch?v=c3C7GBuxpNo [https://www.youtube.com/watch?v=c3C7GBuxpNo]
- http://www.nooelec.com/store/qs/ [http://www.nooelec.com/store/qs/]
    1. Plug your NESDR into an available USB port
    2. Open the 'NESDR Driver Installer', Zadig
    3. Select 'List All Devices' from the 'Options' menu in Zadig
    4. From the main dropdown, select the NESDR
    5. Confirm the selected device has a USB ID of '0BDA 2838'
    6. Press the big button to install drivers – button
- http://m3ghe.blogspot.fr/p/adding-support-for-rtl-sdr-usb-dongles.html [http://m3ghe.blogspot.fr/p/adding-support-for-rtl-sdr-usb-dongles.html]

= ⇒SDR console OK

- http://www.rtl-sdr.com/rtl-sdr-quick-start-guide/ [http://www.rtl-sdr.com/rtl-sdr-quick-start-guide/]
- http://rtl-sdr.sceners.org/?p=193 [http://rtl-sdr.sceners.org/?p=193] kalibrate

With a sampling frequency of 31.25 ksps it is 2.5GB of data over 12 hours. It seems heavy but on a 1TB HDD it still allows you to record 1024 / 2.5 = 410 working days.

gear

- http://fr.farnell.com/mipot/32000508e/emitter-fsk-50-pll-5-12v-433-92mhz/dp/1702924 [http://fr.farnell.com/mipot/32000508e/emetteur-fsk-50-pll-5-12v-433-92mhz/dp/1702924] , Frequency range: 433.42MHz to 434.42MHz
- http://www.roue-libre.be/article.php3?id_article=180 [http://www.roue-libre.be/article.php3?id_article=180]
- http://iw3hzx.altervista.org/Antenne/HENTENNA/Hentenna.htm [http://iw3hzx.altervista.org/Antenne/HENTENNA/Hentenna.htm]
- SDR
- SX1212
- http://f5ad.free.fr/ANT-QSP_Descriptions_430.htm [http://f5ad.free.fr/ANT-QSP_Descriptions_430.htm]
- http://users.belgacom.net/hamradio/schemas/jpole.gif [http://users.belgacom.net/hamradio/schemas/jpole.gif]
- http://www.roue-libre.be/article.php3?id_article=258 [http://www.roue-libre.be/article.php3?id_article=258]
- http://radio.pagesperso-orange.fr/Ant.htm#GP [http://radio.pagesperso-orange.fr/Ant.htm#GP] ; https://www.adri38.fr/antenne-ground-plane-446-mhz/

[https://www.adri38.fr/antenne-ground-plane-446-mhz/]

- https://www.elektor.nl/Uploads/Forum/Posts/How-to-make-a-Air-Cooled-433MHz-antenna.pdf [https://www.elektor.nl/Uploads/Forum/Posts/How-to-make-a-Air-Cooled-433MHz-antenna.pdf]
- http://www.qsl.net/ve2ztt/IndexD/moxon_fichiers/moxon.htm [http://www.qsl.net/ve2ztt/IndexD/moxon_fichiers/moxon.htm] ; http://f1rzv.free.fr/moxon/index.php [http://f1rzv.free.fr/moxon/index.php]

antennas

http://www.ta-formation.com/cours/e-antennes.pdf [http://www.ta-formation.com/cours/e-antennes.pdf]

ranking according to http://www.modelisme.com/forum/aero-vol-en-immersion/195087-amplifier-un-signal-uhf-433mhz-optimiser-la-reception.html

from the least good gain to the best

1. 1/2 wave monopoly
2. 1/4 wave monopoly
3. 1/2 wave dipole
4. 1/4 wave dipole (approx 70ohm)
5. 1/2 wave inverted V antenna
6. 1/4 wave inverted V antenna
7. Moxon antenna (approx 50ohm)
8. Yagi, patch or quad antenna (Directional antenna)

Discussion

ouinouin , 11/2014
Hello,
I am looking for the solution to query Cyble RF modules.
I am ready to put my hand in my pocket to have some stuff (equipment to interrogate the RF cyble counters). in the meantime, my internet research shows me that the everblu protocol is compatible with the radian protocol.
if I had enough time to experiment, I will put an SDR receiver close to the frequency and I will wait (one week / one month / three months). while logging the reception. once a very high level emission is detected, it will suffice to look at the frames upstream.
nevertheless I assume that there is an encryption of the data ...

meterfairy , 02/2015

Good to see that your interested in these EverBlu meters. From what I can tell the Everblu Cyble Enhanced meters have no encryption or authentication whatsoever for the RF transmissions. I think the meters communicate using protocol which is very similar if not identical the the Wireless M-Bus standard. It may be the the RADIAN protocol was renamed once the wireless M-Bus strandard was adopted.

I have access to an SDR and understand how the communication frames (size, content, checksums etc.) for these meters work, however I don't own a physical meter to test. If anyone knows where I can buy or obtain an Everblu Cyble Enhanced meter I would really appreciate it!

ouinouin „04/2015

Hi meterfairy

we can find some meters in ebay from times to times (i found a new one in italy), i bought one, but the most difficult material is the programming console to initialize it.

the difficult point is the meter itself doesnt send any frames, it justs lookups up for a snc pattern every 2 secs (you can "listen it" by butting the sdr centered on 433.82mhz very near the meter.)

if you think you can find how to trigger a sleeping meter by trying to send "wake up" patterns, id be ready to offer you a unit if you find one on the ebay.

take care, units already initialized are usually listening for wake up frames from 6am to 6pm from monday to friday (its not a joke, and its the most efficient and clever powerwsaving idea i never heard of).

looks

Stéphane „01/2016

Hi,

Did anybody find how to wake up the Everblu Cyble RF?

What's new since one year?

Best regards

ouinouin „02/2016

Hi,

I managed today to sniff Radian Frames with my sdr during teletransmission to hand held in my building, I captured many frames from different Water meters with the help of my sdr (30 € TNT usb stick), I ll soon upload the raw and demodulated data for getting help to decode.

be ready to download audacity, gnuradio an the latest version of gqrx :)

ouinouin „02/2016

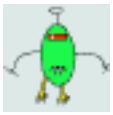
hi,

have a look at

http://ouinouin.net/owncloud/index.php/s/Nt8lnC6PPkO8AeL

im sharing a demodulated file to open with audacity, this is a fm demodulation of a 7minutes capture of radian polling and answers by some water meters.
i just finished the capture + cut, i ll quickly look at the file, calculate the symbol rate and try to find the encoding.

I ll nearly post on the snootlab forum more complete information + link to the raw file captured with my sdr.



fred_ , 02/2016
YESSS great job !!!

Fred , 02/2016
Hello
http://hackaday.com/2014/02/25/using-sdr-to-read-your-smart-meter/
https://github.com/bemasher/rtlamr

Fred

SigmaPic , 03/2016
Hello,

I am also interested!
Have you made progress on the subject?
How can we contribute?

@ +

fred , 03/2016 , 03/2016
yes we have advanced you can watch the §tests of julien.
at the end we have decoded the messages (at bit and byte level), now we need:
- understand how the message of the reading tool is constructed (we are interested in another record if in addition we have the number counter marked on the label that could help)
- try to replay a pre-recorded message to see if we get an answer

from my side I'm waiting for a CC1101 based tranceiver who comes from China to be able to play with it.

Fred (site admin)

frederic34 , 03/2016
Hello
My meter is 868MHz, there is a Homerider label on it with the address of the meter in the style 5322 / 11.81.xx.xx.xx
I have a sdr key (rtl2832 with rt820t) bought for ten euros
I am near Montpellier and it's Veol! who put the

frederic34 counter

Sigma Pic , 04/2016
Hi,

I have just attempted an acquisition with SDRSharp software and a TNT RTL2832U + RT820 dongle (Saturday 12:00 pm).
The antenna is 20cm from the meter.

At 433.92MHz, I have no signal. Nothing at all ...

Is it normal at this time of the week that there is nothing?

Sigma Pic , 04/2016
Small question about the data in Julien's Excel file.

Is the data transmitted with a start + stop + parity bit?

fred , 04/2016
hi
the working hours of the meter are from Monday to Saturday 6:00 am to 6:00 pm, so Saturday around 12:00 am it's not bad, but to "wake up" the meter you have to send it a wake-up frame.
2.5s of 0/1 @ 1.2khz followed by a frame like the one at house2: compt_d_eau: 14270.png.
the problem is that this frame is specific to each counter.

to have this frame you have to listen when the guy passes in the street to read your meter (once a year ...) or if you are lucky every week when the remote reading is installed on the telephone pole or streetlights.

we did not identify any start + stop + parity bits, but we noticed that each byte was separated by 3 bits when it is the reading tool which speaks and by 4 bits when it is the counter which speaks. in the out_raw.zip file these separator bits are present. in the out.zip and out.xls files they have been deleted.

Sigma Pic , 04/2016
Ok, it's rolling.

I quickly looked at the Excel file and this is what I understood.

Hand recorder frame:
Byte 0 to 1: ????
Byte 2 to 7: A sort of address of the sender (which can be an id linked to the manufacturer)
Byte 8 to 13: Address of the recipient
Byte 14 and 15: (0x00 0x28) ????
Byte 16:?

Byte 17 and 18: Maybe a CRC but with which polynomial ???

First response from the counter with an empty frame can be to say "I'm here, I'll send you the data":
Byte 0 to 1: ????
Byte 2 to 7: Address of the counter
Byte 8 to 13: Address of the hand recorder which sent the request
Byte 14 and 15: (0x00 0x28) ????
Byte 16 and 17: Maybe a CRC but with which polynomial ???

Second response from the counter with an empty frame can be to say "I'm here, I'll send you the data":
Byte 0 to 1: ????
Byte 2 to 7: Address of the counter
Byte 8 to 13: Address of the hand recorder which sent the request
Byte 14 to 121: Data with perhaps indexes on the last months ???
Byte 122 and 123: CRC ??

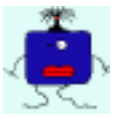
Has anyone managed to find the CRC algo that is being used?

@ +

Sigma Pic , 04/2016
In fact it is rather:

Byte 2 to 7: Address of the recipient

Byte 8 to 13: Address of the sender



Yoann , 04/2016
Since then, has anyone made any new discoveries?
Since, is somebody have made some new discovers?

4u9ur , 05/2016
See on the Hackaday website, dated February 24, 2016
-> http://hackaday.com/2014/02/25/using-sdr-to-read-your-smart-meter/

Patrick , 09/2016
Hello,

I also have a Veolia water meter in HRF at 868Mhz and an RTL-SDR nearby. Can I help take some captures? analysis ? tests ?
RF operates at 433.82 Mhz. Do we know the frequency of 868Mhz?
Thank you,

--- Patrick

ouinouin , 11/2016

Hello,

on the 868 mhz part, the phsic layer will be more of everblue, which is encrypted, but always make recordings if the meter emits continuously, with gqrx or rtl_fm, or bin even try to see if rtl_433 or rtl_amr decodes your frames (to compile yourself).

Sigma Pic , 11/2016

Encrypted or signed ????

Could someone post a frame with the numbers that are on the corresponding counter and why not the index.

SigmaPic , 11/2016

Can someone re-uplode the julien capture zip archives?

fred , 11/2016

hi patrick i am not an expert in RTL-SDR, julien is much more, i will try to write some advice

Sigma Pic , 02/2017

Hi Patrick,

Experience has shown us that Cyble RF and EverBlu Cyble Enhanced use the same protocol at 433MHz.
Have you been able to check if your meter is constantly emitting.
If you have a TNT dongle like "RTL2832 + R820T", it's almost won.
There are many software that allow you to record the baseband at the frequency you choose (SDR # for example).
If your meter does not emit permanently, you will even need a "wolf trap" in place to capture frames during remote reading.

@ +

Telectroboy , 04/2017

Hi,

Does anyone test this out?
https://github.com/merbanan/rtl_433

You can easily change the frequency to 433.82, I think it's worth a try.

Jayce , 04/2017

Hello,

How do you actually go about recovering the data?

Software ....

I have a TNT key type RTL2832 + R820T

Thank you in advance

fred , 04/2017

I have developed a solution based on rpi + CC1101, for the moment the software is not publishable, and sigma pic has made a solution based on an Mbed + C1101 card, I do not know where it is is his code

Miriam , 05/2017

Hi Fred,

I have some Everblue Cyble Sensor with RADIAN protocol,

I have both C1101 + Mbed and RPI + CC1101.

Could you help me with protocol?

Thanks

MM

Jayce , 07/2017

Hello

What is the stuff you need finally?

thanks in advance

fred , 07/2017

you need an RF transceiver, we chose the CC1101.

and you need a microcontroller to control it I have chosen a RaspberryPI and

sigma an Mbed card

for the debugging the use of a dongle USB RTL-SDR key (with R820T2) is strongly recommended to check that you emit something and also check the emission spectrum.

the first step consists in sending an interrogation frame of your meter (see Master request in the paragraph "example") (do not forget the 2s of WUP), during the working hours of your meter => to be sure to be inside 9 am-5pm on weekdays

Jayce , 07/2017
You need this CC1101 module: https://www.amazon.fr/Neuftech-Wireless-Module-%C3%A9mitter-r%C3%A9cepteur-Transceiver/dp/B01CI01F94/ref=sr_1_1?ie=UTF8&qid=1500308377&sr=8 -1 & keywords = CC1101 or https://www.amazon.fr/dp/B01LLQ3B98/ref=sr_1_2?ie=UTF8&qid=1500308377&sr=8-2&keywords=CC1101?

Thank you in advance for the info

fred , 07/2017
the 2 are equivalent, it is indeed necessary to choose the version with SPI protocol, even if it is not marked in the description, I recognize the image :-)

Jayce , 07/2017
Thank you

Jayce , 07/2017
I have all the stuff, now I miss the sources of your programs, can you provide them?

I thank you in advance.

Krotof1a , 07/2017
+1

I just discovered this page while looking for information on the RADIAN protocol since I have a meter with an Everblu module. I have an RPi, different Arduino, and my CC1101 module is on the way. If there is any code to be based on, I'm a taker. Well done for all the work already done and thank you in advance for your support.

Jean , 09/2017
Hello,

Congratulations on this great retro job!
I so want to do the same thing, but my counter seems to have a new type of address which is like in the following photo:
http://www.endetec.com/endetec/ressources/files/1/31837, homeriderdplaquettecompteurs.pdf

Do you have any idea how to decode it and do you think the frames are the same?

Strangely enough, my counter is 868Mhz when I thought it was the US frequency.
Thanks for your help.

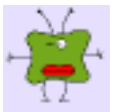
fred , 09/2017 , 09/2017
I would say that you can try the same protocol as in 433Mhz.
indeed the label does not have the same format
5322 / 10.81.09.05.09.89 (01/2009)
against
YY-AAAAAAA-CCC

I would go for this
TYPE / AA.AA.AA.AA.YY.CC mapping

if you don't no answer try to double the data rate.
and if not you will have to make a recording when the guy passes ...

Clement , 11/2017
Hello,
Great job! Do you think this kind of solution could be integrated into Gateway RFLink? http://www.rflink.nl

Q , 2017-12
I have applications on the android to read these modules, you would need to make a bluetooth device rf433 if you can do something like this I can share the apk



max , 01/2018
have a look here - this is the official reading & programming interface for Radian 433 in walk by reading applications
https://www.itron.com/eu/technology/product-services-catalog/products/c/8/1/bluetooth -rf-master-433-radian

Le Gnoutu , 04/2018
Hello everyone,

I'm digging up a bit but I'm interested in electromagnetic pollution of all kinds and I was surprised not to see anything when I approach my spectrum analyzer (between 430 and 440mhz) from my EverBlu Cyble in 433mhz, from suddenly I looked for the technical data and what I understood is that:
1) the RF module of the meter only emits if it receives the "request"
2) this RF module checks every 2 seconds that it is not receiving this request
3) the only way to read the meter (and that it emits) is to use a reading mobile terminal (I'm talking about "normal" use here, eh;)

Is it fair?

I also read in the comments that there are also readout systems integrated in the direct environment of the meter, avoiding the displacement of a technician. Is this indeed the case?

Thank you in advance for your answers!

JohnDoe , 04/2018
Hello everyone,

This page is a real gold mine, it is full of valuable information when looking to query your meter. Unfortunately, it is difficult to access and it would benefit from having an "Implementation" section which, in a few steps, explains how, starting from nothing, one manages to recover the desired data in very detail. I can help you write it, but for that I would have to complete it myself! :)

Today the points which block on my side:
1) [Connection CC1101 - RPi] Confirm the correctness of the following connections:
[CC1101] <=>

GDO2 PIN13
CSn PIN24
GDO0 PIN11
GND PIN25
GND -

2) [Determination of FREQ0] Specify the base values for High Byte, Middle Byte and Low Byte as well as the associated search method for these values. Could you detail that?

3) [Compilation] Resolve the many errors that appear during compilation (missing #include <> in cc1101.c apparently). Do you have the list for him to compile the first time?

Thank you in advance for your wonderful work and hoping that the resolution of my difficulties can help the next ones who will embark on the adventure! :) Have a

nice Sunday.
Alex

fred , 05/2018 , 05/2018
thank you for your feedback

1) yes it looks like http://www.lamaisonsimon.fr/wiki/doku.php?id=maison2:compteur_d_eau:compteur_d_eau#schema_de_cablage
2) determining FREQ0 is not easy, I was lucky because the counter responded and therefore I was able to see the frequency of the response on my SDR and therefore adjust the transmission frequency to be the closest.
I recommended to scan the 433.82Mhz in steps of 2-3khz starting from the center
3) you should not compile CC1101.c alone, but radian_trc.c with the following command line: gcc radian_trx.c -o radian_trx -lwiringPi -lpthread -Wall.
there is indeed a "c" character to delete in line 5 of radian_trc.c

fred , 05/2018
I updated the § on the compilation there are 2 tips to correct in the code ;-)

JohnDoe , 05/2018
Hello Fred,

Thank you for these first elements. In order:

1) The link you point does not directly give the information. I'm unfortunately still not sure.
2) Ok, I will now try to have it compile, hoping the wiring is good to avoid toasting everything! :)
3) Ah yes with this command line + the correction of typos it works! Be careful, it is not a 'c' that should be deleted at the end of line 5, but an 's'.

Thanks, Have a nice week end.

JohnDoe , 05/2018
Hello,

Apparently the counter is reacting on my side, since I see a "bump" appear on SDR # when I run the compiled tool.
However, I don't get any value ... Here is what I get:

./radian_trx
raspian radian trx builded: Apr 29 2018 14:18:51

command list:
exit: x; cc1101 version: v; read config: c
m: MARCSTATE a: MCSM1_val s: full_status
H: scenario of the recovery tool!
A: Reset CC1101

What should be done next?

Thank you in advance. Good week.

JohnDoe , 06/2018
Hello,

After trying to enter all the possible letters, no data. I'm losing hope ... Could you give me some leads?

Thank you so much.
Good week

fred , 06/2018
Hello,

press H (capitalized h) between 9 a.m. and 5 p.m. on weekdays, you should see a signal on your SDR that will last 2 seconds followed if you have a chance of the response of the counter

JohnDoe , 07/2018
Hello,

I get this, after doing it just now:

HMARCSTATE: raw: 0x13 0x13 free_byte: 0x0F sts: 0x02 sending 2s WUP ...
0free_byte: 0x0F sts: 0x02
MARCSTATE: raw: 0x0D 0x0D (RX RX)
TMO on REC
MARCSTATE: raw: 0x0D 0x0D (RX RX)
TMO on REC

How to interpret it? What is the value of my counter?

Thank you again for your help. Good week.

Spout91 , 08/2018
Hello, great

work. I really want to test on my meter. it is a HomeRider system G2 HRF-c at 868 Mz. For info, before I had an ITRON (but replaced because more battery and therefore more readings) so I imagine that the new one must be compatible.

the label indicates:

53.22 /

50.81.17.37.0D.0D

it was installed 3 weeks ago and it is operational because I see my daily readings on the Véolia site.

Do you have an idea of the address of this meter?

thank you for your help, see you soon,

Spout91 , 08/2018

Hello,

After analysis: the 17 in my counter number is the year. By doing research on the internet, I saw that Cyble HRF meters always have this format

53.22 / XX.81.AA.YY.YY.YY. With AA the year of the counter. So I suspect that the serial number must be YY.YY.YY because in RADIAN protocol it only takes 3 bytes for the address.

Has anyone made this observation?

Ilya Erte , 11/2018

Hello And what is the password for the radian_trx.zip file?

bublboblz , 04/2019

| Hello And what is the password for the radian_trx.zip file?

the file name without the extension

Michael , 04/2019

Hello,

thank you for this article and all the painstaking work that allowed this reverse engineering!

My home being equipped with this meter since 2007 and having an RPI, CC1101 and SDR I tried to make them communicate.

Using the radian_trx script and pressing H I was able to observe with SDR # that the RPI and the counter seemed to be communicating well with each other. On this screenshot: https://ibb.co/hFq2rDY we see 3 frames. The first comes from the

RPI, the next 2 from the water meter. Unfortunately the script does not seem to be able to decode the frames sent back.

Do you have an idea or advice?

Thank you

Michael , 04/2019

Finally IT WORKS! :) I made a mistake in the connection of the CC1101 ...
Did someone write a script with a more usable output?
I see in the article a reference to a script called via cron: web_tx_releve but it is not in the zip.

paul , 07/2019

Hello, thank you for this info. I wanted to know if the Cyble RF was toxic in terms of electromagnetic wave and if it emitted often and for a long time. I understood from reading this blog that it never emits except when it is questioned 1x / year or 1x / week if the lifting module on a nearby pole. Ok and how much does it emit, how long does it cause when awake? Thank you for your response and well done for your work.

fred , 07/2019 , 07/2019

hi

here is the content of web_tx_releve
cpt_response = `sudo / home / pi / cpt_eau / radian_trx r`
echo $ cpt_response
wget -4 -O / home / pi / cpt_eau / phpout -o / home / pi / cpt_eau / out http: // www.tonserveur.com/traitement.php?data=$cpt_response

it only sends the data to a server, if you want more data you can try the output. \ radian_trx, without parameter it causes more

in terms of RF pollution is like a car key, or almost nothing

philippe , 10/2019

hi, I would like to know if it will be possible to adapt the code to a simple solution like this https://fr.aliexpress.com/item/32877048266.html

It is a CC1101 USB, that would make the thing much more simple, and accessible to all!

Flop , 10/2019

Hello,

Thank you for posting all this info, thanks to you I managed to read my recently installed water meter.

Not having a TNT key, I added a function that scans the frequencies and tries a recovery. I may have been lucky, but it worked to find the setting for Freq0

```
uint8_t cc1101_scan (void)
{
uint8_t ret = 0;

for (uint8_t freq = 0; freq <255; freq ++) {
halRfWriteReg (FREQ0, freq);
printf ("\ n \ nTry with Freq0 =% d \ n", freq);
ret = scenario_releve ();
if (ret! = 0) {
printf ("\ nResponse !!!!");
show_cc1101_registers_settings ();
//break;
}
}
return 1;
}
```

Ced , 11/2019

Hello and above all congratulations!

Thank you, thanks to your great work, I was able to recover the data from my AnyQuest Cybel counter, all that remains is to integrate it into Domoticz :)

The SDR key helped me a lot, and especially to see that my CC1101 does not 'did not emit: in the wiring diagram, you must remember to connect the 3.3V (VCC) of the CC1101 to the Raspberry (PIN 1 or 17).

I didn't need to change the frequency, the line value 233 (0xB7) worked straight out for me.

My meter actually only communicates during working hours (9 a.m. to 5 p.m.? - I haven't checked the range)

For all those who are embarking on the adventure, it can be scary but the most complicated is to do the wiring between the raspberry and the CC1101 (do not make a mistake in the connections!

A +!

Ced , 11/2019

PS: the meter does not emit waves regularly: it must be "woken up" with the 2 second signal (which contains the serial number of the meter) so that it transmits its

data

Marc , 12/2019

Hello,

Thank you very much for the work done. I am in the process of getting into electronic editing but do any of you have details on the integration into Domoticz?

Thank you in advance.

Marc , 12/2019

FYI, everything works as expected. I still had to use Flop's scan function (THANKS !!!!) to find the right frequency.

Next step: integration into Domoticz to log my daily consumption and set up an alarm on high threshold to detect possible leaks (it happened to me so I know what I'm talking about :-()

Thanks again for the great job.

Ced , 01/2020

Hello,

for the integration into Domoticz:

1. modify the cc1101.c file: add the functions

```
void writeres (char * tow)
{
FILE * fptr;
char file_name [] = {"./litres.txt"};
fptr = fopen (file_name, "w");

if (fptr == NULL)
{
printf ("Error!");
exit (1);
}
fprintf (fptr, "% s", tow);
fclose (fptr);
}

void display_meter_cron (uint8_t * decoded_buffer, uint8_t size)
{
```

```
char output [1000];
if (size> = 30)
{
printf ("% u \ n", decoded_buffer [18] + decoded_buffer [19] * 256 +
decoded_buffer [20] * 65536 + decoded_buffer [21] * 16777216);
sprintf (output, "% u", decoded_buffer [18] + decoded_buffer [19] * 256 +
decoded_buffer [20] * 65536 + decoded_buffer [21] * 16777216);
writeres (output);
}
}
```

and replace in the scenario_releve function: the line:
else show_in_hex_one_line_GET (meter_data, meter_data_size);
with the line:
else display_meter_cron (meter_data, meter_data_size);

2. recompile, put the program in the / home / pi / radian /

3. folder in Domoticz, create a new "Dummy" type device
then create a new "Counter" type virtual sensor
Retrieve its index number in the devices (Idx column)
Your counter appears in the Measurements menu: modify it to put a "Water" type and a divisor at 1000

4. create a /home/pi/radian/script.sh file on the PI, replace the value 167 in the script by that of your previously found index number:

```
#! / bin / sh
cd / home / pi / radian
FILE = "/ home / pi / radian / liters.txt"
HISTORY = "/ home / pi / radian / liters_history.txt "
dt = $ (date '+% d /% m /% Y% H:% M:% S');
rm -f $ FILE
/ home / pi / radian / radian_trx r
if test -f "$ FILE"; then
value = `cat $ FILE`
echo" $ value "
curl" http: // localhost: 8080 / json.htm? type = command & param = udevice &
idx = 167 & svalue = $ value "
echo"

fi
```

5. for information, the script logs the values in the

/home/pi/radian/litres_history.txt file with the date and time

6. Edit your crontab (crontab -e) and add:
0 9.17 * * 1-5 /home/pi/radian/script.sh
this launches the script at 9 a.m. and 5 p.m. every working day of the week.

7. to delete from Domoticz the first value which risks distorting the trends and the reading, press shift and click on this value: you can then delete it.

Still to be done: I do not yet know why but Domoticz does not count the liters correctly when there has been no value for some time ...
A solution would perhaps be to create a script which is launched outside collection hours (9 a.m. and 5 p.m.) and which would systematically push the last value to be tested!

PS: I'm not sure it's a good idea to read the meter too regularly for leak detections: the battery might not last the duration, any advice?

++!

Ced , 01/2020
not yet tested over time with Domoticz, but for the script which retrieves the last value from the history file and returns it to Domoticz:

1. create the file /home/pi/radian/dummy.sh, replace the value 167 in the script by that of your previously found index number:
#! / bin / sh
cd / home / pi / radian
HISTORY = "/ home / pi / radian / liters_history.txt"
if test -f "$ HISTORY"; then
value = `tail -1 $ HISTORY | cut -d \; -f2`
echo "$ value"
curl "http: // localhost: 8080 / json.htm? type = command & param = udevice & idx = 167 & svalue = $ value"
fi

2. Edit your crontab (crontab -e) and add:
30 * * * * /home/pi/radian/dummy.sh
this launches the script every hour at 30 minutes (to avoid the conflict at the fixed time of 9 a.m. and 5 p.m.!)

fred , 02/2020
thank you to flop and ced for your contributions

garycooper , 02/2020

Hello, I have two water meters equipped with a Cyble RF and I would therefore also like to create this "sniffer" based on raspberry pi 0W and a CC1101 module. Would there be a complete tutorial to facilitate the implementation?

In addition to the Pi0W, I thought to acquire this CC1101 module:

https://fr.aliexpress.com/item/4000310314726.html?spm=a2g0s.9042311.0.0.38fd6c37s7T6jA

and this PCB:

https: //netxing.files.wordpress. com / 2017/09 / photo_2017-09-20_22-11-18.jpg

vaguida ,.04/2020

Hello hello,

Has anyone managed to retrieve the data from Homeridersystems HRF-C-G2 water meter in the end?

vaguida ,.04/2020

It really makes me want to try! Do you think it would work with RFLink? I'm just wondering, if it works, how then to send the information to Home Assistant that I use on my Raspberry Pi 4 ... In reality, I wish I hadn't had an Arduino or ESP board on top of that, and didn't use only my Pi 4 but it seems compromised to me. I am wrong ?

I really hesitate to start because it is not very clear for my environment and my need for 868MHz ... Many

thanks to anyone who can bring me their lights!

guillaume ,.05/2020

Thanks for all the hard work.

I took advantage of the confinement to test and snort my meter. This is done thanks to the function of Ced to browse the frequencies.

I added a curl just to send the statement via the Domticz API

Everything works on Raspberry, but impossible to make the CC1101 work on orange Pi zero .. to be continued

garycooper ,.05/2020

Hello, I ended up receiving the material (CC01 + RPi0W) but I cannot find what to do to be able to receive the signals from my 2 meters. I installed raspbian lite on the micro SD but what next? Are there files to copy to the root of the memory card? A git to clone? I'm a little confused ... Could someone indicate how to proceed?

Subsequently, I would like to send this data to my domoticz installed on RPi4.

garycooper ,.05/2020

I advance a little bit (well, it seems to me), but now I stumble on the coding of the meter number and where it must be entered. My number is 06-0306576-243

garycooper ,06/2020
Weird, when I run the compilation, I have this:

In file included from radian_trx.h: 96,
from radian_trx.c: 5:
cc1101.c: In function 'scenario_releve':
cc1101.c: 685: 13: warning: variable 'TS_len_u8' set but not used [-Wunused-but-set-variable]
uint8_t TS_len_u8;
^ ~~~~~~~~

Nikola ,07/2020
can you help me with advice on how to lower the frequency by 20khz because it now broadcasts to 433.846MHz

nikola ,07/2020
i have a different serial number 23820591 only that number is written on the heatmeter sontex ... which also uses 433.820 radian 0

is there a possibility to send the command I sniffed with this protocol when communicating gateway and heatmeter?

Francois ,08/2020
Hello everyone,
First of all, a big thank you to all those who made it possible to find the solutions to take the readings of our water meters: Fred, Julien, SigmaPic and then more recently the other contributors for Domoticz, etc. .

I managed to read my water meter (EverBlu Cyble Enhanced V2.1) thanks to a Raspberry Pi 4 and a small CC1101 module (https://www.amazon.fr/dp/B07YX92NMP?ref_=pe_3044141_248816771_302_E_DDE_dt_1) .
The main difficulty encountered was with the serial number of my computer: "0123456". I entered "0123456" in the "Make_Radian_Master_req" function and it didn't work. After removing the "0" at the beginning, ie entering "123456" in the "Make_Radian_Master_req" function, that is put to work perfectly (without changing the frequencies, which suited me well ...) . For the explanation of the "0" at the start of a value in C / C ++, it's here: https://stackoverflow.com/questions/29325822/c-int-with-preceding-0-changes-entire-value

I started to make some modifications in the code (more info in particular) and I would like maybe to pass it in C ++ rather than C. What is the license associated with the source code?

@Fred: Does the code use licensed pieces of code?

Last question: given that the meter returns an indicator on the number of readings, there is no risk (not physical, but rather on the "legal" side) to often read your meter ...? For those who have integrated their meter with a home automation system, how many readings do you take per day / hour?

fred , 08/2020
Nikola, the tunning of frequency is done by configuring halRfWriteReg (FREQ0, ??) you can try to shift from some digit and check the result using an SDR

Francois
actually the example given for the serial number is not ideal.
I didn't license this code maybe I should, I didn't really do much about licensing.
this code was made by "looking" at the radian protocol which is said to be open source earlier in the page, i don't know if that helps?

the reading meter can be monitored by your water manager especially in the event of a self-reading.
personally I only do one reading per day I have not seen any impact on the life of the built-in battery

Alex , 08/2020
Firstly thank you for the research and development.

I managed to set them all up; on the other hand I have a question on the automation of the launching of the exe created on the pi.

What is given above launches the executable because an execution in relief must be indicated to him the path H: scenario of the survey tool! and the crontab simply asks to launch the exe:

"sudo crontab -e

55 9 * * * sudo / home / pi / radian_trx / web_tx_releve> / dev / null 2> & 1

55 9 * * * sudo / home / pi / radian_trx / web_tx_releve >> /var/log/crontab.log
"

Didier , 09/2020
Hello
I don't have a raspberry Pi but an arduino + CC1101.
Maybe someone would have developed a code on arduino to read cyble RF counters
You never know

Charles , 09/2020
Hello and congratulations for this superb work.
Before I start I have a question which I believe has not yet been raised:
How far from your meter is your reading system and have you done maximum distance tests?

frangarrob , 10/2020
Hi Francois. I also have an EverBlu Cyble Enhanced V2.1. I don't know how to register on the forum. Can you pass me the source code you used to read?

frangarrob , 10/2020
I leave you my email frangarrob@yahoo.es

avsantos , 10/2020
Hello everyone,

First of all thank you for the fantastic job you have done.

I share with you the problems I had:

1) The CC1101 board I bought did not work properly, I suggest you buy this:

https://www.amazon.es/gp/product / B07YX92NMP / ref = ppx_yo_dt_b_asin_title_o00_s00? Ie = UTF8 & psc = 1

2) The connection to the RaspberryPi 3 is not 26 pin, but 40, please note the connections. I was wrong to connect the Csn (CC1101) - CE0 (pi) and the CC1101 did not work.

3) Verify that the CC1101 is running by running radian_trx and choosing the option: v. If the answer is not different from 00 or FF, it is because they are not communicating with cc1101.

3) The frequency FREQ0 chosen was the defective frequency and worked correctly (halRfWriteReg (FREQ0,0x75);).

4) The serial number of my Cyble everblue started at 0. Do not place 0 in the cc1101.c file

5) The cyble pairs with the physical counter, ie it has an association. This association is made by counting and serial number, which is read in the communication.

Corrections Required: The serial number of the physical meter is backwards. In other words, the last digit is the first and so on.

Suggested implementations:

1) Obtain Water Leak Information - This device allows the water leak to be in place and should be read.

2) Check the possibility of changing the Cyble + physical counter pair. For example, I bought the Cyble + physical meter. So they make a pair. However, I removed the cyble from the physical meter and now wanted to put in the physical meter of the water company, which has another account and another serial number. The account and serial number must be possible to change.

Thank you all

Pacific , 01/2021

Hello,

Found this blog by chance and very happy because I wondered how to read my ITRON Everblue Cyble V2.1 meter in order to include the info in my Jeedom home automation.

I am not a programming specialist but hack a bit. I will enter a TI interface and a PiZero. I think it should be fine and then tackle the script for the link with Jeedom (that's where it will get complicated ;-))

Has there been any progress on the software? I tear my hair out to understand the frequency calculation. I'm playing around with TI's SmartRF Studio and it seems that the algorithm isn't that simple, several things come into play. We fall back on your FREQ0 suggestions by taking the various parameters already recorded in the

init. As soon as I have the equipment I will compare with an SDR, after having calibrated its offset (on aero weather frequency ..) Will keep you informed of my progress It's a great job that has been done, thank you again

Didier , 01/2021
Hello

I will be interested in the software that "sigma PIC" would have developed on Mbed + CC1101.

Bule , 02/2021
Hello, thank you very much for your work, the truth is that it has helped me a lot.

I just said that.

Pacific , 02/2021
Hello,

Too bad this blog seems to have fallen asleep but for the curious still listening, I confirm that it works very well. I kept the default settings and the first try, I got the results. This allowed me to see that the electronic part of my meter, even if it works and reviews the information, is blocked. As it was a new meter, mounted to zero, this made it possible to note the error of reading from the town hall and to determine a blockage of more than 6 months. I hope they will replace it for me because now that I can read it and include it in my home automation .... It's annoying ;-)

Good, as far as the frequency is concerned, well it's relatively simple and above all more precise than the empirical method of

I was inspired by different libraries (Github) for uses of CC1101 with Arduino and found the calculation method.

There are mainly 2, a relatively heavy to implement because it is based on information in binary with rotations to the left and to the right all with a recalculation in decimal / hexa each time. We are working on 32 bits so you can see the job but it works. I used Excel and its various options to make a table.

On the other hand, the second is much simpler but also requires Excel to facilitate the calculations.

The principle uses 7 main cells and three more to convert the results from decimal to Hex for entering them into the program.

Cell 1: 433.920 - selected midpoint

cell 2: 26 - frequency of the quartz of the circuit (fixed)

cell 3: = ENT (Cel1 / cel2) - FREQ2 in decimal (integer value)

cell 4: = MOD (Cel1; cel2) - Modulo of FREQ2

cell 5: = ENT (cel4 / 0.1015625) - FREQ1 in decimal the value of the divisor is fixed and do not ask me how we find it ..... don't know

cell 6: = MOD (cel4; 0.1015625) - Modulo of FREQ1

cell 7: = ENT (cel6 / 0.00039675) - FREQ0 in decimal the value of the divisor is fixed and do not ask me how we find it

the last 3 cells use = DECHEX (celx) to convert the FREQx values into Hexa in order to complete the program correctly.

Have fun just change the frequency and everything increments automatically.
Results have been verified with TI's Smart RF Studion. It's OK

compare with the empirical values and you will see.

@ +

dckiller , 03/2021
Hello,
I have performed the tests. I managed to receive the data. On the other hand, I have a lag.
Counter = 1555 received 1595
Counter = 1613 received 1656
Is this a problem with the setting of freq?

Pacific , 03/2021
Hello,
I don't think this is a frequency problem because, after frequency control tests, either it works or it doesn't. If on reception the frame is complete and therefore the display of the result is clear on the last line, the difference can, in my opinion, only come from a slight shift in the mechanical transmission (visual sensor) I think having this problem on my meter since everything is working except the volume increment.
If your results are in liters the difference is not convincing between a mechanical meter reading and an electronic one.

vincent , 04/2021

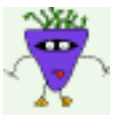
hello,

Very interesting forum and I want to do my editing for the same water sensor to Domoticz.
I do not see how to register on this forum and recover the sources :(
could someone have those mentioned by François?

if there is someone who reads this bottle in the sea, do not hesitate please do not contact me / give me the useful links:
harko_tank at yahoo.fr

thank you anyway!
vincent

Pacific , 04/2021
Hi,
No registration needed for the sources. All you have to do is download the radian_trx.zip file in the code section (the password is the name of the file, quite simple) With the default frequency setting it works the first time (at home ..) you just have to enter the number of the meter without the leading 0 and make the 2 corrections in the files as indicated.
For Domotiz, the explanations are given, for my part I simply made a few modifications to make it work in a virtual Jeedom.
Good hack



Nono , 06/2021
Hello,

Have there been any improvements to make editing more accessible and use it with home assistant and why not with an ESP32?

Because after careful reading, I did not really understand what to do exactly.

Thank you.

Jonathan , 06/2021
Hello everyone and a thank you for all of this work!

For my part, it does not work for the moment. No response from the meter (tested in the middle of the day, on a weekday) despite the scan function and by testing

various possibilities (year in decimal and hexadecimal, serial number with / without the numbers reversed). A priori, the CC1101 works since I see the two seconds of "waking up the counter" on SDR # via my SDR key.

Thanks again anyway.

Laurent , 07/2021
Hello - After a lot of mistakes, I did receive a frame but nothing else:
MARCSTATE: raw: 0x0D 0x0D (RX RX)
GDO0! 00 1st synch received rssi = 177 lqi = 128 F_est = 255
MARCSTATE: raw: 0x0D 0x0D (RX RX)
GDO0! frame received
RAW buffer
received radian frame size = 0
TMO on REC

Has anyone ever had this type of situation?
I think it is either a ghost response (but it appears to have 433.82) or it is another counter which reacts but not mine.
Not easy to know more. .
Thank you!
