

Playing with ICS devices with RF

What can a small device do in modern industrial World

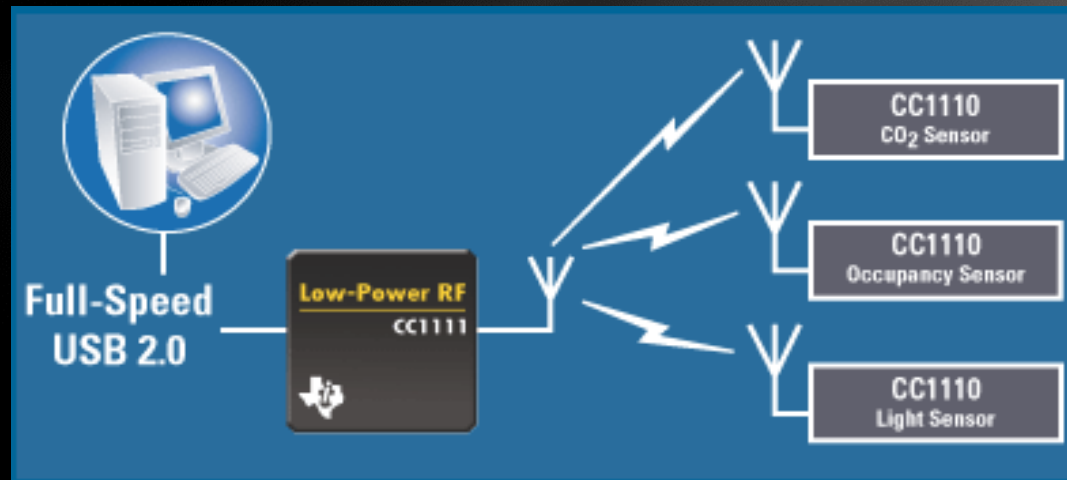
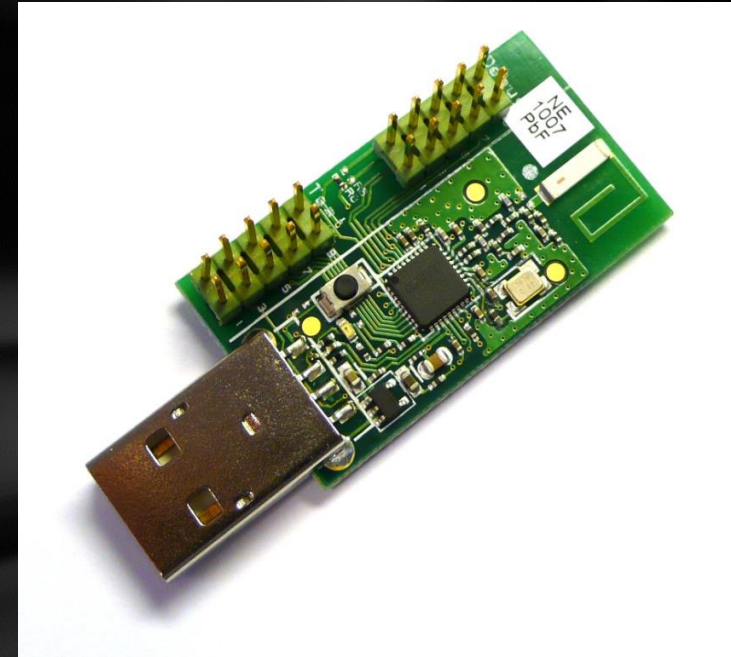
Alexey.Polyakov@kaspersky.com

Konstantin.Sapronov@kaspersky.com

Agenda

- Smart badge
- Sub 1Ghz RF
- Demo with RFCat
- Smart Grids
- Inside Smart Meters
- Threats for smart devices by RF
- Conclusion

ToorCon 14 Badge and DK_Dongle



HardWare – Texas Instrument CC1111 chip



CC1111F32 – Sub 1-Ghz

Max power 1W, good to transmit to 230Meter!

With external antenna can transmit even miles away

32 kB of in-system programmable flash memory

4 kB of RAM, can buffer up to 500 bytes in memory

full-speed USB 2.0 interface

Sub 1Ghz RF

Sub 1Ghz ISM bands:

900Mhz Cell phones, Cordless phones, Personal Two-Way Radio;

433MHz Medical equipment

315 MHz Car/Garage Remotes

915/868MHz (US/EU) Smart meters and more ... P25 Policy radios



Using Sub 1GHz device: Demo with RFCat

Establishing peer-to-peer session with 2 CC1111 devices

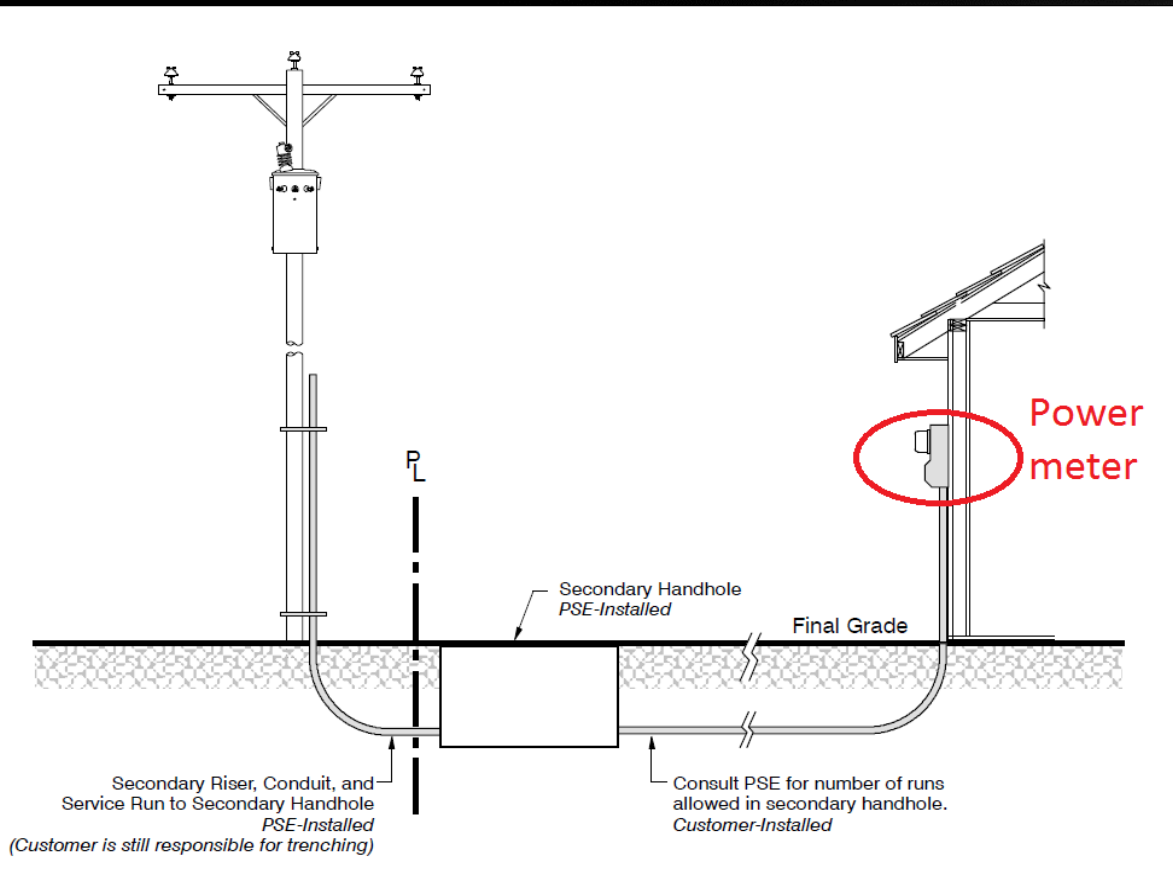
We will show how simple it can be done.

Advantage: not able to capture unless you have another one. You can use it without risk of been detected 😊

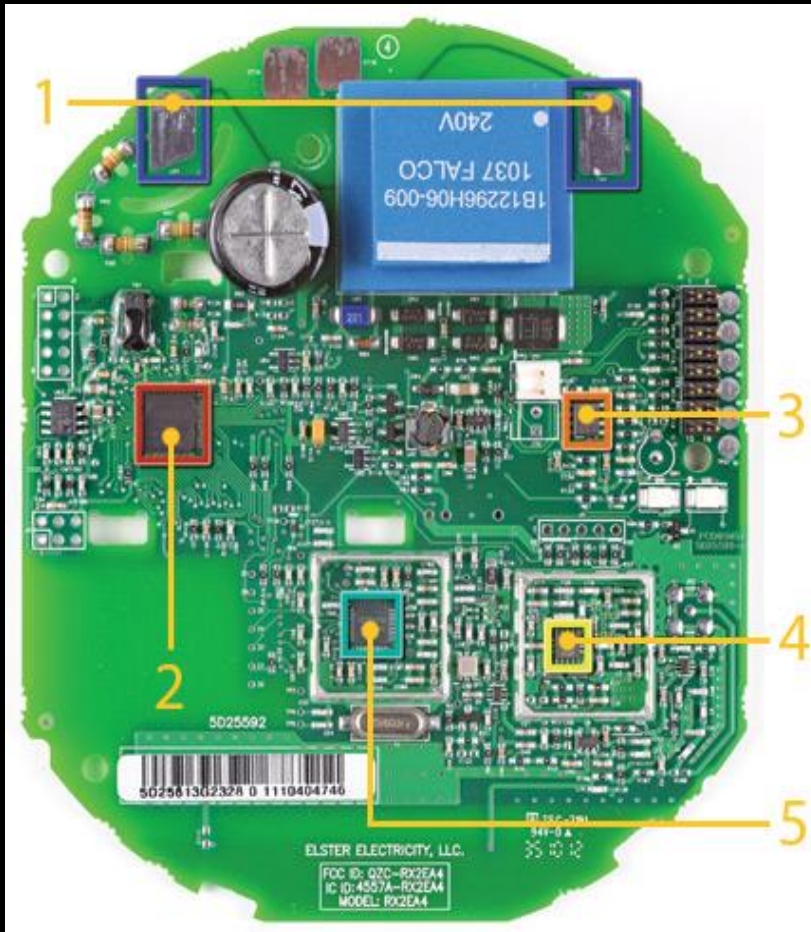
Discovering RF World: Home Devices

Power Meters (also as for gas, water measuring devices) – 90% in US household, used by all Power Providers

- Use 902-928 MHz to operate, FHSS, Remote reading



Inside Smart Meters



Elster Rex2

1. Power converts

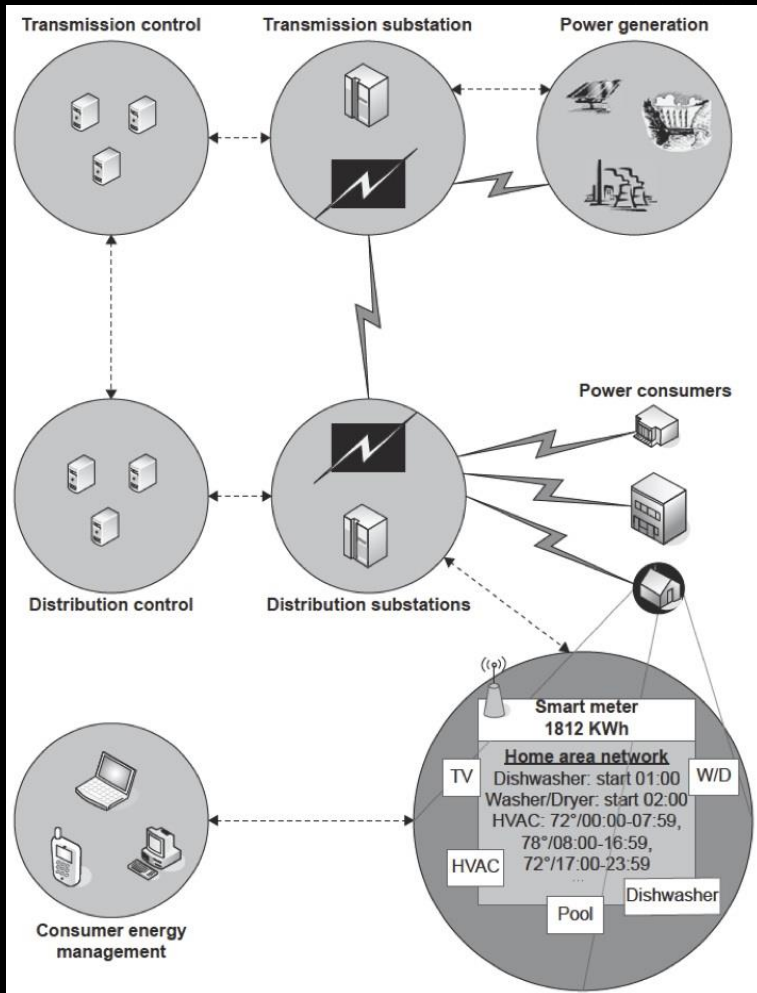
2. Teridian 71M6531F SOC with a microprocessor core, a real-time clock, flash memory, and an LCD driver

3. Texas Instruments low-power LM2904 dual operational amplifier.

4. medium-power RFMD RF2172 amplifier IC.

5. less-than-1-GHz Texas Instruments CC1110F32 SOC with a microcontroller and 32 kbytes of flash memory.

Smart Grid Infrastructure



Power Line equipment

- Transformers, Isolators, Condensers, Switches and line breakers;
- Power meters, field equipment
- 90% still with Leased line (expensive). Moving towards RF grid
- Remote area Readers and Control devices may use RF feature

Impacts of exploitation for RF devices

If you exploit such devices you can :

- remote keys / car fobs : open or close
- 2-ways phones : listen
- power meters : monitor and control
- Smart Grids : power outage
- SCADA : damage
- medical devices: kill

Threats by RF for smart devices

Attacks :

- Reading private data
- Theft of service
- Jamming Tx/Rx signals
- Possible damaging power line equipment:
 - Isolators
 - condensers
 - Switches
 - power transformers

Cost of repair can be small (5K) to high (2M for Transformers)

Discovering Smart Meters – troubles

- Before able to read, need to understand next Tx frequency
 - Usually, it is shifted from original basic frequency
- May take days or week of analysis ...
- The transmission is preset with SYNCWORD
 - Usually 2 bytes, but, need to look at thousands of transmission to find correct one.
 - RFCAT is able to help, but, luck and luck needed!
- Another challenge is package length and transmission data ratio

“Security” ?

Current prevention solutions:

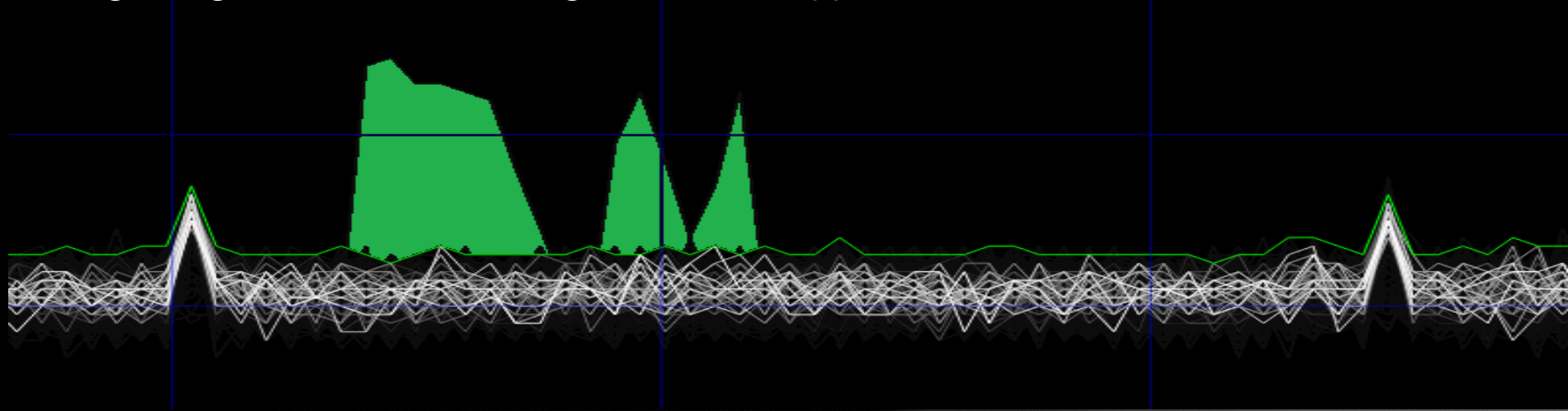
- FHSS
- SYNCWORDS
- DSSS
- dynamic routing tables

Security:

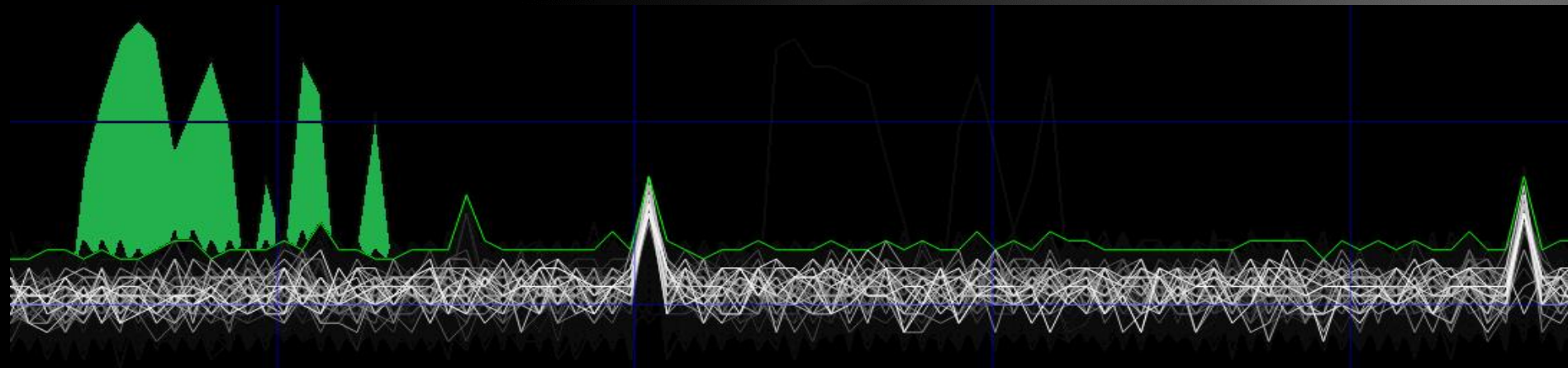
- encryption. AES 128
- session authentication

Discovering Smart Meters – FHSS

Beginning: transmitting session #1 (approx 913MHz)



3 min later: transmitting session #2 (approx 904 MHz)

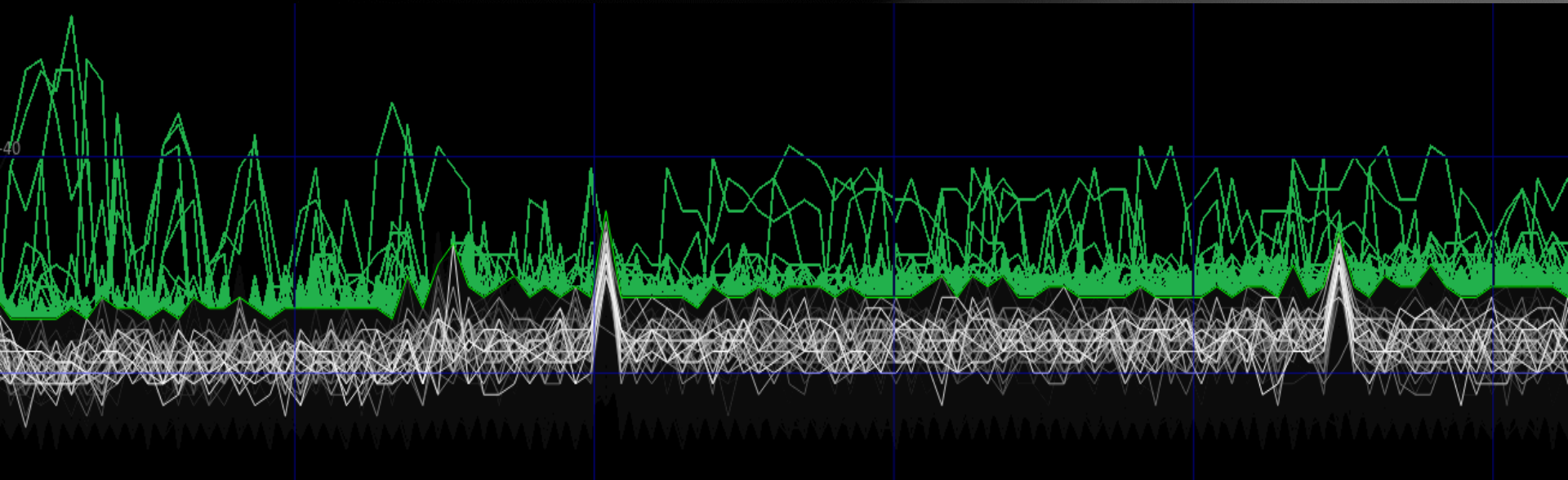


Discovering Smart Meters – more

5 hours later

Full 902-928MHz spectrum is covered

- FHSS – predefined rules for selecting next transmitting frequency
- Unknown Baud rate unknown packet length
- Same packets sent over and over many times
- Remote receiver



Discovering Smart Meters - SYNCWORD

```
1358536379.853) Received: 84724811c57cf5c286e830d18a2896d4c0891819f44662b568d0be83b361
1358536380.249) Received: dfe1766f6fffd914f2ed297b647185d140e8aafe7e85c4ec685fed7ef6f20
1358536380.327) Received: 77f288db9c74d77bdcedfb07fb4fdc9c72f82e8ef7f5de00bfe89adf0a2c
1358536381.937) Received: d957330121a27432007441b892cb9afe031db491be0bf17504079f011bb9
1358536382.836) Received: 359bd23b7bba2dd115ec8228b70ae0006d71d06cbc748d0fffc06540b9401
1358536384.293) Received: 0419f021d3f6e0aed69d7812f35dbfde8e33bb776f0726df003a9e08e46c
1358536386.224) Received: c11977862ccff30160a310e30db19dbde9114bf0fa47f200e25d10d5aa40
1358536387.798) Received: 9aee8cc1f96c588f00619fb2914581ba6795baef1674febfffdfb21d16bd
1358536389.384) Received: 1d4a70517dee15cc580e916e8165c2085b06fff07fbb7b00353fd144b1ec1
1358536391.650) Received: 1b4d39872f7ce6c03d2806002aa55b5ec46a1aea20186ef83c60d08433e0
1358536393.453) Received: 5b33a440e303e35dd45454641c024dd647637968180433fb04fc8641f4b4
1358536394.657) Received: 8595c05e4eea39c924a9b7e143c22114646963fa091c28bdf080cb8ca072
1358536396.346) Received: 21b1fb297ad5e26bdb559ca6449a567a1effff13bbfb4cc520079f010f9f
1358536398.084) Received: e59efe5faccf9a6294c142593d6afb0960029dee06eb87d3c0e16e1c0001
1358536410.122) Received: 002fd8b9ec5181550aa0818053c297e81b324e384257800d2868e5237feb
1358536404.126) Received: 36fb638f492befc7f7f4b7dd0654569233e216d05919812e6c1cbdd2007e
1358536406.808) Received: fef3cc4410c6bfab220c8a681cf128c5100157573c3b03b843ef87f12d04
1358536409.098) Received: 19c4e7c26288b7145eb7fee40711fedf87da194a3bb75e34bd0830580487
1358536412.146) Received: b0e0d5c671e7c79e453110480d0ba07d06b04633be6e03bcf8390ac38faf
1358536415.155) Received: bbed71bcb5fbc201287924c092747000f0663abc245513f001039223ff60
1358536416.165) Received: de16874ff0138f1c22ccfec7f9e021397f34756dba52acd27eb87dbdf2
1358536416.310) Received: cfb37621c1541a54f9c9381f5a0e43436bf9f80e81f1927305fba36ffd5e
1358536416.339) Received: d7ce090bc93a867ffca91f1b9a7bf157c45f2e086aacb0d9f94487420610
1358536416.367) Received: 79cf643dde0e595a9d6d9d449abfe46c5e79d236f8ab81f8dcffa8e34d60
1358536416.637) Received: 3b4fcedcd8b060a04db12fefbfff7915a990d12a5665efcd3157bbe8e34c2
1358536416.712) Received: c5e463e2c34bff358adc9b356b181b59bc16ded5f844fa7d8f29293f6a29
1358536416.740) Received: 45a7f3fb187e583eb84f0b2913bd135e777bee0eb47d7af77f7da2c5ebd01
1358536417.137) Received: b4e1bf1cda48ee85eef82509246de08e49413fdd551f6c21879daf9b77f6
1358536417.755) Received: fd2f647fadd6d6c2fba9735b10a6dbc1ef914b741444aaaa44647b99a194
possible Sync Dwords: ['0x1191L', '0x88c8L', '0x4464L', '0x2232L', '0x9119L', '0x488cL',
1358536419.526) Received: f0323667ef9c901b6cb6c00fbb75ae75dffdb812d8c2a3f82dfc140a9540
1358536424.125) Received: 970220157af3f3ddb8ebadee355b323b215faed92f4b33c0210082a8514c
1358536425.247) Received: fbf8be217dd9dca3d9e8fae48d682477ff3c31fbbefbb44d3bc31c188
1358536425.325) Received: dffff7ff5dee5ff5ff7c97e660ee065db1d5afefbd9fb8f54d9a43d0da08e
1358536426.204) Received: a55fbd8f8f0b991d4dfbe7e32a7e85200075304459c44221a520061c9d010
1358536429.399) Received: e31591e6c22ef875903a290900f905a916cd2031e0dbffa0111b0041e3eb
1358536432.607) Received: 2f4c7f087345b438428fbd3f94cf3846395ee0436018e04069c5428b6eb9
1358536435.011) Received: 1891ba07cfec2de0442196a01ea0e4957021195365a0b8c7a98113275421
1358536436.334) Received: 53636633a7171fa8ceac31f5e2dca455000a430887471dac7f00251e0a96
1358536437.452) Received: 1c8c0e8effcefc8f21575295a04a8f26a5041c0af88fcf0f002d6058c342
```


Conclusion

- Power Meters is a good and typical example of Industrial reading devices
- More recently, they were not easy ways to find equipment for security researches in this area
- Now, we have a good RF device for testing Smart Meters. However, it takes a lot of time to understand how Smart Meters work
- “Security” by design (FHSS, frequency hopping, predefined communication list) is widely used but it is not enough. Some advanced ideas (data encryption, session authentication) is less used
- You can discover what happens around by just using available devices like the one presented earlier. The cost is between \$50-\$100.

Thanks to

Toorcon team for badge

Mike Ossman for specan

Atlas for RFcat

And YOU for attention

Questions ?!